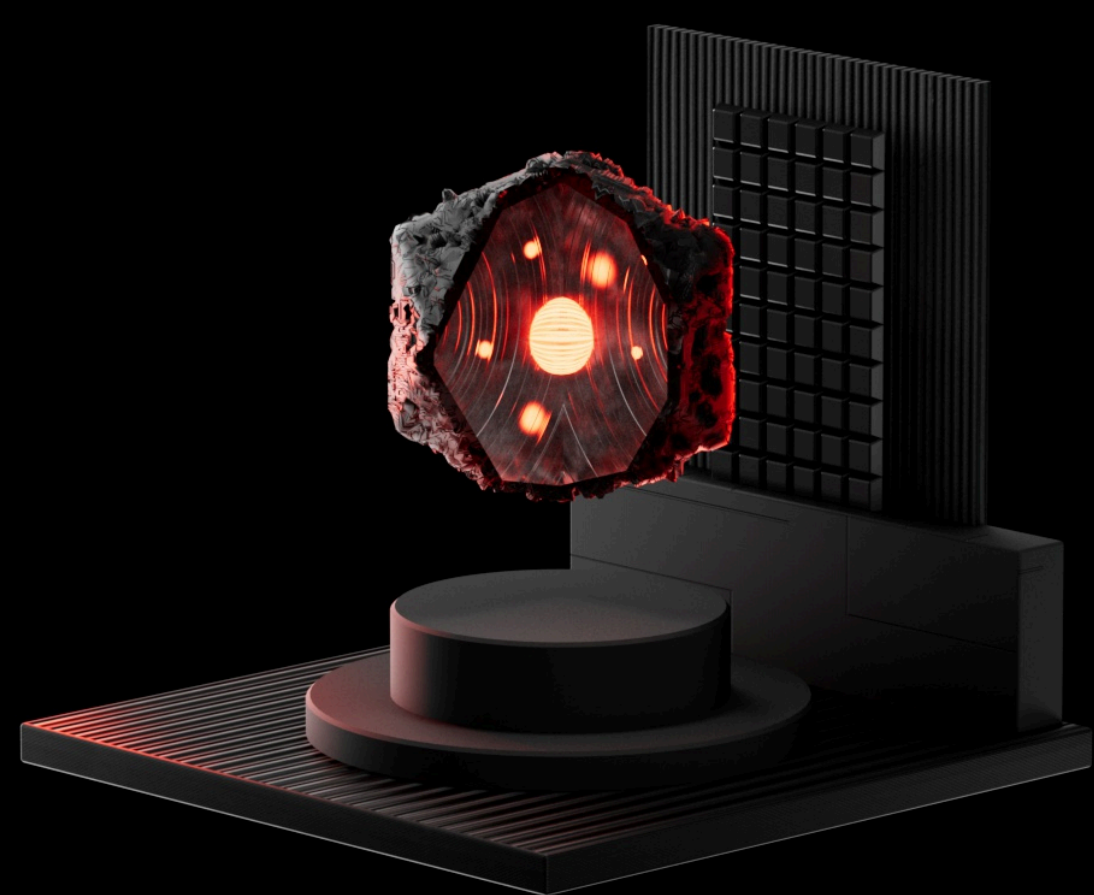




# Digital risk highlights 2025: Scams don't respect borders



# Global trends



Cybercriminals are scaling their operations worldwide by combining automation, AI, and social engineering to defraud individuals and businesses alike.

## \$1 trillion+

lost to scams globally  
each year (GASA)

## \$50 billion

in identity fraud expected  
in 2025 (SNAPPT)

## \$10.7 billion+

sent to fraud in 2024  
(TRM Labs)

## \$5.7 billion

lost to US investment  
scams in 2024 (FTC)

## \$2.7 million

lost to fake job offers in Q1  
2025 (BackOffice Pro)

## \$92 million

lost to impersonators in  
Australia (Anti-Scam Centre)

# Classiscam



Cybercriminals use Telegram bots to mass-generate fake courier and payment service pages designed to trick victims into disclosing their financial details.

More and more often, such operations are also used to deliver malware — especially remote access Trojans (RATs).

