GROUP-IB

SCAMADVISER

The Global State of Scams Report - 2022

How are countries worldwide fighting online scams?

GASA
Global Anti-Scam Alliance

Online scams have become a Global Epidemic

An estimate 293 million scam reports were filed and $55.3 billion was lost in scams in 2021 worldwide

Scammers Scam Everything

Scammers have proven more successful in 2021 than ever before. The number of scams reported increased with 10.2% from 266 in 2020 to 293 million reports in 2021. The amount of money lost in scams grew from with 15,7% from $47.8 billion in 2020 to $ 55.3 billion in 2021, mainly due to the rise in Investment Scams (also read: About the Data).

Scammers are using any crises to scam people; moving from pre-ordering your Coronavirus vaccination in the beginning of 2021, to cheap flight tickets for Hajj pilgrims, "supporting" victims of the Australian bush fires, "helping" Ukrainian refugees and more recently, tickets to Queen Elizabeth's funeral memorial and energy crisis government subsidies.

The Bloody Facts

With 4.72 billion internet users (60.1% of the global population) now spending nearly 7 hours every day online, the economy continues to digitalize at an increasing rate. Crime is following quickly. In most Western countries **online scams** are now the **most reported type of crime**.

According to the Australian Competition & Consumer Authority, **96% of Australians** have been exposed to a scam in the last 5 years with half of these contacted weekly or daily by scammers. In **France, 61% of the people** have been exposed to "alternative" investment offers last year. In the **United Kingdom, 50%** of telephonic survey respondents reported receiving an email, text, or social media message that may have been phishing in one month.

No Longer a Western Disease

However, scams are no longer a "Western" disease. **53% of Filipinos** stated they were targeted by fraudsters in 3 months time. 11% of the respondents said they ended up as victims. Likewise, other developing countries like **Brazil, Ghana, Nigeria and Kenya** are **reporting huge increases** in online scams, especially via mobile phones.

The introduction of a new, easy-to-use, mobile payment method called Pix in Brazil, led to an influx of scams. In Nigeria, the number of transactions via mobile channels increased by 164% in 2021. As a result, **scams via mobile boomed** as well. 62% of Saudi Arabian consumers received spam & scam messages, mainly on their mobiles. 14% admitted that they fell for the scam and lost money. In South Africa, two massive data breaches caused a tsunami of phishing attacks using highly personal data. Indonesia reports that 25% of their citizens has been a victim of an online fraud, making it the 2nd largest reported type of crime in the country.

Investment Scams Continue to Rise

The strong increase in scams is not only caused by the **accelerated rate of digitalization** but also by high **inflation**, quickly increasing **cost of living**, and, in some countries, high **unemployment rates**. This is forcing people to look for new ways to invest or simply make ends meet. Despair makes bad councel.

In 2020 we already saw a **sharp increase in investment**, mainly in cryptocurrency scams. The **Turkish** government felt forced to suspend a cryptocurrency exchange, freezing more than $2 billion in assets. **Canada** reports that investment scams were one of the fastest growing types of online fraud, from 501 reports and 16.5 million lost in 2020 to 3,442 reports and 164 million in 2021. The **United States** reports a loss of $575 million in investment scams. **Singapore** reports the largest amount taken in a single case: $6.4 million.

Scam Blurring

2021 introduced a blurring of investment with romance scams. Where victims of **romance scams** used to lose money to pay for hospital, travel or other urgent needs of their virtual lovers, these scammers are increasingly switching to **making "joint" investments** together. To make matters worse, scam victims are approached by "**money recovery**" firms. These often are the same scammers, promising the victim retrieve his loses after first paying an "administration" fee. The money is never actually recovered. As a result, the number of scam reports has not only increased, but they report an **ever-stronger growth in money lost**.

Scams remain one of the most under reported types of crime

Depending on the country only between 3% to 17% of all scams are reported

One of newest types of scams are loan apps. Especially in developing countries like Brazil, Mexico, Nigeria, India and Tanzania, these kind off scams are on the rise. Here too scams are blurred, in some cases the loans start as advance fee scams, asking the victim to first pay money before the loan can be given (which in the end never happens). In other cases, an online loan is provided (often much less than applied for) with huge interests. If the victim cannot pay, the lender starts calling and messaging with threats until the victims pays a multitude of what was borrowed. Finally, loan apps are often misused to get the necessary data to apply for loans or credit cards elsewhere.

Scams remain one of the most under reported types of crime

As scam victims often feel ashamed or, according to previous research, do not know where to report a scam, scam reporting remains low.

In nearly all countries, **reporting scams remains fragmented** across CERTs, consumer protection organizations, financial authorities, banks, telecom operators, local police offices, cybercrime teams, victim support organizations, private initiatives, review sites and social media. In several countries like Kenya and Pakistan, action from **law enforcement** is described as **slow, fragmented and inconsistent**. The process of reporting must often be done physically rather than digitally.

In **Australia** an estimated **13% of all scams are reported**. **Canada** estimated **only 5%** of the cases reach law enforcement while **Israel** estimated this number to be **9%** and the **Dutch and French** estimates range between **12%–17%**.

Some countries are **centralizing scam reporting** and are **investing** in **making reporting easier**. France has launched a new online platform for reporting internet scams without having to go to a police station. Several countries like the **Belgium, Poland, New Zealand** and the **United Kingdom**, now offer citizens the option to **forward dubious emails and text messages** for further analysis and action.

Social Media Steppingstone for Scammers

In nearly all countries, social media are plagued by scammers trying to lure victims. According to **Pakistani** authorities, **23%** of the reported online crimes, started on Facebook. **Indonesia** states that **51% of the scams start on social media**. In the **United States** more than one in four people who reported losing money to fraud in 2021 said it started on social media with an ad, a post, or a message.

There seems to be a trend to make social media more accountable. The **Australian Competition & Consumer Commission** for example is taking legal action over alleged misleading conduct by Meta for publishing scam celebrity crypto ads on Facebook. On a positive note, in Malaysia, Meta is supporting an online scam awareness campaign.

Get Them while They are Young

Another scam trend several countries, like Brazil, China, Finland, the Netherlands, New Zealand and Thailand are reporting, is that young people are targeted more and also lose more frequently money then elderly. Seniors still lose the most money, especially to investment/crypto scams.

In **Finland** especially, **students** seem to be a **targeted** group. The worst-hit age group were individuals between 18 and 30 years old (**23.3%**), who were scammed 8% more compared to 2020. Likewise, the **Dutch** University of Twente found that **young people** are **21.5% more likely** to be scammed than older people (13.1%). **New Zealand** reports that **55%** of the people who report scams are now **younger than 40** and a study from **Thailand** shows that **Generation Y and Z** are the most vulnerable to online scams due to the amount of time they spend online. Finally, a **Chinese** survey amongst **college students** reported that more than **a tenth** of the respondents had lost money to scammers. This has prompted the Chinese government to launch a new wave of education campaigns aimed at making young adults more wary.

Scamming is becoming an Industry

Scams have been industrializing for years

The most well-known are the call centers in India which specialize in Helpdesk/Tech Support scams. A more recent development has been that mainly Taiwanese and Chinese citizens are tricked by **human traffickers**. The traffickers are targeting mostly young Asian people via social media, offering well paid work and accommodation in countries like Cambodia, Thailand, Myanmar and Laos. On arrival, their passports are taken, and they are sold to different groups and **forced to** work in offices running illegal phone **or online scams**. Taiwan authorities say almost 5,000 citizens have been recorded travelling to Cambodia and not returning.

Another development, which is reported by Group IB, is the rapid growth of SaaS (Scam-as-a-Service). Scams are automated and increasingly finetuned to specific target groups. Scam scripts (websites) are developed and distributed to local scam organizations. Cybercriminals also professionalize in specific specializations (traffic generation via social media, text and email spamming, cryptocurrency laundering, retargeting of scam victims. According to Group-IB scams (57%) now outstrips phishing (18%) and malware 25%) as cybercrime type.

Spread Love; Not Scams

An increasing number of governments is **investing in raising scam awareness**. With the title 'Spread Love; Not Scams" the Tanzania government is trying to educate its citizens on online fraud. In many cases, **awareness campaigns are fragmented** on state (Brazil, Germany) or even municipality level (Netherlands) and different stakeholders (banks, telecom operators, law enforcement).

China has started the **"people's war" against fraudsters**, a nationwide anti-fraud education campaign which was launched by the Chinese authorities in 2019, after president Xi Jinping announced in a conference that fighting fraud was a "top priority". The campaign culminated early this year with the **launch of National Anti-Fraud Center** and a **mobile app** that has been **downloaded** more than **500 million times**, making it one of the most popular in the world. The government uses a variety of channels, from street posters to TV commercials, to inform the public about what scams look like and how to avoid them.

Scam Prevention Initiatives are Growing

Like private companies such as ScamAdviser.com and Trend Micro, more countries are starting to **offer tools** to their citizens **to check for malicious websites**, email addresses, bank accounts, cryptocurrency addresses and phone numbers.

Lists of malicious media are **piecemeal published** by an increasing number of financial authorities and police websites such as in **Canada, Mexico, Netherlands, New Zealand** and **South Africa**. Likewise, the **Polish** CERT has started publishing a Domain Warning List.

Malaysia is taking this one step further by offering a search engine and app allowing the public to check telephone and bank account numbers used by the crime syndicates.

Cybercrime Fighting: Centralizing & Scaling up

More and more countries such as France, Malaysia, Mexico, Switzerland are (slowly) centralizing their anti-cybercrime efforts. In Switzerland for example, the Nationale Zentrum für Cybersicherheit (NCSC) is gaining a more central role in reporting fraud, in the analysis of the phenomenon, and in the prosecution. Like in Japan, this is a rare phenomenon, as both countries used to have a strict federal/prefecture approach.

Countries are also investing in resources. Indonesia is hiring 200 additional cybercops. Italy now has more than 2,000 police officers specialized in IT related crimes and a special Cyber Crime Analysis Unit has been set up in close cooperation with Italian Universities.

Also, more time is invested into training. The Qatar National Cybersecurity Agency for example trained 25,000 employees in different aspects of cyber security in less than one year, also in preparation for the FIFA World Cup.

Scams are not a Priority

The focus is on fighting the “Big Cybercrimes”

However, the investments listed above, are **mainly** made to **combat “big cybercrimes”** targeting infrastructure and companies. In no country scam fighting receives the same level attention. On the one hand, this is understandable as the damage of a big cybercrime case is often in the millions. On the other hand, the quantity of scams hurting individual consumers and the level of personal suffering, demands attention as well.

Apart from the money lost per individual case, the **biggest reason** for law enforcement either ignoring or simply admitting it cannot handle the case, is that investigations have proved to be **unfeasible** due to the **bureaucracy** involved in communication between the investigation agencies of the countries involved. **Singapore** Police, for example, states at least **90% of the scams** in Singapore **originate from overseas**, and described the scammers as syndicated, well-resourced and technologically sophisticated. The police said these cases are difficult to investigate and prosecute as efforts depend on the level of cooperation from overseas law enforcement agencies.

The Cure for Scams?

According to a study by the World Economic Forum only **0.05% of all cybercrimes are prosecuted**. This number is probably even larger for online scammers and becoming more unacceptable as the number of scams continue to grow at a rapid pace.

Countries have, in many cases already for years, invested in awareness campaigns. However, as scams become more sophisticated and advance, scams will continue to grow. **Raising awareness is not enough**.

The warning lists posted by law enforcement, CERTs and financial authorities are often too little; too late. The victims have already lost their money and, as scammers operate around the globe, consumers cannot be asked to check all warning list sites. **More preventive action is needed**.

Prevention could take the form of a **global sharing system of scam data** (be it domains, email addresses, cryptocurrency addresses and bank accounts). The data cannot only be used to help consumers check if they may run a risk of being scammed, but also be **used to proactively block or take down malicious assets**. National initiatives like those of the **Belgium Cybersecurity Center**, where consumers can forward phishing emails and where this data is used **real time to block websites** by Belgium Internet Service Providers have already proven to reduce the number of scams. The **next step** is **taking** these kind of **initiatives international**.

To **allow faster take down** of scam assets, especially those platforms which are used to promote scams (the Big Tech search engines and social media) and those that facilitate their infrastructure (registrars, registries and hosting providers) have to take on more responsibility. While some are already taking more responsibility, **new legislation will be required to make platforms more accountable**.

To find more answers to counter the rise of online scams, GASA is organizing the **Global Anti Scam Summit** bringing together governments, consumer & financial authorities, law enforcement, Internet Service Providers, and cybersecurity organizations to share knowledge and insights on fighting online scams and define concrete actions to combat online fraud more effectively and efficiently.

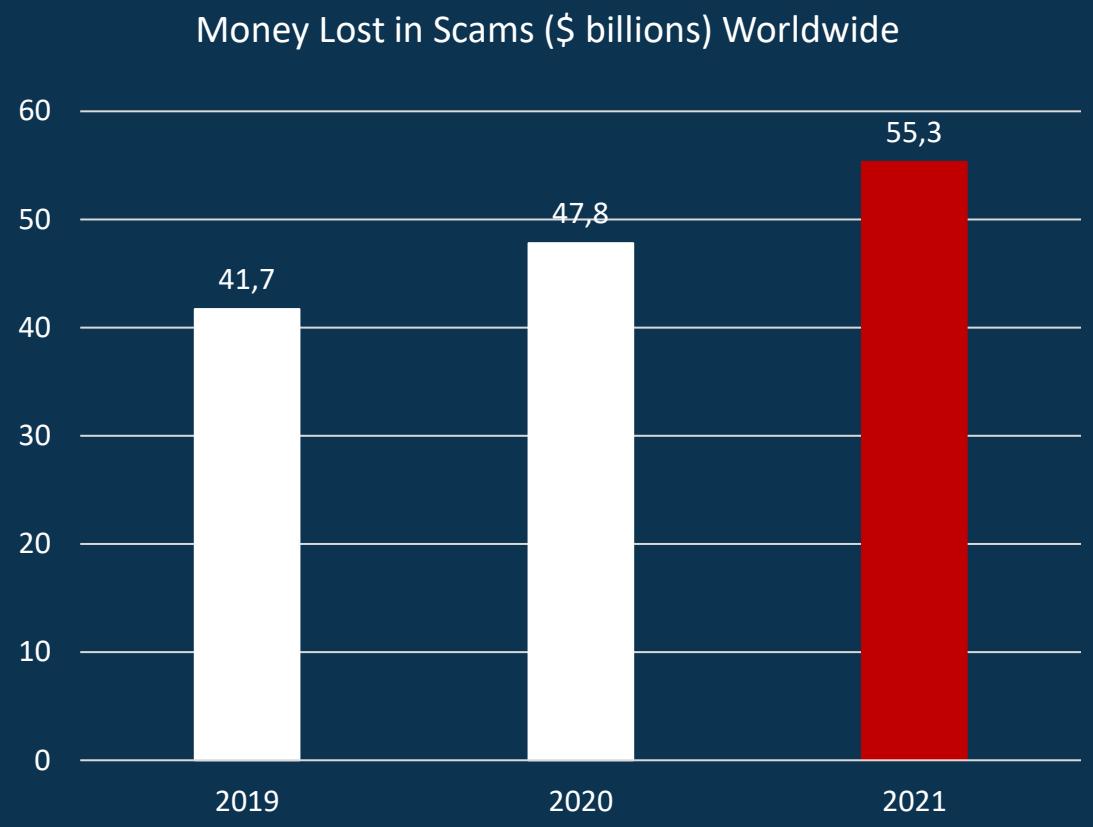
In the next few years, the number of reports and amounts lost in scams will continue to rise. I do hope this 4th Global State of Scams report will help you gain insights into how other nations are fighting online cybercrime and inspire you to join forces with us to turn the tide on scams.

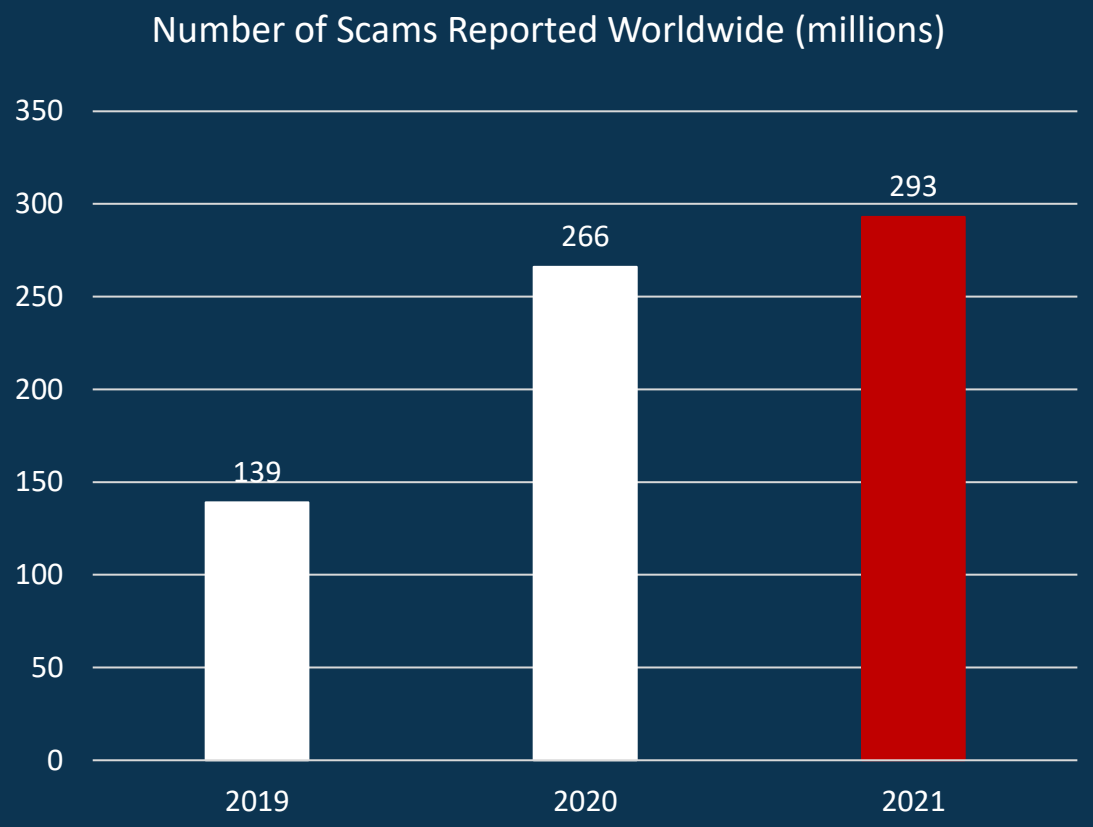
Best regards,

General Manager ScamAdviser
& The Global Anti Scam Alliance

The number of scams reported increased with 10.2% to 293 million reports

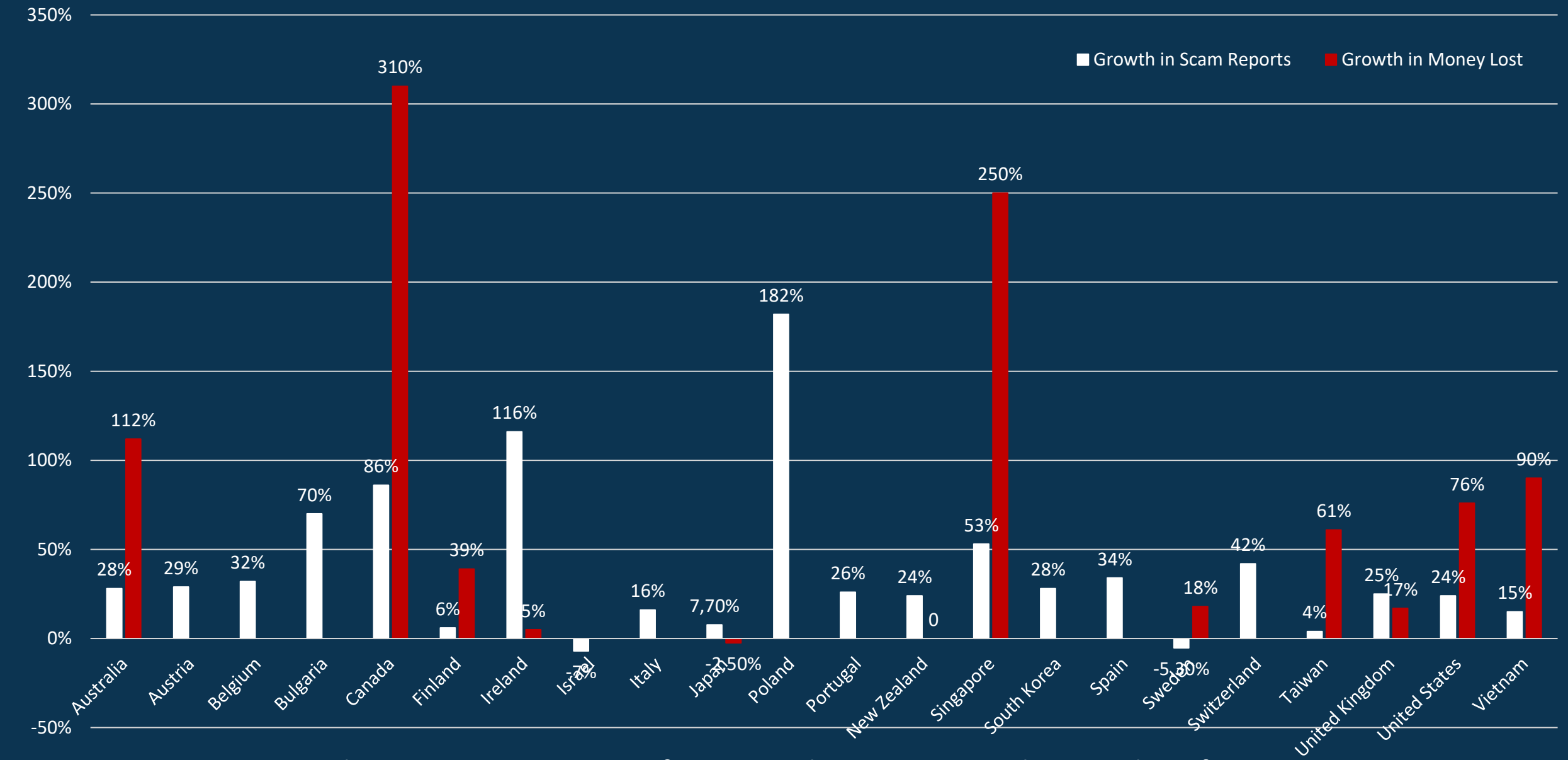
The amount of money lost in scams grew from with 15,7% to $ 55.3 billion, mainly due to the rise in Investment Scams





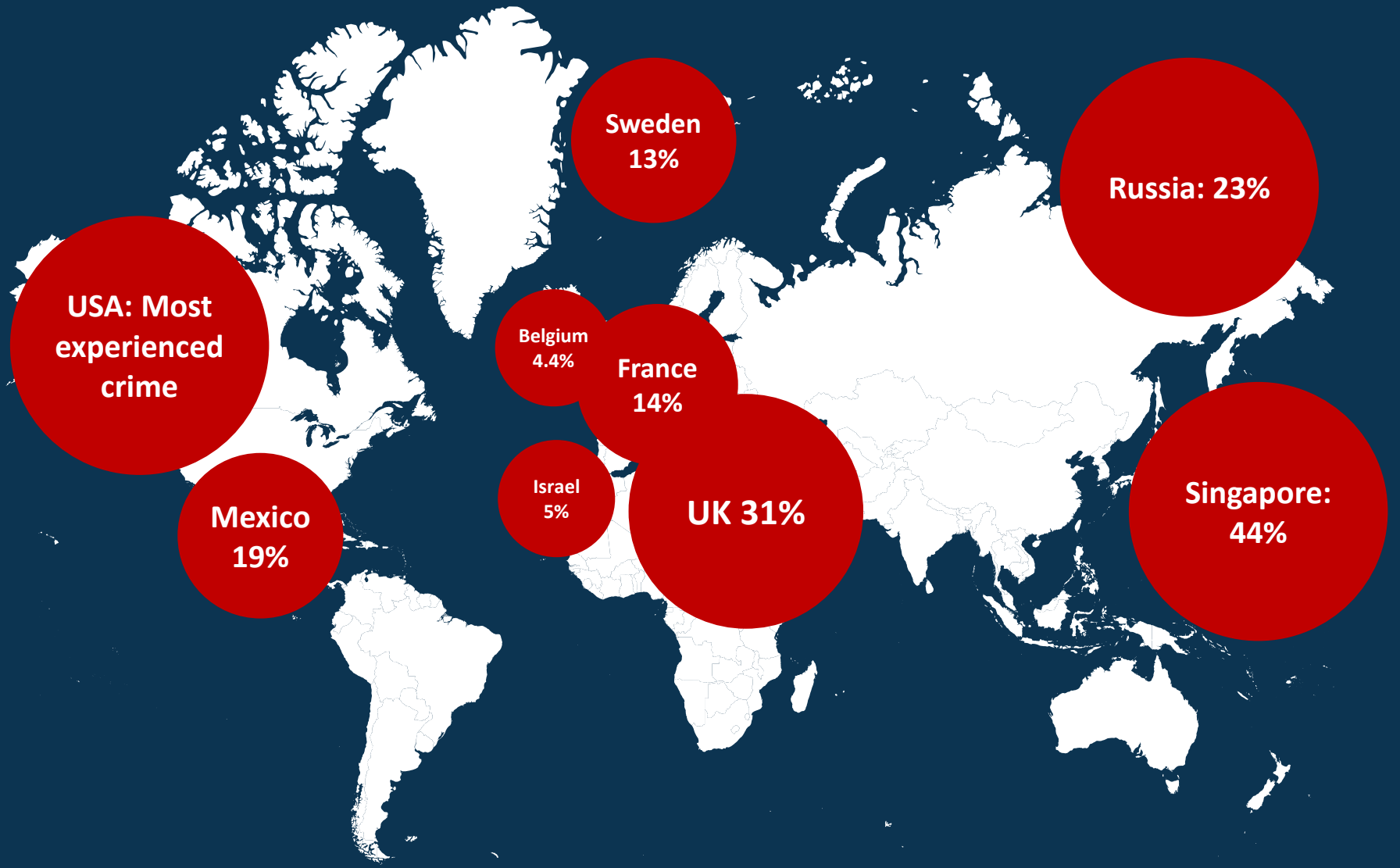
The actual growth in reports and money lost is likely to be much higher but for some countries who reported massive growth figures in 2020 no data is yet available for 2021

The growth in the number of scams reported differs strongly per country



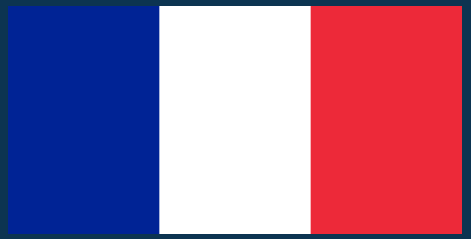
In general, most countries report a faster growth in Money Lost than Number of Report Scams

Online scams are now the (2nd) most reported type of crime in many countries



This is only the tip of the iceberg as an estimated 7% of all scams are reported

Australia
13%



France
17%

Netherlands
12%

Canada
5%

Israel
9%

Scam victims feel ashamed, reporting is difficult or unclear,
and not all law enforcement agencies accept scams to be reported

A Big “Thank You” to our Supporting Partners

Foundation Partners

GROUP-IB

TREND MICRO™

eurodns
YOUR WORLD OF DOMAIN NAMES

ever
Nothing to hide. Everything to gain.

EBRAND

Corporate Partners

BARCLAYS

builtwith

cira

CleanDNS

Crystal

CYBERTRACE

.dk hostmaster

DOMAIN CRAWLER

DNSFilter

EURid

F-Secure

Flash&Start®
INTERNET PROTECTION

globaleyez

moosend

netsweeper

opentext™

Secutec

WhoisXMLAPI

TRM

Xolphin
A SECTIGO COMPANY

Want to join our fight against online scams? Join us!

The following people contributed to this report

Diego Migliorisi	Asociación Argentina de Lucha contra el Cibercrimen (AALCC)	Argentina
Alex Meaney	Scamwatch Australia (ACCC)	Australia
Jayde Richmond	Scamwatch Australia (ACCC)	Australia
Thorsten Behrens	Österreichisches Institut für angewandte Telekommunikation	Austria
Miguel De Bruycker	Center for Cyber Security Belgium	Belgium
Érico Rodrigues de Melo	PROCON	Brazil
Luiz Eduardo Roncato Cordeiro	CERT Brazil	Brazil
Gabriella Santos	About Fraud	Brazil
Giovanni C. Pina Oliveira	Police for Repression of Cyber à Crimes	Brazil
Alexandra Tsvetkova	LIBRe Foundation	Bulgaria
Vladimir Dimitrov	Police Bulgaria	Bulgaria
Guy Paul Larocque	Canadian Anti-Fraud Centre	Canada
Jeff Morris	National Cybercrime Coordination Unit (NC3)	Canada
Tanya O'Callaghan	The Canadian Internet Registration Authority	Canada
Li-Xiong Chu	Dr2 Consultants Shanghai	China
Tiffany Zhang	Dr2 Consultants Shanghai	China
Leena-Kaisa Åberg	RIKU	Finland
Kristian Meismaa	Police Finland	Finland
Éric Freyssinet	Gendarmerie Nationale	France
Philippe Lebon	Scams Alerts - Cyber Prevention Webinars	France
Stephane Robinot	Europol	France
Karolina Wojtal	European Consumer Center (ECC) Germany	Germany
Joachim Feits	mindUp	Germany
Paul Asinor	Ecommerce Association of Ghana	Ghana
Tushar Bhagat	Ahaan Foundation (responsiblenetism.org)	India
Michael Cryan	Police Ireland (An Garda Síochána)	Ireland
	Cybercrime Department	Israel
	Israel National CERT	Israel
Francesco Collini	FlashStart Internet Protection	Italy
Laura Bartolini	FlashStart Internet Protection	
Alisa Kayfadzhyan	Group-IB	
Eiichiro Mandai	ODR Room Network	Japan
Ono Katsumi	Japan Cybercrime Control Center (JC3)	Japan
Mohd Shamil Bin Mohd Yusoff	CyberSecurity Malaysia	Malaysia
Hasnida Zainuddin	CyberSecurity Malaysia	Malaysia
Saral James	Malaysian Association Of Standards Users	Malaysia
Saravanan Thambirajah	Federation of Malaysian Consumer Associations (FOMCA)	Malaysia
Pablo Corona Fraga	Associacion de Internet Mexico (AIMX)	Mexico
Philippe Boulanger	Associacion de Internet Mexico (AIMX)	Mexico
Marianne Junger	University of Twente	Netherlands
Sean Lyons	Netsafe New Zealand	New Zealand
Confidence Staveley	CyberSafe Foundation	Nigeria
Enyinna Abazie	CyberSafe Foundation	Nigeria
Asif Riaz	Pakistan Standards & Quality Control Authority	Pakistan
Ayesha Masood	Digital Rights Foundation	Pakistan
Muhammad Asad Ul Rehman	Cyber Security of Pakistan	Pakistan
Pawel Pawlinski	CERT Polska	Poland
Pedro Mendonça	Centro Nacional de Ciberseguranca	Portugal
Covita Sónia	DECO Proteste	Portugal
Cláudia Maia	DECO Proteste	Portugal
Dmitry Tunkin	Group-IB	Qatar
Alisa Kayfadzhyan	Group-IB	Russia
Dmitry Lobanov	RLab Realty	Russia
Mohammed Iraqi	Consumer Protection Association, Saudi Arabia	Saudi Arabia
You Jung Kee	Interpol	South Korea
Carles Garrido	Mossos d'Esquadra	Spain
José A. Merino	Mossos d'Esquadra	Spain
Richard (莊明雄) Chuang	Police Taiwan	Taiwan
Shubert Mwarabu	OKOA Tembo wa Tanzania	Tanzania
Raisa Fedorovska	EMA	Ukraine
Mike Haley	CIFAS	UK
Donna Gregory	Federal Bureau of Investigation	USA
Laureen Kapin	Federal Trade Commission	USA
Nicholas Mastrocinque	Federal Trade Commission	USA
Hieu Minh Ngo	Chong Lua Dao	Vietnam
Luong Van Cua	scamvn.com	Vietnam
Alexandre Francois	WhoisXML API	Data
Anna Danilova	WhoisXML API	Data

We sincerely thank them for their support and feedback!

