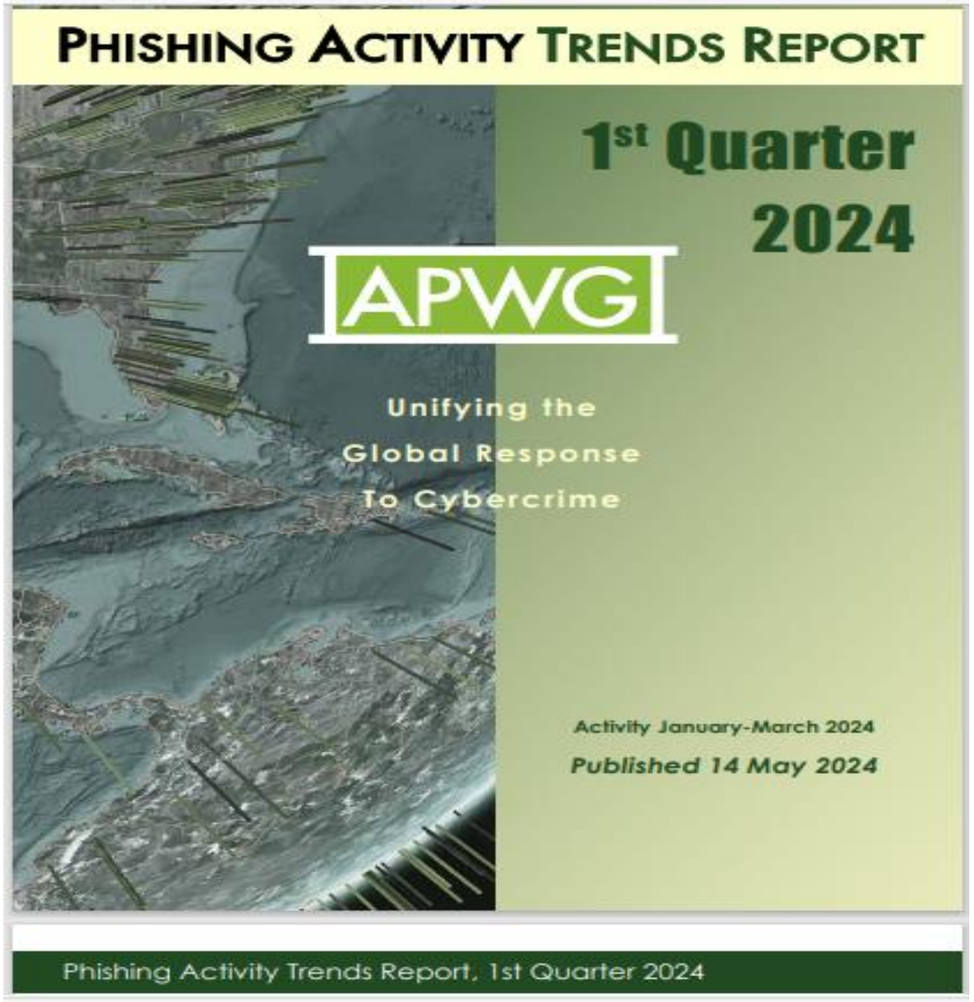
CYBER ATTACKS CASE STUDIES

Cyber Attacks

- Social Engineering / Phishing:
  - Social engineering refers to the manipulation of individuals into divulging confidential information through psychological manipulation rather than technical means. Phishing involves the use of deceptive emails, messages, or websites to trick individuals

Cyber Attacks

- Social Engineering / Phishing:
  - Anti-Phishing Working Group (APWG) Founded in 2003, is an international coalition of counter-cybercrime responders, forensic investigators, law enforcement agencies, technology companies, financial services firms, university researchers, NGOs etc