1,000+

active groups

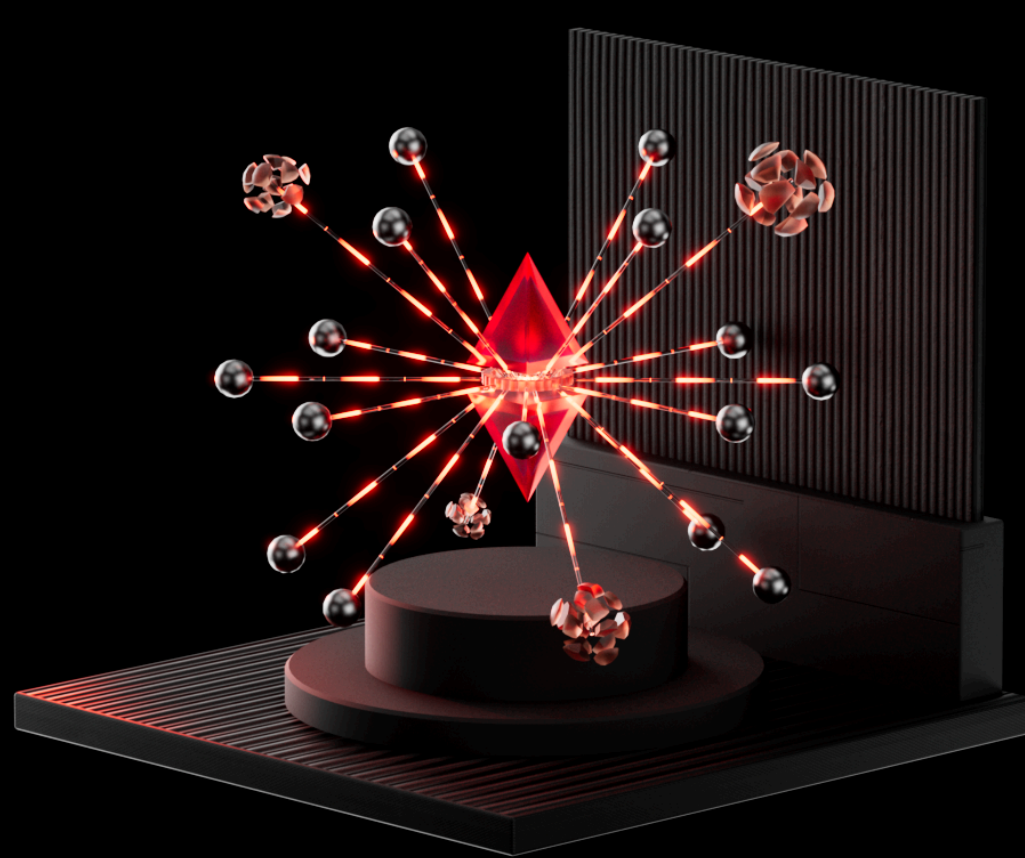
\$10,000  
–\$60,000

monthly profit  
per group

\$120 million  
to \$720 million

estimated total  
yearly damage

# Investment scams

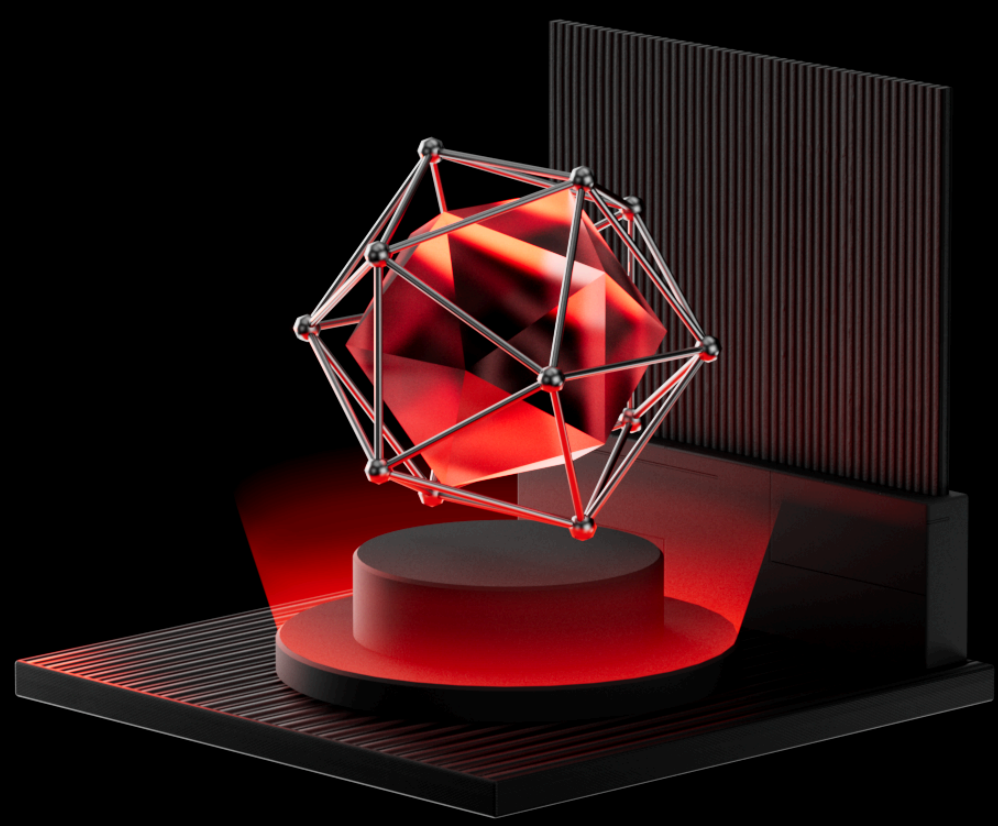


AI-generated scam websites, fake trading apps, and messaging app campaigns (“Pig Butchering”) lure victims with promises of high returns.

Once engaged, victims are manipulated into making repeated transfers — often losing all their savings.



# Lucky draw scams



Often tied to the Fangxiao threat actor, fake prize campaigns redirect users to malicious destinations — including adware, phishing sites, and malware installers.

**191 victims**



of Lucky Draw  
scams lost

**\$521,000+**



lost in Q1 2024 alone  
(Singapore Police)

## New levels of impersonation



**HR scams**

Fake job offers are used to collect personal data or extort “processing” fees.



**Identity theft**

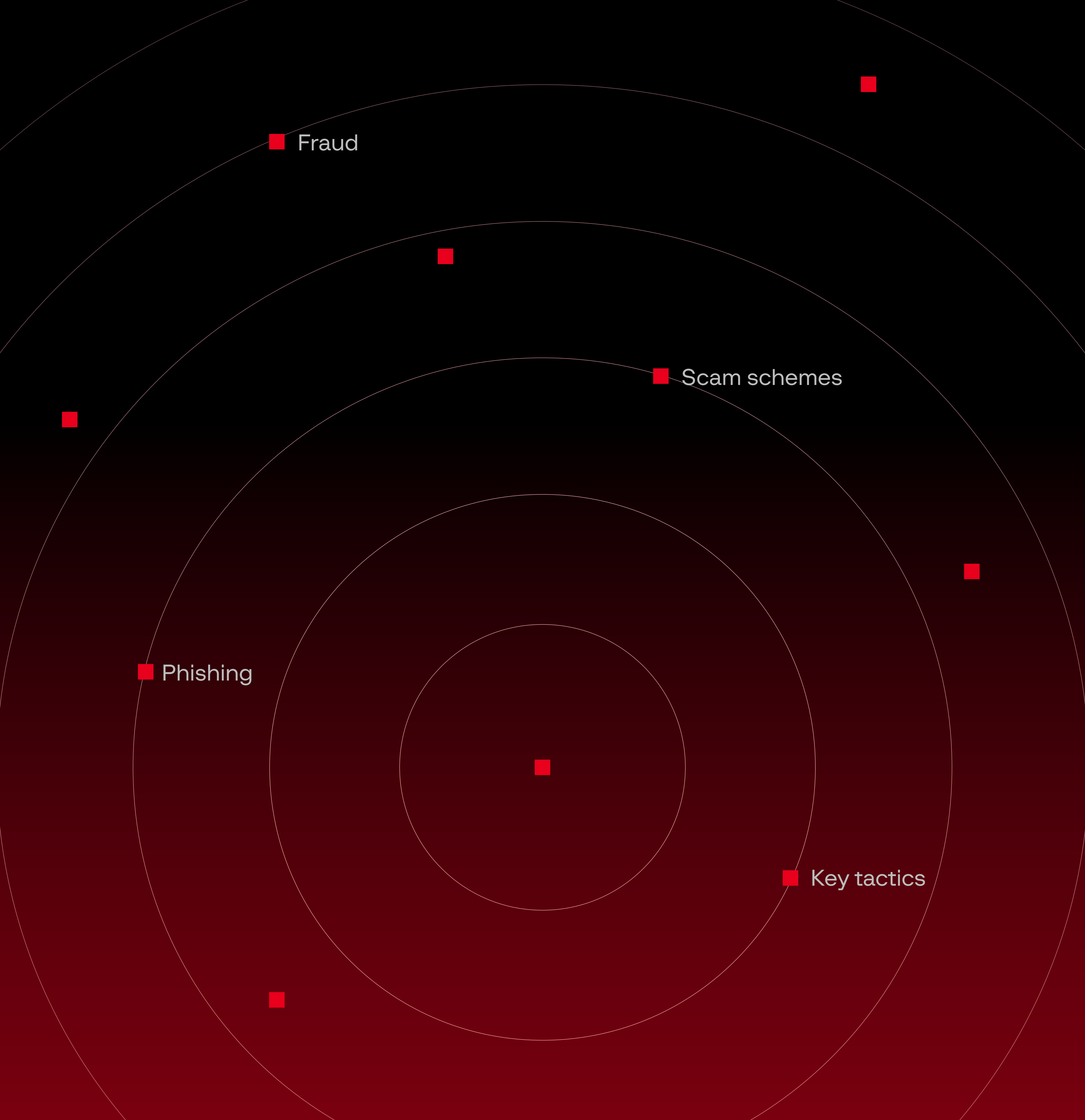
Attackers hijack or mimic celebrity and influencer accounts to appear more credible.