How did we collect the data?

We used desk research to find country-related cybercrime statistics. Unfortunately, most countries do not yet have ready made available statistics on online scams. In some cases, we had to report the number of cyber-incidents, phishing attempts or frauds (both online as well as offline) as these were the only data available.

We also used LinkedIn to search for national experts in the area of cybercrime. In many cases we were able to contact the national (cyber)police. We asked these expert to provide and/or verify the collected data.

The key sources per country are listed on each country page. Additional sources used are available at request.

For population and GDP related data we used the World Bank. The number of Internet users was retrieved from Internet World Stats. For currency conversion XE.com mid-market exchange was applied. The source of the flags is CountryFlags.com.

Country Overview

	Population	GDP ($, millions)	Internet Population	Internet Penetration (%)	Number of Scams	Scams per 1000 pop	Estimate value Lost (USD)	Amount Lost per Capita	Amount Lost per Case
Argentina	45.808.750	$ 491.493	33.561.876	73	26.000	0,57	$ 12.702.674	$ 0,28	$488,56
Australia	25.739.260	$ 1.542.660	21.159.515	82	566.648	22,01	$ 1.257.533.325	$ 48,86	$2.219,25
Austria	8.956.280	$ 477.082	7.681.957	86	22.440	2,51	$ 27.483.798	$ 3,07	$1.224,77
Belgium	11.587.880	$ 599.879	10.021.242	86	38.186	3,30	$ 52.149.634	$ 4,50	$1.365,67
Brazil	213.993.440	$ 1.608.981	160.010.801	75	117.700.000	550,02	$ 777.000.000	$ 3,63	$6,60
Bulgaria	6.899.130	$ 80.271	4.492.326	65	31.025	4,50	$ 26.135.460	$ 3,79	$842,40
Canada	38.246.110	$ 1.990.762	33.950.632	89	104.295	2,73	$ 295.530.624	$ 7,73	$2.833,60
China	1.412.360.000	$ 17.734.063	989.080.566	70	2.100.000	1,49	$ 3.000.000.000	$ 2,12	$1.428,57
Finland	5.541.700	$ 299.155	4.831.170	87	20.000	3,61	$ 33.602.791	$ 6,06	$1.680,14
France	67.499.340	$ 2.937.473	59.470.000	88	423.000	6,27	$ 1.484.000.000	$ 21,99	$3.508,27
Germany	83.129.290	$ 4.223.116	77.794.405	94	249.254	3,00	$ 3.710.109.115	$ 44,63	$14.884,85
Ghana	31.732.130	$ 77.594	15.065.541	47	35.000	1,10	$ 25.000.000	$ 0,79	$714,29
India	1.393.409.030	$ 3.173.398	755.820.000	54	120.000.000	86,12	$ 16.300.097.131	$ 11,70	$135,83
Iran	85.028.760	$ 231.548	67.602.731	80					
Ireland	5.028.230	$ 498.560	4.950.000	98	16.929	3,37	$ 26.872.612	$ 5,34	$1.587,37
Israel	9.364.000	$ 481.591	7.002.759	75	210.000	22,43			
Italy	59.066.220	$ 2.099.880	50.540.000	86	131.059	2,22	$ 476.527.304	$ 8,07	$3.635,98
Japan	125.681.590	$ 4.937.422	117.400.000	93	581.943	4,63	$ 448.913.167	$ 3,57	$771,40
Kenya	54.985.700	$ 110.347	53.005.614	96			$ 120.000.000	$ 2,18	
Malaysia	32.776.190	$ 372.701	25.343.685	77	39.525	1,21	$ 482.719.925	$ 14,73	$12.213,03
Mexico	130.262.220	$ 1.293.038	92.010.000	71	5.400.000	41,45	$ 246.000.000	$ 1,89	$45,56
Netherlands	17.533.400	$ 1.018.007	15.877.494	91	1.500.000	85,55	$ 2.805.000.000	$ 159,98	$1.870,00
New Zealand	5.122.600	$ 249.992	4.273.353	83	18.331	3,58	$ 19.731.652	$ 3,85	$1.076,41
Nigeria	211.400.700	$ 440.777	154.301.195	73	500.000	2,37	$ 175.000.000	$ 0,83	$350,00
Pakistan	225.199.930	$ 346.343	118.800.000	53	102.356	0,45	$ 100.000.000		
Philippines	111.046.910	$ 394.086	73.003.313	66	6.471.300	58,28	$ 448.900.000	$ 4,04	$69,37
Poland	37.781.020	$ 674.048		87	26.535	0,70	$ 10.368.450	$ 0,27	$390,75
Portugal	10.299.420	$ 249.886	7.622.142	74	1.781	0,17	$ 1.587.245	$ 0,15	$891,21
Qatar	2.930.520	$ 179.571	2.532.059	86					
Romania	19.115.150	$ 284.088	12.545.558	66	5.052	0,26			
Russian Federation	143.446.060	$ 1.775.800	124.000.000	86	249.200	1,74	$ 815.000.000	$ 5,68	$3.270,47
Saudi Arabia	35.340.680	$ 833.541	27.048.861	77	3.000.000	84,89	$ 2.000.000.000	$ 56,59	$666,67
Singapore	5.453.570	$ 396.987	4.821.119	88	23.931	4,39	$ 452.568.709	82,99	18911,39982
South Africa	60.042.000	$ 419.946	31.858.027	53	30.000	0,50	$ 100.000.000	1,67	3333,333333
South Korea	51.744.880	$ 1.798.534	49.421.084	96	174.328	3,37	$ 233.845.073	4,52	1341,40857
Spain	47.326.690	$ 1.425.277	42.400.756	90	257.907	5,45	$ 750.000.000	$ 15,85	$2.908,02
Sweden	10.415.810	$ 627.438	9.554.907	92	131.254	12,60	$ 500.767.800	$ 48,08	$3.815,26
Switzerland	8.697.720	$ 812.867	7.942.864	91	15.221	1,75	$ 426.996.447	$ 49,09	$28.053,11
Taiwan	23.570.000		21.920.626	93	24.000	1,02	$ 168.000.000	$ 7,13	$7.000,00
Thailand	69.950.840	$ 505.982	62.300.000	89	48.513	0,69	$ 2.282.826.000	$ 32,63	$898,00
Turkey	85.042.740	$ 815.272	69.107.183	81	1.940.000	22,81	$ 1.163.234.847	$ 13,68	$599,61
United Arab Emirates	9.991.080	$ 358.869	8.913.217	89	1.740	0,17	$ 24.000.000	$ 2,40	$13.793,10
United Kingdom	67.326.570	$ 3.186.860	65.001.016	97	965.162	14,34	$ 2.813.834.887	$ 41,79	$2.915,40
United States	331.893.740	$ 22.996.100	312.320.000	94	2.800.000	8,44	$ 5.800.000.000	$ 17,48	$2.071,43
Ukraine	43.814.580	$ 200.086	40.912.381	93	209.016	4,77	$ 16.824.062	$ 0,38	$80,49
Vietnam	98.168.830	$ 362.638	68.172.134	69	87.302	0,89	$ 374.400.000	$ 3,81	$4.288,56

Some countries are remarkable exporters of their domain extension

According to WhoisXML API 2.4 million more .ru domains are registered outside Russia than inside. Other big “exporters” are Taiwan and Poland

Country	TLD	Population	Domains registered in Country	Share of all Domains Worldwide	Domains Registered per Capita	Country Extension Registrations	Country Extension Market Share	Diff Registered vs TDL registrations	Own Country Extension Share of Total Registered	Import / Export
Argentina	ar	45.808.750	330.665	0,05%	0,007	647.767	0,11%	-317102	196%	Exporter
Australia	au	25.739.260	2.025.306	0,33%	0,079	3.681.927	0,61%	-1656621	182%	Exporter
Austria	at	8.956.280	1.306.961	0,22%	0,146	1.826.558	0,30%	-519597	140%	Exporter
Belgium	be	11.587.880	573.130	0,09%	0,049	2.009.672	0,33%	-1436542	351%	Exporter
Brazil	br	213.993.440	3.031.703	0,50%	0,014	5.640.583	0,93%	-2608880	186%	Exporter
Bulgaria	bg	6.899.130	236.766	0,04%	0,034	95.352	0,02%	141414	40%	Importer
Canada	ca	38.246.110	17.659.802	**2,91%**	**0,462**	3.789.518	0,63%	13870284	21%	Importer
China	cn	1.412.360.000	25.778.606	**4,25%**	0,018	25.576.846	**4,22%**	201760	99%	Importer
Finland	fi	5.541.700	753.036	0,12%	0,136	570.592	0,09%	182444	76%	Importer
France	fr	67.499.340	7.710.860	1,27%	0,114	5.479.805	0,90%	2231055	71%	Importer
Germany	de	83.129.290	6.751.398	1,11%	0,081	23.030.607	3,80%	-16279209	341%	Exporter
Ghana	gh	31.732.130	48.132	0,01%	0,002	4.518	0,00%	43614	9%	Importer
India	in	1.393.409.030	4.686.957	0,77%	0,003	3.343.975	0,55%	1342982	71%	Importer
Indonesia	id	276.361.790	886.915	0,15%	0,003	787.131	0,13%	99784	89%	Importer
Iran	ir	85.028.760	381.795	0,06%	0,004	1.290.484	0,21%	-908689	338%	Exporter
Ireland	ie	5.028.230	379.096	0,06%	0,075	385.119	0,06%	-6023	102%	Exporter
Israel	is	9.364.000	503.977	0,08%	0,054	75.921	0,01%	428056	15%	Importer
Italy	it	59.066.220	3.824.194	0,63%	0,065	4.004.149	0,66%	-179955	105%	Exporter
Japan	jp	125.681.590	6.347.506	1,05%	0,051	2.163.319	0,36%	4184187	34%	Importer
Kenya	ke	54.985.700	165.679	0,03%	0,003	170.096	0,03%	-4417	103%	Exporter
Malaysia	my	32.776.190	1.605.703	0,26%	0,049	401.814	0,07%	1203889	25%	Importer
Mexico	mx	130.262.220	1.388.813	0,23%	0,011	1.227.893	0,20%	160920	88%	Importer
Netherlands	nl	17.533.400	12.736.528	**2,10%**	**0,726**	6.636.385	**1,10%**	6100143	52%	Importer
New Zealand	nz	5.122.600	333.231	0,05%	0,065	668.289	0,11%	-335058	201%	Exporter
Nigeria	ni	211.400.700	406.824	0,07%	0,002	5.420	0,00%	401404	1%	Importer
Pakistan	pa	225.199.930	275.731	0,05%	0,001	18.535	0,00%	257196	7%	Importer
Philippines	ph	111.046.910	849.552	0,14%	0,008	1.844.039	0,30%	-994487	217%	Exporter
Poland	pl	37.781.020	577.976	0,10%	0,015	3.385.334	0,56%	-2807358	586%	Exporter
Portugal	pt	10.299.420	311.480	0,05%	0,030	424.368	0,07%	-112888	136%	Exporter
Qatar	qa	2.930.520	36.552	0,01%	0,012	24.990	0,00%	11562	68%	Importer
Romania	ro	19.115.150	282.835	0,05%	0,015	855.571	0,14%	-572736	302%	Exporter
Russian Federation	ru	143.446.060	1.531.406	0,25%	0,011	10.708.609	**1,77%**	-9177203	699%	Exporter
Saudi Arabia	sa	35.340.680	196.652	0,03%	0,006	63.153	0,01%	133499	32%	Importer
Singapore	sg	5.453.570	991.647	0,16%	**0,182**	227.266	0,04%	764381	23%	Importer
South Africa	sa	60.042.000	1.577.102	0,26%	0,026	63.153	0,01%	1513949	4%	Importer
South Korea	kr	51.744.880	1.312.893	0,22%	0,025	1.104.232	0,18%	208661	84%	Importer
Spain	es	47.326.690	2.364.653	0,39%	0,050	2.211.718	0,36%	152935	94%	Importer
Sweden	se	10.415.810	989.007	0,16%	0,095	2.616.157	0,43%	-1627150	265%	Exporter
Switzerland	ch	8.697.720	1.014.548	0,17%	0,117	2.669.953	0,44%	-1655405	263%	Exporter
Taiwan	tw	23.570.000	333.516	0,06%	0,014	2.745.510	0,45%	-2411994	823%	Exporter
Tanzania	tz	61.498.440	13.365	0,00%	0,000	32.464	0,01%	-19099	243%	Exporter
Thailand	th	69.950.840	456.729	0,08%	0,007	113.199	0,02%	343530	25%	Importer
Turkey	tr	85.042.740	1.817.201	0,30%	0,021	448.531	0,07%	1368670	25%	Importer
United Arab Emirates	ae	9.991.080	415.479	0,07%	0,042	247.587	0,04%	167892	60%	Importer
United Kingdom	uk	67.326.570	7.497.721	**1,24%**	0,111	19.822.070	**3,27%**	-12324349	264%	Exporter
United States		331.893.740	128.029.365	**21,13%**	**0,386**			128029365		Importer
Ukraine	ua	43.814.580	650.675	0,11%	0,015	931.443	0,15%	-280768	143%	Exporter
Vietnam	vn	98.168.830	953.696	0,16%	0,010	562.610	0,09%	391086	59%	Importer

The Nigerian extension on the other hand is hardly bought, while Nigerians have bought 400,000 foreign domains

21% of all domains are registered in the USA and with 0.7 domains per capita, the Dutch seem to love registering domains

The number of scams has increased 20% worldwide in H1 2022

Interview with Ariel Lin, Senior Product Manager, Trend Micro

Which scam trends to you see arise across the world?

Up to now in 2022, **Trend Micro** has helped business and individuals block over 1,100 millions of online scams. If we compared January 2021 to August 2021, the overall number of scam cases has increased with 20% worldwide. Based on Trend Micro scam data analysis, we can tell that scam cases in the US has grown the most (25%) while Japan increase is 'limited" to 18%.

Regarding to the scam categories, there are no big surprises in Japan. The dating scam is still prevalent in consumer's digital life. 63% of Japanese scam cases are related to online dating. Online shopping scam and investment scams are the top 2 (22%) and top 3 (9%).

In the United States, 38% of the scam cases are in the form of surveys spread as phishing (email) or smishing (text messages). We also see online shopping scam and dating scams growing in United States. In addition, the cryptocurrency scam or bitcoin scams have increased significantly in 2022, which usually trick consumer with fake crypto trading websites that look identical to legitimate ones.

How does Trend Micro fight online scams?

Trend Micro has over 30 years of cybersecurity experience and is powering the world's largest scam database. Our anti-phishing technology is proven by AV Comparative to detect and block up to 95% of phishing and scam sites. To combat sophisticated scams targeting consumer, we have studied various scams tactics and provide solutions to help individuals and families to protect them from scams in their digital life.

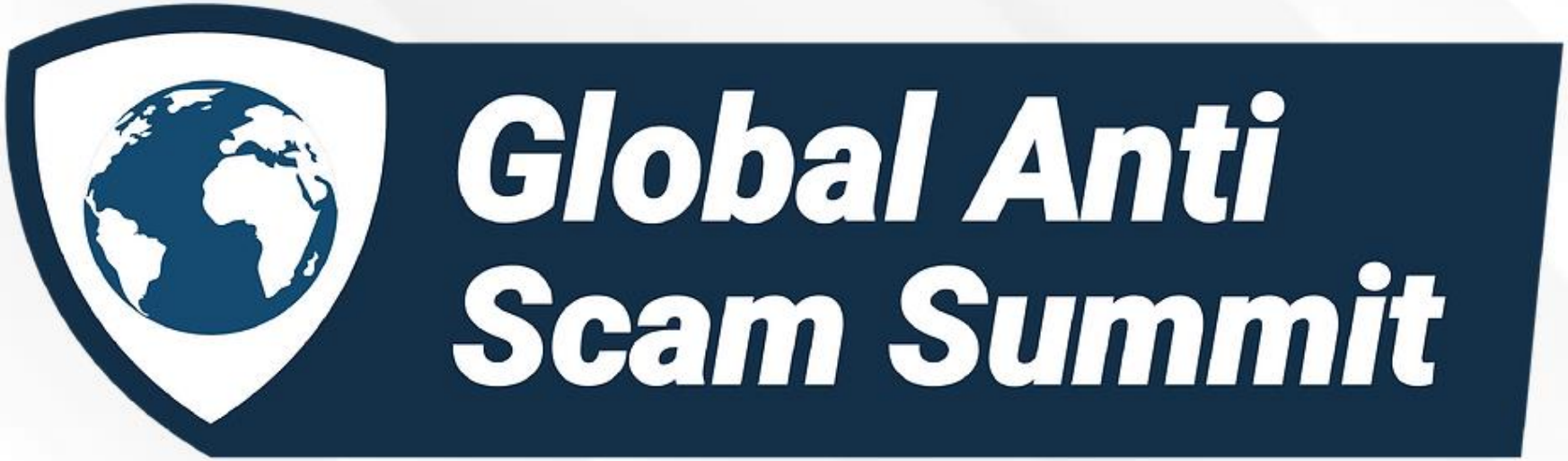
We see that text messages besides phone calls has become one of the most popular scam contact methods in 2021. Users are looking for solutions not only to detect dangerous scams, but also block unsolicited spams calls and text messages. Our product, **Trend Micro Check**, empowers the users to fight against annoying spam/scams and take back control over their phone

What is your view on how we can combat scams better on a national and international level?

Scams are an international business. Online scammers, more than other criminals, target victims especially outside their own country. As a result, governments and law enforcements have an even harder time to track the scam, independent if he operates mainly via the web, email or text. Hence, Trend Micro is Founding Partner of the **Global Anti Scam Alliance** and main sponsor of the **Global Anti Scam Summit** to share knowledge and help governments, consumer protection organizations and law enforcement prevent and combat scams better.

Ariel Lin
Senior Product Manager
Trend Micro

Join us at the Global Online Scam Summit!



Presents

GLOCAL TRENDS, GLOCAL SOLUTIONS

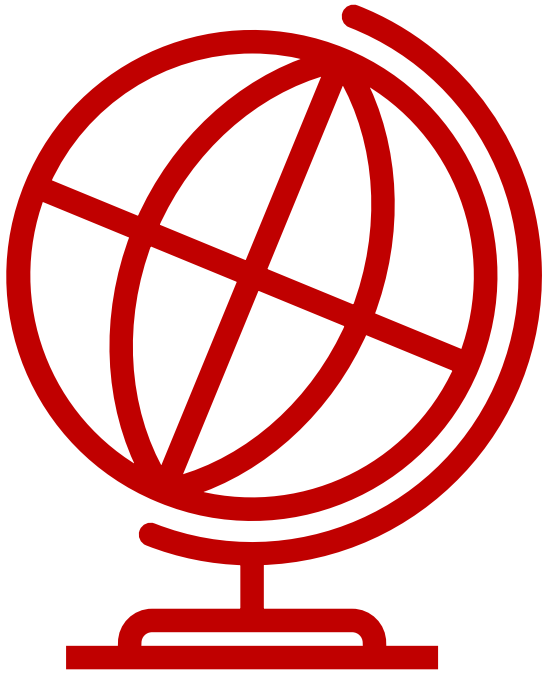
Powered by

APWG.EU

GASA
Global Anti-Scam Alliance

GLOBAL CYBER ALLIANCE

All findings will be presented at the Summit. Register for free at: www.globalonlinescamsummit.org



ANALYSIS PER COUNTRY

Theft of personal data grew by 200% in Argentina

The number of incidents received by the CERT of Argentina increased with 262%

Scam reporting is fragmented in Argentina. Most crime prevention is done on a state level and not shared on a national plain.

The National Computer Emergency Response Team recorded a total of 591 computer incidents during 2021. This was an increase of 261% compared to 2020. Online fraud consisted of 331 cases, 56% of all reports.

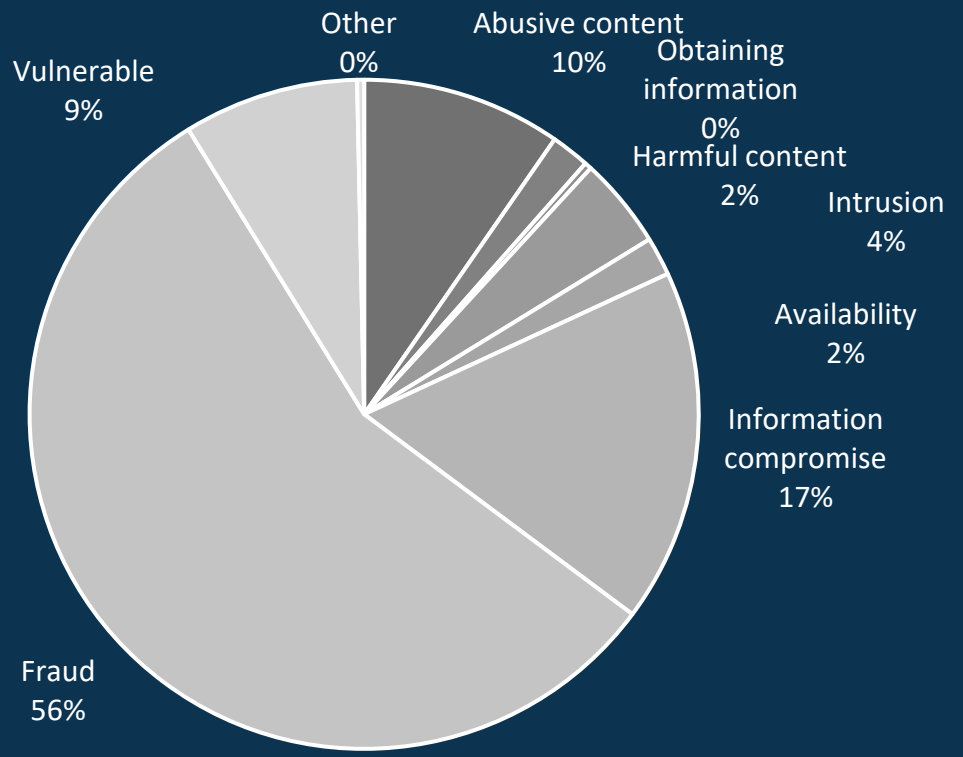
One of the biggest scams in 2022 in Argentina were 160 reported cases where victims were asked to send their ID, money and several selfies in order to receive a package. The information was however used to create bank accounts at Fintech companies.

There are several organizations focusing on cybercrime. Consumers can report a cyber crime to the local police station, the municipality, the state or they can contact the office of the Attorney General who has a special cybercrime fiscal unit called **Unidad Fiscal Especializada en Ciberdelincuencia** (UFECI).

For IT related crimes, consumers can also email the federal police. There is a special unit called the **National Cybercrime Directorate**. The CERT is part of this organization.

It is also possible to report online fraud to the **National Directorate for Consumer Defense** (Defensa de las y los consumidores) who will refer the consumer to the appropriate body.

The **Argentine Association for the Fight Against Cybercrime** (AALCC) is a non-profit association whose main objective is to eradicate computer crimes and crimes committed through the Internet by providing guidance, training, and prevention.



Incidents Reported to the Argentina CERT

Key Statistics:

Population:	45.8 million
Internet:	73%
# of Scams:	26,000 (100%)
Scams / 1,000 :	0.57
Money lost:	€ 12.7million*
Per capita:	€ 0.28
Per report:	€ 488

Key Organizations:

- AALCC (reporting, nonprofit)
- UFECI (fiscal cybercrime)
- Cybercrime Directorate

WhoisXML API:

Domains/capita	0,007
Domains registered	330,665
TLD registrations	647,767

cibercrimen.org.ar/2022/08/09/los-ciberdelitos-son-una-modalidad-que-va-a-seguir-creciendo/
argentina.gob.ar/sites/default/files/2022/02/informe_2_cert_2021_f__0.pdf

* ScamAdviser Estimate

Australia reports AUS$ 2 Billion lost in 2021

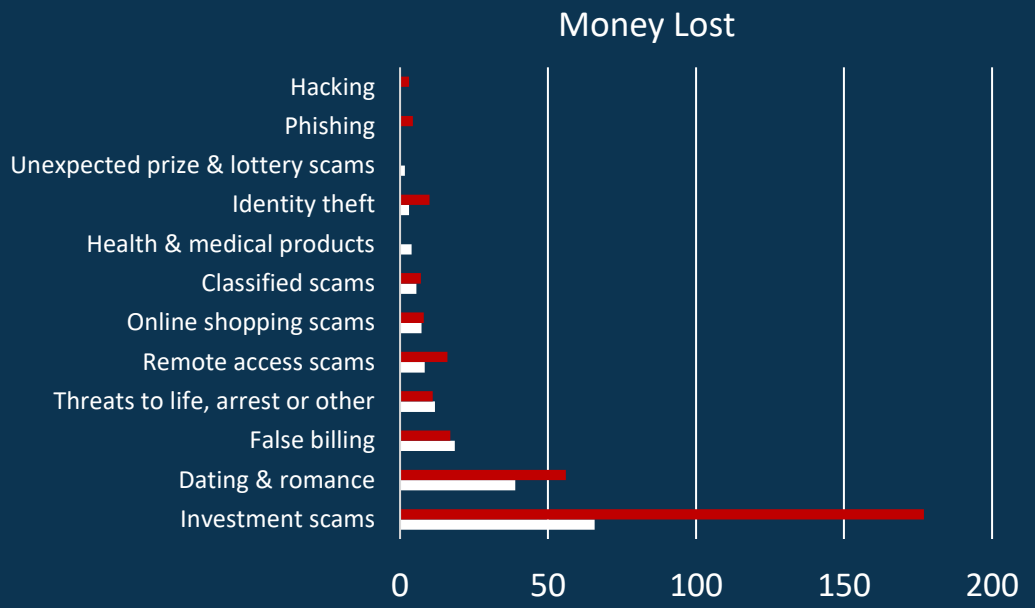
Australia reported an increase of 28% in scam reports and a 112% growth in money lost

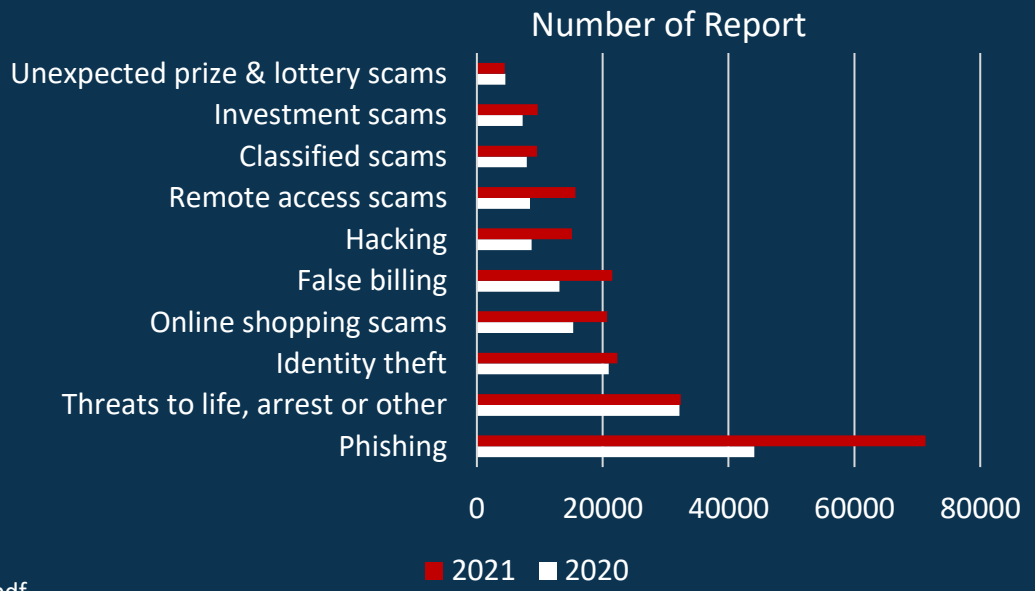
The **Australian Competition & Consumer Commission** (ACCC) has been monitoring scams for 13 years. In its annual report it states that **Scamwatch**, ReportCyber, other government agencies, banks and money remitters received a combined total of over **566,648 reports**, with reported losses of almost **$1.8 billion** in 2021. One third of victims do not report scams, so actual losses were well over $2 billion.

Investment scams caused the most financial loss, with combined losses of $701 million. This was followed by payment redirection with $227 million lost, and romance scams with $142 million lost. Only 13% of victims report to to Scamwatch.

Research commissioned by the ACCC in 2021 found that 96% of people have been exposed to a scam in the last 5 years with half of these **contacted weekly or daily by scammers**. 30% of victims do not report the scam to anyone.

The ACCC continued to advocate for digital platforms to take more action to address scams. In March 2022, the ACCC commenced proceedings in the **Federal Court against Facebook** owner Meta alleging that they engaged in false, misleading or deceptive conduct by publishing scam advertisements featuring prominent Australian figures.





Key Statistics:

Population:	25,7 million
Internet usage:	82%
# of Scams:	566,648 (28%)
Scams / 1,000 :	22
Money lost:	$ 1,257 mil (112%)
Per capita:	$ 49
Per report:	$ 2219

Key Organizations:

- Australian Competition & Consumer Commission
- ScamWatch (consumer reporting portal site)
- ReportCyber (consumer & business reporting site)

WhoisXML API:

Domains/capita	0,07
Domains registered	2,025,306
TLD registrations	3,681,927

https://www.accc.gov.au/system/files/Targeting%20scams%20-%20report%20of%20the%20ACCC%20on%20scams%20activity%202021.pdf

The Austrian Cybercrime Police received 46,179 reports (+28.6%)

One of its key actions in 2021 has been to centralize and optimize the cooperation with Internet Service Providers and Social Platforms

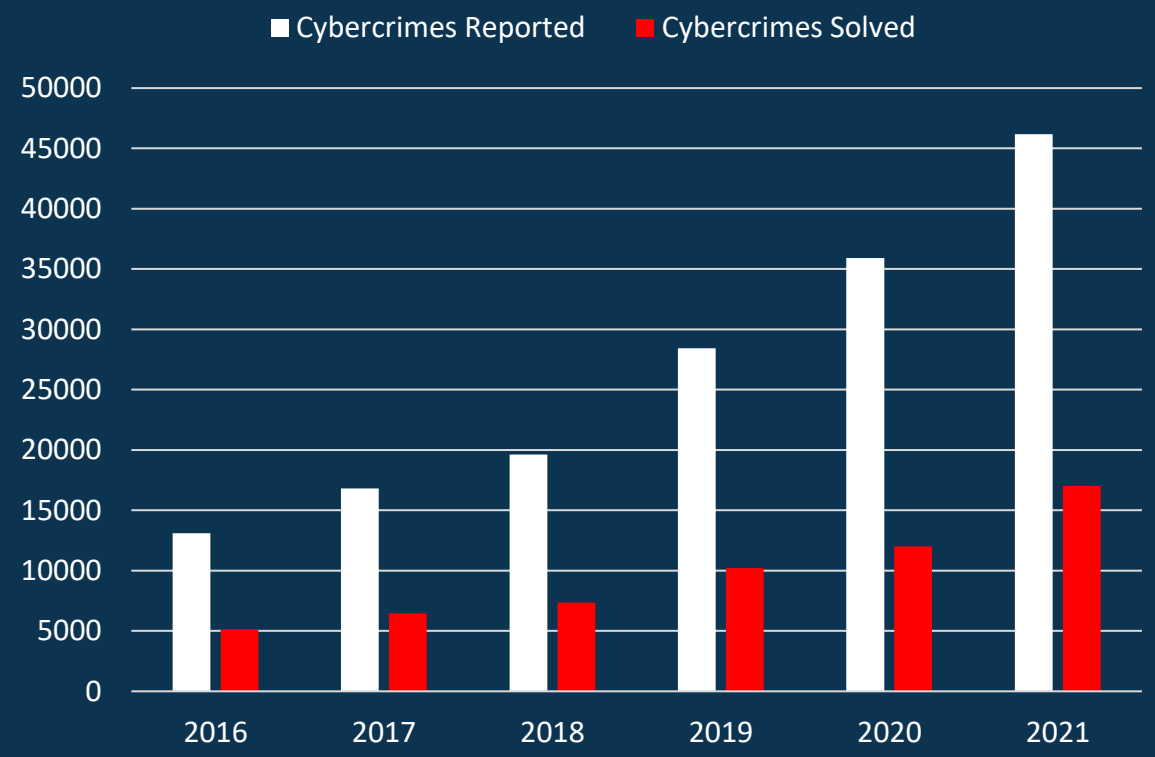
Online scams can be reported to the local, state or federal police . On the federal level, a separate unit, the Cyber Crime Competence Center (C4), has been set-up. C4 focuses especially on cyber crimes such as hacking and DDoS attacks. Online scams and child pornography are also part of its assignment. Consumers can report crime directly to C4 via **against-cybercrime@bmi.gv.at**

Since 1997 **OIAT** (the Austrian Institute for Applied Telecommunication) has launched several initiatives to make the Internet a safer place. OIAT offers a trust seal for reliable online stores, maintains **Saferinternet.at** with tips and tricks on how to use the Internet safely, runs **Watchlist Internet** with a manually vetted list of malicious and dubious websites and **Fake-Shop Detector**, a browser extension to check sites using artificial intelligence. In 2021, OIAT reported 4,276 fake webshops and received 13,453 reports of fraud made by our users.