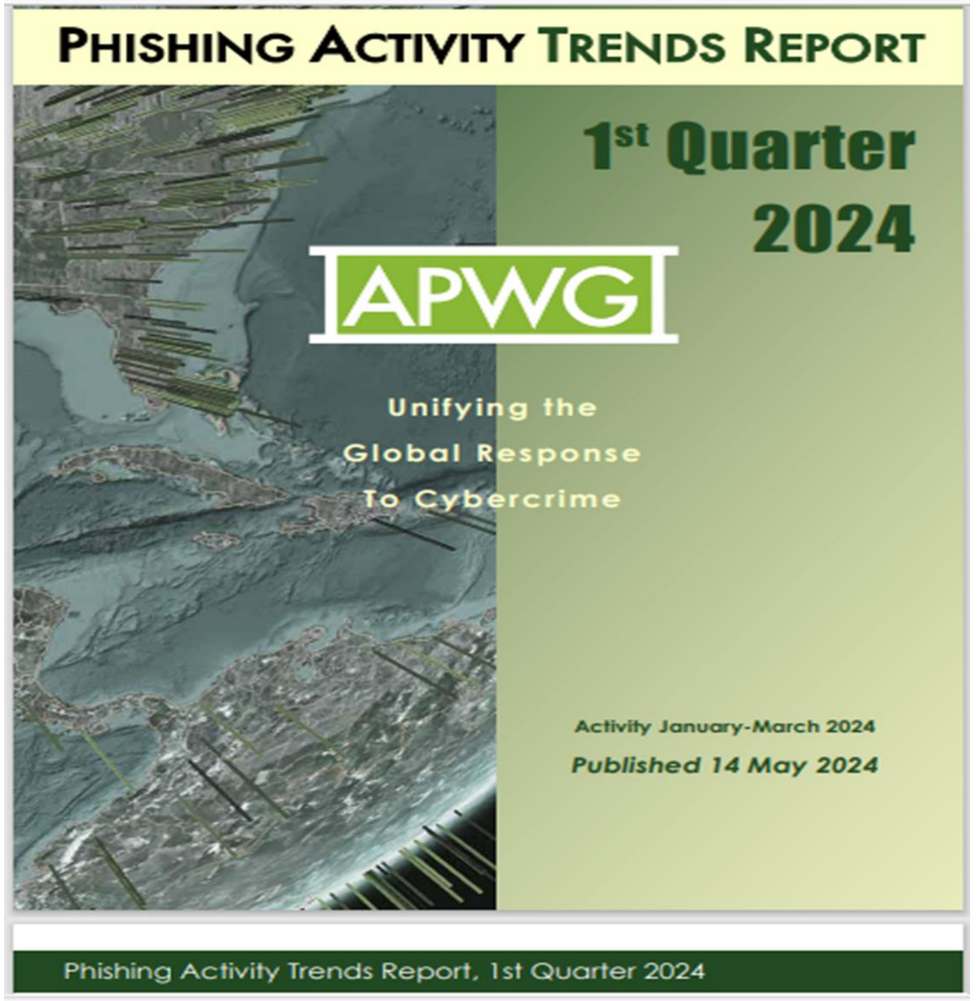
Cyber Attacks

- Social Engineering / Phishing:

Cyber Attacks

- Social Engineering / Phishing:

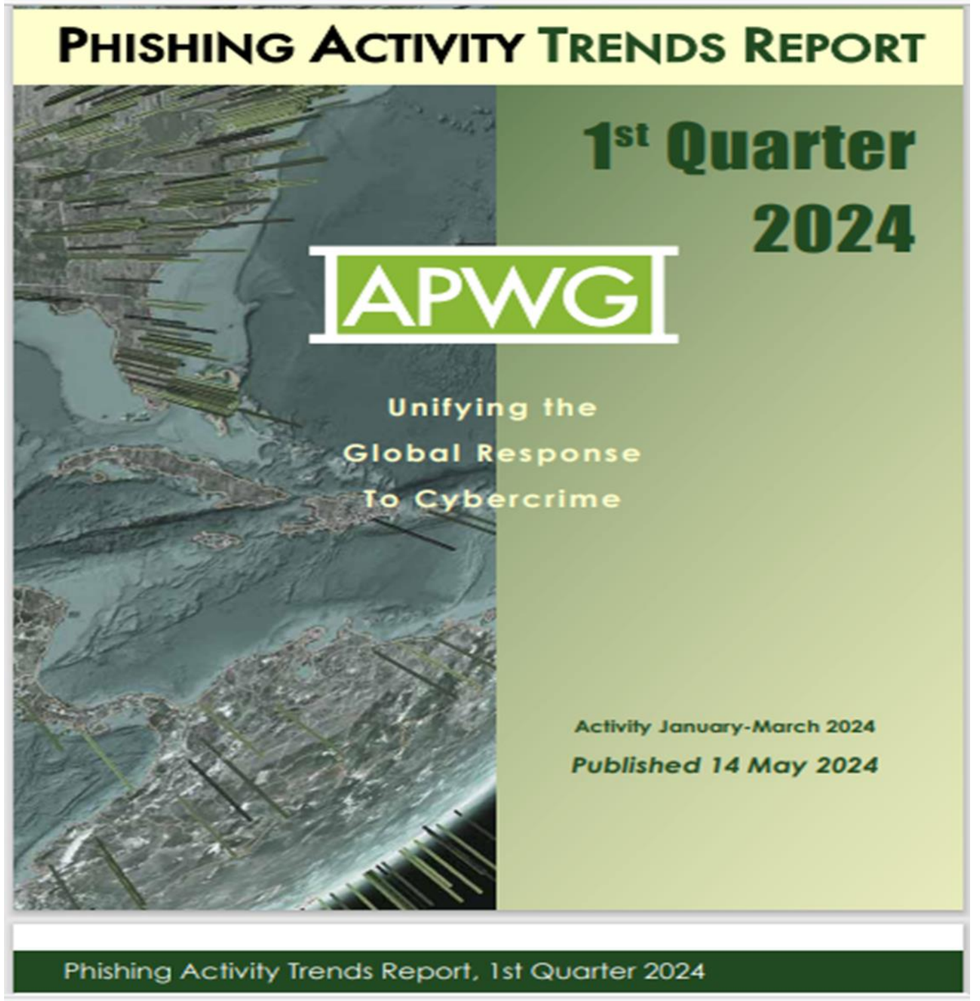
- APWG identity a theft technique known as “business e-mail compromise” or BEC, which was responsible for $2.9 billion dollars in losses in the U.S. in 2023 according to the FBI’s Internet Crime Complaint Center (IC3).