**Deepfakes**

AI-generated voices and videos are used to impersonate executives or public figures and commit fraud.

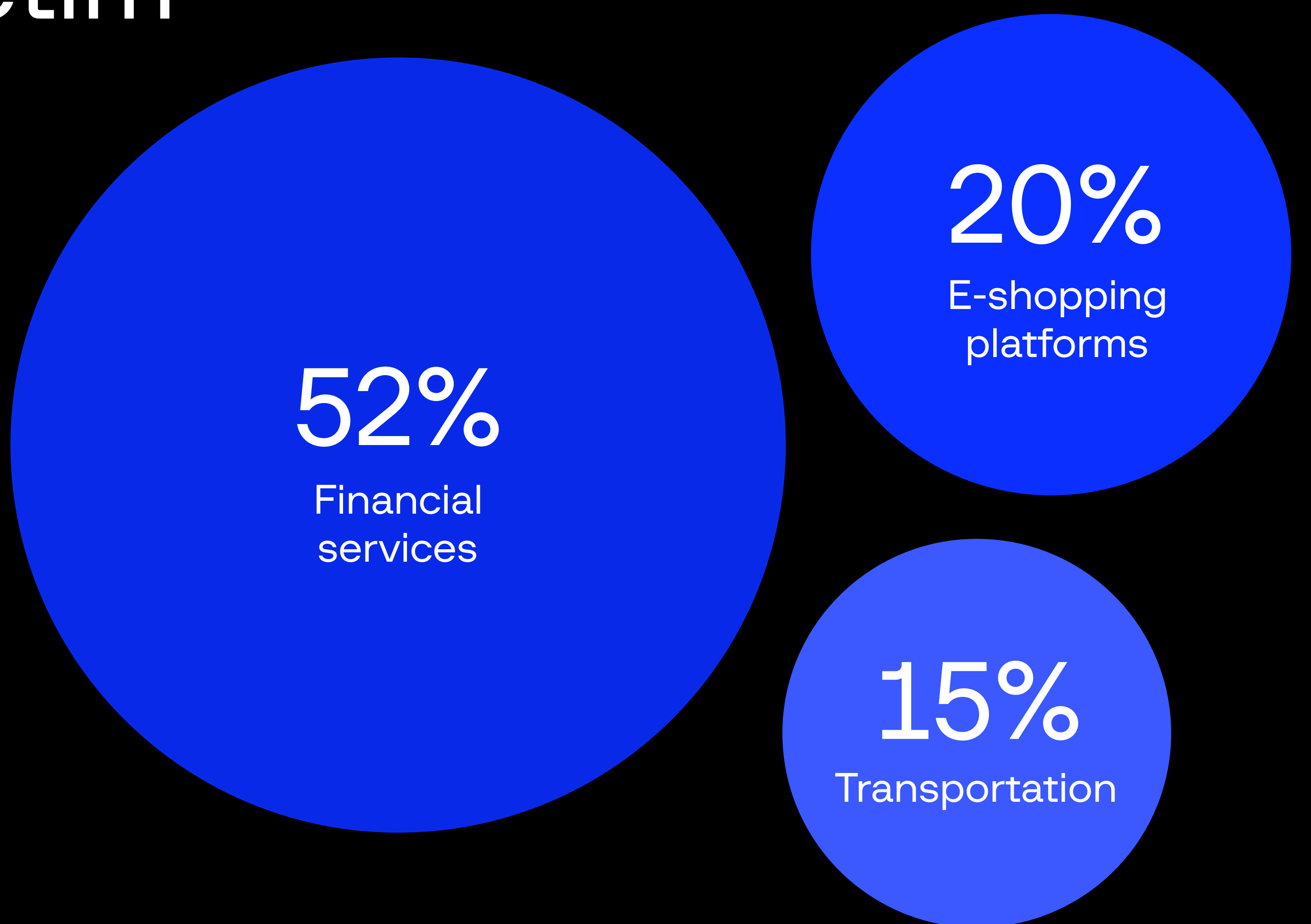




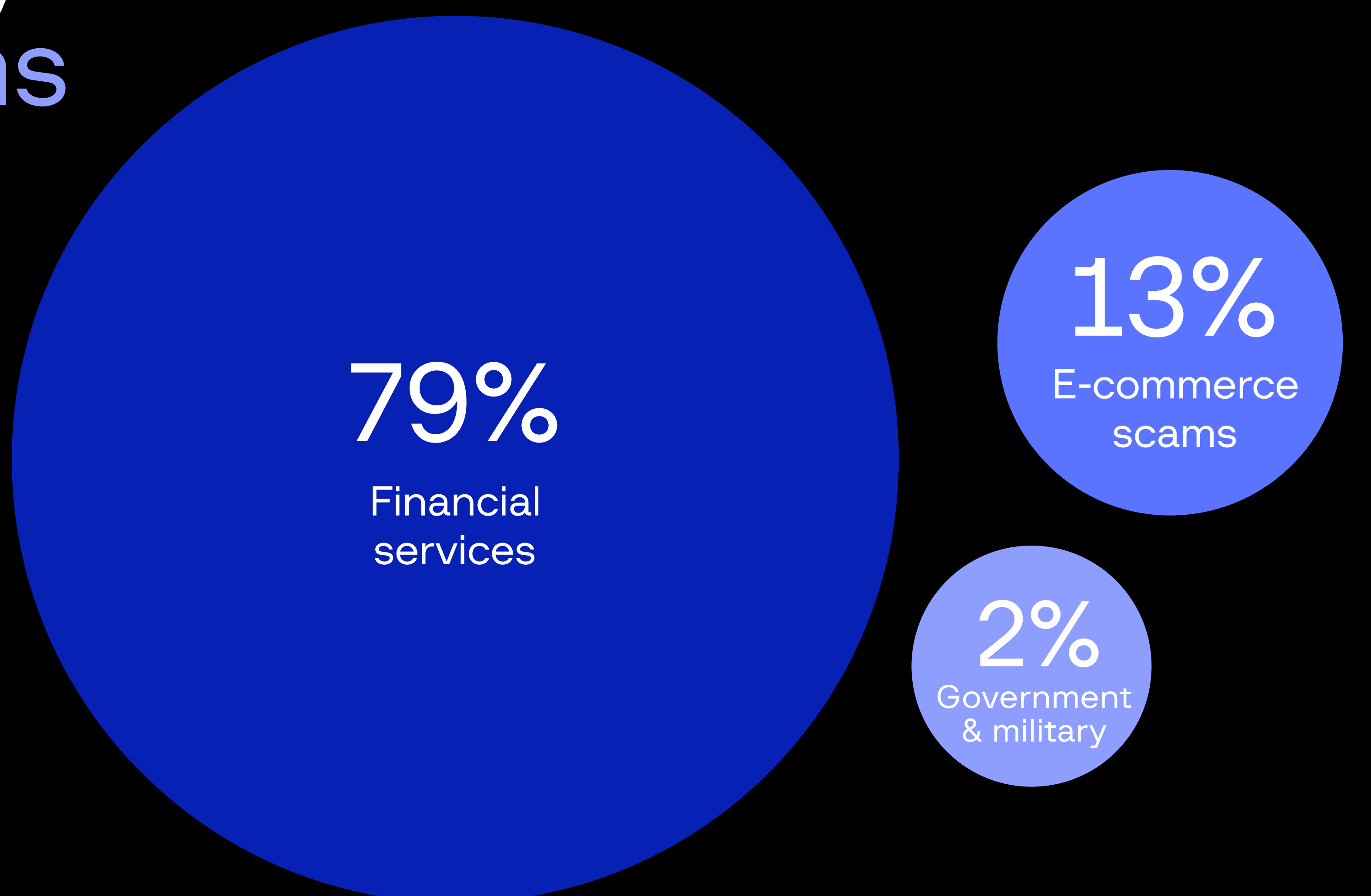
# Cyber threats reshaping APAC in 2025



# Who's falling victim to phishing?



# Scam economy: the main victims



# Key schemes



## Fake shops

Fraudulent online stores offer deals that are too good to be true but effective. Many people fall for them and lose money.



## Government scam

Fraudsters impersonate representatives of government agencies and threaten victims into surrendering money or sensitive information.



