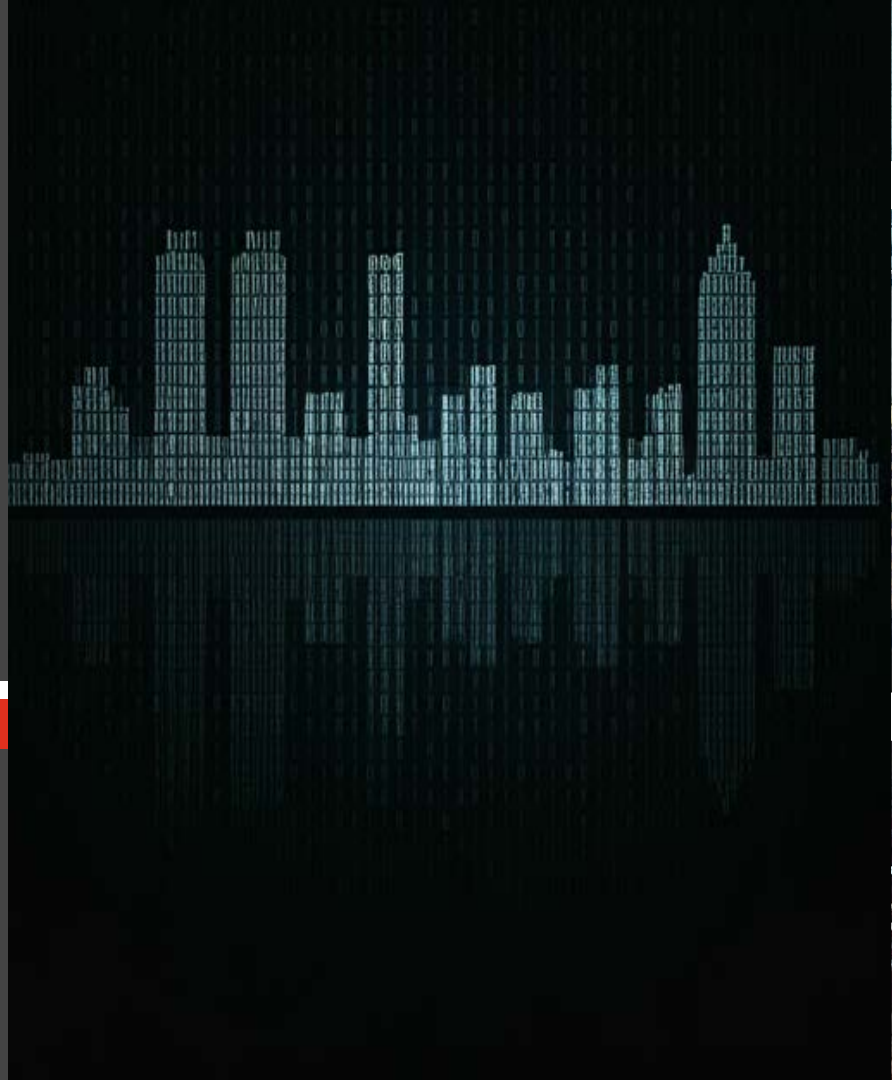
Behind the screen:

Navigating today's cyber threat landscape

2025

pwc



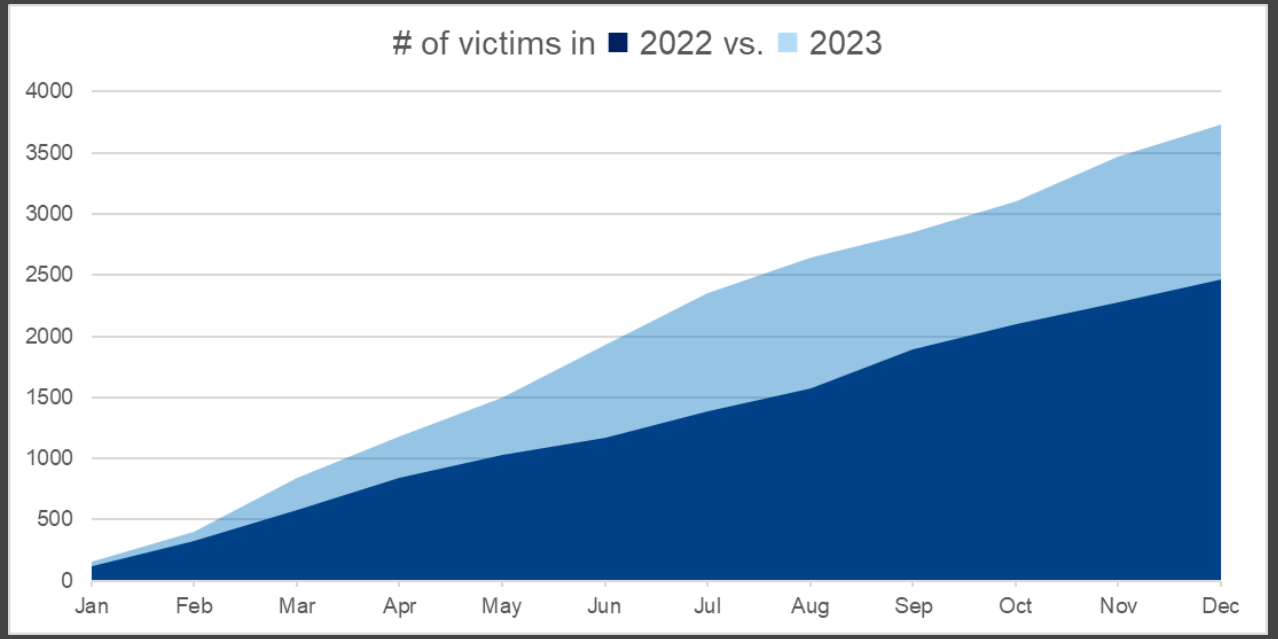
Ransomware

72%

Increase in reported data breaches since 2021
(Barracuda)

$3B

In losses in 2023 to Business Email Compromise (FBI IC3)



Who are the bad guys?

Threat Actor Continuum

Hacktivists

Organized Crime

Nation States

Terrorist Groups

Insiders

What do we mean by **Dark Web**?

- Accessible via The Onion Router (TOR)
- Is not anonymous
- A marketplace for both legitimate and criminal activities/goods

Ransomware

- Continues to evolve
- Is a business
- Size, or lack of, is not a protection
- Infections via phishing, credential theft/stuffing, waterhole attacks, or unpatched vulnerabilities

Business Email Compromise

- Continues to grow – US losses last year ~$3B
- Can be an indicator of a breach
- Insurance claims outpaced ransomware in 2023
- Targets well-meaning employees, hoping they don’t follow procedure

Call-backs and verification are the key defenses.

Phishing

- Is the root cause of most breaches
- Continues to grow in sophistication

Always consider:
1. Do I KNOW where this is coming from?
2. Would this person communicate with me this way?
3. Was I expecting this?
4. Does this make sense?

Money Schemes

- Romance scams
- Investment / crypto scams
- Job jacking

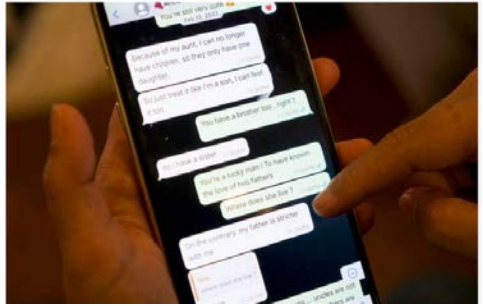
Friends don’t ask friends to pay them in gift cards

What’s next?

AI Scams

'Pig-butchering': The online scam that's raked in $75 billion and counting

April 03, 2024 By Daniel Ackerman, Mayhna Chakrabarti and Tim Skipp



AI voice scammers are posing as loved ones to steal your money — here's a foolproof trick to stop attacks

By Ben Cost
Published May 7, 2024, 12:38 p.m. ET

Elon Musk deepfake crypto scam highlights risks to Hong Kong as AI-related fraud rises

- The Securities and Futures Commission has warned of a fraudulent crypto trading platform called Quantum AI, a long-time scam that uses deepfakes of Elon Musk
- Hong Kong has proven particularly susceptible to AI-related scams, with fintech industry fraud growing 3.8 per cent in the first quarter

Leading practices

- Assess all requests for wire transfers/payments, any changes in banking information – without exception
- Implement multifactor authentication (MFA) everywhere
- Don’t click on links you’re unsure of
- Use good password hygiene – don’t reuse passwords across accounts and never provide your password to another
- Police your social media presence (New York Times rule)
- Enable end-to-end encryption to reduce risk of digital eavesdropping or intercept
- Avoid using free internet connections and consider a VPN
- Report suspicious activity to your Infosec team

Security is about behaviors.

Both individuals and organizations as a whole hesitate to establish a cyber strategy.

Once you and your family come to understand you can control your safety online and off, you'll naturally take actions needed to keep yourself secure.

Location Services

Turn off location services and deny permission to applications that want to track movement or GPS. Consider also preventing applications from communicating with one another and blocking application to application data sharing.

Social Media

Ensure your social media presence is private and reduce your social media footprint. If you're an influencer, keep the accounts separate from one another and include a separate email account for personal versus public facing social media accounts. Limit the number of requests accepted from unknown accounts.

Phishing

Do not click on links from unknown senders or from sources that may look questionable. Often, these are attempts to gain additional information for future use or to deploy malicious software onto devices. These links may come from emails or from text messages.

Online Hygiene

Police your online presence, set ground rules amongst your friends and family about what can and cannot be shared online, and educate them on the risk to both their safety and your own.

Thank you

pwc.com