The largest type of cybercrime reported to the Austrian police is Internet fraud, which grew from 16,831 (2019), to 18,780 (2020) to 22,440 cases in 2021. Despite the considerable increase, the percentage of solved cases improved from 33.4% in 2020 to 37.2% in 2021.

Like 2020, the year 2021 was marked by the effects of the COVID 19 pandemic. The cybercrime police notices an increasing professionalization of online fraud. The specialized groups of perpetrators work in a division of labor, are technically experienced and act with a correspondingly high degree of deliberation. In this field of crime, the responsible department of the Department 7 of the Federal Criminal Police Office focuses in particular on online shopping fraud.

One of the key milestones of the Austrian Cybercrime Police in 2021 has been to centralize and optimize the cooperation with Internet Service Providers and Social Media platforms such as those of Meta.



Key Statistics:

Population:	8.9 million
Internet:	86%
# of Scams:	22,440 (19%)
Scams / 1,000 :	2.5
Money lost:	$ 27.4 mil (19%)
Per capita:	$ 3,07
Per report:	$ 1.224*

Key Organizations:

- Bundeskriminalamt (police)
- OIAT (scam awareness not profit)

WhoisXML API:

Domains/capita	0,15
Domains registered	1,306,961
TLD registrations	1,826,558

Sources: Watchlist Internet & Bundeskriminalamt Austria

*** ScamAdviser Expert Estimate**

In 2021, 38,000 cases of Internet fraud were reported in Belgium

After a decline in 2020 of 14%, fraud cases are up 32% in 2021, especially the number of reported phishing cases grew rapidly

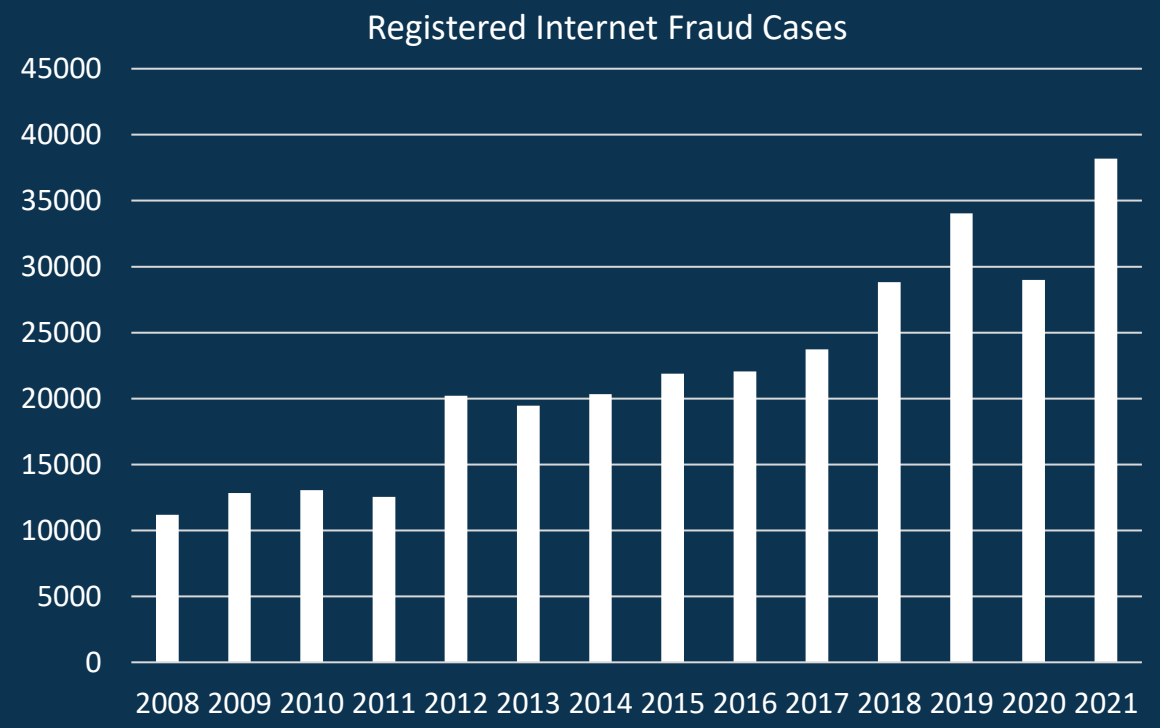
The impact of the Coronavirus epidemic was still visible in 2021 in Belgium crime figures. While cybercrime figures continue to rise (although not as shapely as in 2020) the number of physical crimes kept declining. The total number of crime reports dropped with 12.4% to 866,588. Internet Fraud now makes up 4.4% of all cases.

There are several places where Belgians can report online fraud. Online fraud can be reported to both the local police and centrally on **Police On the Web**. If reported online, the report is handed over to the local police force.

Belgians (both consumers as well as businesses) can also report misleading practices, fraud or swindles to **Report Belgium**. The information is passed along to the appropriate authority who subsequently analyzes the report and may carry out a further investigation. Report Belgium is a joint venture of the Federal Agency for the Safety of the Food Chain, the Federal Agency for Medicines and Health Products, the FPS ELSD, the Federal Police, the FPS Finances, and the Federal Public Service (FPS) Economy. The latter is also the technical manager of the system.

In 2020, the **Centre for Cybersecurity Belgium (CCB)** has launched **SafeOnWeb.be** to help consumers to be safe online. It also offers an email address where consumers can report phishing emails. The service seems to work. The amount of money lost due to phishing dropped from 34 million euro in 2020 to 25 million in 2021 (-26%). The actual amount stolen was more than 100 million, however in 75% of the cases the banks were able to identify the scam and block or reverse the transaction.

Other places where Belgians can report cybercrime include the **Belgium CERT** and **The Financial Services and Markets Authority** (FSMA). The FSMA reports that 25.5 million was reported to them to be lost in 2021. The number of reports increased with 53%. Other info sites include **ClickSafe** (focused on children), **Cybersimple** and **SpotTheScam**.



Key Statistics:

Population:	11.6 million
Internet:	86%
# of Scams:	38,186 (32%)
Scams / 1,000 :	3,3
Money lost:	$ 52 mil (-39%)
Per capita:	$ 4.50
Per report:	$ 1365

Key Organizations:

- Belgium Police
- Centre for Cybersecurity Belgium
- FSMA (financial authority)

WhoisXML API:

Domains/capita	0,05
Domains registered	573,130
TLD registrations	2,009,672

cybercrimeinfo.nl/cybercrime/981596_belgische-politie-ziet-aangiften-van-cybercrime-en-internetfraude-verder-stijgen
safeonweb.be/en/news/number-suspicious-messages-sent-suspicioussafeonwebbe-explodes
ccb.belgium.be/nl/nieuws/phishingfraude-2021-de-cijfers
fsma.be/en/news/fraudulent-online-trading-platforms-53-cent-increase-reports

*** ScamAdviser Expert Estimate**

Brazil is one of the most targeted countries for phishing and phone scams

Especially the introduction of a new payment method: Pix caused an influx of scams

In Brazil, **scam fighting is mainly organized per state**. A growing number of states have police teams focusing on cybercrime. However, in June 2022 the federal government also set-up a **Special Investigation Unit of Cyber Crimes (UEICC)** a public/private partnership by the Ministry of Justice and Public Security (MJSP), with support from the Brazilian Federation of Banks (Febraban), to prevent and fight cybercrime.

Consumidor.gov.br, set-up by SENACON, the national consumer secretariat, allows consumers to file a complain about a company's service. In 2021, 1,4 million complains were received (up 16% compared to 2020).

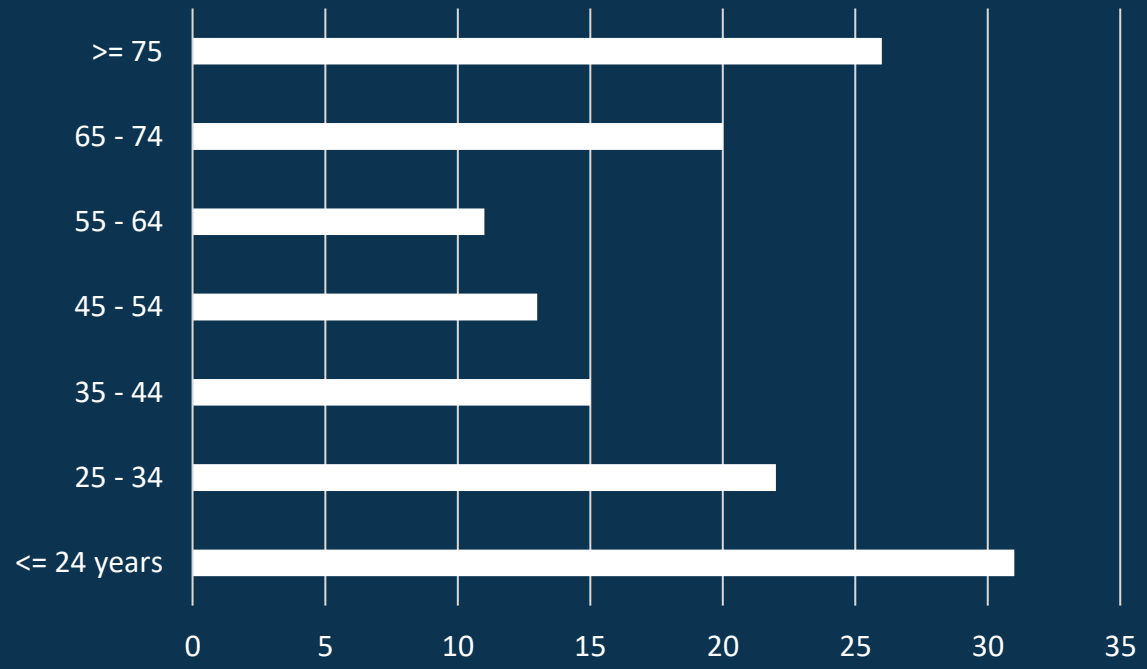
There are nearly 1000 **PROCON's** (consumer protection agencies) in Brazil. The PROCON's are funded either on the state or on the municipality level. A non profit initiative to help customers identify scams and fake websites has also been set up; this is called "**Posso Confiar**" (or Can I Trust?). **ReclameAqui** is a commercial initiative which allows consumers to rate companies and it is the most popular review website in Brazil.

Brazil is one of the most targeted countries for phishing and phone scams. 35% more Brazilians were victims of these scams in 2021. 55% of Brazilians were faced with phishing via e-mail or cell phone, a huge increase compared to the last assessment, in which 39% of the interviewed population claimed to have received malicious messages.

Most scams, 72% , happen via the phone. Brazil has retained its title in 2021 as the most spammed country in the world for the 4th year with 32.9 spam calls per user per month. The number of call bot-initiated scams grew with 473%, by humans with 138%.

The launch of a new payment method Pix, caused chaos. The cybersecurity company PSafe estimates that there are more than four fraudulent attacks per minute via Pix and the number seems to be increasing month by month.

Growth in the number of frauds in 2021 by age group



Source: LexisNexis Risk Rolutions

Key Statistics:

Population:	214 million
Internet:	75%
# of Scams:	117,7 million
Scams / 1,000 :	550
Money lost:	$ 777 million
Per capita:	$ 3.63
Per report:	$ 6.60

Key Organizations:

- Federal Police
- Consumidor.gov.br
- PROCON

WhoisXML API:

Domains/capita	0,014
Domains registered	3,031,703
TLD registrations	5,640,583

folha.uol.com.br/mercado/2022/05/fraudes-digitais-crescem-mais-entre-geracao-z-e-maiores-de-75-anos.shtml
valor.globo.com/empresas/noticia/2022/02/02/tentativas-de-fraude-on-line-crescem-58-pontos-percentuais-e-somam-r-58-bilhes-em-2021.ghtml

Pix Payment: “Faster Payments, Faster Fraud”

Pix payment, a government backed method of payment, has made money transfer in Brazil very easy. With over 100 million people able to settle payments quickly, the method is becoming quite popular. People with a Pix account only need a phone number or a QR code to transfer money to other people or businesses and without knowing their account details.

How does Pix work in Brazil?

Pix operates similarly to domestic payment networks in other countries, such as Zelle in the United States or Bizum in Spain. However, there are certain limitations and user behaviors that are unique to Pix. To use Pix, you must register an address key. This is your account’s unique identifier. The address key can then be associated with a phone number or an email address. This allows Pix to integrate with communication apps like WhatsApp, where it’s possible for Brazilians to send each other money via the Pix network.

But scammers are now using the same method to fraud people bring back memories of “sequestro relâmpago” (“lightning kidnapping”) which first appeared in Brazil in the 1990s. These are violent crimes in which people would be nabbed off the street– often at gunpoint – to withdraw cash from a nearby ATM.

So, what’s the correlation?

Fraud and crime always go hand-in-hand with new financial technologies. Any time a new payment method – checks, credit cards, digital payments, whatever – emerges, criminals find a way to exploit them. Now, criminals abduct the victim and force them to make a Pix transfer. On top of lightning kidnappings crimes Pix users face other scams like Authorized push payment fraud, Fake supplier scams, Session capture, & WhatsApp cloning.

Brazilian authorities are now outing measures to curb the rising cases of scam. The mechanisms include limiting the value of transfers made between 8 p.m. and 6 a.m., when most kidnappings occur, and a feature that allows individual users to limit transfer amounts.

The São Paulo Legislative Assembly proposed a bill to stop all Pix activity “until the Brazilian Central Bank introduces mechanisms to ensure consumer safety,” Angelica Mari at ZDNet reported at the time.

This article has been published earlier on About Fraud by Gabriella Santos

Brazilians are experiencing a frightening new, online, reality

Interview with Giovanni C. Pina Oliveira Agent of the Civil Police of Sergipe - Police Station for Repression of Cyber à Crimes

How would you describe the situation of online scams in Brazil?

The feeling of insecurity is constant, whether when relating to another person through social networks or when carrying out a financial transaction. Since the beginning of the Internet we have observed a gradual growth of online scams. With the policy of social isolation due to COVID-19 and the consequent migration of social activities to the Internet, the number of online fraud cases has exploded.

As for the types of scams, my personal perception is that online banking frauds rank number 1. Banking scams are especially practiced through social engineering, where the victim provides data that allows the illicit movement of their financial resources. Phishing, Vishing and Smishing are associated with this practice, as are Sim Swaps.

Number 2 is the hacking of accounts on social networks, especially Instagram and WhatsApp, with the aim of further misleading people related to the victim of the hacked account. Fraudulent contracting of financial loans on behalf of other parties is most likely the third most common scam. In this case, social engineering is used to induce victims to provide images their personal and biometric documents, which are
improperly used to contract loans from financial institutions.

Other common scams are online purchases using stolen credit cards, online stores that never deliver the ordered products and scams committed through an alleged romantic relationship with the victim (Nigerian 419 and its variations).

What actions is your state taking to combat scams?

Unfortunately, despite the fact that the Brazilian legislature has recently promoted changes in the penal legislation, assigning more severe penalties to fraud carried out over the internet, this measure does not seem to me to be effective in combating this type of crime. In addition, there are no educational campaigns promoted by the government and investments in new technologies and human resources are scarce.

What actions should we take internationally to combat online scams more effectively?

When dealing with online scams with international repercussions, the investigations have proved to be unfeasible due to the bureaucracy involved in communication between the investigation agencies of the countries involved. This is the first challenge that needs to be faced.

Giovanni C. Pina Oliveira
Agent of the Civil Police of Sergipe - Police Station for Repression of Cyber à Crimes

Cybercrime is estimated to have grown with 70% in 2021 in Bulgaria

However, officially only 51 cybercrime incidents were reported by the Ministry of Internal Affairs

Several organizations are involved in fighting cybercrime in Bulgaria. The General **Directorate Combating Organized Crime (GDCOC),** part of the Bulgarian Ministry of Internal Affairs, has set-up a special **Cybercrime Police** department in Sofia and consisting of 40+ officers who tackle local and transnational organized criminal structures related to computer crimes or crimes committed in or through computer networks and systems.

The **national computer emergency response team** (CERT) helps its users to reduce the risks of information security incidents and to resolve incidents which have already occurred. There is also a **National Computer Security Incident Response Team (NCSIRT)** functioning under the umbrella of the 'e Government Infrastructure' Executive Agency to the Bulgarian Ministry of Electronic Government. The SCSIRTs are set up locally for various sectors (i.e., energy, transport, banking, financial market infrastructure, health, and digital) in compliance with the instructions of European Union Cybersecurity Agency (ENISA). They coordinate their activities with the national CERT.

In 2020, NCSIRT reported 2,100 cyber incidents an increase of 9% compared to 2019. The highest percentage of registered incidents was due to fraud (47%), followed by malware (38%). For 2021, no data was reported.

The Chairman of the **Bulgarian Cybercrime Association** indicated that cyberattacks had increased by a double-digit percentage in Bulgaria, and – according to their unofficial statistics, there was a growth of 70% to the targeted small and medium-sized enterprises (not including important state infrastructure such as hospitals, banks, etc.). The two most common types of attacks are ransomware and phishing attacks.

The open data statistics of the Ministry of Internal Affairs reports on (only) 51 cybercrimes registered for 2021. At the same time, in a March 2022 press release the Ministry of Internal Affairs reports a 3-4 times increase in the number of cybercrimes. The number of received signals in the GDCOC has increased by 30 to 50 times.

The state e-government authority reported that in September 2021 cyberattacks jumped twice compared to August – from 831,966 to 1,680,932. The main attacks in the last year have been fraud (40%) and malicious code (49.5%).

Online fraud can now be directly reported to the office of the Cybercrime Department within GDCOC. The unit receives approximately receives between 20 and 150 reports daily.

Should personal data be involved, complains can be submitted directly to the Commission for Personal Data Protection. In case of consumer protection cases, complaints can be submitted to the Bulgarian Commission for Consumer Protection.

Key Statistics:	
Population:	6.9 million
Internet:	67%
# of Scams:	31,000
Scams / 1,000 :	4,5
Money lost:	$ 26 million
Per capita:	$ 3.79
Per report:	$ 842

Key Organizations:

- GDCOC
- CERT.bg
- Bulgarian Cybercrime Association

WhoisXML API:	
Domains/capita	0,034
Domains registered	236,766
TLD registrations	95,352

Source: LIBRe Research Group

Online Scams through the DNS Lens

Interview with Jonathan Zhang, CEO and founder of WhoisXML API.

Which developments in the domain industry have you observed in the past year?

The demand for domain names and therefore the total number of registered domains has kept increasing, notably driven by sustained digital transformation even as the effects of the COVID-19 pandemic lessened. While a sizeable share of this surge can be attributed to legitimate online efforts, new angles for fraud, scams, and other unlawful operations never stop emerging. Another significant development is the number of top-level domains (TLDs) that continue to be launched, giving digital users and, unfortunately, scammers every time more room to pick the perfect domain names for their activities. The domain industry aims to proactively tackle the problem, as shown by the heightened awareness of DNS abuse and actions taken by legitimate domain owners and relevant parties.

How widespread is the problem of business scams and impersonation from your perspective?

We recently concluded a study on **Business Impersonation in the DNS** and found more than 49,000 cybersquatting domains and subdomains added over a 12-month period. Most of the properties in our sample appeared to potentially exist to imitate the legitimate online presence of Fortune 500 companies and their CEOs. Few digital properties, however, could be explicitly linked to the actual organizations or individuals. Moreover, many of them had already been flagged for figuring in fraudulent or malicious events.

Overall, every angle seems worth exploring by scammers and malicious actors, as the COVID-19 pandemic showed with suspicious vaccination- or medical equipment-related domain registrations. More recently, scammers have also taken advantage of worldwide conflicts or events like Mother's day or tax-filing deadlines through dubious web properties.

How can WhoisXML API help combat online fraud? What role does your company play?

Our company primarily delivers DNS and WHOIS intelligence via downloadable footprints and APIs. We help our clients fight fraud by aiding security teams and cybersecurity companies in real-time DNS-based threat contextualization. Law enforcement agents, threat hunters, and private investigators also work with us to find DNS cues, add context to lists of indicators of compromise (IoCs), and find new artifacts with hidden connections.

Jonathan Zhang
CEO and founder
WhoisXML API

In 2021, the CAFC received 104,295 fraud reports with a CA$379 million loss

Only 5% of Canadians file a fraud report with the CAFC when they are victims of scams

Online scams can be reported to the **Canadian Anti-Fraud Centre (CAFC),** managed by the Royal Canadian Mounted Police, the Competition Bureau Canada, and the different State Police forces.

The number of fraud reports CAFC received grew from 36,000 in 2019, 56,000 incidents in 2020, to 104,295 cases in 2021. The amount of money lost also increased, from CA$81.2 million lost in 2019, to CA$92.4 million in losses from 2020's to CA$379 million in 2021. In 2021, CAFC was able to recover CA$3.35 million.

Investment scams were one of the fastest growing types of online fraud, from 501 reports and 16.5 million lost in 2020 to 3,442 reports and 164 million. Identity theft cases nearly doubled from 16,970 to 30,849 reports. The same is true for the number of extortion reports. Finally, the number of reported Romance Scams grew with 114% while the amount lost grew with 249%.

The **Canadian Competition Bureau** is the driving force behind the **Fraud Prevention Forum,** a group of 60 private sector firms, consumer and volunteer groups, government agencies and law enforcement organizations, who are committed to fighting fraud aimed at consumers and businesses. Each March, the forum organizes a Fraud Prevention campaign. The organization also maintains the Little Black Book on Scams.

CIRA, the **Canadian Internet Registry Authority**, fights scams by offering a free DNS service to protect consumers from malware and phishing, a firewall solution for companies and cybersecurity awareness trainings for companies.

Fraud type	Reports 2021	Reports 2020	Reports Change	Loss 2021	Loss 2020	Loss Change
Loan	570	N/A	N/A	6,9	N/A	
Identity fraud	30849	16970	82%	N/A	N/A	
Extortion	30361	17390	75%	16,5	12,5	32%
Personal information	9666	6649	45%	N/A	N/A	
Phishing	6953	3672	89%	N/A	N/A	
Counterfeit merchandise	52	N/A	D	1,1	N/A	
Service	5106	2009	154%	11,6	8,5	36%
Merchandise	4994	3354	49%	12,3	8,7	41%
Victim vendor	4038	2320	74%	7,7	4,2	83%
Job	3796	2297	65%	9,4	2,6	262%
Investments	3442	501	587%	163,9	16,5	893%
Bank Investigator	2212	835	165%	4,6	3	53%
Romance	1928	899	114%	64,6	18,5	249%
Spear phishing	1817	1049	73%	54	14,4	275%

Key Statistics:

Population:	38 million
Internet:	89%
# of Scams:	104,295 (86%)
Scams / 1,000 :	2.7
Money lost:	$ 295 M (310%)
Per capita:	$ 7,73
Per report:	$ 2833

Key Organizations:

- Canadian Anti Fraud Centre (CAFC)
- Canadian Competition Bureau
- Canadian Internet Registry Authority

WhoisXML API:

Domains/capita	0,461
Domains registered	17,659,802
TLD registrations	3,789,518

https://www.antifraudcentre-centreantifraude.ca/features-vedette/2022/02/frauds-10-fraudes-eng.htm

China has started the “people’s war” against fraudsters

Bonus winning scams are the most experience form of scams (40.7%) followed by online shopping fraud (35.3%)

A nationwide anti-fraud education campaign was launched by the Chinese authorities in 2019, after president Xi Jinping announced in a conference that fighting fraud was a “top priority” when it came to making people feel secure.

The campaign culminated early this year with the launch of National Anti-Fraud Center, a mobile app that has been downloaded more than 500m times, making it one of the most popular in the world. The government uses a variety of channels, from street posters to TV commercials, to inform the public about what scams look like and how to avoid them.

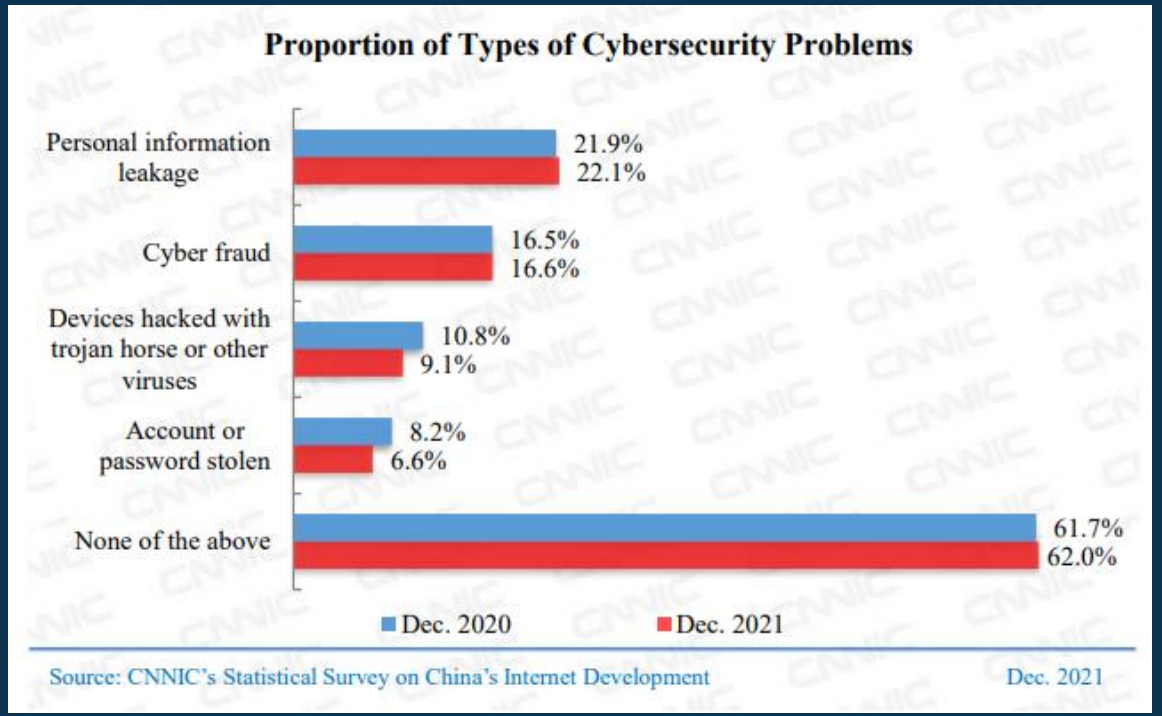
The **Ministry of Public Security (MPS)** prevents, investigates, and stops criminal activities in general, including online fraud. Chinese citizens can report scams online or call 110 to report the crime directly to the **Cyberpolice** which is part of the MPS.

Recently, MPS released the top 5 sources of online fraud:

- Brushing; sending small items victims never ordered, demanding payment
- False Investment; promising high rates of return with low risk
- Wealth Management; promising high rates of return with low risk
- Loan Schemes; dodgy and unclear payment terms
- Customer Service Impersonation; to collect rewards, accounts need to be set up against costs that will be returned with the reward

Chinese police in 2021 investigated and handled 62,000 cybercrime cases. A total of 103,000 individuals were captured. A total of 394,000 criminal cases involving telecom fraud have been investigated nationwide. The Cyberspace Administration of China has investigated and shut down 878,000 websites involved in fraudulent activities this year.

cnnic.com.cn/IDR/ReportDownloads/202104/P020210420557302172744.pdf
12377.cn/tzgg/2021/c93838d1_web.html



Key Statistics:

Population:	1,412 million
Internet:	70%
# of Scams:	2,1 million*
Scams / 1,000 :	1.5
Money lost:	$ 3,000 million*
Per capita:	$ 2.12
Per report:	$ 1,428

Key Organizations:

- Ministry of Public Security
- National Internet Information Office

WhoisXML API:

Domains/capita	0,182
Domains registered	25,778,606
TLD registrations	25,576,846

China is fighting scammers more, both nationally and internationally

Li-Xiong Chu, owner of Chu Consulting. Born in the Netherlands and living in China for over 10 years. Li helps companies interested in the Chinese market, providing a ‘soft landing’.

China is suffering from the ongoing dangers of COVID-related measures that limit people in their work and life, but it sees the e-commerce sector getting stronger. People are more hesitant about offline shopping nowadays and with the well-developed digital infrastructure, increasingly more time is being spent online and on mobile devices.

Of course, this means there are more opportunities and channels through which online fraud can happen. Since 2019, China has already tightened its data security laws, an equivalent to the GDPR in Europe. In 2021, the Cyberspace Administration of China – CAC, China’s internet watchdog, formulated many new laws and regulations in cybersecurity and data protection. These are also known as the QingLang Operation laws (清朗“系列专项行动). Under this operation, campaigns are launched to create a better internet environment. There is a special focus on targeting online fandom culture, unlawful internet account operations, and malicious internet sites targeting minors. This has already resulted in the closure of 2,160 illegal apps and mini-programs, the deletion of 1.34 billion illegal accounts, and the shutdown of over 3,200 illegal websites.

For the bigger e-commerce platforms, such as JD.com and Tmall, there will be mechanisms in place that provide protection against scammers and help dispute settlements. In addition, the government provides channels where complaints can be filed against businesses and provide assistance to resolve commercial disputes. For example, the Chinese Ministry of Commerce operates a complaint hotline in both Chinese and English, and the China Council for the Promotion of International Trade can help in resolving disputes.

Internationally, China has also been active in working together with other countries to fight cross-border scams. Recently, because of Interpol efforts between 76 countries, including China, a crackdown on social engineering scams and organizations have taken place. It was reported that $ 50 million worth of illegal funds were intercepted and over 2,000 arrests were made.

Li-Xiong Chu
CEO
Chu Consulting

Finns lost €33m to online scammers in 2021, up from €25m in 2021

A number of senior citizens and young adults, particularly students, have lost all their savings to online scams

Finnish consumers can report online scams to the **police**, both locally and online. Finland has a police cybercrime unit as well, which is part of the National Bureau of Investigation (NBI) which mainly focusses on cybercrime targeting companies. There is no specialized team for consumer related online fraud.

Consumers can also report scams to the **Finnish Competition and Consumer Authority** (KKV). KKV offers consumer advice both online and by phone. It also works with other organizations such as the **Finnish Financial Supervision Authority** for financial scams.

RIKU, the national victim support organization, offers free support and advice face-to-face and via phone, chat and online. The organization helps all kinds of victims and works intensively together with volunteers.

Victims have reportedly been targeted with a wide variety of online hoaxes, including romance scams. Other methods used by fraudsters to get people to part with their money include impersonating a relative or a government or police officer. Investment scams are also on the rise involving cryptocurrency. Likewise, the number of fraudulent text messages or emails claiming to be from a bank or national mail carrier Posti have increased. Finally, a high number of fake versions of existing websites were set-up to gain access to personal information.

25% of the scam victims are aged 70–79 age. 20% of the victims are between 60 and 70 year old. However, the number of scams targeting men and women aged 20 and above is growing rapidly as well. Especially students seem to be a targeted group.

Many Finnish young people, and even children, commit cybercrime every year. To address this trend, NBI has launched an early intervention project. This includes a hacking challenge to help young people develop IT skills in the right direction.

https://yle.fi/news/3-12191980

Interview: Leena-Kaisa Åberg - Executive Director, RIKU

RIKU helps all kinds of victims. In 2021, 5% of the cases were committed online. This includes all kinds of crime just as long as they happen online. This year, from January until the end of July, the percentage is the same. We do see a growth in the number of victims of online scams in our services but by percentage the growth is not so big.