■ Fraud

■ Scam schemes

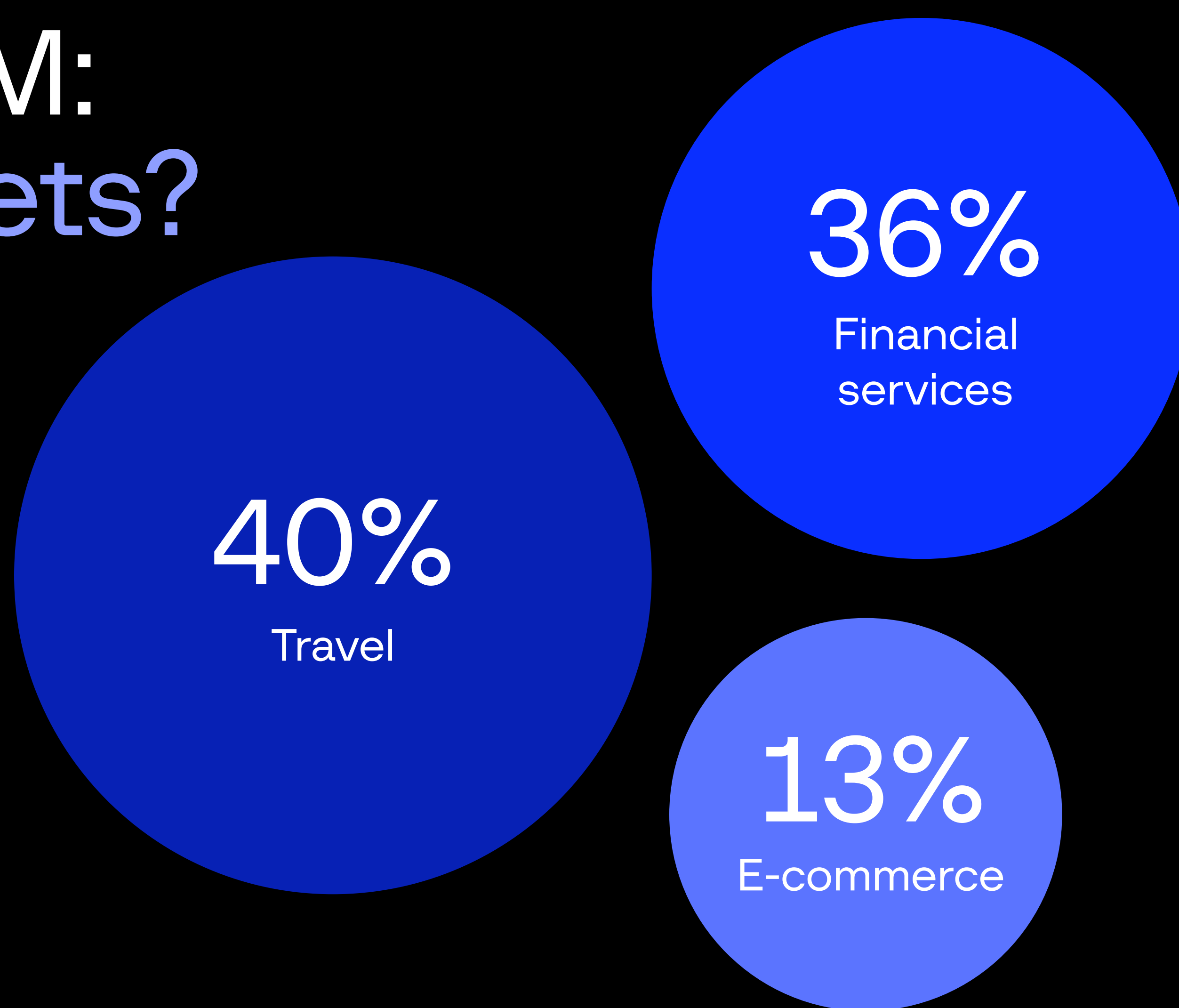
■ Phishing

■ Key tactics

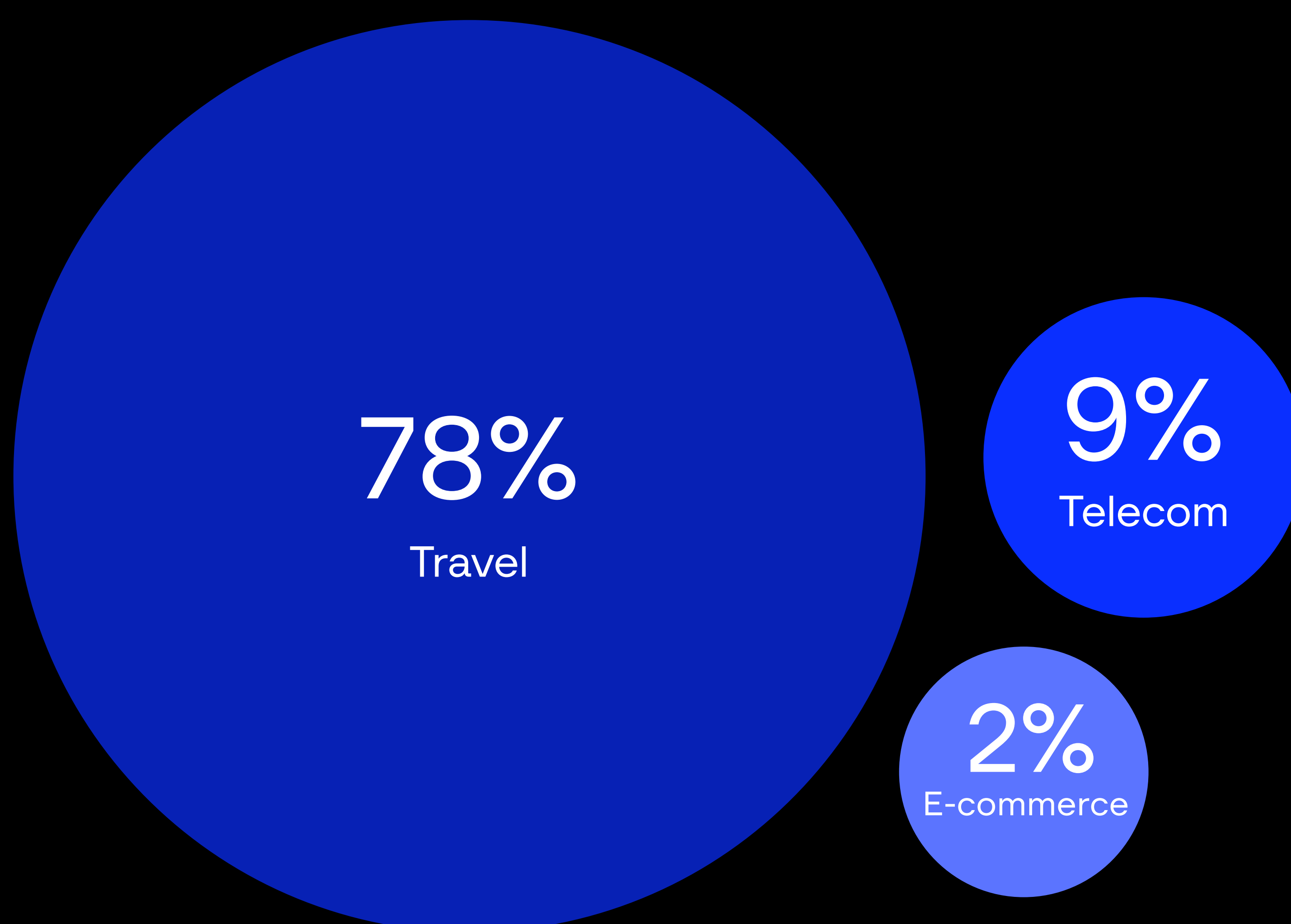
# Digital threats in Latin America: What you need to know



# Phishing in LATAM: Who are the targets?



## Scams at scale: Where the focus lies



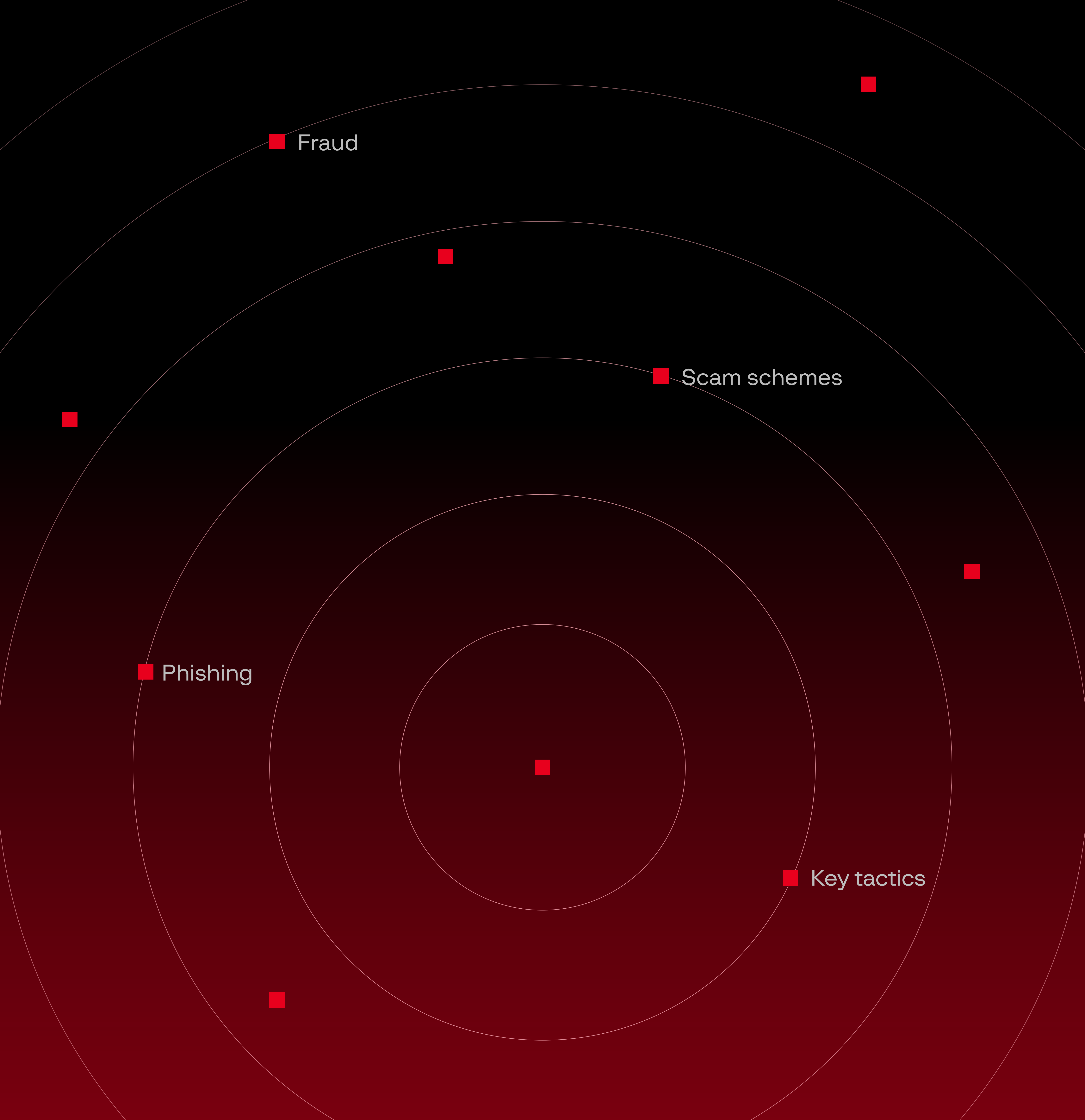
## Key tactics



Phishing content is now delivered only after it has been confirmed that the victim is a viable target — often by requesting a phone number, national ID, or other official data.