Of course, one challenge is that the police does not have enough resources to investigate all online scams, especially minor frauds. And as we know, quite often the chance to get any lost money back from e.g. love or investment scams is so low that there isn't much the police can do with the current resources. So there are challenges here but as far as I understand, the police is putting more effort on developing their knowledge in cybercrime. More training is organized, etcetera.

It is also an ongoing challenge that many victims feel ashamed of being tricked by the perpetrators. We have developed special webpages for Investment scams and love scams to increase awareness.

Key Statistics:

Population:	5.5 million
Internet:	87%
# of Scams:	20,000 (6%)
Scams / 1,000 :	0.4
Money lost:	$ 33 (39%)
Per capita:	$ 6.06
Per report:	$ 1,680

Key Organizations:

- Finish Police - NBI
- RIKU (non-profit victim support)
- KKV (consumer authority)

WhoisXML API:

Domains/capita	0,159
Domains registered	753,036
TLD registrations	570,592

423,000 fraud cases were reported in France in 2021 (14% of all crimes)

61% of French people have been exposed to an alternative investment offer

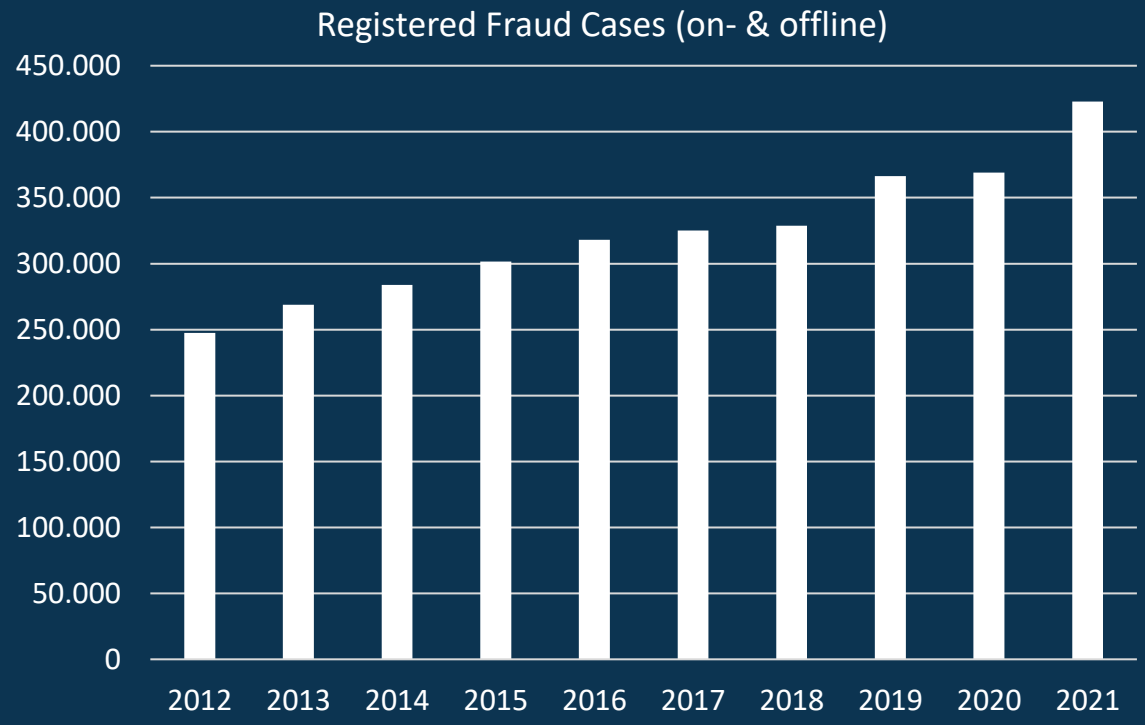
France has launched a new online platform for reporting internet scams. THESEE enables people to alert the authorities to crimes including romance scams, blackmail and ransomware without having to go to a police station.

Reports will be examined by Police Nationale and Gendarmerie investigation teams, who will contact the person if their complaint has been validated. A team of 17 police officers and gendarmes will then cross-check the statement with other reports they have received and launch an investigation if appropriate.

There are several other reporting sites as well. Internet Signalement (for illegal content), ACYMA (Actions Against Cybermalveillance), a public private partnership focused on awareness building and prevention of cybercrime in general. The Ministry of Economy and Finance also offers a portal to report all kinds of complaints, SignalConso. Signal Spam focusses on reporting and blocking spammers. Signal Arnaques is a private initiative exposing scam sites.

An interior ministry study from March 2022 called 'Cadre de vie et sécurité' (Living environment and security) suggested that only a quarter of scam victims report scams to the police, and only 17% make an official statement.

The Gendarmerie Nationale Cyberspace Command (COMCYBERGEND) has been fully operational since August 2021 and has brought together all the Gendarmerie's specialized units. It has 11 local branches, and it coordinates a network of 7,000 specialized officers from local correspondents who are trained to carry out simple cybercrime investigations, to departmental, regional and national expert investigators. This new organization aims at streamlining the cybercrime fighting activities.



Key Statistics:

Population:	67 million
Internet:	88%
# of Scams:	423,000 (816%)
Scams / 1,000 :	6,27
Money lost:	$ 1,484 million*
Per capita:	$ 22.99
Per report:	$ 3.508

Key Organizations:

- French Police
- ACYMA (public private partnership)

WhoisXML API:

Domains/capita	0.114
Domains registered	7,710,860
TLD registrations	5,479,805

cybermalveillance.gouv.fr/tous-nos-contenus/actualites/rapport-activite-2021
connexionfrance.com/article/French-news/France-launches-new-online-platform-for-reporting-internet-scams

* ScamAdviser Estimate

In 2021, 383,469 Internet related crimes were reported, up 19.7%

65% was online fraud related. In total, €223.5 billion was lost in cybercrime.

According to the German Constitution, police jurisdiction lies with the federal states. Germans can report online crimes to the police authority of their state. Most states offer an **Internet Wache** (Internet Watch) service. In addition, consumers can also turn to the **Verbraucherszentrale**, the consumer protection centers. The Verbraucherzentrale are likewise mainly organized at the state level with some of them supporting online reporting.

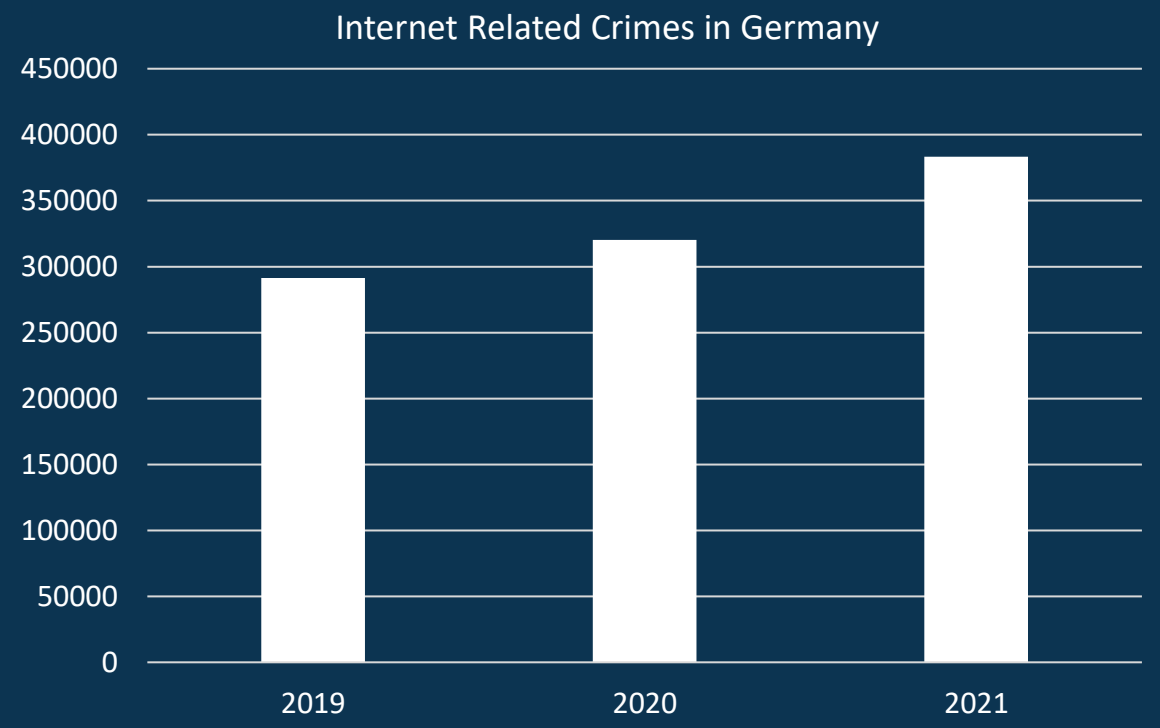
The **Bundeskriminalamt (BKA)'s** main goal is to coordinate crime suppression. Within the BKA the Serious and Organized Crime (SO) subdivision Cybercrime (SO-4) conducts investigations, coordinates (inter)national activities, and analyzes cybercrime trends and focusses mainly on "big" cybercrimes. BKA - SO4 also coordinates the **Zentrale Ansprechstelle Cybercrime** (ZAC). Each state has its own ZAC.

The **German Federal Office for Information Security** also advises and counsels consumers on digital risks and recommendations.

The joint police forces offer a website to prevent crime called **Polizei Beratung**. The website also provides general statistics on cybercrime (see graph) 59% of the reported cases were solved. Of the criminals identified 70% were male.

Verbraucherschutz.com is a popular private initiative that allows consumers to report scams and warns consumers about new kinds of scams.

25% of all Germans has been a cybercrime victim in one way or another in 2021. For young people (19 – 29y) this is a third. Most common cybercrimes were online account break-in (9%), smishing (7%), online shopping fraud (6%) and phishing (5%).



Key Statistics:	
Population:	83 million
Internet:	94%
# of Scams:	249,254 (20%)
Scams / 1,000 :	3
Money lost:	$ 3.7 billion*
Per capita:	$ 44,63
Per report:	$ 14,884

Key Organizations:

- Bundeskriminalamt - SO-4
- Central Contact Cybercrime (ZAC)
- Verbraucherschutz.com

WhoisXML API:	
Domains/capita	0,081
Domains registered	6,751,398
TLD registrations	23,030,607

https://www.polizei-beratung.de/fileadmin/Dokumente/Digitalbarometer-2021.pdf
https://www.polizei-beratung.de/fileadmin/Dokumente/infotext-tatmittel-internet-p.pdf
https://www.bka.de/SharedDocs/Downloads/DE/Publikationen/JahresberichteUndLagebilder/Cybercrime/cybercrimeBundeslagebild2021.html?nn=28110

* ScamAdviser Estimate

We need artificial intelligence to fight online store hackers

Joachim Feist is CEO of mindUp Web + Intelligence and researching solutions in the interdisciplinary research project INSPECTION

What can you tell about Project INSPECTION?
The research project INSPECTION finds hacked web pages whose resources are being misused to redirect users into fake online shops.

What advantage do these website hackers hope to gain?
By hacking existing domains, the fraudster takes advantage of the reach that has grown over the years, the good search engine ranking, and the positive reputation of the hacked site. Even if there is no thematic match between the fake store and the so-called hacked host site, the attacker can place ten thousand thematic pages of his fake store in the search engine index overnight, generating a high number of web visits.

Which websites are particularly often the target of such attacks?
Very small website operators are often targeted. The victims are therefore mainly associations, freelancers or self-employed people, for example from the craft sector. But also private individuals. Security gaps often exist because the operators see their websites as a one-off investment, they do not keep the site secured.

Why can fake stores become so widespread on the Internet?
The hackers know: The risk of prosecution is low. In most cases, the servers used for the crimes are located outside of Germany and Europe, making it difficult to identify and apprehend the criminals in this country. Our attempts to refer fake stores to law enforcement agencies, Internet registrars, or consumer protection for closure in order to stop them have also failed. Our current legal regulations can do little against cybercriminals operating internationally. Moreover, it is difficult to adequately inform operators of an attack that has taken place, because an e-mail of a hacked site is usually not read. Even if you can contact the site owner, in most cases, those affected cannot act quickly enough due to a lack of IT expertise.

How will INSPECTION help in the future?
The focus of our idea is, on the one hand, the detection of hacked sites and, on the other hand, the targeted, largely automated and early warning of the operators of the hacked sites. After all, mere detection remains useless if there are no measures to remedy the problem.

Joachim Feist
CEO
mindUp Web + Intelligence

Momo Fraud (mobile money) is Ghana's biggest type of scam

45% of all cybercrime cases are related to fraud

In Ghana, scams are widespread. Both nationals and foreigners fall victim to various forms of scams. These can be 'love scams' in which seemingly attractive ladies contact men via online channels such as social media, e-mail or Skype with the intention to establish a romantic relationship. In reality the 'ladies' are often men who manage several relationships at one time based on different identities with the aim of enriching themselves through funds they are able to talk their victims into transfer to them. Business proposals that look too good to be true are another type of scam.

The Cyber Security Authority (CSA) has been established by the Cybersecurity Act, 2020 (Act 1038) to regulate cybersecurity activities in the country and to promote the development of cybersecurity in the country. Both foreigners as well as citizens from Ghana can report scams to the National Cyber Security Centre of Ghana in several ways (see visual on the right).

The Cybercrime Unit of the Criminal Investigations Department (CID), Ghana Police Service, says cyber fraud makes up 45 per cent of all cybercrime cases. In money lost, cyber fraud is the second highest after crimes such as online hacking and stealing. In 2020, $19.8 million was lost to cyber fraud. In 2019, this amount was $11 million.

The Bank of Ghana reports a decline of 12.09% in the number of attempted fraud cases of 2,347 for the Banking and SDI sector as compared to 2,670 in 2020. However, the year 2021 recorded a loss value of GH¢61million as compared to a loss of GH¢25 million in 2020, representing a 144% increase in year-on-year terms.

The Ghana Chamber of Telecommunications blacklisted 28,000 SIMs. Ghanaians can report scams by calling or texting 419. A total 35,000 reports were received last year.

Key Statistics:

Population:	31.7 million
Internet:	54%
# of Scams:	35,000
Scams / 1,000 :	1,10
Money lost:	$ 25 million*
Per capita:	$ 0,79
Per report:	$ 714

Key Organizations:

- Cyber Security Authority (CSA)
- Cybercrime Unit Ghana Police

WhoisXML API:

Domains/capita	0.002
Domains registered	48,132
TLD registrations	4,518

https://ghana.um.dk/en/about-us/about-ghana/report-scams-and-cybercrime

https://www.ghanaweb.com/GhanaHomePage/business/Total-loss-in-value-of-MoMo-fraud-reached-GH-12-8-million-in-2021-Report-1572518

* ScamAdviser Estimate

Mobile Fraud Awareness Campaign by the Ghana Chamber of Telecommunications

commsrisk.com/ghanas-telcos-collectively-block-28000-sims-in-common-bid-to-stop-mobile-money-fraud

India reported more cyber crimes in the first 2 months of 2022 than 2018

The (local) governments are acting by speeding up the investigation process and freezing of accounts

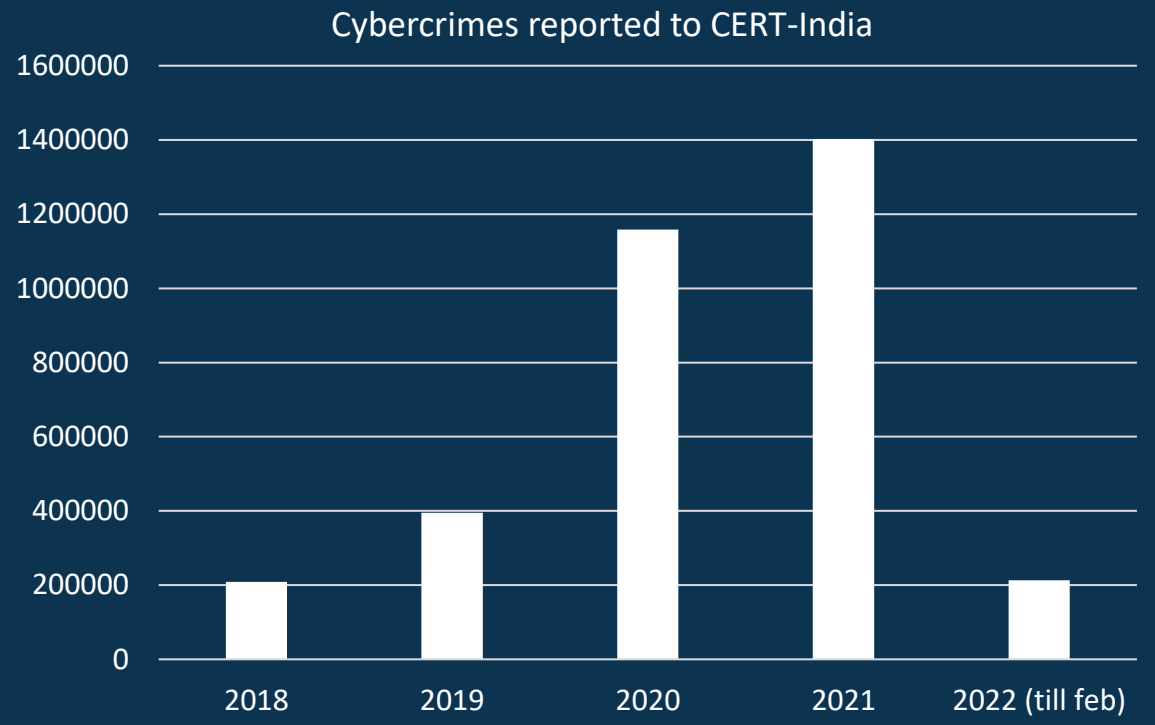
The first two months of 2022 reported more cyber crimes than the entire 2018, according to data by **CERT-In** (Indian Computer Emergency Response Team). CERT-In is the nodal agency to deal with cyber security threats and operates under the information technology ministry.

Cyber crime cases have witnessed a steady spike since 2018. India reported 208,456 incidents in 2018; 394,499 incidents in 2019; 1,158,208 cases in 2020; 1,402,809 cases in 2021; and 212,485 incidents in the first two months of 2022. The above figures show that cyber crimes increased almost seven times in three years between 2018 and 2021, and more sharply during the pandemic.

The **National Cybercrime Reporting Portal** is an initiative of the Ministry of Home Affairs launched to facilitate victims/complainants to report cybercrime complaints. The National Crime Records Bureau (NCRB), presents a different set of data. According to NCRB, India reported 50,035 cyber crimes in 2020; 44,546 cases in 2019 and 27,248 cases in 2018. Online fraud made up 60% of the reported cases. This was followed by sexual exploitation (6.6%) and extortion 4.9%.

To fight cybercrime (local) governments are speeding up the investigation process. In Bangaluru, only 1 in 8 cases is solved. Victims can now call 112 and register a scam. Action is then undertaken within 90 minutes to freeze the money in the bank account of the suspect.

Likewise, Reserve Bank of India (RBI) has issued instructions to banks to report all unusual cyber incidents to RBI within 2 – 6 hours of occurrence. These incidents are analyzed for the pattern of attack and the vulnerabilities exploited, and where needed, alerts are issued so as to avoid repeat attacks/exploitation of the same vulnerabilities



Key Statistics:

Population:	1,393 million
Internet:	54%
# of Scams:	120 mil.*
Scams / 1,000 :	87
Money lost:	$ 16 bil.*
Per capita:	€ 15.42
Per report:	€ 177.29

Key Organizations:

- National Cyber Crime Report Portal
- CERT India

WhoisXML API:

Domains/capita	0.003
Domains registered	4,686,957
TLD registrations	3,343,975

zeenews.india.com/technology/two-months-of-2022-saw-more-cyber-crimes-than-entire-2018-why-e-fraud-is-a-ticking-time-bomb-2458733.html

* ScamAdviser Estimate

In Indonesia, online fraud is the second largest kind of crime

Approximately 25% of all Indonesians become victim of online fraud

In Indonesia, online fraud makes up the second largest category of cases filed in police reports. It contributes to more than a quarter of all cybercrime cases, according to data from the National Police's Criminal Investigation Agency.

The National Cyber and Crypto Agency (BSSN) noted that in 2021 there will be more than 90,000 criminal acts in the Indonesian Internet world. In addition, the 2021 cyber security monitoring report issued by BSSN also detected 1.6 billion suspicious attempts to infect cyber security systems or internet traffic anomalies in Indonesia. That number has tripled compared to 2020.

Especially investment scams are a concern. The number of consumers investing has tripled since 2019. More than 3,000 online trading and investment platforms have been shut down as scams.

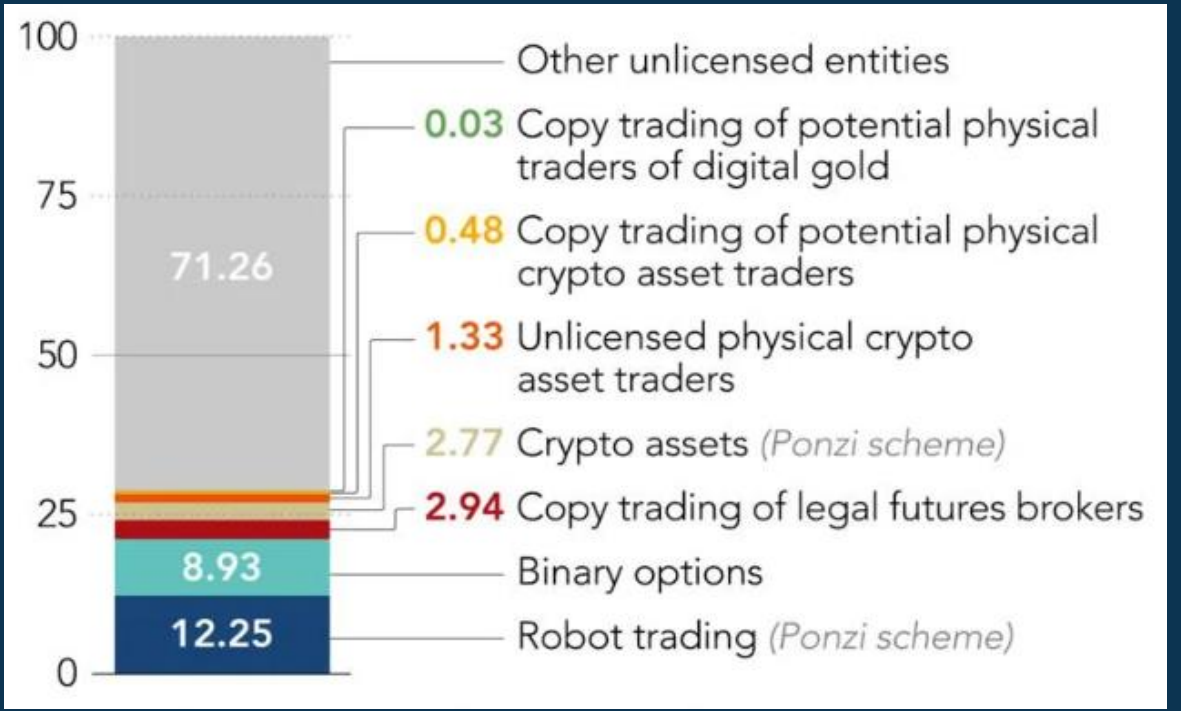
Several studies by Kaspersky and Experian state that 25% of the consumers have fallen for scams. Most of these scams (51%) happen on social media.

Indonesians are directed to several organizations to report online scams. For suspicious investment schemes, the Enforcement and Investor Protection Department of the SEC can be contacted via phone and email.

For malicious messages, reports can be lodged to the **National Bureau of Investigation (NBI) Anti-Fraud Division** online, via email, phone and Facebook. The NBI is investing heavily in both equipment as well as staff, hiring 200 additional cybercops in 2021 alone.

Citizens can also report incidents to the **PNP Anti-CyberCrime Group** online and via phone.

The Department of Finance has also opened its online channels for netizens to report any posts, advertisements, and messages containing false information.



Blocked trading platforms in Indonesia by type, 2923 sites, 2020 – July 2022
Source: Indonesia's Commodity Futures Trading Regulatory Agency.

Key Statistics:

Population:	276 million
Internet:	77%
# of Scams:	-
Scams / 1,000 :	-
Money lost:	-
Per capita:	-
Per report:	-

Key Organizations:

- National Cyber and Crypto Agency
- NBI Anti-Fraud Division
- PNP Anti-Cybercrime Group

WhoisXML API:

Domains/capita	0.003
Domains registered	886,915
TLD registrations	787,131

business.inquirer.net/338991/p2b-feared-lost-to-scams-fraud-bsp
interpol.int/content/download/16106/file/ASEAN%20Cyberthreat%20Assessment%202021%20-%20final.pdf
asia.nikkei.com/Spotlight/Market-Spotlight/Indonesia-s-rising-appetite-for-online-investment-attracts-scams

Iran is cracking down on crypto and betting sites

The Iranian central bank had identified 450,000 bank cards used on illegal gambling and betting websites

The **Cyber Police of the Islamic Republic of Iran** was established in 2011 in order to prevent, investigate and combat cybercrime. It is part of the **FATA police force** of Iran.

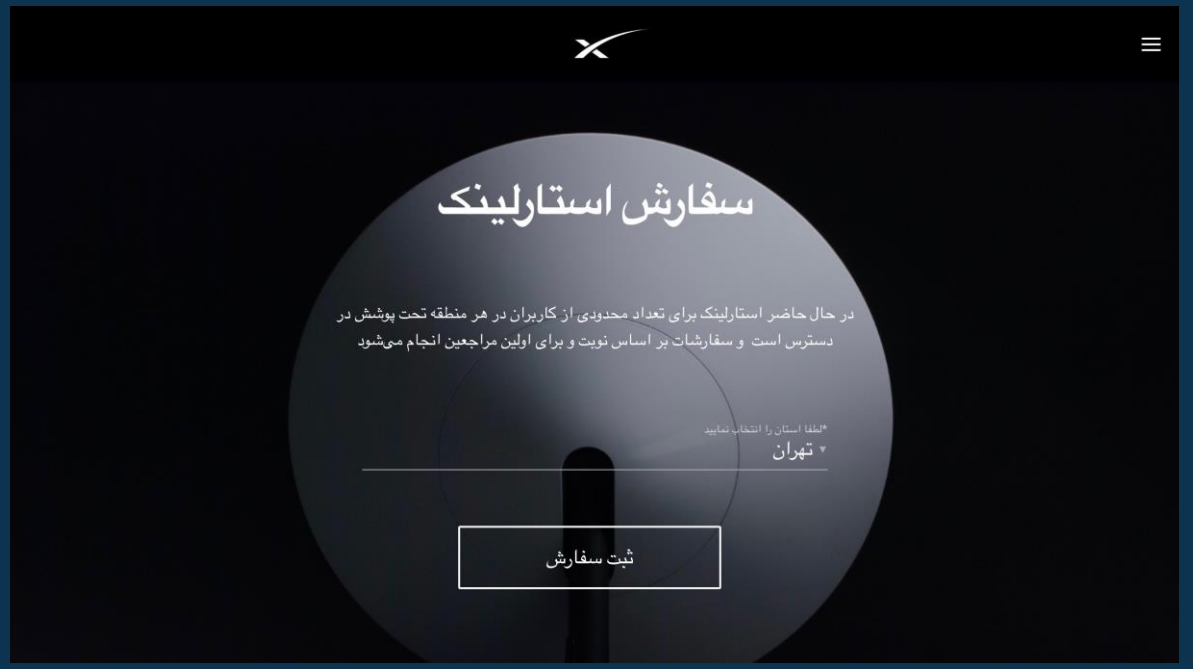
The **Cyber Police** has several duties. It monitors and coordinates actions to protect the religious and national identity or Iran. It also takes preventive and active measures to ensure that the values and norms of Iranian society are enforced. In addition, the police unit fights cybercrime, including foreign attacks on its Information infrastructure. Thirdly, it focuses on protecting consumers from online (credit) fraud, phishing and privacy breaches.

Consumers can report digital crimes both through **cyberpolice.ir** (only accessible from an IP address within Iran) which is maintained by the Cyber Police unit, as well as on the general website of FATA police.

There is a separate court to handle cybercrimes. Cyberfraud can be punished by up to 3 years in prison and confiscation of property.

Iran's, like many other countries has been plagued by generic phishing attacks and email breaches. There are however an increasing number of scams targeted at Iranians specifically, for example, immigration scams.

Many Iranians try to immigrate to Europe and are being offered "help" by "travel agencies" to get a Schengen visa and travel to Europe. Victims are lured to pay amounts up to $ 40,000 to get visa for their families. Contacts are mainly established via Telegram and payments made in cash to local money mules. The journeys are often "cancelled" several times and more money has to be paid until the victim runs out of money or realizes he is being scammed.



Another scam was a look-alike Starlink website, targeted Iranians with claims you can place an order for the beta version of its internet service.

Key Statistics:

Population:	85 million
Internet:	80%
# of Scams:	-
Scams / 1,000 :	-
Money lost:	-
Per capita:	-
Per report:	-

Key Organizations:

- Cyber Police
- FATA Police

WhoisXML API:

Domains/capita	0.004
Domains registered	381,795
TLD registrations	1,290,484

mehrnews.com/news/5270305/
agsiw.org/rising-crime-and-insecurity-in-iran/

In Ireland, online fraud increased with 116% in 2021

The amount of money lost increased with 5%

The **Garda Síochána** facilitates the online reporting of crimes for amounts less than €1,000. Citizens can also visit a local police station or call a specific number. In general, the Garda Síochána encourages victims to personally report crime.

The majority of online fraud in Ireland is investigated by either local Police Units or the **Garda National Economic Crime Bureau** (GNECB), which focuses on the more complicated, international and organized crime cases. The GNECB provides support and expertise to local investigators and trains 50 new Detectives each year in fraud-investigation, in conjunction with University College Dublin (UCD). Staff is seconded to Office of the Director of Corporate Enforcement (ODCE), the Department of Social Protection (DSP), and the Office of the Competition and Consumer Protection Commission (CCPC). The GNECB also operates Ireland Financial Intelligence Unit (FIU).

The **Garda National Cyber Crime Bureau** is the national Garda unit tasked with digital forensic examination and investigations into digital criminal offences. Where the GCECB takes on larger cases of online fraud, the GNCCB, which was reinstated in 2017, focuses on cybercrimes like DDOS attacks and ransomware.

The number of crime incidents recorded on An Garda Síochána's PULSE database which were classified as Fraud, deception and related offences increased by 116.1% or 9,095 to 16,929 in the year 2021. The increase is largely driven by unauthorized transactions and attempts to obtain personal or banking information online or by phone.

FraudSMART is a fraud awareness initiative developed by the Banking & Payments Federation Ireland (BPFI). The Initiative aims to raise consumer and business awareness of the latest financial fraud activity and trends.