The “verification” step helps criminals avoid being detected by law enforcement and cybersecurity companies.

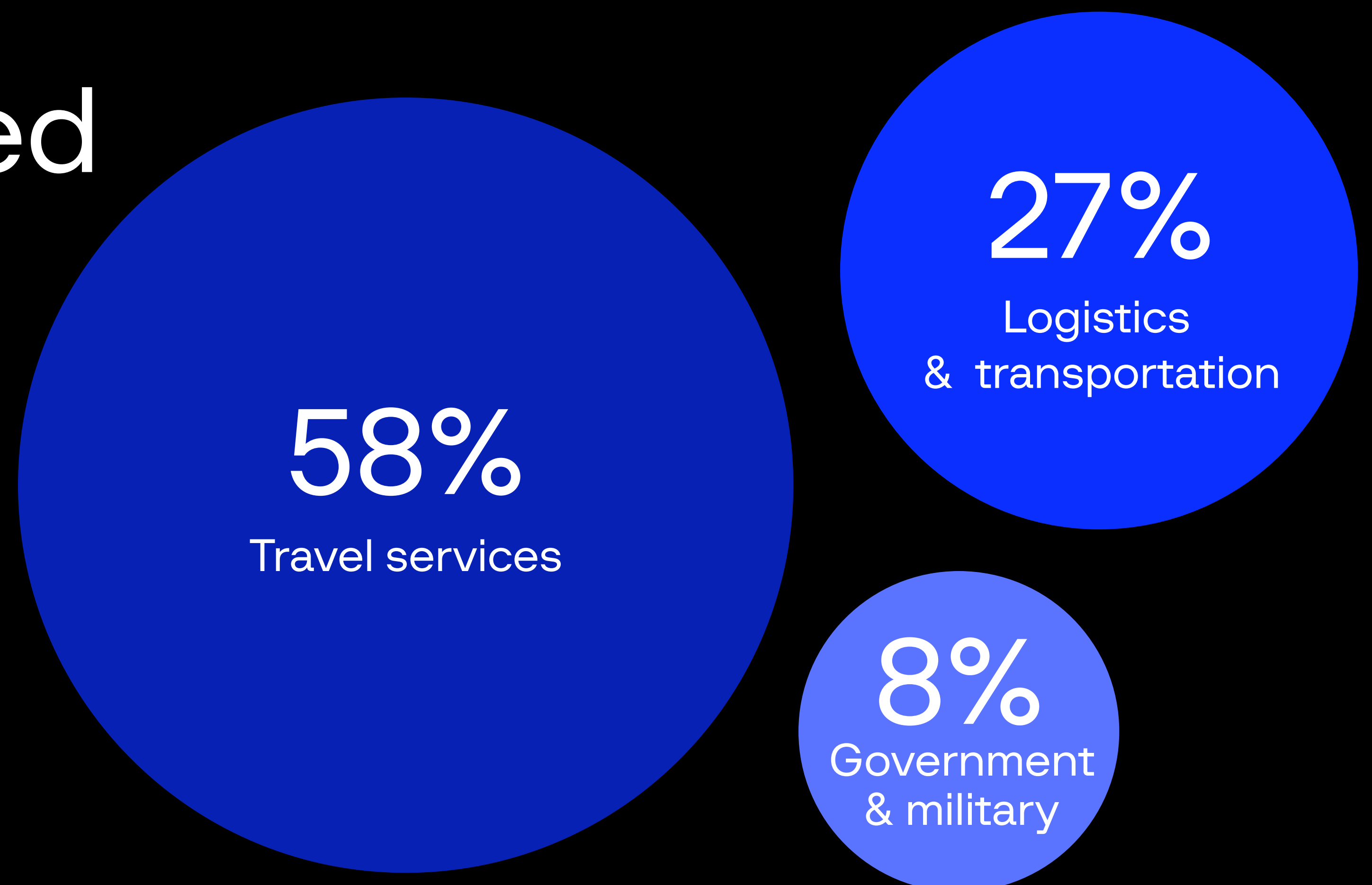




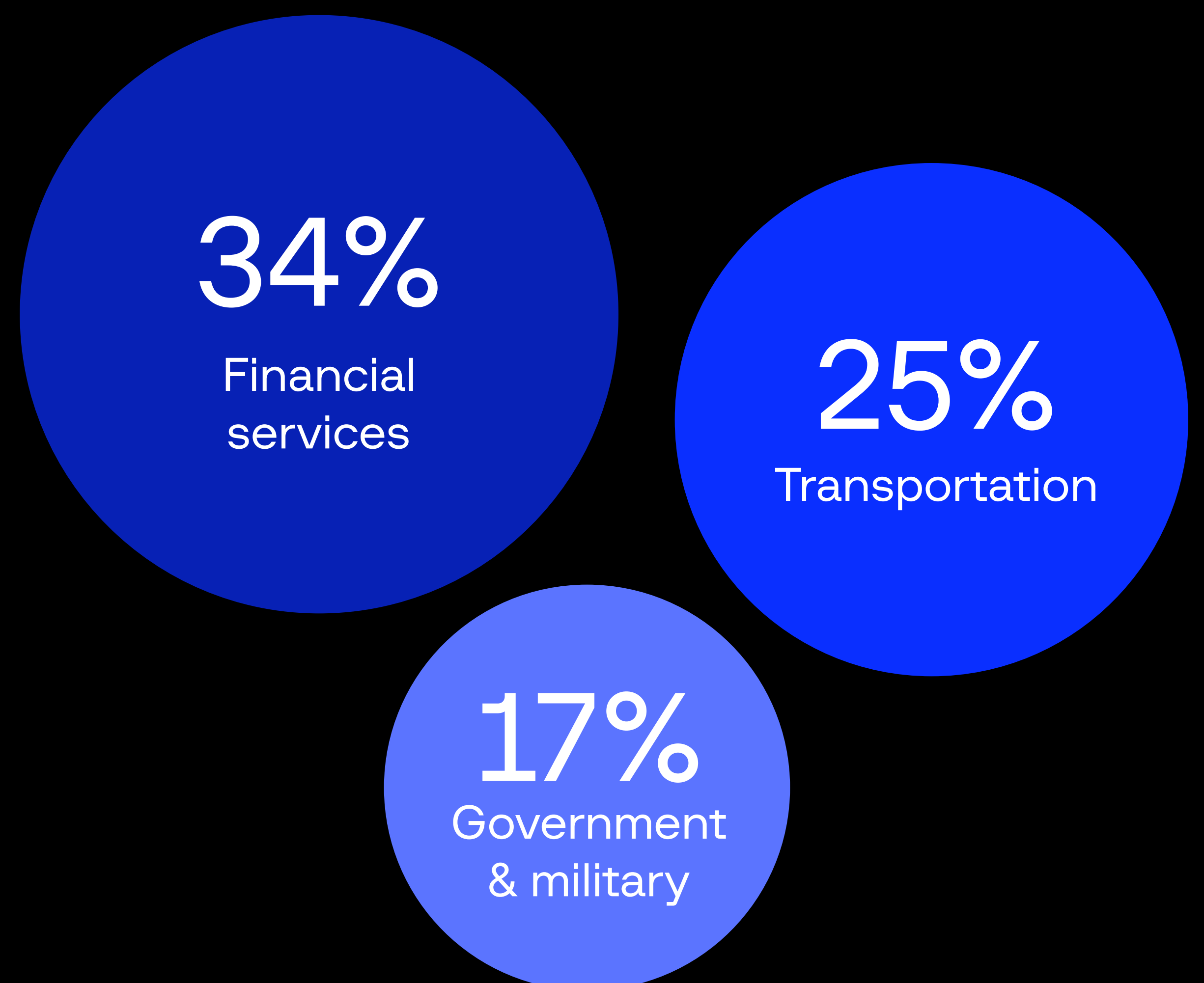
# Digital threats transforming Europe in 2025