Incident Type	2020	2021	2022*	Total
Accommodation Fraud	€349,674	€490,172	€238,637	€1,078,483
Account Take Over Fraud	€3,708,364	€16,875,536	€4,962,112	€25,546,012
Bogus Tradesman Fraud	€311,910	€380,265	€341,188	€1,033,363
Business E-Mail Compromise	€10,356,290	€5,678,684	€6,411,312	€22,446,286
Card Not Present Fraud	€453,640	€2,415,658	€776,518	€3,645,816
Deception/Other	€13,730,144	€15,787,451	€6,823,831	€36,341,426
Investment Fraud	€7,838,516	€13,027,558	€4,942,576	€25,808,650
Phishing/Vishing/Smishing Frauds	€372,041	€806,986	€289,086	€1,468,113
Romance Fraud	€1,647,685	€1,561,114	€1,048,441	€4,257,239
Shopping/Online Auction Fraud	€1,452,424	€1,090,940	€403,161	€2,946,525
Grand Total	€40,220,688	€58,114,364	€26,236,862	€124,571,913

* Incidents reported between January and June 30th

Key Statistics:

Population:	5 million
Internet:	98%
# of Scams:	16,929 (116%)
Scams / 1,000 :	3.37
Money lost:	$ 26.8 million
Per capita:	$ 5,34
Per report:	$ 1,587

Key Organizations:

- Garda Síochána
- FraudSmart

WhoisXML API:

Domains/capita	0.075
Domains registered	379,096
TLD registrations	385,119

Source: Garda Síochána
cso.ie/en/releasesandpublications/ep/p-rc/recordedcrimeq42021/

Other Victim and Offender Statistics from Ireland (2020 – H1 2022)

Average age of victims per incident type

Incident Type	Female	Male	All Victims
Accommodation Fraud	30	31	30
Account Take Over Fraud	44	44	44
Bogus Tradesman Fraud	62	60	61
Business E-Mail Compromise	56	49	52
Investment Fraud	47	50	49
Money Laundering	38	37	37
Phishing/Vishing/Smishing Frauds	45	45	45
Romance Fraud	49	48	48
Shopping/Online Auction Fraud	37	39	38

Victim Age and Sex Breakdown

Victim Breakdown	%Female	%Male
Accommodation Fraud	59%	41%
Account Take Over Fraud	53%	47%
Bogus Tradesman Fraud	54%	46%
Business E-Mail Compromise	36%	64%
Investment Fraud	36%	64%
Money Laundering	42%	58%
Phishing/Vishing/Smishing Frauds	56%	44%
Romance Fraud	74%	26%
Shopping/Online Auction Fraud	40%	60%

Average age / sex of the Money Laundering offenders

Offender Breakdown	Female	Male	Grand Total
Money Laundering	20%	80%	
0-17	3%	14%	17%
18-34	10%	45%	55%
35-54	6%	19%	24%
55+	1%	3%	3%

Offenders are mostly male and there is a high proportion of juveniles (17%) making up the total. The average of an offender was 29.

The total amounts per year of money laundered

Incident Type	2020	2021	2022*	Total
Money Laundering	€4,503,965	€3,413,461	€422,732	€8,340,158

*** Incidents reported between January and June 30th**

Source: Garda Síochána

Cyberattacks directed towards Israel grew 92% from 2020 to 2021

Israel is often in the top countries regarding receiving phishing emails, malware and cyberattacks

Israeli citizens can report online crimes to all kinds of organizations including Israel's CERT team via the 119 hotline.

Cybercrime in Israel is mostly dealt with by 4 main units.

- Israël **Police National Cyber Crime Unit** (Lahav 433) investigates criminal offences.
- The **National Cyber Bureau** at the Prime Minister's Office is responsible for all aspects of cyber defense in the civilian sphere, from formulating policy and building technological power to operational defense in cyberspace. Part of the bureau is Israel's CERT team for Cyber incident handling.
- The **Cybercrime Department in the Israeli State Attorney's Office**, set-up in 2015, prosecutes cyber offences.
- The Israeli **Privacy Protection Agency** investigates database-related offences.

Only 9% of victims of cyber crimes in Israel report them to the police. In 2019 according to the Central Statistical Bureau Israel's Crime Victimization Survey 225,500 citizens experienced cybercrime. In 2020, this number was reduced to 210,600.

In Israel, Check Point noted a 103% increase in phishing emails between November and October, with 56% of the emails containing fake messages related to shipments by Amazon, 36% by DHL and 18% by Fedex.

Israel also made the news in being the basis for several online scams. In October 2021, Israeli police participated in the apprehension of several scam investment networks. 10 different law enforcement actions were executed in 6 different countries. Likewise, "The Tinder Swindler," documentary on Netflix gained a lot of attention where Hayut, under the alias Simon Leviev, masqueraded as the son of Russian-Israeli diamond dealer Lev Leviev as he wined and dined women, proclaiming his love before convincing them to give him money that he said he needed to escape his "enemies."

Key Statistics:	
Population:	9.4 million
Internet:	7%
# of Scams:	210,600 (-7%)
Scams / 1,000 :	22.43
Money lost:	-
Per capita:	-
Per report:	-

Key Organizations:

- National Cybercrime Unit
- National Cyber Bureau
- Cybercrime State Attorney's Office

WhoisXML API:	
Domains/capita	0.053
Domains registered	503,977
TLD registrations	75,921

cbs.gov.il, timesofisrael.com/october-surprise-whos-who-in-the-unprecedented-wave-of-investment-scam-raids/
gov.il/BlobFolder/generalpage/prkfiles2/he/13-12-21%20report.pdf

66% of all reported fraud in Italy is now being done via the Internet

The worst-hit age group were individuals between 18 and 30 years old (23.3%), who were scammed 8% more compared to 2020

On June 15 2021, Italy enacted Decree-Law No. 82 of 2021 defining a national cybersecurity architecture and establishing a National Cybersecurity Agency. It's main goal is to improve the cybersecurity and digital capabilities of Italy in cooperation with the national and European industrial, research and academic stakeholders.

On the operational side, consumers can report scams to the Post and Communication Police, both online as well as locally. Online crime reports are passed along to one of the 20 regional police offices. The Post and Communication Police consists of 2,000 police officers who specialize in IT spread across its regional offices.

Within the Post and Communication Police a special **Cyber Crime Analysis Unit** has been set up in close cooperation with Italian Universities to study computer crimes.

The State Police has largely delegated online crime to the Post and Communication Police. The State Police does, however, support campaigns to warn Italian citizens about online fraud. One of the programs is called **Una Vita da Social which includes a bus traveling across Italy** to raise awareness among young people on the risks and dangers associated with the use of the Internet.

Altroconsumo is the largest independent consumer organization with 700,000 members. The organization offers an "Easy Claim" service to help get money back.

Between August 2020 and July 2021, 155,242 fraud cases were reported, a growth of 16%. 66% of these were online. In 2021 in Italy there were more than 28,600 cases of credit card frauds, a growth of 31%, for an estimated amount lost of over € 124.6 million. Of the reported victims hit by online frauds, 63.5% are males and 36.5% are females. The worst-hit age group were individuals between 18 and 30 years old (23.3%), who were scammed 8% more compared to 2020.

Source: Group-IB, FlashStart
interno.gov.it/sites/default/files/2021-08/dossier_viminale_2021_14.08.2021.pdf

Key Statistics:	
Population:	59 million
Internet:	86%
# of Scams:	102,459 (16%)
Scams / 1,000 :	2,2
Money lost:	€ 476,5 million*
Per capita:	€ 8,07
Per report:	€ 3,636

Key Organizations:

- Post and Communication Police
- State Police
- National Cybersecurity A

WhoisXML API:	
Domains/capita	0.050
Domains registered	3,824,194
TLD registrations	4,004,149

* ScamAdviser Expert Estimate

Cybercriminals are professionalizing at a terrifying rate

Interview with Dmitry Tunkin, Head of Digital Risk Protection, Group-IB

Group-IB is active in several regions around the world. Which trends do you see in different areas?

Throughout 2022 we see continuous growth of the already known trends; however, their expansion and “operational” improvements are terrifying. Ransomware and phishing are still the two in the top, followed by online scams.

However, online scam is a broad definition, and in particular we see a significant spike in investment scams with involvement of the human factor - creation of dedicated online investment platforms on behalf of global brands (most of them are not even operating in the financial sphere), with professionals luring victims by well-set digital marketing campaigns for first contact, and “closing” the new victims a.k.a “customers” with local-speaking professional call-centers.

In this scenario, victims will be forced to make a direct transaction from their personal banking account to a fraudster’s one. Which makes the scheme extremely tough for detection and elimination, as nothing looks suspicious from first sight. The scheme is operable in various regions across the globe by several fraud groups.

Your company collaborates with several law enforcement agencies and financial institutions. How can governments fight scammers better in your opinion?

Generally, the same cooperation is needed, as it happens to hackers and other villains. However, it would be essential to work on a global classification of scams, to develop the same practice or institution for fighting-with-phishing strategy. Unfortunately, nowadays we see it’s not so easy to take down a fraudulent page in comparison to a phishing one. So, both - governmental efforts in improving local laws and self-organization of different third parties (i.e. ISPs, hosting providers, domain name registrars, etc.) raised by themselves or on the platforms, organized by law-enforcement agencies - would be a game changer. As a private agency, we see that cooperation of business, law-enforcement and different regulators brings strong value, and are always ready to collaborate.

What will Group-IB focus on the next year? What do you hope to achieve?

On a global scale, our plans and actions as always will be aimed at proactive researching of uprising attacks, risks, tools, villains and putting all possible efforts to protect our customers and make the world a safer place.

Dmitry Tunkin
Head of Digital Risk Protection
Group IB

In 2021, Japan decided to launch a National Cybercrime Investigation unit

As online fraud cases and phishing continue to rise especially victimizing elderly people for huge sums of money

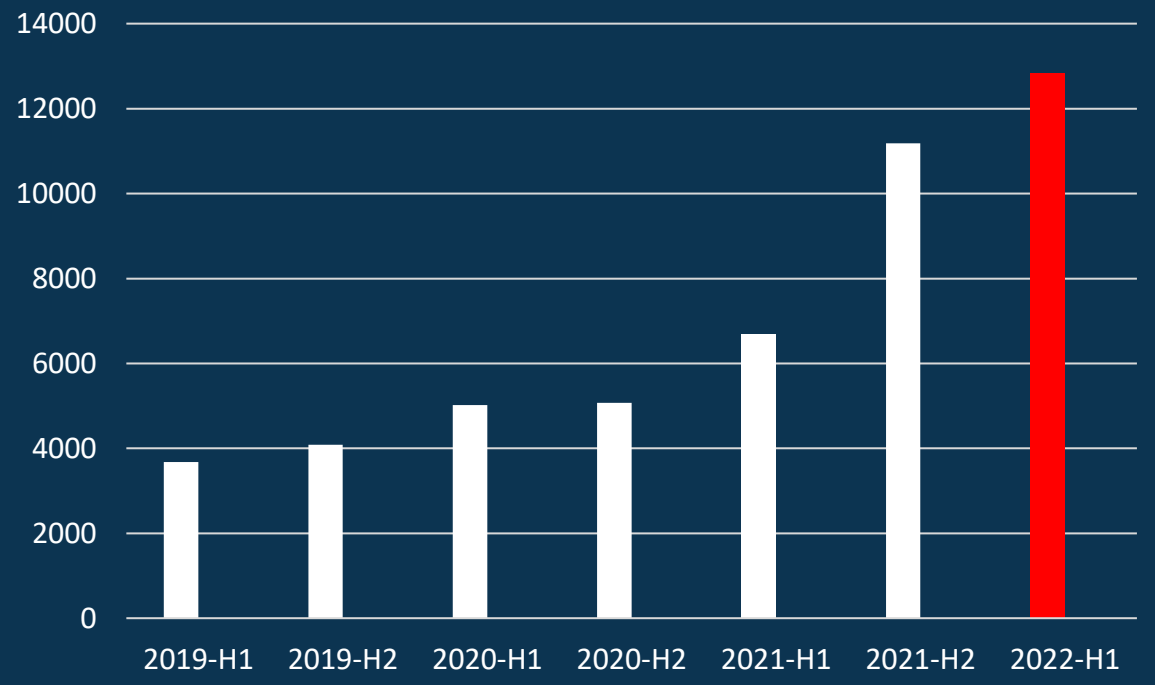
In 2021, Japan decided to launch a National Cybercrime Investigation Unit as part of the **National Police Agency (NPA)**. The new unit integrates the different cyber-related departments. Granting investigative authority to the NPA, a state institution, will mark a major turning point in Japan's police history as prefectural police have overseen investigating crimes since the end of World War II. For now, consumers are encouraged to report scams to the local police station.

The NPA received 14,461 phone/online fraud cases, an increase of 7.7%. Financial losses were **27.8 billion yen**, 2,5% less than in 2020. Especially, elderly loss a lot of money. Most common are “refund frauds,” which is an attempt to defraud people by claiming that they will be reimbursed for medical bills or insurance premiums (4,001 cases), followed by 3,077 cases of ore ore sagi (it’s me, it’s me scams), in which fraudsters impersonated family members and 2,587 “cash card scams”.

Next to the police, there are several other institutions collecting data on online fraud and phishing as well. The **Safer Internet Association (SIA**) gathers data about malicious e-commerce website from consumers. The data is shared with the **Japan Cybercrime Control Center (JC3)** for further analysis and action. SIA and JC3 report **17,878 malicious sites** in 2021. For H1 2022 the number already stands at 12,830.

JPCERT/CC received 44,242 incident reports in 2021 and of that **23,104** were related to phishing sites (others being malware, hacking, etcetera).

According to the Council of Anti-Phishing Japan, approximately **526,500** such scams were reported in 2021. The Japan Consumer Credit Association says damage caused by credit card fraud across Japan reached a record high of over **33 billion yen** in 2021. More than 90% of these victims were scammed due to their credit card numbers being stolen.



Number of reports of malicious shopping sites reported by SIA/JC3

Key Statistics:

Population:	126 million
Internet:	93%
# of Scams:	581,943
Scams / 1,000 :	4,63
Money lost:	$ 449 million
Per capita:	$ 8,07
Per report:	$ 771

Key Organizations:

- Japan National Police Agency
- JC3 / SIA
- Anti-Phishing Japan

WhoisXML API:

Domains/capita	0.051
Domains registered	6,347,506
TLD registrations	2,163,319

Source: Japan Cybercrime Control Center (JC3), Safer Internet Association

Kenyans lost $120 million in crypto scams in 2021

Kenya is losing more to scams compared to its GDP than any other country in the world.

Online scams can be reported to the **Kenya local and national Police**. Action from the police is usually slow and inconsistent. The process of reporting must be done physically rather than digitally. As a result, few consumers report scams.

Kenyan police, through its Directorate of Criminal Investigation opened a new lab for fighting crime. The government, through the various agencies, are providing information on how to fight scams.

The principal aim of the **Digital Forensic Laboratory** (DFL) is to identify, seize, acquire and analyze all electronic devices related to cyber-enabled offences reported in order to collect digital evidence which can be presented in a court of law.

The **national KE-CERT** was set-up by the Communications Authority of Kenya. It's focus is on the "bigger" cybersecurity threats although it does accept online fraud related incidents as well.

There is little data available on cybercrime in Kenya. Ponzi schemes and crypto currency scams are some of the most common scams. Kenya's ICT Cabinet secretary Joe Mucheru recently stated that Kenyans lose up to $120 million annually (equivalent to 13 billion Kenian Shilling) to online scammers.

A recent survey shows that nearly half of mobile users lost money to fraudsters. Through the popular mobile money transfer, M-pesa, 47.4% of users said to have fallen victim to different types of scams. This is an increase of 8.4% compared to 2019.

Overall, the most common types of scams in Kenya are Investment scams, cryptocurrency scams, mobile money transfer (M-pesa) scams, fake online stores among others. Most phone frauds are 'relative in distress' scams, followed by 'false money reversal request' scams.

Key Statistics:

Population:	55 million
Internet:	96%
# of Scams:	-
Scams / 1,000 :	-
Money lost:	$ 120 million
Per capita:	$ 2.18
Per report:	-

Key Organizations:

- Kenya National Police
- Kenya Police Service
- KE-CERT

WhoisXML API:

Domains/capita	0,003
Domains registered	165,679
TLD registrations	170,096

https://kenyanwallstreet.com/crypto-scams-how-to-spot-and-avoid-them/

* ScamAdviser Expert Estimate

Scammers used a Malaysian minister's phone to dupe victims

Minister Wan Junaidi's Telegram account was misused, one of his contacts had already transferred RM5,000 to the scammer

According to CyberSecurity Malaysia, during the COVID-19 outbreak, online scams have dramatically increased in Malaysia over the past two years. From 2020 to May 2022, 71,833 frauds totaling more than RM5.2 billion in damages were reported. Online scams made up 48,850 of the total number of frauds, or 68%, and 26,213 of those instances were brought to court. 9,569 incidences of e-commerce fraud were reported in 2019 compared to 5,851 cases in 2020. 3,833 cases were reported up to May of 2022. The other scams include loans and investments fraud (350 cases), job scams, and other frauds (11,875 cases).

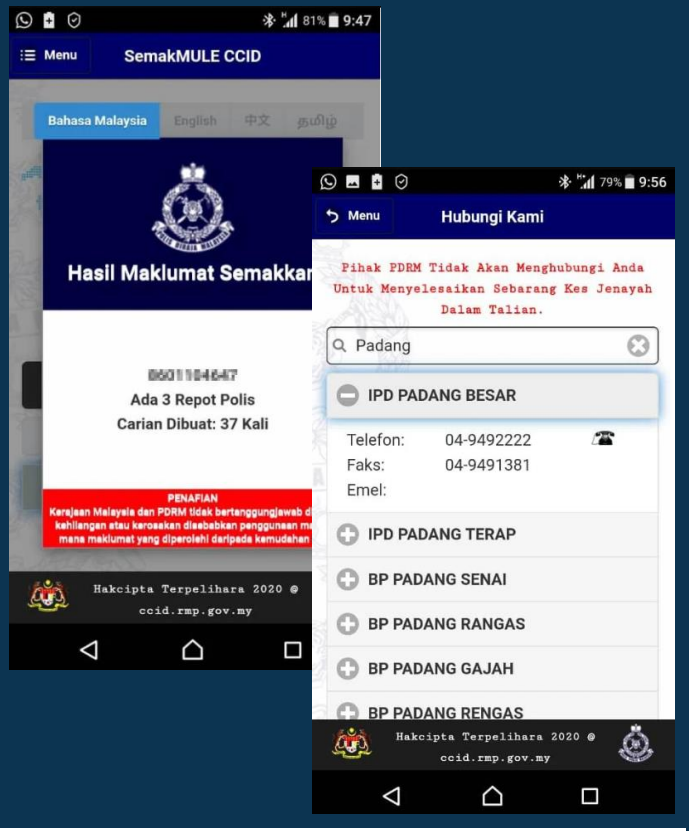
The Domestic Trade and **Consumer Affairs Ministry (KPDNHEP)** received 12,348 scam complaints as of June 30, 2022, where 4,114 of them involved online scams.

Consumers can report online scams both to the local police, the Central bank of Malaysia, and the **Commercial Crime Investigation Department (CCID) Scam Response Centre**. The CCID Scam Response Center was set up in March 2021 as a one-stop report and response center.

The CCID has developed a **portal** to enable the public to check telephone and bank account numbers used by the crime syndicates. The same functionality is also available **via an app**.

First launched in July 2021, the broadly supported #TakNakScam campaign aims to create awareness on how to spot, check and report scammers. During the campaign period, there was a downward trend in the number of scam cases reported.

The campaign, which ran for five months, reached 6.7 million people with a total of 234,000 engagements. This year the campaign is repeated and will focus on the top five online scams (e-commerce, loans, jobs, investment scams and money mulling).



Key Statistics:

Population:	32.7 million
Internet:	77%
# of Scams:	39,525
Scams / 1,000 :	1,21
Money lost:	$ 482 million*
Per capita:	$ 14,73
Per report:	$ 12,213

Key Organizations:

- CCID Scam Response Center
- Royal Malaysia Police
- Consumer Affairs Ministry

WhoisXML API:

Domains/capita	0.049
Domains registered	1,605,703
TLD registrations	401,814

Source: Federation of Malaysian Consumer Associations (FOMCA), ASEAN Cyberthreat Assessment 2021

* ScamAdviser Expert Estimate

Malaysia launched the TakNakScam awareness campaign for a 2nd year

The campaign, which ran for five months, reached 6.7 million people with a total of 234,000 engagements

Things you need to Report an e-Commerce Scam

Source: Kementerian Perdagangan Dalam Negeri dan Hal Ehwal Pengguna Malaysia

- The address of the premise
- Information of the individual/business
- Proof of purchase and/or receipt
- Pictures (If any and necessary)
- Communication records (If any and necessary)
- Type of Goods/services that you lodge the report on

#TakNakScam

for more information on this reporting process, please visit www.kpdnhep.gov.my

#TAKNAKSCAM

3 STEPS TO COMBAT SCAMS

STEP 01 SPOT

When dealing with unknown contacts, always be vigilant and cautious to consider the risk that the person may be a scammer. By being able to spot scams or impostors, you can avoid being a victim.

STEP 02 CHECK

When you suspect a content or contact to be a scam, do check with the authorities through official channels.

STEP 03 REPORT

If a content or phone call appears strange and if you think you were the victim of a scam, you can reach out to local authorities and the police. Also make sure to report any suspicious activities, person or account to Facebook, Instagram and WhatsApp.

We are the leading technical agency fighting online scams

Interview with Dato' Ts. Dr Haji Amirudin Abdul Wahab, CEO of CyberSecurrity Malaysia

Can you share what CyberSecurity Malaysia role is?

CyberSecurity Malaysia is the national cyber security technical agency under the purview of the Ministry of Communications and Multimedia Malaysia (K-KOMM). We are responsible to advice and implement cybersecurity related matters and supports Malaysia's National cyber security related strategic policies and plans such as the Malaysia Cyber Security Strategy (MCSS), Malaysia Digital Economy Blueprint, National 4th Industrial Revolution Policy, Twelfth Malaysia Plan (RMK-12), K-KOMM Strategic Framework and more.

How would you describe the situation of online scams in Malaysia?

One of the highlights of this year was the SMSSpy campaign, where threat actors attempt to steal financial credentials by using fake websites that pose as legitimate services, often outright replicating the original. In their effort, threat actors employ Facebook adverts to persuade potential victims to download Android malware from a malicious website.

Which actions have proven to be successful in combating online fraud?

CyberSecurity Malaysia continuously carries out programs to inculcate cyber safety awareness amongst Internet users on technological and social issues, particularly online danger. CyberSAFE™ (Cyber Security Awareness for Everyone) is our initiative to educate and enhance public's awareness on technological and social issues facing internet users, particularly online risks. CyberSAFE™ program was established to give exposure about cyber security awareness and best practices for the use of ICT including guidelines of using the internet safely and positively.

Activities that have been carried out by CyberSAFE™ include: Awareness Talks & Open Seminars, Training of Teachers/Ambassadors, Onsite Awareness Days/Week, Awareness Activity Kits, Awareness Roadshows and Competitions, Consultation with the community and various interest groups, National ICT Security Discourse (NICTSeD), Safer Internet Day (SID), Cyber Discovery Camp, Cyber SAFE Mentor program for the Institute of Higher Learning Centres, and much more.

Which plans does CyberSecurity Malaysia have for the future?

We have launched SiberKASA, an initiative aimed at developing, empowering, sustaining and strengthening cyber security infrastructure and ecosystem in Malaysia to ensure network security preparedness. We provide services that covers people, process, and technology and predictive, preventive, responsive and detective services. As such, we will continuously provide technical expertise and advice to the law enforcement agencies, governing bodies and other relevant departments and agencies. This collaborative effort is to enhance the cyber security climate in the country.

Dato' Ts. Dr Haji Amirudin Abdul Wahab
CEO
CyberSecurrity Malaysia

(Online) Fraud is the 2nd most reported kind of crime in Mexico (19%)

Robbery or theft in the street or public transport is the most reported type of crime with a share of 22.5%

Cybercrime in general and online fraud specifically is handled mainly at the state level in Mexico. Several of the states have their **own cybersecurity team.** However, several federal organizations are also actively involved in scam fighting.

The **National Guard (Guardia Nacional)** offers a helpdesk number, to receive reports from consumers. The Government of Mexico created the **Cyber Prevention and Investigation Unit** (formerly Policía Cibernética) as part of the Guardia Nacional.

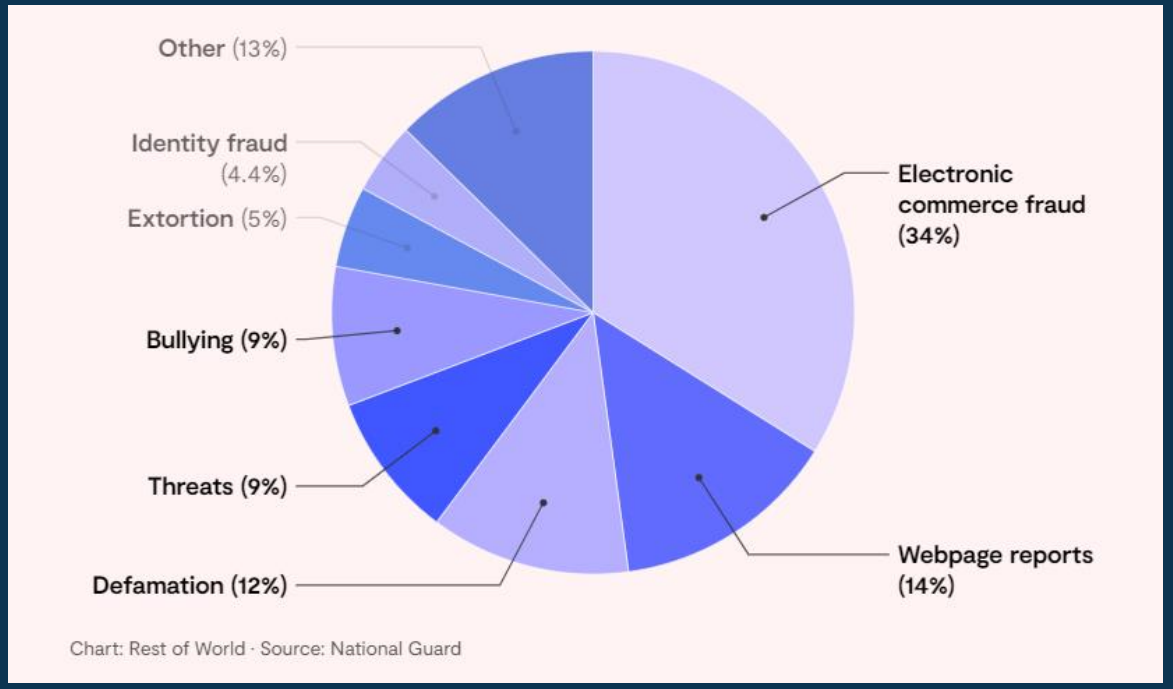
PROFECO is the national authority for consumer protection, collects reports of fraudulent activities and processes them for further investigation and maintains a list of complaints against online stores as well as a blacklist of malicious ones.

CONDUSEF is part of the national government and monitors the financial service providers in Mexico. It offers a financial fraud portal where consumers can enter a phone number, website, company name or email address and check if it is known for fraud. According to Condusef more than 5 billion pesos were lost in financial scams in 2021. According to the National Survey on Victimization and Perception of Public Safety, 5.9% of the Mexicans experienced a fraud crime incident in 2021, an increase with 0.8% point compared to 2020. In 45.1% of the cases were debit or credit card fraud. In 43.4% of the cases, a service/product was not delivered.

The **Mexican Internet Association** (AIMX) focuses on raising both consumer and company awareness concerning cybersecurity, as well as pleading for better legislation.

One of the newest types of scams are loan apps. Mainly poor Mexicans apply for an online loan. A loan is given (often less than applied for) and if the victim cannot pay, the lender starts calling and messaging with threats that range from saying the lenders would distribute photoshopped photos of María as a thief to threatening to rape and kill her family if she didn't repay.

Cybercrimes reported to the Mexican police Sept. 2020 – Sept. 2021.



Key Statistics:

Population:	130 million
Internet:	71%
# of Scams:	5.4 million
Scams / 1,000 :	41.5
Money lost:	$ 246 million
Per capita:	$ 1.89
Per report:	$ 46

Key Organizations:

- National Guard
- Profeco | Condusef
- Mexican Interner Association

WhoisXML API:

Domains/capita	0.011
Domains registered	1,605,703
TLD registrations	1,227,891

Source: Mexican Internet Association (AIMX), CONDUSEF, negi.org.mx/programas/envipe/2022/, restofworld.org/2022/mexico-scam-loan-apps/

Nearly 2.5 million Dutch were victim of cybercrime in 2021

The amount lost in online fraud is estimated to be € 2.75 billion by the University of Twente

According to the Dutch Central Bureau of Statistics, in 2021, nearly 2.5 million people in the Netherlands aged 15 or older (17 percent of the population) said they had fallen victim to cybercrime.

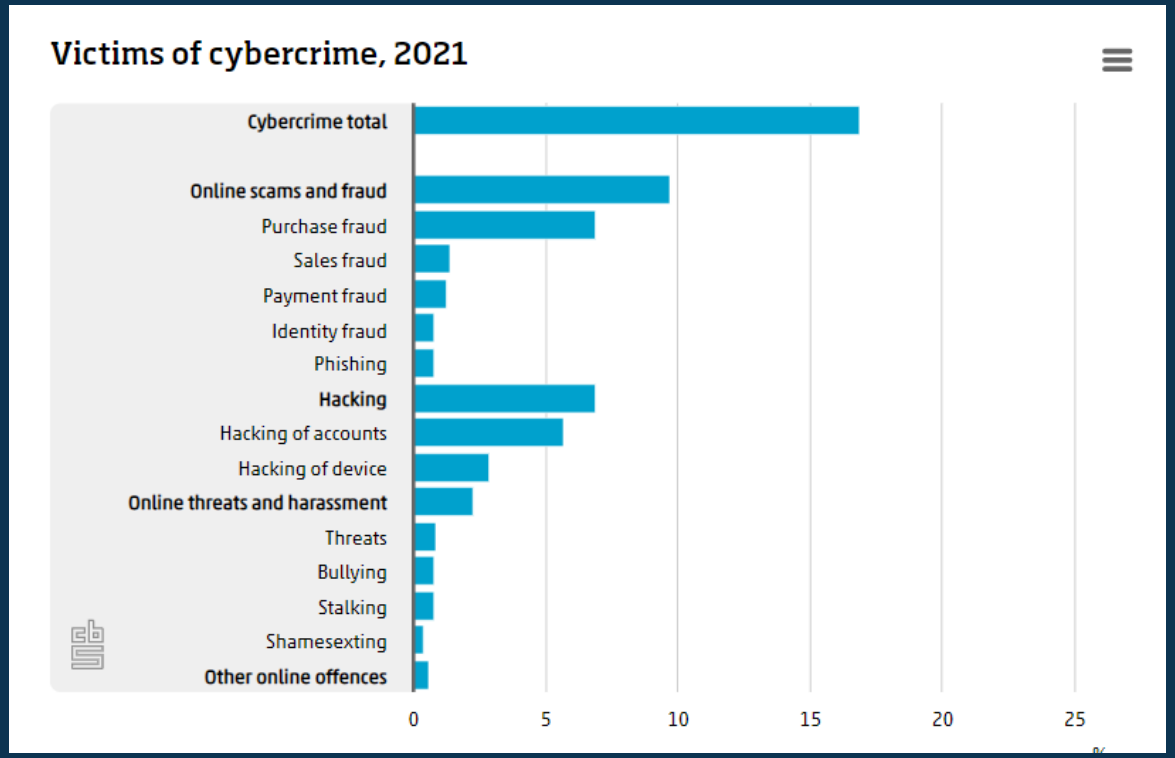
Most victims encountered online scams and fraud. One in three victims have had to deal with mental or financial problems because of the experience. Less than half of the victims reported the case, while less than 20 percent filed a police report. Over 1.5 million people - fell victim to online scams and fraud. Most cases concerned purchase fraud (7 percent), i.e. goods or services they purchased online were not delivered despite the payment. Seven percent were victims of hacking, in most cases into an account.

More than two out of three (68 percent) of all Dutch people aged 15 years or older say they have received at least one phone call, email or other message in the past 12 months that was (probably) from a scammer. Two percent said they fell for it. Almost half of them (0.8%, over 100,000 people) ended up losing money because of it.

The University of Twente found that in 2020, 15.7% of Dutch people aged 16 and older were victims of fraud. Young people are 21.5% more likely to be scammed than older people (13.1%). Researchers estimate the total loss due to fraud at € 2.75 billion. The research shows that only 12% of fraud cases are reported to the police.

There are several organizations working together in the Netherlands to combat online fraud. The most important ones are **FraudeHelpdesk**, a public private-partnership (PPP) which helps consumers to find the right support, and the **Dutch Police Online Crime Report Center** which aggregates all online crime reports coming in and coordinates these across the 10 regional police units. **ECP** is a PPP which stimulates cooperation to create a safe and prosperous Dutch digital community.