## Europe: Top industries targeted by phishing



## Europe: Top industries targeted by scams



## Key scheme: Tax scam



Scammers impersonate representatives of tax authorities to deceive individuals into paying fake debts, disclosing personal information, and making money transfers under false pretenses.



■ Fraud

■ Scam schemes

■ Phishing

■ Key tactics

# Navigating the digital threat landscape in the Middle East and Africa

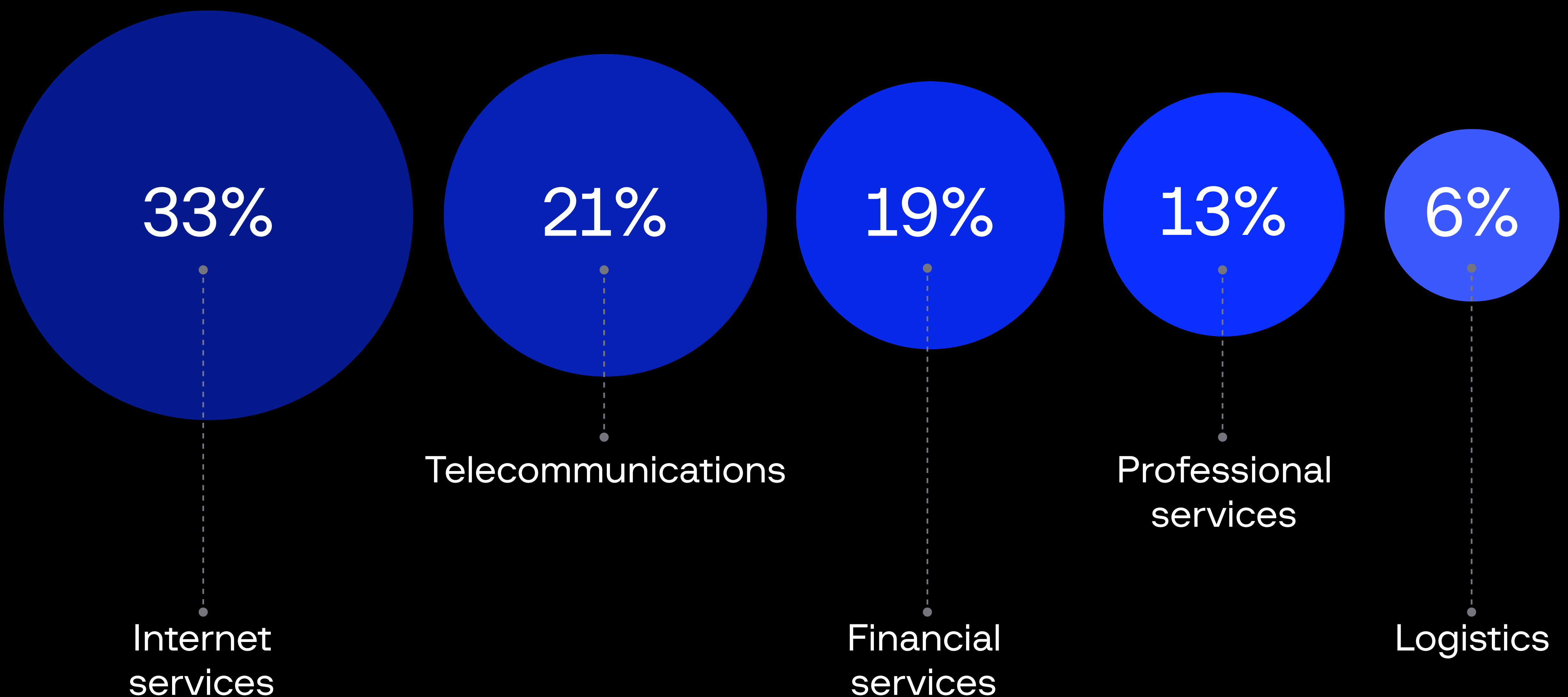


# Phishing attacks

Internet services are the most frequently targeted sector, reflecting cybercriminals' strategy of exploiting high-traffic online platforms.

Telecommunications and financial services follow closely, with professional services and logistics also facing notable threats amid the region's expanding digital ecosystem.

## Middle East and Africa: Top industries targeted by phishing attacks in 2024



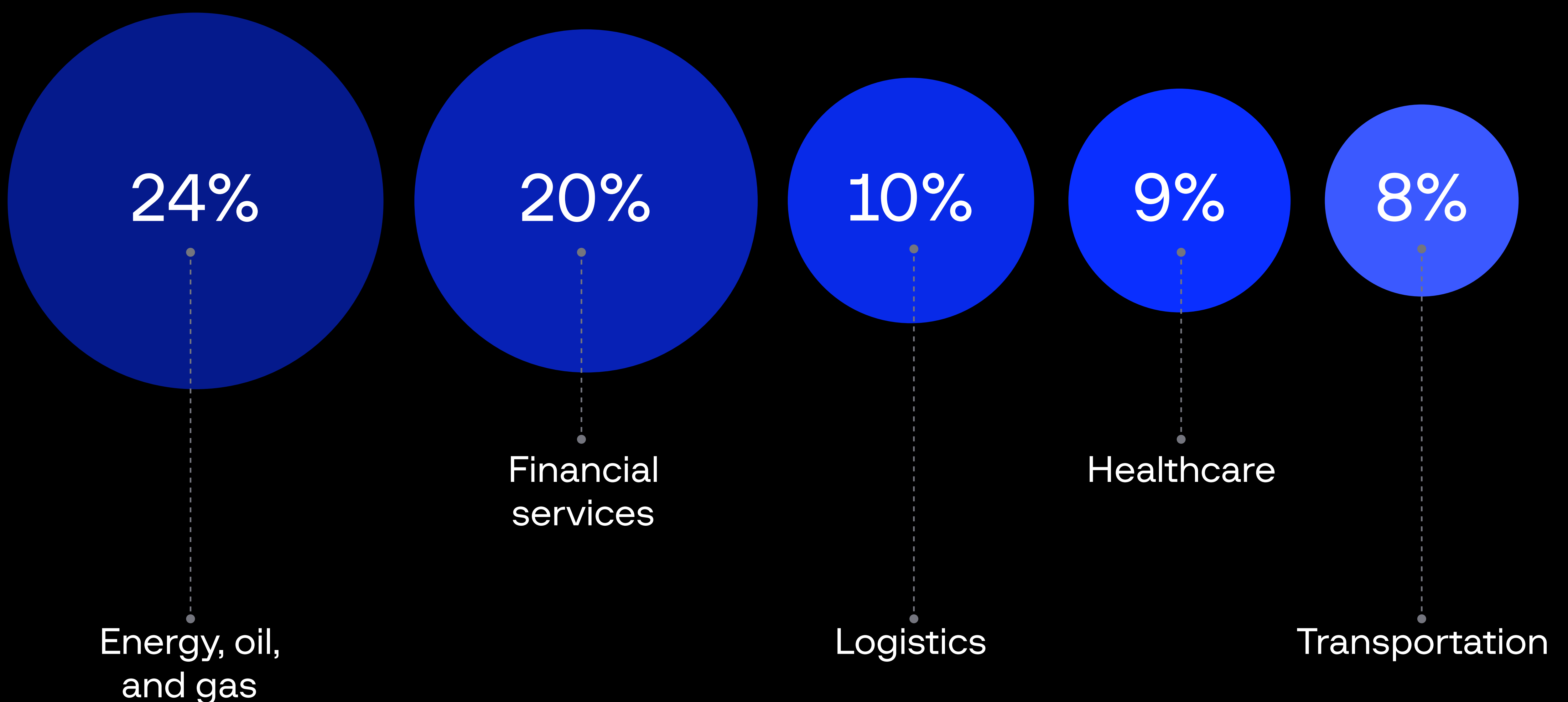


# Scams

Energy, oil, and gas top the scam targets, reflecting cybercriminals' focus on the region's economy, critical infrastructure and the potential for high-stakes disruption or ransom.

Financial services remain a close second, with attackers exploiting sensitive data and transaction-based systems, while logistics, healthcare, and transportation also experience significant scam activity aimed at both monetary gain and operational interference.

## Middle East and Africa: Top industries targeted by scams in 2024





# The most pressing digital threats in 2024

## VIP impersonation and deepfake fraud

Cybercriminals are leveraging AI-generated deepfake voices and videos to impersonate high-level executives and trick employees into transferring money or sharing sensitive data.

## Fake investment schemes

AI-generated scam pages and WhatsApp campaigns lure victims with “AI-powered” trading platforms, promising false high returns.

## Religious and charity scams

Scammers exploit cultural and religious events like Ramadan and Hajj, creating fake donation campaigns to steal money.

## HR and job vacancy scams

Fake job postings impersonate well-known brands to collect personal data and scam job seekers.

## Scam-as-a-service (Classiscam)

Cybercriminals leverage Telegram bots to generate fake courier and payment service pages, tricking victims into revealing their personal and financial details.



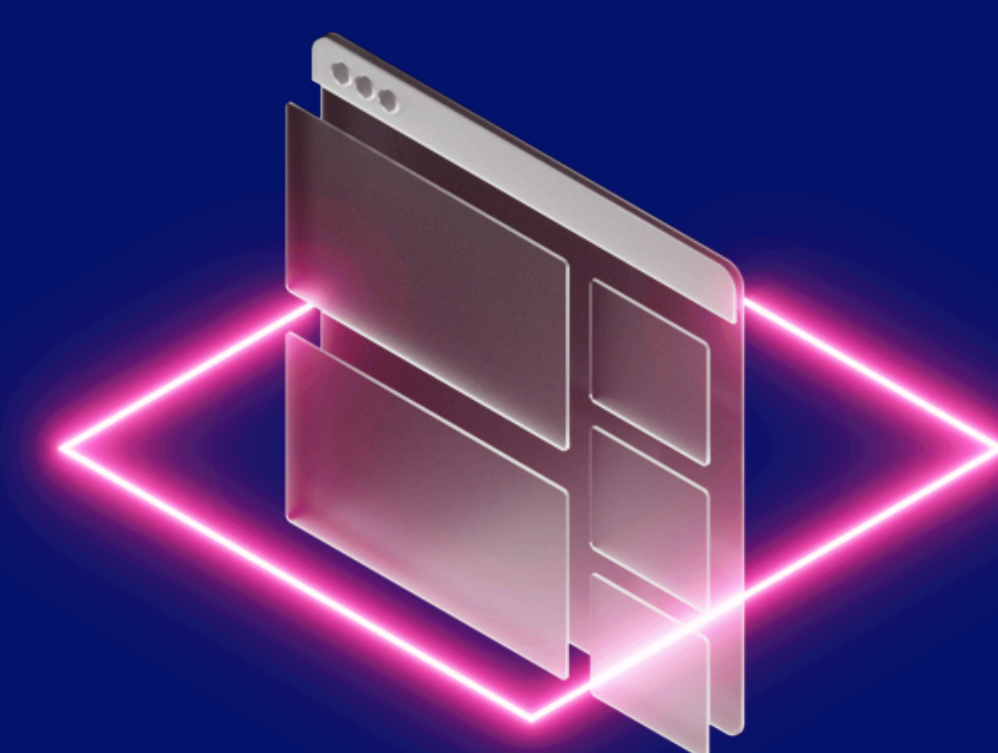
# Protect your digital assets with Group-IB

15

years of experience  
in Digital Risk  
Protection

90%

success rate in  
scam and phishing  
takedowns



Group-IB  
Digital Risk Protection

Collaboration with law  
enforcement and CERT  
teams to disrupt fraud  
networks

60+

professional  
analysts globally

Learn more  
about it

[GROUP-IB.COM](https://GROUP-IB.COM)