Sources: https://www.utwente.nl/nl/bms/fraudvic/fraudevictimisatie-in-nederland.pdf
https://www.cbs.nl/en-gb/news/2022/09/nearly-2-5-million-people-victims-of-cybercrime-in-2021



Source: Dutch Central Bureau of Statistics

Key Statistics:

Population:	17.5 million
Internet:	91%
# of Scams:	1.5 million
Scams / 1,000 :	85.5
Money lost:	$ 2.81 billion
Per capita:	$ 160
Per report:	$ 1870

Key Organizations:

- Police Internet Crime Reporting Unit
- Fraudehelpdesk
- ECP – Veiliginternetten.nl

WhoisXML API:

Domains/capita	0,726
Domains registered	12,736,528
TLD registrations	6,636,385

In New Zealand, the number of scams continued to rise with 24%

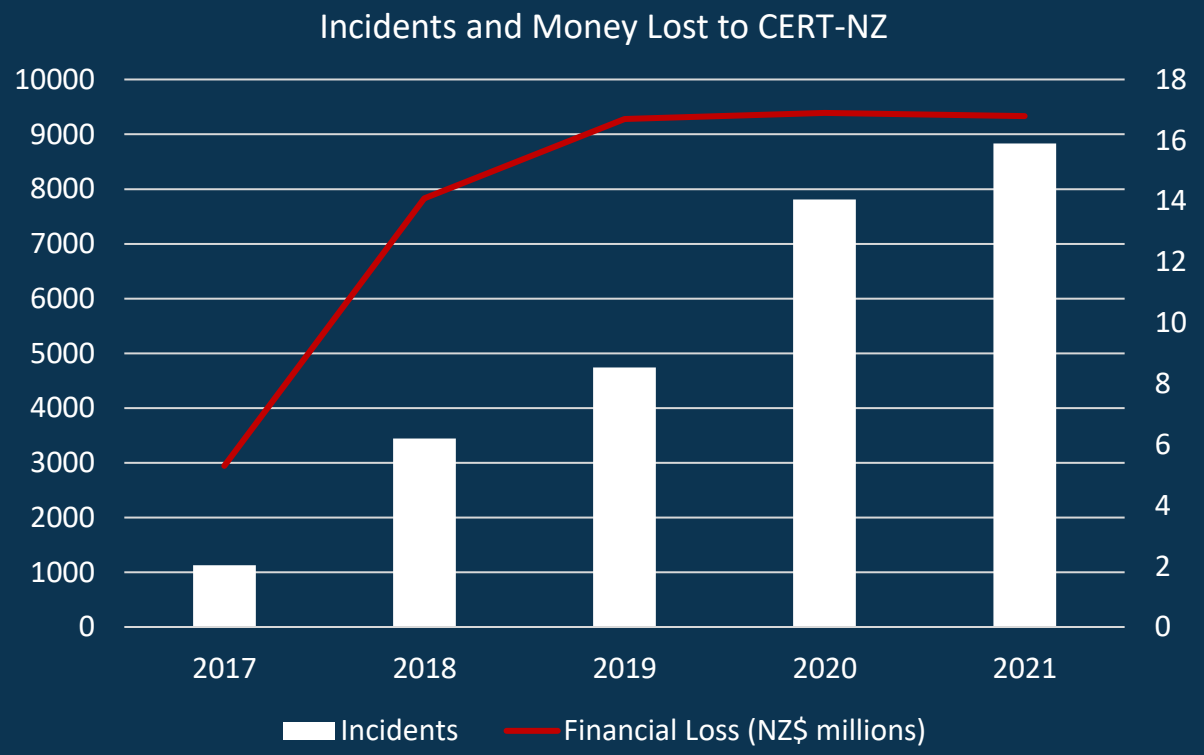
Remarkably, 55% of the people who report scams are now younger than 40

Citizens in New Zealand can report scams to several organizations. Cybercrimes can be reported to the **New Zealand Police** and the **Financial Market Authority** which also maintains a investor warning list of individuals and companies.

CERT NZ received 8,831 incident report in 2021, a 13% increase on 2020. **3,709** were **phishing and credential harvesting**, up 9%, 1,930 were related to malware (up 24%) and **scams** were down 1% to **1,897**. 15% of incidents reported to CERT NZ included direct financial loss, with a combined total value of NZ$16.8 million. Scams and fraud accounted for almost **NZ$11.9 million** (71%) of the total financial loss reported. Of that loss $3.9 million was lost when buying, selling or donating goods online. Over $2.1 million was lost to scams about employment and business opportunity offers and $2 million was lost to unauthorized or falsified money transactions.

The **Department for Internal Affairs** also offers the opportunity to send unsolicited emails to scam@reportspam.co.nz and SMS messages to 7726 (SPAM) for further analysis and action. **ID Care** is a non-profit that offers victim support for fraud and identity theft victims.

All organizations also revert to **Netsafe** which helps internet users stay safe online. Netsafe's research indicates that one in two people has experienced at least one online safety issue in the past year. The most common being **scams** (**12,725 reports**) and harassment. People reported a combined loss of NZ**$20,446,970** from online scams in 2021, with the average amount lost increasing over 18 percent, to $5,668.69. Those aged 40 and under made up over 55 percent of reports. Products And Services Fraud received the most reports (2067) with NZ$ 1.9 million lost. Investment scams were reported far fewer (460) but much more money was lost (NZ$9.6 million).



Key Statistics:	
Population:	5.1 million
Internet:	86%
# of Scams:	18,331 (24%)
Scams / 1,000 :	3,58
Money lost:	$ 19.7 million
Per capita:	$ 3.85
Per report:	$ 1,076

Key Organizations:

- New Zealand Police
- FMA, Cert-NZ
- Netsafe, ID-Care

WhoisXML API:	
Domains/capita	0.065
Domains registered	333,231
TLD registrations	668,289

netsafe.org.nz/wp-content/uploads/2018/11/2021-Netsafe_Annual-Report_Web2.pdf
cert.govt.nz/about/quarterly-report/2021-report-summary/

Nigerian banks are losing an estimated N14bn annually to fraud

Transactions via mobile channels increased by 164.4 per cent in 2021, as a result, scams via mobile boomed as well

Where consumers can report a scam depends on the type of scam in question. Victims can report to the (local) police or go to the **Nigerian Police Cybercrime** Reporting Portal. If the scam is financial in nature the crime can be reported to the **Economic and Financial Crimes Commission** (EFCC).

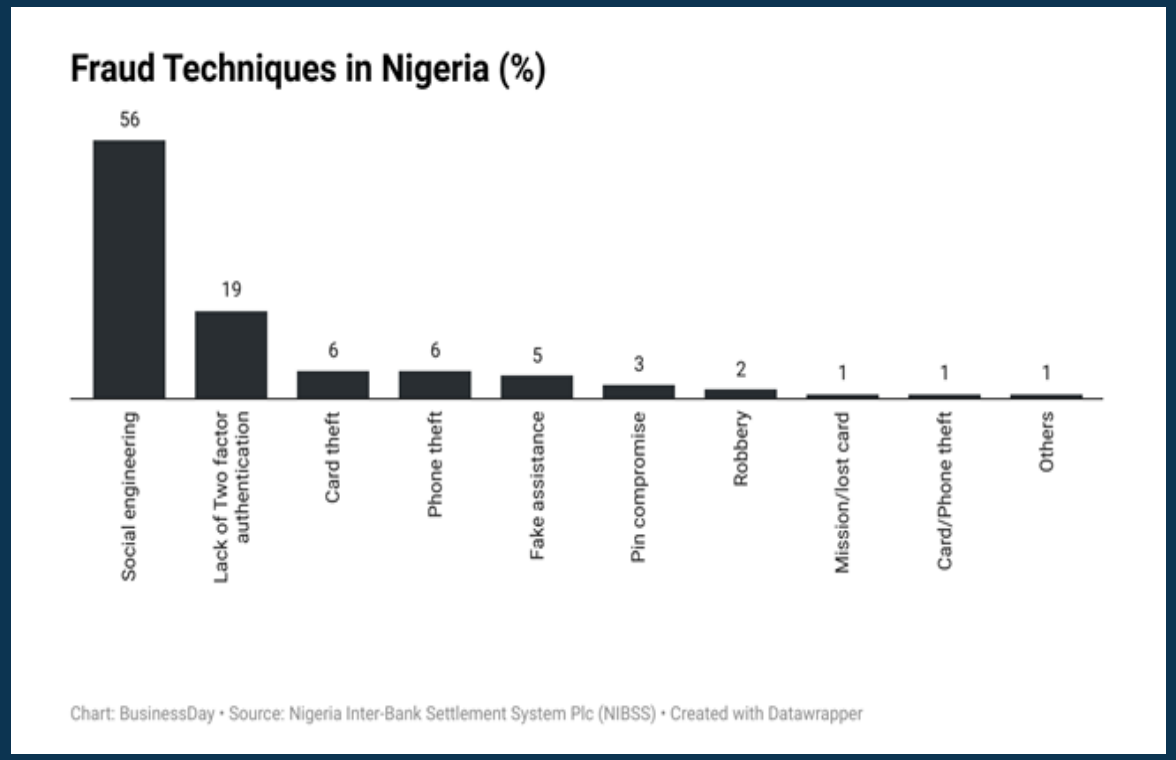
The Nigerian Inter-Bank Settlement Service (NIBSS) states that "the increase in transaction processing, speed and available channels comes with an unavoidable side effect – more vectors for fraudulent activities." NIBSS reported that fraud-related transactions cost Nigerian banks an average of **N14 billion yearly**.

The Nigeria's major anti-fraud agency, the **Economic and Financial Crimes Commission (EFCC)** arrested 10 operators who scammed people of N12 billion (742 million USD) between October 2020 and August 2021

Ponzi schemes continue to grow in Nigeria as the country is suffering from an economic depression. In the last 5 years it is estimated that Nigerians lost **N300 billion** ($ 713 million) in Ponzi schemes.

There is little to no enforcement of cyber laws as stipulated in the 2015 Cyber Crime Prohibition and Prevention Act. This is worsened by the fact that most of the punishments stipulated in the Act tend do not match the crimes committed. While regulators such as the Securities and Exchange Commission have tried to clamp down on such scams and Ponzi schemes, their proliferation continues to rise.

There are several NGOs trying to built scam awareness in Nigeria. One of them is the **CyberSafe Foundation** that facilitates a safer internet space for everyone with digital access in Nigeria.



Key Statistics:

Population:	211 million
Internet:	73%
# of Scams:	500,000*
Scams / 1,000 :	2.37
Money lost:	$ 175 million*
Per capita:	$ 0.83
Per report:	$ 350

Key Organizations:

- Nigerian Police Cybercrime
- Nigerian Inter-Bank Service (NIBSS)
- Economic & Financial Comm. (EFCC).

WhoisXML API:

Domains/capita	0,002
Domains registered	275,731
TLD registrations	18,535

stears.co/premium/article/nibss-data-shows-nigeria-needs-to-get-better-at-fighting-fraud/
punchng.com/four-banks-lost-n1-77bn-to-fraud-in-2021-says-report/#:~:text=NIBSS%20had%20earlier%20said%20that,9m%20respectively.

* ScamAdviser Expert Estimate

Pakistan recorded over 100,000 cases of fraud in 2021

Financial frauds, especially on social media platforms continue to grow.

Citizens can report scams and other cybercrimes online at the **Federal Investigation Agency** (FIA). Complaints are then passed along to the **National Response Centre for Cyber Crime** (NR3C). The NR3C was set-up in 2007, as part of FIA, and it is the law enforcement agency in Pakistan dedicated to fighting cyber crime. Scams are also reported to the **Pakistan Telecommunications Authority**, to telecom operators, and to banks.

Cyber Security (CS) Zone with the collaboration of Vice Chancellor Dr. Athar Mehbob established a Cyber Security Training center in The Islamia University Bahawalpur. The institute is training local police (also called Cybercrime Wings) as first responders for cybersecurity issues. FIA is planning to open a cyber-wing in every district.

The FIA received over 102,356 complaints of online crimes with Facebook being used as a median in 23% of them. 1,202 cases were registered under the Prevention of Electronic Crimes Act with 1,300 arrests made.

Most of the complaints were filled by students who accounted for 32% of the total cases. The most common types of scams included financial scams, forgery, extortion and blackmailing.

Crypto scams continued to rise with one scheme seeing investors lose $100 million (roughly PKR 7.39 crore). This has led to the government banning crypto and launching investigations into Binance, a popular crypto exchange program, in Pakistan.

FIA had taken new initiatives as the agency introduced e-investigation, getting record and testimony online like email and video calls with security checks, just to provide relief to the common man.

Cybercrime Categories investigated by FIA

Key Statistics:		**Key Organizations:**	
Population:	225 million	• Federal Investigation Agency (FIA)	
Internet:	53%	• National Response Centre cyber (NR3C)	
# of Scams:	102,356	• Digital Rights Foundation (DRF)	
Scams / 1,000 :	2.37	**WhoisXML API:**	
Money lost:	$100 million*	Domains/capita	0,001
Per capita:	€ 0,47	Domains registered	275,731
Per report:	€ 200	TLD registrations	18,535

dawn.com/news/1667248
gadgets360.com/cryptocurrency/news/binance-pakistan-scam-usd-100-million-2702202

* ScamAdviser Expert Estimate

One in every two Filipinos has been targeted by Fraudsters

The number of Cybercrimes in general increased exponentially in the first quarter with over 1.76 million cases reported.

Several organizations are responsible for fighting cybercrime in the Philippines; among them is the Department of Justice Office of Cybercrime (OOC). The OOC is the central authority in all matters relating to international mutual assistance and extradition for cybercrime and cyber-related matters. It also acts as the focal agency in formulating and implementing law enforcement investigation and prosecution strategies in curbing cybercrime and cyber-related offenses nationwide.

The **Cybercrime Investigation and Coordinating Center** (CICC), which was set-up in 2012, is an agency linked to the Department of Information and Communications Technology (DICT). The CICC is responsible for the formulation of the National Cybersecurity Plan, the National Computer Emergency Response Team (CERT), and the facilitation of international intelligence cooperation, especially regarding cybersecurity matters that are transferred to the Department.

The Philippines' **National Police Anti-Cybercrime Group** (PNP-ACG) focuses on cyber forensics, investigations and arrests. The organization has 21 Regional Anti-Cybercrime Units across the country.

According to the TransUnion Consumer Pulse Survey, of the over 1,000 Filipino adults polled, 53% said they were targeted by fraudsters in the previous 3 months (up 3% on the previous quarter). 11% of the respondents said they ended up as victims. Phishing scams led the way (42%), followed by money and gift card scams (38%) and third-party seller scams on legitimate online retail sites (30%).

Bangko Sentral ng Pilipinas Governor Benjamin Diokno noted that investment scam losses alone have reached over P25 billion (448.9 million USD).

Industry	The Philippines	Across the globe
Insurance	N/A	+134.5%
Gambling	+67.2%	+50.1%
Logistics	+104.5%	+42.7%
Travel & Leisure	+17.0%	+13.3%
Gaming	-27.6%	+6.9%
Communities (online dating, forums, etc.)	+4.6%	-6.1%
Retail	-23.2%	-7.6%
Telecommunications	+0.9%	-20.4%
Financial services	-24.5%	-63.6%

Suspected Digital Fraud Attempts Shift to New Industries - Fraud rate change Q1–Q1 2022, Source: TransUnion

Key Statistics:

Population:	111 million
Internet:	66%
# of Scams:	6,471,300
Scams / 1,000 :	58,28
Money lost:	$ 449 million
Per capita:	$ 4,04
Per report:	$ 69,37

Key Organizations:

- Cybercrime office Justice Dept (OOC)
- Cybercrime Coordinating Center (CICC),
- Police Anti-Cybercrime (PNP-ACG)

WhoisXML API:

Domains/capita	0.008
Domains registered	849,552
TLD registrations	1,844,039

transunion.ph/blog/fraud-trends-Q3-2021
philstar.com/headlines/2020/10/25/2052110/online-scams-spike-during-quarantine

90% of the cyber incidents in Poland are related to online fraud

29,483 incidents were reported, a growth of 182% compared to 2020

NASK (Research and Academic Computer Network) is the registry of the .pl TLD and its key tasks also include that of ensuring Poland's internet security. Early on, it set up a **Computer Incident Response Team (CERT.PL)** where users can report incidents (incydent.cert.pl).

In addition, NASK offers a contact point for reporting illegal content (dyzurnet.pl) especially related to the sexual abuse of children. NASK also set up **saferinternet.pl** which is part of the **Polish Safer Internet Center** (PCPSI).

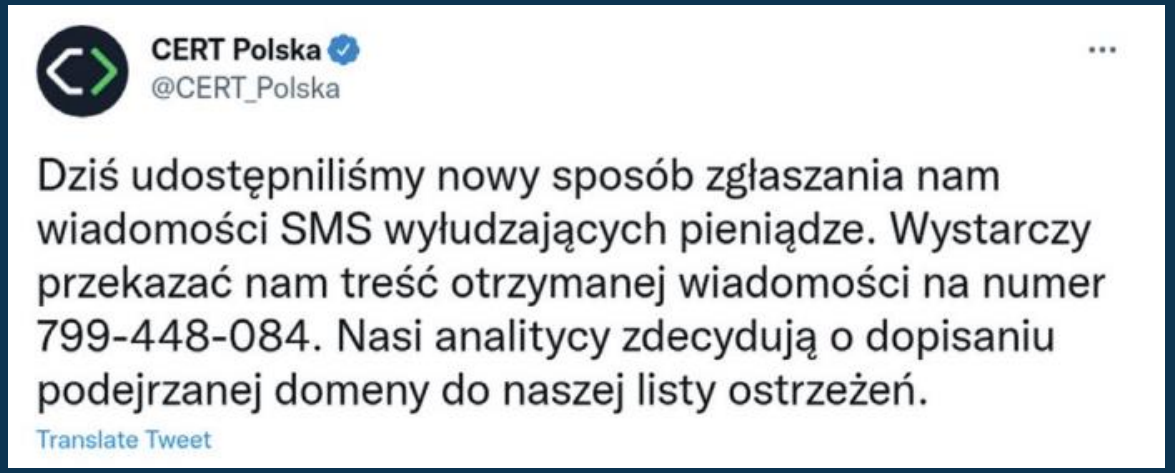
The police offers citizens the option to report cybercrime online. The government is committed to expanding the cyberteam within the police to 1,800 officers by the year 2025.

CERT PL recorded a total of 29,483 unique cyber security incidents, an increase of 182% compared to 2020. The most common incident was phishing - accounting for as much as 76.57 percent of all incidents handled. This is an increase of 196 percent compared to the previous year. The economic sectors most frequently affected by incidents were media, wholesale and retail trade, and postal and courier services.

CERT PL has started publishing a Domain Warning List. 33,000 domains made it to their Warning List. The most common phishing campaign scheme we observed was phishing for Facebook login credentials. This was a threefold increase compared to 2020.

Criminals have focused on perfecting known phishing scenarios: taking over Facebook accounts, fake payment gateways payments, and extorting money from sellers via advertising portals. Due to the increase of SMS messages as a means of distributing malicious links, CERT PL launched a special number, to which consumers can report an incident by forwarding received SMS message containing a suspicious link.

Criminals have started using a new fraud scheme for fake cryptocurrency investments. The most popular were two scenarios. In one, phone calls were made with information about allegedly previously invested funds. In the other, sites that offered fake investments were promoted on social networks.



CERT PL launches a service for reporting suspicious messages via SMS.

Key Statistics:	
Population:	38 million
Internet:	87%
# of Scams:	26,535 (182%)
Scams / 1,000 :	0,70
Money lost:	$ 10.4 million*
Per capita:	$ 0,27
Per report:	$ 391

Key Organizations:

- NASK / CERT.PL
- SafterInternet
- Policja

WhoisXML API:	
Domains/capita	0.015
Domains registered	311,480
TLD registrations	424,368

https://cert.pl/posts/2022/05/krajobraz-bezpieczenstwa-polskiego-internetu-w-2021-roku/

* ScamAdviser Expert Estimate

In 2020, Portugal reported 26% more cyberincidents

Government agencies and the police have started paying more attention to online fraud

The **Portuguese National Cybersecurity Centre** (CNCS) mission is to contribute to a free, reliable and safe use of the Internet in Portugal. It acts as the operational coordinator and national authority on cybersecurity between state departments, national critical infrastructure operators, essential and digital service providers.

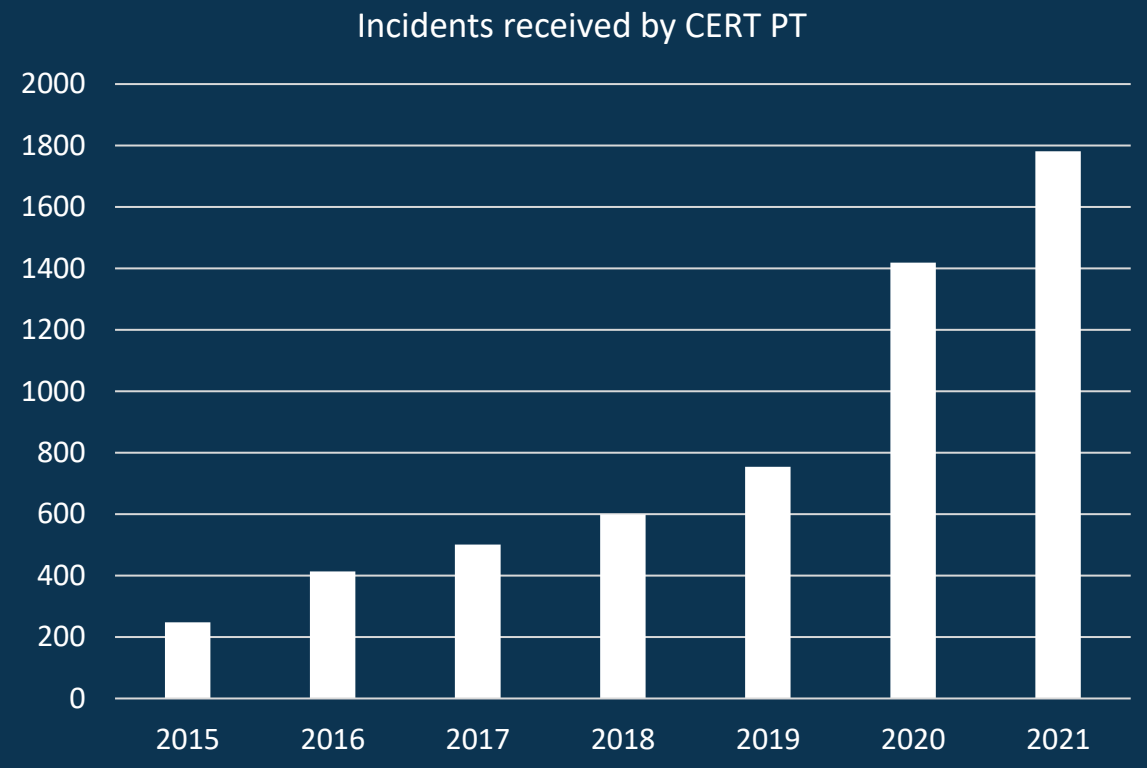
CERT PT, as part of CNCS, identified 1,781 cybersecurity incidents in 2021 a growth of 26% compared to the 1,418 incidents reported in 2020. Phishing attempts for the biggest category of cyberincidents (715) followed by other social engineering related incidents (246).

According to CNCS, the dominant cyber threats in Portugal during the year 2021 were phishing/smishing/vishing, ransomware, online fraud, account compromise or attempt and exploitation of vulnerabilities. CNCS noticed a growth by reasonably organized cybercriminals and an increase in fake pages of well-known brands and cryptocurrency investments scams.

Apart from CNCS, the **National Unit to Combat Cybercrime and Technological Crime** (UNC3T) is involved in cybercrime fighting. Its main competencies are prevention, detection, criminal investigation and assistance of judicial authorities regarding crimes committed by computerized means. Portuguese citizens can report scams online on the websites of the Polícia Judiciária, of the Public Prosecution Service and its Cybercrime Office, and of CNCS.

Several organizations are also building awareness around scams. The CNCS informs the public via **Internet Segura**. **APAV** is an association that supports scam victims and is part of the Internet Segura Initiative. **Deco Proteste** is the largest consumer protection organization in Portugal and offers an online complaint forum. The organization offers both information on scams online and support via phone.

cncs.gov.pt/docs/relatorio-riscosconflitos2022-obciber-cncs.pdf



Key Statistics:	
Population:	10,3 million
Internet:	74%
# of Scams:	1,781 (26%)
Scams / 1,000 :	0.17
Money lost:	$ 1.6 million*
Per capita:	$ 0.15
Per report:	$ 891

Key Organizations:

- National CyberSecurity Center
- UNC3T
- Policia Segurance Publica

WhoisXML API:	
Domains/capita	0.030
Domains registered	311,480
TLD registrations	424.368

* ScamAdviser Expert Estimate

Qatar bolsters cyber security in preparation for World Cup

Qatar's National Cybersecurity Agency trained 25,000 employees in different aspects of cyber security in less than one year

Qatar has also set up governmental organizations to combat cyber crime. In 2013, it established the **National Cyber Security Committee** to address cyber security at national level. In March 2021, Qatar established the **National Cybersecurity Agency**, which, as of May 2022, has trained 25,000 employees in different aspects of information security.

Qatar hosts the FIFA World Cup this year – the first time the event has been staged in the Arab world. Cyber security experts in the country predict that ticketing, hotel bookings and restaurant reservations will be faked to capture personal data from people travelling to Qatar. Also, phishing and social engineering will be used to steal personal and financial information from anyone using the internet to get information about the World Cup championship.

Cyber security has been a concern in Qatar for at least two decades now. One of the organizations that has been instrumental in securing the country's information infrastructure is the **Qatar Computer Emergency Response Team (Q-Cert)**, which was set up in 2005 by the **Qatar Ministry of Transport and Communications (MOTC).**

Q-Cert has launched several projects recently. One is to develop a fully automated threat monitoring system to collect security-related data and perform preliminary analysis on that information. Data is collected from distributed sensors and mechanisms, such as spam traps. Scams can now also be reported by phone.

The Ministry of Internal Affairs also launched a **Cyber Crime Investigation Centre**. Qatar citizens can report scams via phone and email to the ministry.

Group-IB exposes fraud schemes in Qatar

Group-IB, has identified a widescale phishing campaign targeting users in Qatar using 12 well local known brands (banks, delivery and postal services). All the domains were part of a single massive phishing infrastructure.

Customers awaiting an order may receive an email or an SMS from the national postal service requesting payment for a delivery or customs clearance fee. Following the link from the message, customers are redirected to a phishing page that requests their bank card details in order to process the payment. As soon as the customer submits the form, the sum of the "fee" is deducted from their bank account and transferred to cybercriminals, along with their bank card details.

Group-IB estimates that each victim on average lost 656 euro.

Key Statistics:	
Population:	2.9 million
Internet:	86%
# of Scams:	-
Scams / 1,000 :	-
Money lost:	-
Per capita:	-
Per report:	-

Key Organizations:

- Q-Cert
- Cybercrime Investigation Center
- National Cybersecurity Agency

WhoisXML API:	
Domains/capita	0.012
Domains registered	36,552
TLD registrations	24,990

computerweekly.com/news/252521418/Qatar-bolsters-cyber-security-in-preparation-for-World-Cup, Group-IB

Cybercrime Victims In Romania Lose USD145m Each Year

In 2021, 5,052 cases were reported and 1,623 cases were resolved

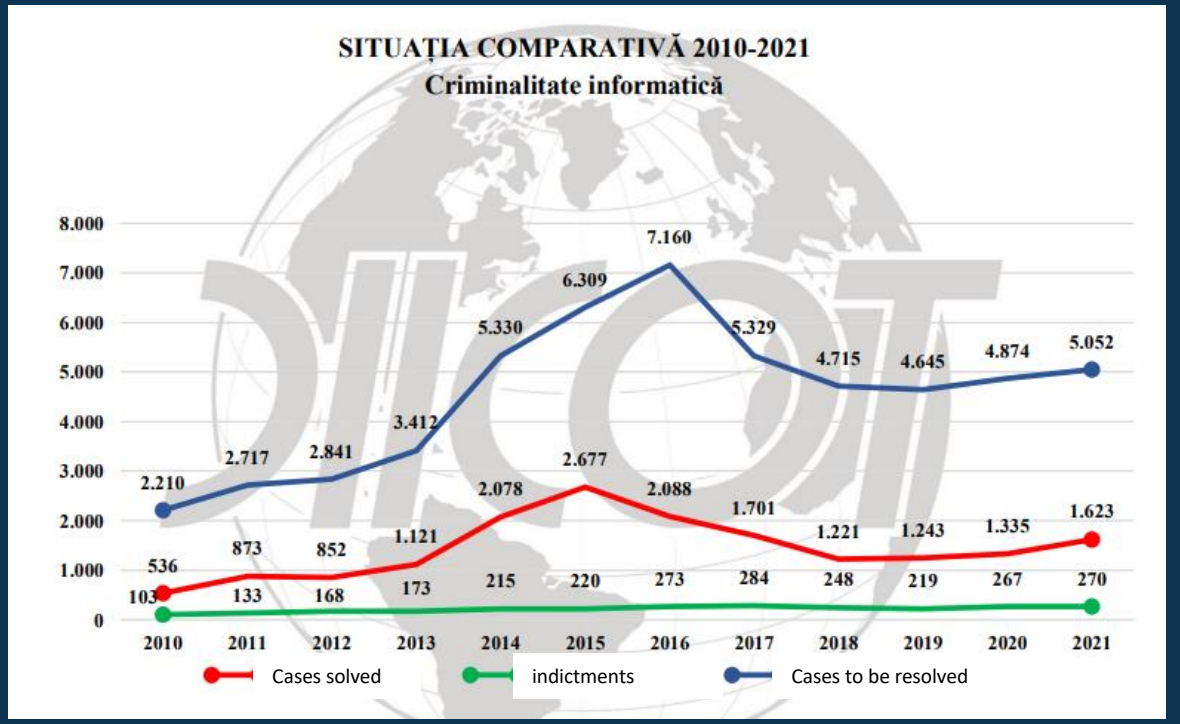
Cybercrime is common in Romania mainly due to two reasons: the high level of computer skills amongst its population and the large number of young people who are not able to find a job after graduation, who are lured into cybercrime. Hence, several organizations are fighting cybercrime and fraud.

The **Directorate for Investigating Organized Crime and Terrorism** (Direcția de Investigare a Infracțiunilor de Criminalitate Organizată și Terorism, DIICOT) is the Romanian agency tasked with investigating and prosecuting organized crime and terrorism-related offenses. 18% of the cases handled are related to cybercrime. In 2021, 5,052 cases need to be resolved and 1,623 cases were resolved.

The **National Directorate for Cybersecurity** has taken over the role of CERT-RO. **CERT-RO** is the Romanian National Computer Security Incident Response Team, established as an independent structure for research, development and expertise in the field of cyber-security.

It is estimated that victims in Romania lose $145 million annually in scams.

Cybercrime Cases



Key Statistics:

Population:	19 million
Internet:	66%
# of Scams:	5,052
Scams / 1,000 :	0.26
Money lost:	145 million
Per capita:	7,59
Per report:	28.701

Key Organizations:

- DIICOT (organized crime)
- DNSC (CERT)

WhoisXML API:

Domains/capita	0.015
Domains registered	282,835
TLD registrations	855,571

diicot.ro/informatii-de-interes-public/raport-de-activitate
romaniajournal.ro/society-people/law-crime/cybercrime-victims-in-romania-lose-usd-145m-each-year-study-finds/

Fraud tops Russia's most frequently recorded crimes, 25% of all crimes

One fraud case is registered every three minutes in average, according to the statistics of the Office of the Prosecutor General

Russians can report online fraud to several organizations including the Russian **Consumer Protection Agency**, the **Health Inspection Service** (for drugs), the **prosecutor's office** and the police. The police recently also set up a special CyberSecurity team. **Department K** (short for Kompyuternye Prestupleniya, or computer crimes) is a division of the Ministry of Internal Affairs that has been active since 2001 and focuses primarily on information technology-related crimes.

To combat financial scams **Financial CERT** has been set-up by the Bank of Russia as a Computer Emergency Response Team. Financial CERT facilitates information exchange between financial market participants, law enforcement agencies, telecom providers and operators, system integrators, anti-virus software developers, and other companies engaged in information security activities.

ROCIT is a public organization uniting active Internet users in Russia. One of its services is a hotline where Russians can report fraud, low quality Internet services, unscrupulous online stores, hacked accounts, etc.

The Bank of Russia reports that in 2021, the number of fraudulent telephone numbers detected increased more than seven times to compared to 2020 to 179,000 cases. Over the year, the Bank of Russia initiated the blocking of over 6,000 websites created by swindlers. the amount of unauthorized (made without the consent of customers of financial institutions) banking transactions amounted to **45 billion rubles**. The amount of damage from a single scam varies from 15,000 rubles to tens of millions of rubles. The largest scam encountered was 25 million rubles (€287,000).

In addition, the Ministry of Internal Affairs of Russia reported the damage from phone scam in 2021 to be 13.5 billion rubles.

Several actions have been taken to combat online fraud. On March 9, 2021, Russia signed a law to block communications in prisons in order to reduce the volume of phone scam and in the Federal Antimonopoly Service and the "Big Four" mobile operators signed a memorandum on combating telephone spam. Also, in June it was reported that Russia will work with the U.S. to identify ransomware hackers as part of an agreement between the presidents of the two countries. Finally, a law was passed to block calls and text messages from abroad to spoofed numbers.

AMOUNT OF UNAUTHORISED TRANSACTIONS ▲	PROPORTION OF SOCIAL ENGINEERING IN UNAUTHORISED TRANSACTIONS ▼	FRAUDULENT TELEPHONE NUMBERS DETECTED BY THE BANK OF RUSSIA ▲	BLOCKING OF FRAUDULENT WEBSITES INITIATED BY THE BANK OF RUSSIA ▼	ACCESS TO FRAUDULENT WEBSITES WAS LIMITED* ▲
₽13.6 BILLION	49.4%	179,071	6,213	3,100
9.8 (2020)	61.8 (2020)	26,397 (2020)	7,680 (2020)	377 (2020)

Source: Annual Report Bank of Russia 2021

Key Statistics:

Population:	143 million
Internet:	86%
# of Scams:	249,200
Scams / 1,000 :	1.74
Money lost:	$ 815 million
Per capita:	$ 5.68
Per report:	$ 3,270

Key Organizations:

- Prosecutor's Office
- Financial CERT
- ROCIT

WhoisXML API:

Domains/capita	0.011
Domains registered	1,531,406
TLD registrations	10,708,609

Sources: GroupIB , cbr.ru/Collection/Collection/File/41054/rb_2021.pdf,

62% of Saudi Arabia consumers received spam & scam messages

Users in Saudi Arabia are targeted the most by phishing scams in the Middle East

According to a survey by the King Abdul Aziz Center for National Dialogue, 62% of the people living in Saudi Arabia got scam calls or communications. The survey found that in 72% of the cases, scammers impersonated banks, in 18% of the time they mimicked police, and 10% of the instances they claimed to be delivery services. Of the 62%, fourteen percent admitted that they fell for the phone or online scam and lost money.

There are several organizations trying to fight scams. Consumers can report commercial related scams to the **Ministry of Commerce** online, via an app as well as by phone. The **Consumer Protection Association** launched a website (scam.sa) in collaboration with the Ministry of Commerce to help consumers spot signs of online fraud and learn Other scams from individuals or from outside Saudi Arabia can be reported to the **Ministry of Interior**.

The **Saudi Federation for Cyber Security and Programming** (SAFCSP) is the national institution whose goal it is to build national and professional capabilities in the fields of cyber security through awareness, education, and support.

The **Saudi Central Bank** (SAMA) has been accelerating its efforts in fighting fraud and scams in the financial sector. They launched the Joint Operations Center for banks to follow up and monitor cases of financial fraud, as part of its efforts to support the stability of the banking sector allows consumers to file a complaint related to a financial service, including forex and investment scams.

Saudi Central Bank (SAMA) 2021 annual report stated that fraudsters use multiple methods to gain access to people's banking data and personal credentials to steal their money, where impersonation of bank officials being the most popular method.

saudigazette.com.sa/article/619345
arabnews.com/node/2027646/saudi-arabia
itp.net/business/over-half-of-saudis-face-scam-attempts-most-from-fake-bankers

Saudi Arabia warns against Hajj scams
https://www.arabnews.com/node/2100056/saudi-arabia

Key Statistics:	
Population:	35 million
Internet:	77%
# of Scams:	3 million
Scams / 1,000 :	85
Money lost:	$ 2 billion
Per capita:	$ 56,59
Per report:	$ 667

Key Organizations:

- Saudi Central Bank (SAMA)
- Ministry of Commerce
- The Saudi Fed. for Cyber Sec. (SAFCSP)

WhoisXML API:	
Domains/capita	0.006
Domains registered	196,652
TLD registrations	63,153

Over $644 million was lost to scams in Singapore in 2021

While the number of cases grew with 53%, the amount of money lost exploded by 2.5 times from $268.4 million in 2020

The **Singapore Police Force Anti-Scam Centre (ASC)** was set up in 2019. The ASC is the "nerve center" for investigating scam-related crimes and its focus is to disrupt scammers' operations and to help mitigate victims' losses.

ASC's four core activities are Enforcement, Engagement, Engineering and Education. ASC works closely together with more than 20 stakeholders comprising banks, fintech companies, telecommunication companies and online marketplaces in its fight against scams.

A 52.9% increase in scam cases drove up the total number of reported crimes to 46,196 cases, from 37,273 cases in 2020.

Police said at least 90 per cent of scams in Singapore originate from overseas, and described the scammers as syndicated, well resourced & technologically sophisticated. The police said these cases are difficult to investigate and prosecute as efforts depend on the level of cooperation from overseas law enforcement agencies. Job scams, which were not even among the top 10 scams in 2020, were the most common ruse last year with 4,554 cases, up from 132 the year before.

Investment scams accounted for the most amount of money stolen, with victims losing $190.9 million in total. The largest amount taken in a single case was $6.4 million. There were 5,020 cases of phishing scams with a total of 23,931 cases reported.

Job scams, non-banking related phishing scams, e-commerce scams, investment scams, loan scams and banking related phishing scams remain of particular concern. They made up 80.4% of the top ten scam types reported in 2021. The total number of reported cases for these top six scam types rose by 99.2%, compared to 2020.

Type of scam	Cases reported (2020)	Cases reported (2021)	Amount cheated (2021)	Largest sum lost (2021)
Job	132	4,554	$91m	$4.3m
Non-banking- phishing	644	2,783	$15.3m	$3.4m
E-commerce	3,359	2,707	$5.8m	$400k
Investment	1,096	2,476	$190.9m	$6.4m
Loan	1,978	2,274	$18.3m	$361k
Banking-related phishing	1,340	2,237	$19.4m	$1m
Social media impersonation	2,919	1,614	$5.5m	$1m
Internet love	823	1,099	$46.9m	$3m
Impersonation of China officials	442	752	$106.4m	$6.2m
Fake friend call	0	685	$4.5m	$616k
Total	12,733	21,181	$504.4m*	

Top 10 Scams in Singapore in 2021

Key Statistics:

Population:	5.4 million
Internet:	88%
# of Scams:	23,931 (53%)
Scams / 1,000 :	4.39
Money lost:	$453 million
Per capita:	$ 82,99
Per report:	$ 18,911

Key Organizations:

- Anti-scam Centre (ASC)
- Crime Prevention Council (NCPC)
- Singapore Police Force (SPF)

WhoisXML API:

Domains/capita	0,182
Domains registered	991,647
TLD registrations	227,266

straitstimes.com/singapore/courts-crime/victims-lost-6333-million-to-scams-in-2021, straitstimes.com/stop-scams

Due to data breaches, South Africa reports a massive increase in fraud

Scams are not reported centrally but per police station making it difficult to get a national overview

There is no centralized system for reporting cybercrime in South Africa. Citizens are requested to report scams to their local police office. The **Cybersecurity Hub** is South Africa's National Computer Security Incident Response Team (CSIRT). Cyber incidents (not so much scams) can also be reported here.

In 2020, the Cybercrime Act was set up, criminalizing cybercrime. It has however not yet been operationalized. Since 2011, the **South African Police Service** (SAPS) has an **Electronic Crime Unit.**

To fill the gap, the **Financial Intelligence Centre's** contributes to safeguarding the integrity of the country's financial system. Consumers can check the registration of financial companies on FIC's website as well as report suspicious activities.

The **South African Banking Risk Information Centre** (SABRIC), is a non-profit organization formed by the four major banks to combat organized bank-related crimes. The SAFPS pointed to an increase in the money mule scam where a person approaches someone else and asks them if they can use their account to send money to a relative in another country.

Two recent breaches of credit bureau TransUnion and Experian are expected to have wide repercussions for South African consumers. The South African Fraud Prevention Service (SAFPS) reported that, in the year after the Experian breach, it saw a massive jump in fraud across the country. Fraud listings increased by 62%, victim listings increased by 54% and impersonation fraud tripled, rising 337%.

The strong increase in scams is also caused by high inflation and an unemployment rate of 34.5%. This is forcing people to look for new ways to make ends meet which makes them increasingly vulnerable to scams.

On a local level, compared to last year's figures, Claremont Police Station states it has experienced a 29% increase in reported fraud cases. 40% were online purchasing, 40% were online banking or calls from imposters claiming to be bank representatives, 10% were so-called "Tinder Swindler" scams (con-artists known to the victim) and 10% were in-house corporate fraud/white-collar crime.

At Wynberg Police Station, many reported fraud cases involved vishing and phishing. Especially emails entice recipients to respond by claiming they have won a prize or that there is money owed to them, are popular. Another scam they see almost daily involves fraudsters advertising vehicle sales on social media.

Claiming that there is lots of interest in the vehicle, 'sellers' ask the 'buyers' to transfer a deposit into their bank account to secure the sale. Once the money is paid, the 'sellers', along with their fake social media account, just disappear.

Key Statistics:

Population:	60 million
Internet:	53%
# of Scams:	30,000*
Scams / 1,000 :	0.5
Money lost:	$ 100 million*
Per capita:	$ 1.67
Per report:	$ 3,333

Key Organizations:

- South African Police Service (SAPS)
- Cybersecurity Hub
- SABRIC

WhoisXML API:

Domains/capita	0.026
Domains registered	1,577,102
TLD registrations	63,153

news24.com/news24/community-newspaper/peoples-post/sharp-increase-in-online-fraud-20220530

* ScamAdviser Expert Estimate

In South Korea, the number of Cybercrimes increased with 28% in 2020

The number of cybercrimes increased from 136,074 in 2019 to 174,328 in 2020

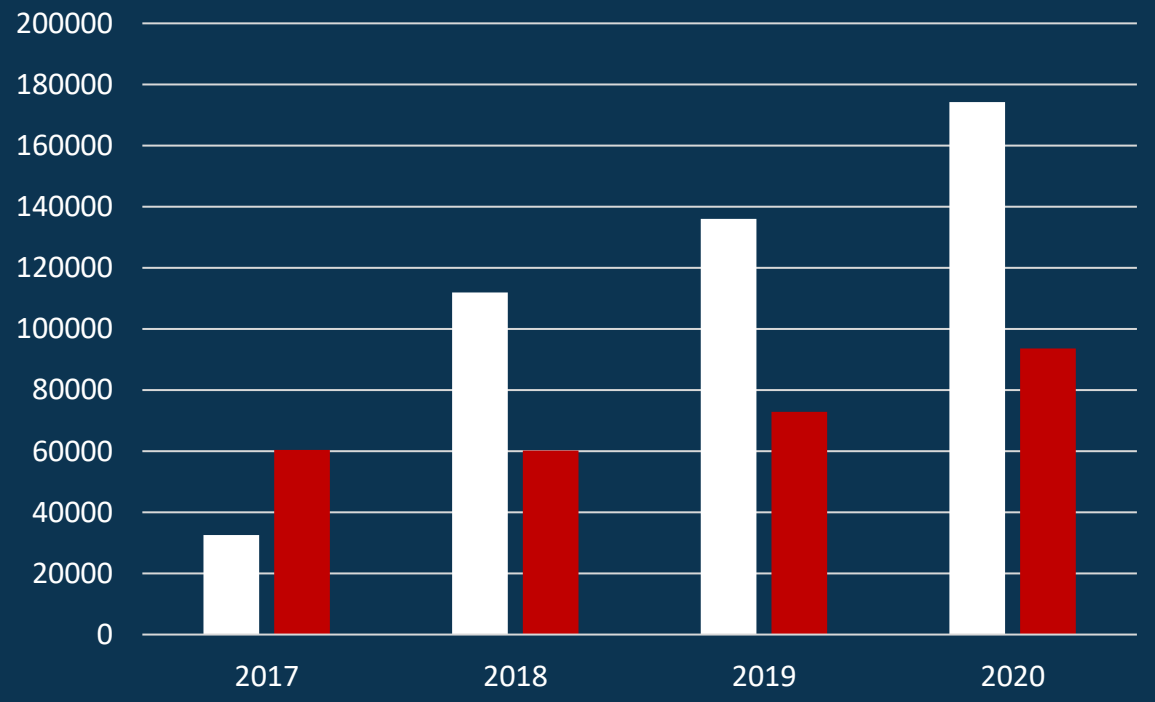
The **Korean National Police Agency** (KNP) has integrated all reports through its own **Electronic Crime and Report Management System**. Cybercrimes can be reported here as well. The KNP has a separate Cybercrime Bureau where citizens can check for scams and apply for cyber-awareness training.

The KSA works closely with civilian cybersecurity experts and related organizations such as the **Korea Internet & Security Agency** (KISA). KISA's focus lies on strengthening the competitiveness of the Internet in Korea. Their aim is also that of developing and spreading information regarding online security.

The Cheat is an online platform where people can share scam information. It was launched in 2006. Fraud victims can share a total of 10 types of information such as the name, ID, account number, and cell phone number of the fraudster to prevent other consumers from being scammed.

According to the South Korea Public Data Portal, 174,328 cybercrimes were reported in 2020 (no data is yet available for 2021). An estimated amount of 332 trillion Won was lost in scams.

Especially phishing scams involving instant messaging spiked in 2021 due to increased not-in-person activities amid the coronavirus pandemic. The amount in damages from messenger phishing grew to 99.1 billion won ($80.3 million), up 166 percent from the previous year, according to the Financial Supervisory Service. The figure accounted for nearly 59 percent of last year's total damages of 168.2 billion won resulting from phishing.



Cyber crime cases in South Korea from 2017 – 2022 reported/solved

Key Statistics:

Population:	52 million
Internet:	96%
# of Scams:	174,328 (28%)
Scams / 1,000 :	3,37
Money lost:	$ 234 million
Per capita:	$ 4.52
Per report:	$ 1.341

Key Organizations:

- KNP & Cybercrime Bureau
- Korea Internet & Security Agency
- The Cheat

WhoisXML API:

Domains/capita	0.025
Domains registered	1,312,893
TLD registrations	1,104,232

data.go.kr/data/15064572/fileData.do?recommendDataYn=Y
koreaherald.com/view.php?ud=20220502000835
korea.kr/docViewer/skin/doc.html?fn=777f00240c259eaa3c154dd111b74f3b&rs=/docViewer/result/2021.11/17/777f00240c259eaa3c154dd111b74f3b

Computer fraud represents 89.6% of cybercrimes in Spain

To offer more support, INCIBE has launched a 9AM to 9PM, 365 days a year phone and digital support number: 017

There are several organizations in Spain involved in cybersecurity and online fraud. Consumers can report online fraud both to the local police, the **Guardia Civil**, and to the **National Police**, both online and by phone. The Guardia Civil has both a Central Cybercrime Unit as well as local cybercrime teams in each of Spain's 17 regions.

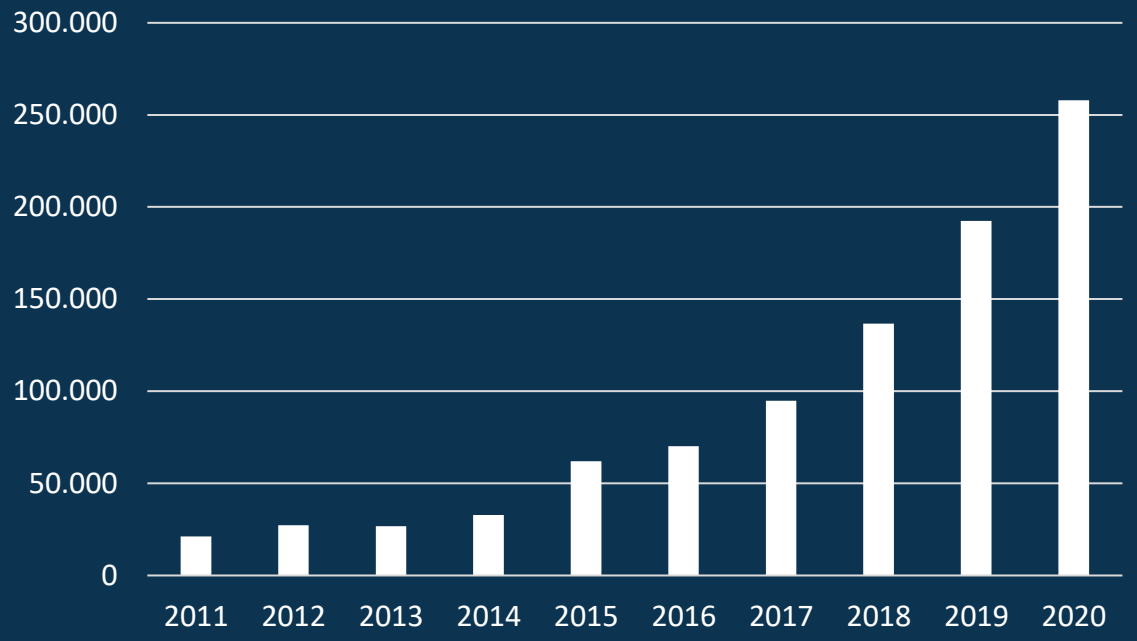
The **Spanish National Cybersecurity Institute** (INCIBE), focuses on cybercrime research, prevention and development of the cybersecurity industry of Spain. INCIBE has launched 017, a national, free and confidential cybersecurity service for companies and consumers to help solve cybersecurity problems. 017 can be reached by email, phone, Telegram & Whatsapp. INCIBE reported 109,126 incidents in 2021. A sharp drop from 133,155 incidents in 2020. 30% of these were related to malware, 28.6% to fraud, and 19% to unauthorized access of a system.

The Ministry of Internal Affairs reported 287,963 cybercrimes in 2020. 89% or 257,907 cases were related to online fraud. Nearly 61 percent of all internet scams in Spain defrauded amounts under 100 euros that year. In contrast, only 3.3% of the surveyed population had suffered an economic loss that amounted to 1 thousand to 5 thousand euros in the first semester of 2020.

The **Department for National Security (DSN)** reports that computer related fraud are increasing significantly and steadily, especially investment & cryptocurrency scams.

The **Association of Spanish Companies Against Fraud,** a non-profit organization to coordinate the exchange of anti-fraud knowledge and data to protect both consumers and companies, estimates 1 billion was lost in fraud in Spain, 75% of this was online.

Online Fraud Cases Reported to Spanish Law Enforcement



Key Statistics:

Population:	47 million
Internet:	90%
# of Scams:	257.907 (34%)
Scams / 1,000 :	5,54
Money lost:	€ 750 million
Per capita:	€ 15,85
Per report:	€ 2,908

Key Organizations:

- Incibe | CCN-CERT
- Policia Nactional |Guardia Civil
- Department National Security (DSN)

WhoisXML API:

Domains/capita	0.049
Domains registered	2,364,653
TLD registrations	2,211,718

*ScamAdviser Expert Estimate

estadisticasdecriminalidad.ses.mir.es/publico/portalestadistico/
https://www.dsn.gob.es/es/documento/informe-anual-seguridad-nacional-2020

In Catalonia alone, 80,000 scams were registered in 2022

Interview with Mr. J.A. Merino, Deputy Inspector, Chief of the Financial Crime Department, Mossos d'Esquadra

Mossos d'Esquadra is the regional police force of Catalonia. It is a police force that serves a population of more than 7 million people, and has units specialized in the fight against cybercrime and especially internet scams.

Every year, more than 80,000 scams are registered in Catalonia, 90% of which are computer scams. In fact, scams are the second most reported type of crime in Catalonia, only behind theft, and they are also experiencing an exponential increase year after year of between 3% and 5%.

Although there are many different types of internet fraud, the highest volume of complaints are related to CNP (Card Not Present), phishing/smishing scams, fraud through the sale of products and services on websites and false property rentals.

Similarly, special attention needs to be paid to cybercrime types that also have a high incidence due to the serious economic damage they generate, such as ransomware, false investments and impersonation of service providers, which target public and private companies.

On the other hand, for some time now, the impact of new technologies in the current criminal scenario has also been studied, such as cryptocurrencies, whose illicit use accounts for more than 1,000 complaints every year.

Finally, the Mossos d'Esquadra police force is also giving a strong impetus to actions that allow progress in the field of prevention, as education and awareness-raising, especially at an early age, is essential to reduce the impact of cyber-scams on citizens.

Mossos d'Esquadra

In Sweden, fraud is declining but online fraud is growing

Online scams now constitute 2/3 of all fraud crimes reported and 13% of all reported crime

Online fraud can be reported to the **Swedish police** at their offices, via email or online. You can also call 114 14 and if the crime is in progress, the general alarm number 112.

In 2021, 1,480,577 offences were reported to the police, the customs authority or the prosecution service. This represents a decrease of 86,315 reported offences by comparison with the figure for 2020. In particular, a decrease was noted in the offence categories theft offences and fraud offences. The number of reported fraud offences decreased by 10 per cent since last year, with 195,902 offences being reported. The types of crimes in fraud offences for which the number of reported offences decreased the most between 2020 and 2021 were payment card fraud and identity fraud.

According to the Swedish Crime Survey, 2021 of the population (aged 16–84), 5.5 percent state that they were victims of sales fraud in 2020. The proportion is larger compared to 2019 (5.1 %), and an increasing trend can be seen since 2016 when the percentage of self-reported victimization was 4.5 percent. Self-reported victimization due to card/credit fraud amounted to 4.1% of the population (aged 16–84) in 2020 down from 5.3% in 2019. In 2021, 32% of the population (aged 16–84) state that they are concerned about being a victim of fraud on the internet, which is at the same level as 2020.

While the number of online scams have dropped, the money lost has increased. During the first half of 2021, the profits made by fraudsters are estimated to have increased by 186 per cent, compared with the same period in 2020.

Key Statistics:

Population:	10.4 million
Internet:	92%
# of Scams:	131,254 (-10%)
Scams / 1,000 :	12.6
Money lost:	$ 501 million*
Per capita:	$ 48
Per report:	$ 3,815

Key Organizations:

- Swedish Police

WhoisXML API:

Domains/capita	0.049
Domains registered	2,364,623
TLD registrations	2,211,718

bra.se/bra-in-english/home/crime-and-statistics/crime-statistics.html
bra.se/download/18.1f8c9903175f8b2aa7011256/1633959998072/2021_Swedish_Crime_Survey_2021.pdf
riksbank.se/en-gb/payments--cash/payments-in-sweden/payments-report-2021/2.-safety-and-efficiency/are-payments-in-sweden-safe/new-types-of-fraud-increasingly-common/

The number of cybercrime cases roughly doubled in 2021

The NCSC received an impressive 21,714 reports in 2021, roughly double the previous year's number of 10,833.

Switzerland is a confederation of 26 cantons. As a result, Swiss citizens can report online fraud to the police agency of their canton.

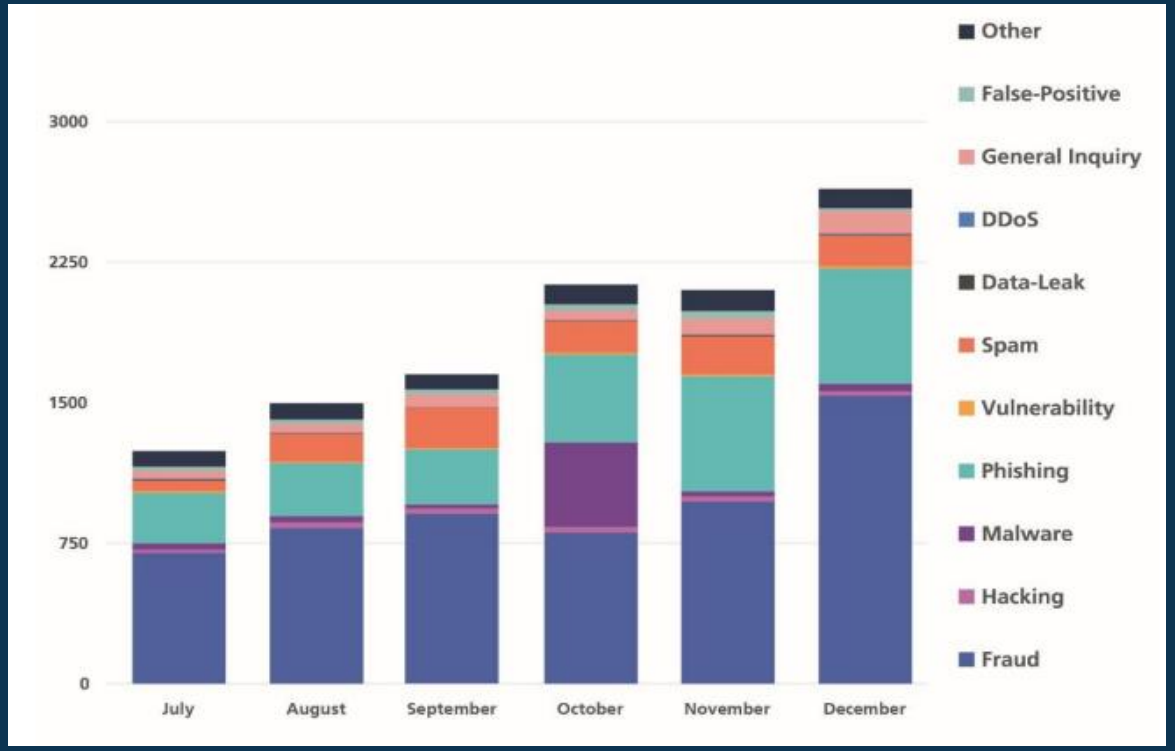
The **Nationale Zentrum für Cybersicherheit** (NCSC) is gaining a more central role in reporting online fraud, in the analysis of the phenomenon, and in the prosecution. Both consumers and companies can report any kind of cybercrime to the center, from DDOS attacks and digital extortion to advanced fee fraud. In 2018, the Netzwerks digitale Ermittlungsunterstützung Internetkriminalität (NEDIK) was set up to work closely with NCSC in the collection of cybercrime-related data and the coordination of cybercrime cases across all cantons.

The **Swiss Crime Prevention** (SKP) is an inter-canton specialized agency in the field of prevention. It offers information to consumers on several topics including Internet-related crimes and fraud.

In addition, the **Cyber Crime Police**, an initiative of the Canton police of Zurich, informs German-speaking consumers about online scams and cyber-related incidents. Other cantons are developing special consumer awareness sites as well.

As in the previous year, the incidents most frequently reported to the NCSC in 2021 were cases of attempted fraud. There was a total of over **11,300 reports**. Whereas fake sextortion dominated in the first half of the year and numerous waves of it were observed. From October on, there was then a sharp increase in reports of threatening emails purporting to be from the criminal prosecution authorities and demanding payment of a fine or deposit. Other frequently reported categories in 2021 included advance payment scams (2,704), investment fraud (397), CEO fraud (394) and classified ad fraud (820).

Reports to the NCSC in the second half of 2021



Key Statistics:

Population:	8.7 million
Internet:	91%
# of Scams:	15,221 (42%)
Scams / 1,000 :	1.75
Money lost:	$ 426 million*
Per capita:	$ 49
Per report:	€ 28,053

Key Organizations:

- Zentrum für Cybersicherheit (NCSC)
- Swiss Crime Prevention (SKP)
- Cyber Crime Police,

WhoisXML API:

Domains/capita	0.117
Domains registered	1,014,548
TLD registrations	2,669,953

https://www.ncsc.admin.ch/ncsc/en/home/dokumentation/berichte.html
bfs.admin.ch/bfs/en/home/statistics/crime-criminal-justice/police/digital-crime.html

* ScamAdviser Estimate

In 2021, the money lost in Taiwan to scams grew with 61%

A browser extension has been launched by 10 organizations to better protect consumers

Consumers can report scams to the **Taiwan National Police**. This can be done via the local police office, via phone, mobile app and online. The police has also launched a **separate website** to warn the public about scams and allow easy reporting.

According to **Trend Micro**, more than 24,000 online scams were reported in 2021, a small increase of 4%. The amount lost grew however much faster from NT$3.1 billion in 2020 to NT$ 5 billion in 2021. A growth of 61%.

The police is working closely together with Trend Micro, the country's largest Cybersecurity company. Together with 10 partners, it has launched a **browser extension** to help consumers stay safe. The browser extension blocks malicious websites and links, cleans up harmful browsing history and identifies fake news and rumors.

Another innovation has been the integration of a scam check bot into Line. Line can be compared to WhatsApp and is extremely popular in Japan, Taiwan and several other, mainly South Asian countries.

Users can add the scam check bot to a Line group as friend. The bot will monitor the conversation and alert all users in the group if dubious links are placed.

Another development has been that Taiwanese citizens have been tricked by human traffickers. The traffickers, many connected to well known triads, are targeting mostly young Asian people via social media, offering well paid work and accommodation in countries like Cambodia, Thailand, Myanmar and Laos. On arrival, their passports are taken, and they are sold to different groups and forced to work in offices running illegal phone or online scams. Taiwan authorities say almost 5,000 citizens have been recorded travelling to Cambodia and not returning. Police said they had identified at least 370 of them as being held against their will, but victims have said the number is likely to be much higher.

Trend Micro has launched a browser extension with 10 partners to keep Taiwan consumers safe

Key Statistics:

Population:	23,6 million
Internet:	93%
# of Scams:	24,000 (4%)
Scams / 1,000 :	1.0
Money lost:	$ 168 million
Per capita:	$ 7.13
Per report:	$ 7.000

Key Organizations:

- National Police

WhoisXML API:

Domains/capita	0.014
Domains registered	333,516
TLD registrations	2,745,510

Sources: Trend Micro
theguardian.com/world/2022/aug/23/hundreds-of-taiwanese-trafficked-to-cambodia-and-held-captive-by-telecom-scam-gangs

Tanzania

Interview with Shubert Mwarabu, Program Coordinator, Alliance to Counter Crime Online

Nearly half of the population in Tanzania now has access to the Internet, by far the largest part online via mobile. Many people are looking for bargains on the Internet, especially during the Corona epidemic.

There have been several online scams in Tanzania. One of most common is the job scam. In a recent job scam 500 people were scammed. They received messages via text and Instagram, inviting them to a seminar about network marketing. They were promised a salary of 700,000 shilling monthly. To attend the mandatory training, new participants first had to pay a participation fee of 300,000 Shilling ($ 130). 500 Tanzanians arrived at the hotel near Kilimanjaro where the event was to be hosted. Only then it became clear they were scammed. The police gave the victims 48 hours to leave the region.

The hospitality and nature conservation sectors are likewise often being misused for job scams. People are offered attractive salaries for working in these sectors. Often a well-known person's name is misused in fake Instagram accounts. People are lured to first send money but never get employed. They claim a pilot will pick them up from, but they have to pay for the flight via mobile from Dar Es Salaam or Zanzibar. When the ‘flight’ of 350,000 Shilling is paid for, all contact is broken off.

Online shopping scams are also common. Not so much via online stores but via Instagram accounts selling products. Before the product is sent, the money has to be transferred via mobile payment. In the end, the product is never shipped. Finally, there are many loan scams. Many people are being contacted for micro credits, promising to give loans in 12 hours. Again, often fake credentials are used of well-known government officials. They request you to send your identity card and other personal information.

The Tanzanian government has established a permanent national committee to address the raising cases of online fraud. In collaboration with mobile phone service providers, the government has introduced a system through the number "15040“ to receive and lock the numbers that have been reported and confirmed to send messages or make fraudulent calls. Likewise, the Tanzania Communications Authority, has launched a campaign “Spread love and not scams”.

Shubert Mwarabu
Program Coordinator
Alliance to Counter Crime Online

Over 48% Thailand citizens were victims of fraud

There were over 48,513 complaints of online fraud filled in 2021 with over $44 million lost.

The **National Economic and Social Development Council (NESDC)** noted that over 6.4 million fraudulent calls were reported in 2021. This represents a 270% jump from the calls that were reported in 2020.

Fraudulent messages also rose by over 57% showing a growing trend in the phone and SMS scams. In 2021, 48,513 online complaints were filled, which is more than double from 2020 complaints.

Another NESDC survey found that nearly half or 48.1 per cent of the population has been scammed in some way or the other, of whom at least 42.6 per cent have been victims of financial fraud, losing approximately 2,400 baht ($64) per person.

The same study shows that Gen Y and Gen Z are the most vulnerable to online scams due to the amount of time they spend online. Baby Boomers are scammed less but have been found to suffer the highest amount lost.

Besides, more than half of the victims take little or no action because they believe the government's prevention/management methods are not effective enough.

For 2022, the number of scams and money lost increased strongly in the first quarter (see picture on the right). To increase the number of scams reported and fight scammers more, the **Ministry of Digital Economy and Society (DES)** in collaboration with the police's Technology Crime Suppression Division (TCSD) have launched an operation to help civilians report online crimes. Citizens can now report the cases in their local police stations, a feature that was not commonly available.

The Civil Court also opened a division that focuses on online shopping scams which allows citizens to file online petitions if they have fallen victims of online fraud.

The figures for march to May 2022 for Thailand predict a rapid growth for this year

Key Statistics:

Population:	70 million
Internet:	89%
# of Scams:	48,513
Scams / 1,000 :	0,69
Money lost:	$ 2.3 billion*
Per capita:	$ 32,63
Per report:	$ 898

Key Organizations:

- NESDC (Social development)
- DES (Ministry Digital Economy)
- TCSD (Police Tech Crime Division)

WhoisXML API:

Domains/capita	0.007
Domains registered	456,729
TLD registrations	113,199

Source: https://www.nationthailand.com/in-focus/40015882

* ScamAdviser Expert Estimate

A cryptocurrency exchange in Turkey was suspended freezing $2 billion

The trading platform has nearly 400,000 active users

In April 2021, the Turkish authorities raided offices in Istanbul associated with Thodex, a cryptocurrency trading platform, arresting more than 60 people. Cryptocurrency has gained a lot of popularity as Turkey suffers from double-digit inflation and an instable Lira which lost one-quarter of its value against the dollar in the last year.

Thodex promoted itself with ads that featured female Turkish celebrities dressed in bright red outfits and draped over a highly polished black automobile. Apart from Thodex, Turkish investors also lost money to other scams. In the 2021, Dogecoin scam investors lost over **$119 million**.

Phone scams were also quite popular with many senior citizen being targeted by scammers. Likewise, social media platforms are especially used by scammers. Hence, the Department of Cybercrime monitors 45 million social media accounts and receives around **3,000 complaints daily**. Online prostitution, drugs and betting are the most common cybercrimes followed by insulting state authorities.

To report cybercrimes, Turkish citizens may apply to the public prosecutor's offices, to the local police or gendarmerie stations (and to their cybercrime units where available) to the **Cyber Crimes Department of General Directorate of Security Affairs** and to the Presidential Communications Office **CİMER**. Citizens can physically make reports to the office of a public prosecutor or to local stations by stating their complaint verbally or in writing; they can also use the online module of the police department, or call “155”. CİMER complaints are done in writing, online or via post.

Key Statistics:	
Population:	85 million
Internet:	81%
# of Scams:	1.94 million
Scams / 1,000 :	23
Money lost:	$ 1.1 billion
Per capita:	$ 13.68
Per report:	$ 599

Key Organizations:

- Police Cybercrime Unit
- CIMER
- National Cyber Incident Response

WhoisXML API:	
Domains/capita	0.021
Domains registered	1,817,201
TLD registrations	448,531

dailysabah.com/turkey/istanbul/thefts-decreased-fraud-cases-rose-in-istanbul-in-2021
nytimes.com/2021/04/23/business/cryptocurrency-fraud-turkey.html
euronews.com/next/2021/08/27/how-an-alleged-dogecoin-scam-in-turkey-saw-crypto-investors-lose-100-million

Four in Ten UAE consumers have experienced online fraud attempts

39% of UAE consumers have experienced an online scam attempt

Consumers in the United Arab Emirates (UAE) can report any suspicious messages by phone (800 2626), text (2828), email (aman@adpolice.gov.ae) or through the Police smartphone app.

The police are trying to increase community awareness of the dangers of phone and online fraud through social media platforms to help people protect themselves against fraud.

The police also established a new call center through which the Criminal Investigations Directorate enables police officers to communicate directly with banks and receive reports of financial fraud and cybercriminals exploiting bank customers.

Through its new call center, the Abu Dhabi Police has returned **Dh18 million ($4.9)** to 375 people who have fallen victim to mobile scams and online crimes and reported financial fraud. Earlier in the year, the courts jailed over 79 persons for various fraud and money laundering scams.

According to the Head of the Digital Assets Crime Section at the Dubai Police, in the first half of 2021, there were hundreds of crypto scams in Dubai with **Dh80 million ($ 24 million)** lost in total.

Abu Dhabi Police's CID, said they had received **1,740 reports** or complaints of financial fraud through the new call center. Some of the most common scams are Phishing scams, credit card fraud, counterfeit goods and impersonating government officials.

For iths 5th edition of "Be Careful" awareness campaign, the Abu Dhabi Police showed a video of Maitha Muhammad sending a message to the community about the need to beware of telephone and electronic scams, stating that she had been scammed.

newsbeezer.com/uaeeng/a-girl-reveals-a-case-of-phone-scams-and-posts-a-video-of-the-incident/

Key Statistics:		**Key Organizations:**	
Population:	9.9 million	• E-crime, Dubai Police	
Internet:	89%	• Abu Dhabi Police	
# of Scams:	1740	• UAE Government Portal	
Scams / 1,000 :	0.17	**WhoisXML API:**	
Money lost:	$ 24 million	Domains/capita	0.042
Per capita:	$ 2.40	Domains registered	415,479
Per report:	$ 13,793	TLD registrations	247,587

khaleejtimes.com/uae/uae-dh18-million-from-mobile-scams-online-crimes-seized-returned-to-victims
ae.visamiddleeast.com/en_AE/about-visa/newsroom/press-releases/prl-11072021.html

A UK survey estimated 4.5 million fraud offences, a 25% increase

The numbers are based on the annual Telephone-operated Crime Survey (TCSEW) with UK citizens from March 2021 to March 2022

Large increases were seen in “advance fee fraud” and “consumer and retail fraud”. This may indicate fraudsters taking advantage of behavioural changes related to the coronavirus (COVID-19) pandemic, such as increased online shopping. For example, advance fee fraud offences included scams where victims transferred funds to fraudsters for postal deliveries.

Phishing is one of the main methods used to commit fraud. Half (50%) of TCSEW respondents reported receiving an email, text, or social media message that may have been phishing in the last month.

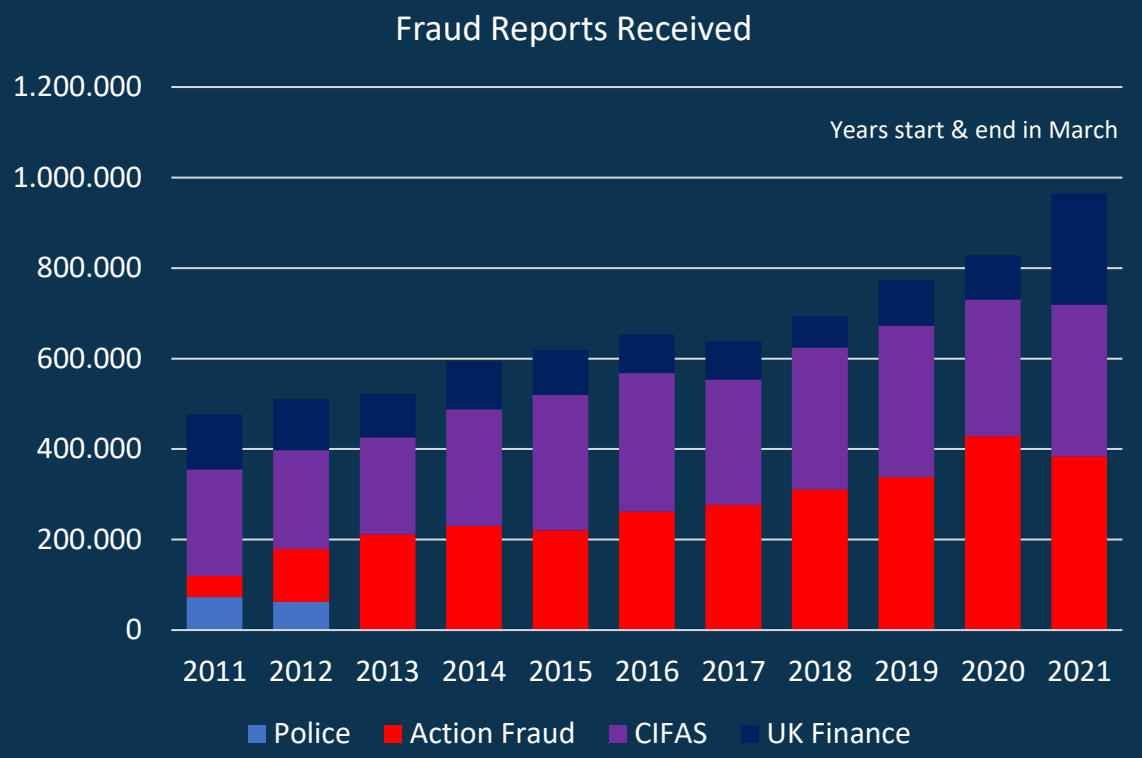
While the 4.5 million is based on an estimate. The actual reported number of fraud cases is much lower. Fraud is reported to 3 instances: Action Fraud, UK Finance and CIFAS.

Action Fraud is the UK's national reporting center for fraud and cybercrime. The service is run by the **City of London Police** working alongside the **National Fraud Intelligence Bureau (NFIB),** responsible for assessment of the reports. The City of London Police is the national policing lead for economic online crime.

Cifas is a not-for profit association with 500 members representing the private and public sectors and is dedicated to the prevention of fraud, including internal fraud, and the identification of financial crime.

UK Finance represents 300 banking and finance organizations. It seeks to enhance competitiveness, support customers and facilitate innovation.

The graph on the right shows the number of fraud cases received by the three organizations since 2011.



Key Statistics:	
Population:	67 million
Internet:	97%
# of Scams:	965,162 (17%)
Scams / 1,000 :	14.34
Money lost:	$ 3.3 billion
Per capita:	$ 41.79
Per report:	$ 2,915

Key Organizations:

- Action Fraud (NFIB) City Police
- Cifas
- UK Finance

WhoisXML API:	
Domains/capita	0.111
Domains registered	7,497,721
TLD registrations	19,822,070

cnbc.com/2022/03/09/britain-to-force-big-tech-to-combat-online-scams.html
ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/datasets/crimeinenglandandwalesappendixtables
ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/bulletins/crimeinenglandandwales/yearendingmarch2022#fraud

Other cybercrime-related organizations in the UK

Apart from the London Police, there are several other organizations involved in cybercrime awareness and combating

The **National Trading Standards eCrime Team** (NTSeT) monitors and investigates several online consumer and business frauds including website dating scams, misleading websites, subscription traps, and online shopping frauds. NTSeT is the owner of the **Friends Against Scams** initiative. More than one million people have registered as a Friend Against Scams. The site offers a short awareness session in person or online training and participants are asked to help and invite others.

Get Safe Online is a public-private sector partnership supported by organizations in banking, retail, internet security, and other sectors. Its website offers information on online safety. In addition, it organizes national events - such as Get Safe Online week - and works with law enforcement agencies and other bodies in support of their outreach activity, internal awareness, and customer online safety.

The **National Cyber Security Centre** was launched in 2016 and has as its mission to make the UK the safest place to live and work online. The center supports the most critical organizations in the UK, the public sector, companies, and the general public.

The **National Crime Agency** fights serious and organized crime threats including cybercrime and fraud. Key partners include the Serious Fraud Office, the City of London Police, the Metropolitan Police Service, the Financial Conduct Authority, and the National Cyber Security Centre.

Take Five to Stop Fraud in a national campaign to help everyone protect themselves from preventable financial fraud. It is led by UK finance. Stop Scams UK is an industry-led collaboration including communications, financial services and technology sectors. It is especially known for 159, the number you can call to connect directly to your bank.

www.actionfraud.police.uk/useful-organisations

The United States recorded $5.8 billion losses to online scams

The US continues to be one of the most targeted countries with losses increases from $3.4 billion in 2020 to $5.8 billion, a 70% jump

Americans can report online fraud to multiple agencies. From local law enforcement, to credit card companies and PayPal, the **Better Business Bureau**, **FBI Internet Crime Complaint Center (IC3)** or the **Federal Trade Commission** (FTC).

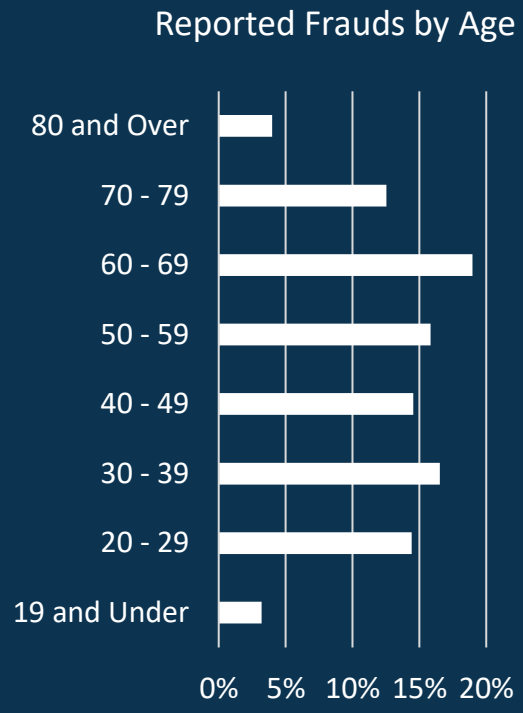
In 2021, the FTC received 2.8 million reports from consumers and law enforcement agencies, the highest ever since 2001. According to the FTC, the 5 most common scams were imposter scams, online shopping scams, prizes, sweepstakes, and lotteries; internet services; and business and job opportunities.

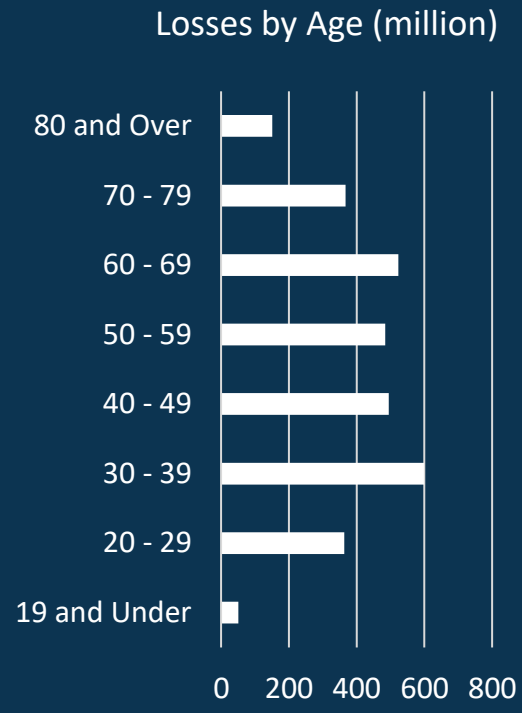
Imposter scams are the most common type of scams. Via its Consumer Sentinel Network, the data shows that consumers lost $2.3 billion to imposter scams up from $1.2 billion in 2020 with a median loss of $ 1,000. The phone (increasingly text messages) is the most common medium used by scammers. The most commonly misused payment methods are gift cards and reload cards.

Online shopping was the second most common scams (410,399 cases) with consumers losing $392 million up from $246 million the previous year. The median loss was $ 150 with top payment method being credit card and the preferred "scam medium" being website or app.

There were "only" 81,923 reported Investment scams with a total loss of $ 575 million and a median loss of $ 3,000. The most common payment method was cryptocurrency while the primary contact method were social media.

The FTC shares its data with 3,000 federal, state, and local law enforcers across the country. There are now 25 states that are now contributing to the Sentinel database, which shows collective effort to fight scams.





Key Statistics:

Population:	331 million
Internet:	94%
# of Scams:	2.8 mil. (24%)
Scams / 1,000 :	8.4
Money lost:	$ 5.8 bil (76%)
Per capita:	€ 17.48
Per report:	€ 2,071

Key Organizations:

- FBI IC3
- Federal Trade Commission (FTC)
- Better Business Bureau

WhoisXML API:

Domains/capita	0.386
Domains registered	128,029,365
TLD registrations	-

public.tableau.com/app/profile/federal.trade.commission/viz/FraudReports/FraudFacts
ftc.gov/news-events/news/press-releases/2022/02/new-data-shows-ftc-received-28-million-fraud-reports-consumers-2021-0

In 2021, Ukraine Cyber Police stopped 422 online scammers

SIM swapping scams are on the rise with accessing online loans and bank accounts

The **Cyber Police Department** is comprised of approximately 400 law enforcement officers and senior specialists, in every region of Ukraine at local cybercrime units. Ukrainian citizens can report online scams directly at Cyberpolice.gov.ua or by phone.

During 2021, the cyber police received more than 48,000 appeals regarding Internet fraud. The activities of 422 online scammers were stopped in 2021 criminal proceedings for fraud. More and more not individual criminals are involved in committing online fraud but organized criminal groups. Over the past year, the cyber police exposed 13 groups who committed 760 fraudulent actions.

Among the most common schemes: selling non-existent goods, phishing and phone fraud, asking friends for help on social networks, marketplace fraud, offering fake giveaways, mobile top-ups and P2P scams. Also, registration of online loans were often misused by fraudsters by gaining access to a SIM card and open a loan without the owner of the SIM card knowing.

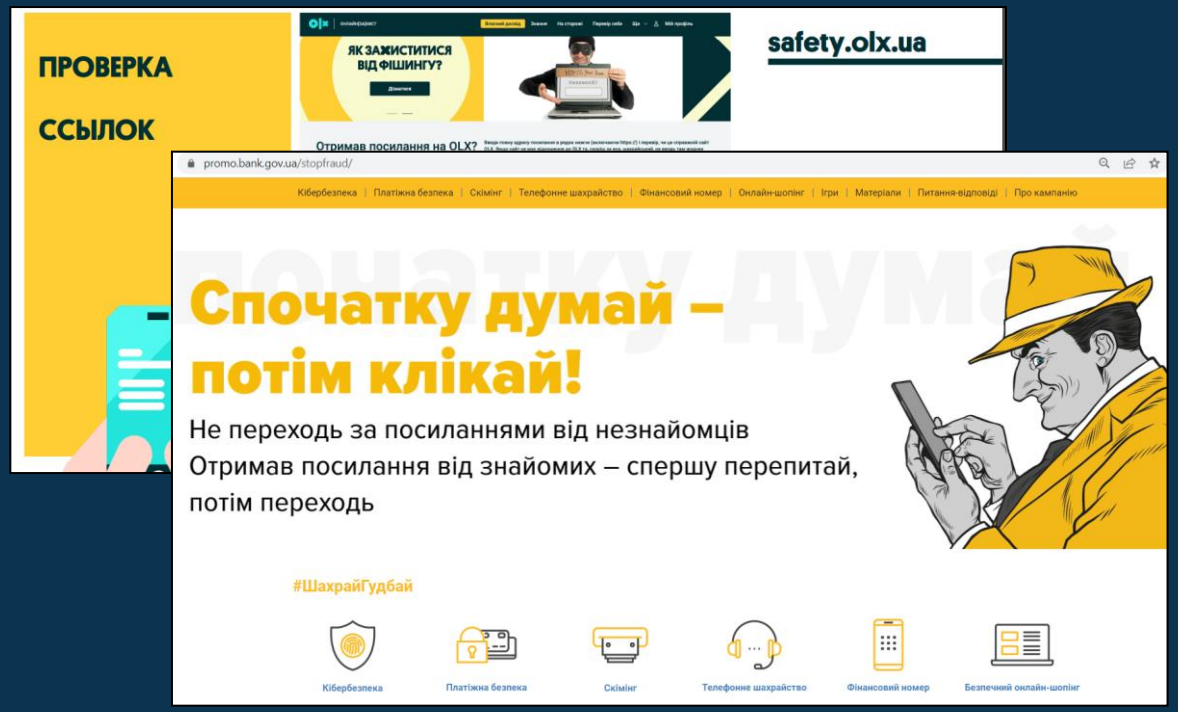
Another organization involved in fraud prevention is **Ukrainian Interbank Payment Systems Member Association** (EMA). EMA and its members (Ukrainian banks and PSPs) registered 209,016 victims' claims about online scams with a loss of 16,494,178 euro.

Several new actions have been undertaken to fight online scams: Firstly, the Ukrainian leading marketplace implemented a link checker to check if a link is legitimate or not. Secondly, a campaign was launched to popularize cyber hygiene and scams awareness by the National Bank of Ukraine, the Cyber Police, banks, mobile operators, marketplaces and PSPs. Thirdly, EMA launched an anti-fraud game for Ukrainian consumers called “Beat a fraudster”.

kmu.gov.ua/storage/app/sites/1/17-civik-2018/zvit2020/npu-zvit-2020.pdf

cyberpolice.gov.ua/news/u--roczi-do-kiberpolicziyi-nadijshlo-ponad--tysyach-zvernen-shhodo-shaxrajstva-v-interneti-8412/

A campaign was launched to popularize cyber hygiene



Key Statistics:

Population:	44 million
Internet:	93%
# of Scams:	209,016
Scams / 1,000 :	4.77
Money lost:	$ 16.8 million
Per capita:	€ 0.38
Per report:	€ 80.49

Key Organizations:

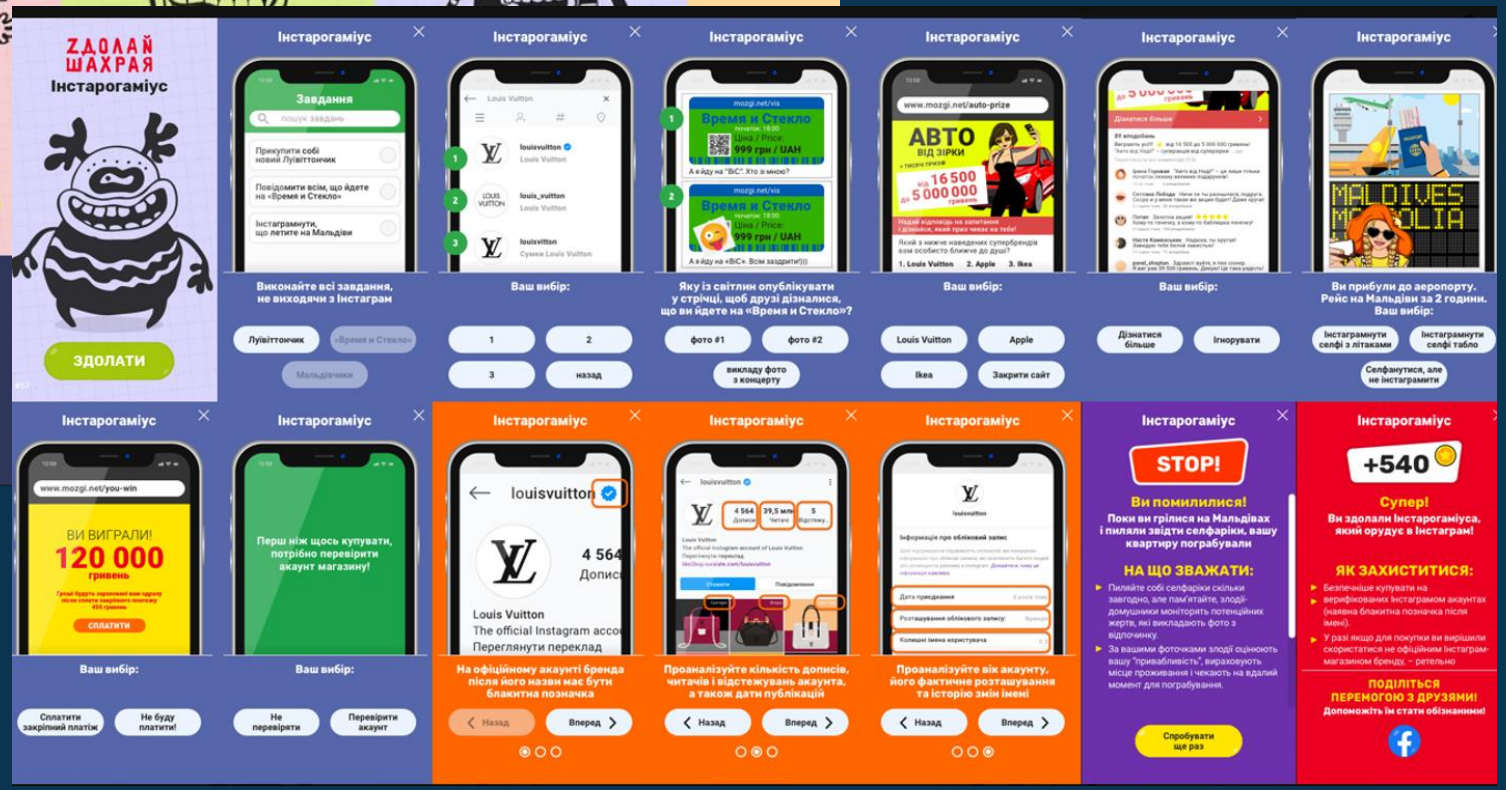
- Ukraine Cyber Police
- Ukrainian Interbank Payment Systems Member Association (EMA).

WhoisXML API:

Domains/capita	0.015
Domains registered	650,675
TLD registrations	931,443

Beat the Scammer Game was launched by EMA to build Scam Awareness

The game Beat the Fraudster can be found at https://game.ema.com.ua/



Vietnam has one of the highest fraud rates in Asia

Especially phishing attacks are increasing and becoming more and more professional

Next to phishing, three of the most common scams in Vietnam are financial scams, identity scams, and romantic scams. Online shopping scams and investment scams, especially through fraudulent apps and websites, are also very common.

Though the “big” cyber-attacks in Vietnam declined in 2021, online fraud continues to get more sophisticated. Vietnam is ranked top in email phishing attacks in South East Asia.

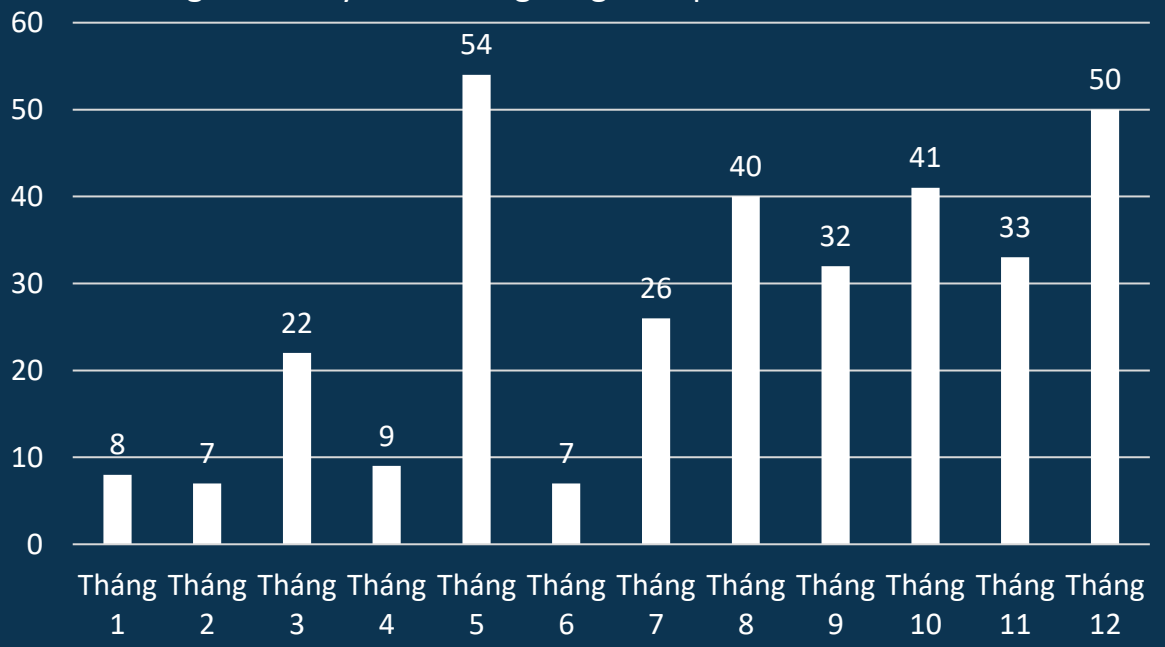
According to Group-IB (2022), there was a massive phishing campaign in which 27 financial institutions and at least 7,800 potential victims were involved in. The methods of scammers are becoming more sophisticated using channels such as SMS, Telegram and WhatsApp, and even comments on Facebook pages of legitimate Vietnamese financial service companies to drive traffic to their phishing pages.

The **National Cyber Security Center** (NCSC) focuses on the safety of Vietnam’s internet infrastructure, but the center also receives scam reports. **TINGIA** combats fake news and is maintained by the Ministry of Radio, TV and Electronic Information. The most common fake news included information about the Corona virus.

There are various private initiatives through which consumers can search and report online scams as well, such as **Chong Lua Dao**, **Coc Coc** and **ScamVN**.

In 2021, 113,384 websites were reported to Coc Coc, ScamVN and to Chong Lua Dao, and 22,518 websites were blacklisted.

Phishing Attack Dynamics targeting Group-IB clients in Vietnam in 2021



Source: Group-IB

Key Statistics:	
Population:	98.51 million
Internet:	71%
# of Scams:	87,302 (15%)
Scams / 1,000 :	0,89
Money lost:	$ 374 M. (90%)
Per capita:	€ 3.81
Per report:	€ 4,288

Key Organizations:

- National Cyber Security Center
- TINGIA
- Chong Lua Dao, ScamVN, Coc Coc

WhoisXML API:	
Domains/capita	0.009
Domains registered	953,696
TLD registrations	562,610

Sources: Chong Lua Dao, ScamVN and Group-IB

SCAMADVISER

About this Report

GASA
Global Anti-Scam Alliance

Who are we?

The Global Anti Scam Alliance (GASA) is a non-profit, bringing together policy makers, law enforcement, consumer authorities, NGOs, brand protection, cybersecurity, and commercial organizations to share insights and knowledge surrounding scams.

ScamAdviser.com checks the likelihood of a website being legit or a scam for more than 4 million consumers monthly. More than 1 million new domains are added to our database every month. Via our Data Partners, we protect more than 1 billion consumers worldwide.

About The Authors

Jorij Abraham
General Manager

Jorij Abraham has been active in the ecommerce community since 1997. He was, among others, an Ecommerce Manager at de Bijenkorf, TUI and Sanoma Media and Director of Consulting at UNIC.

From 2013 to 2017 he has been Research Director at Thuiswinkel.org, Ecommerce Europe (the Dutch and European Ecommerce Association) and the Ecommerce Foundation.

Nowadays, he is professor at TIO University and General Manager of the Global Anti Scam Alliance & ScamAdviser

Adam Collins
Scam Researcher

Adam Collins (not his real name due to security measures) has been working for ScamAdviser for a year. His key roles are analyzing domains and identifying online scam networks and writing about them.

Before, Adam has been an active writer and researcher for many years doing Web Content Creation services for businesses and individuals across the globe.

Feedback is greatly appreciated. You can contact us at partner@gasa.org

Disclaimer
This report is a publication by the **Global Anti Scam Alliance** (GASA) supported by **ScamAdviser.com**, which also owns the copyrights for the report. Although the utmost care has been taken in the construction of this report, there is always the possibility that some information is inaccurate. No liability is accepted by GASA for direct or indirect damage arising from the use of information contained in the report.

Copyright

Global Anti Scam Alliance (GASA)
Keurenplein 41
UNIT A6311
1069 CD Amsterdam
The Netherlands
Email: partner@gasa.org
Twitter: @ ScamAlliance
Linkedin: linkedin.com/company/global-anti-scam-alliance