Cyber Attacks

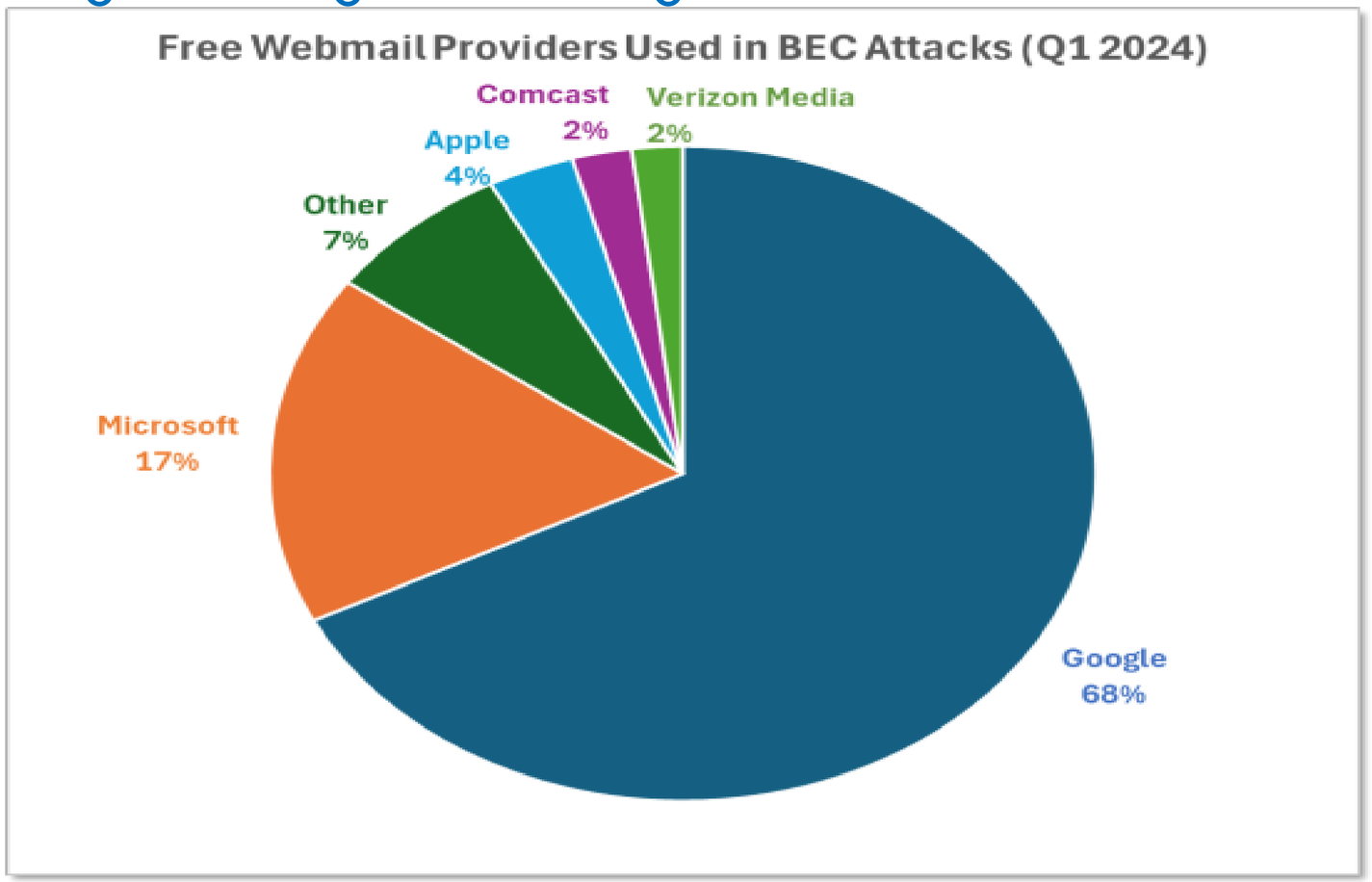
- Social Engineering / Phishing:

- In a BEC attack, a threat actor impersonates an employee, vendor or other trusted party in an email communication and attempts to trick an employee into sending money, privileged information, or some other asset



Cyber Attacks

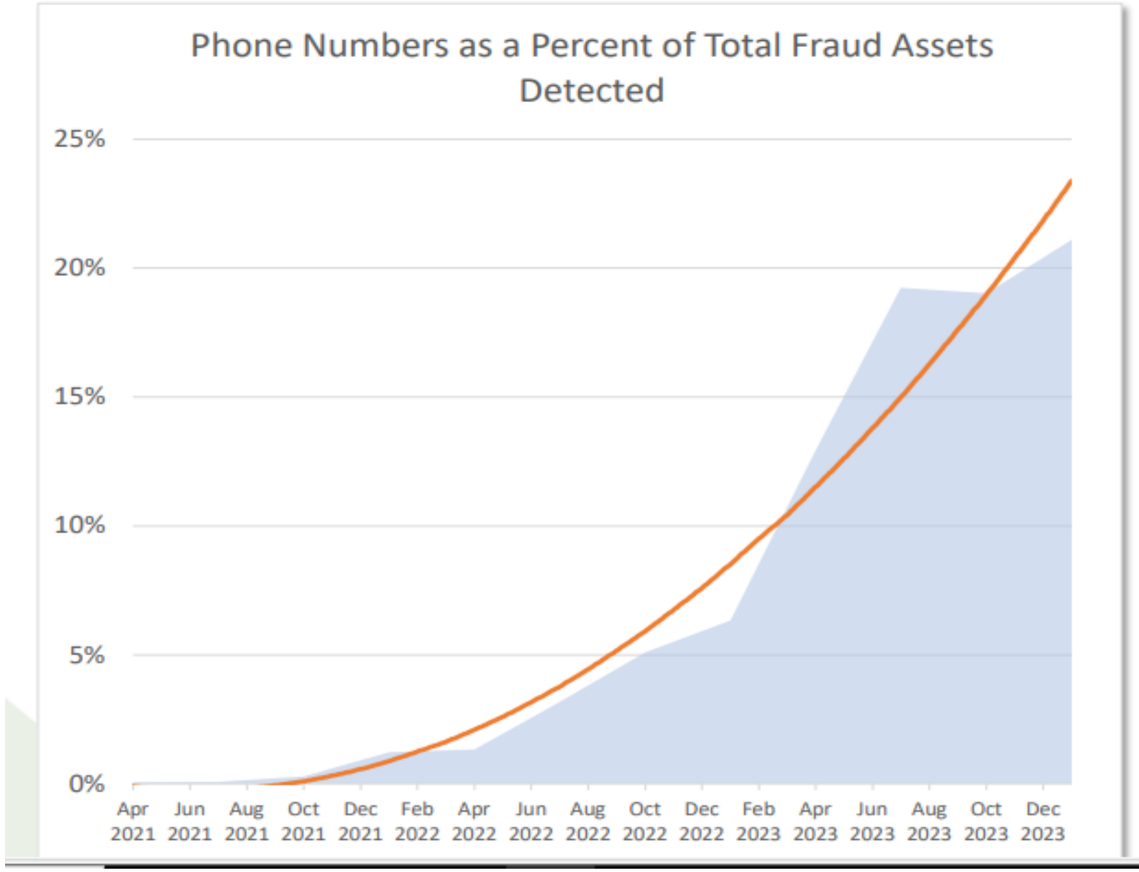
- Social Engineering / Phishing:



Cyber Attacks

- Social Engineering / Phishing:

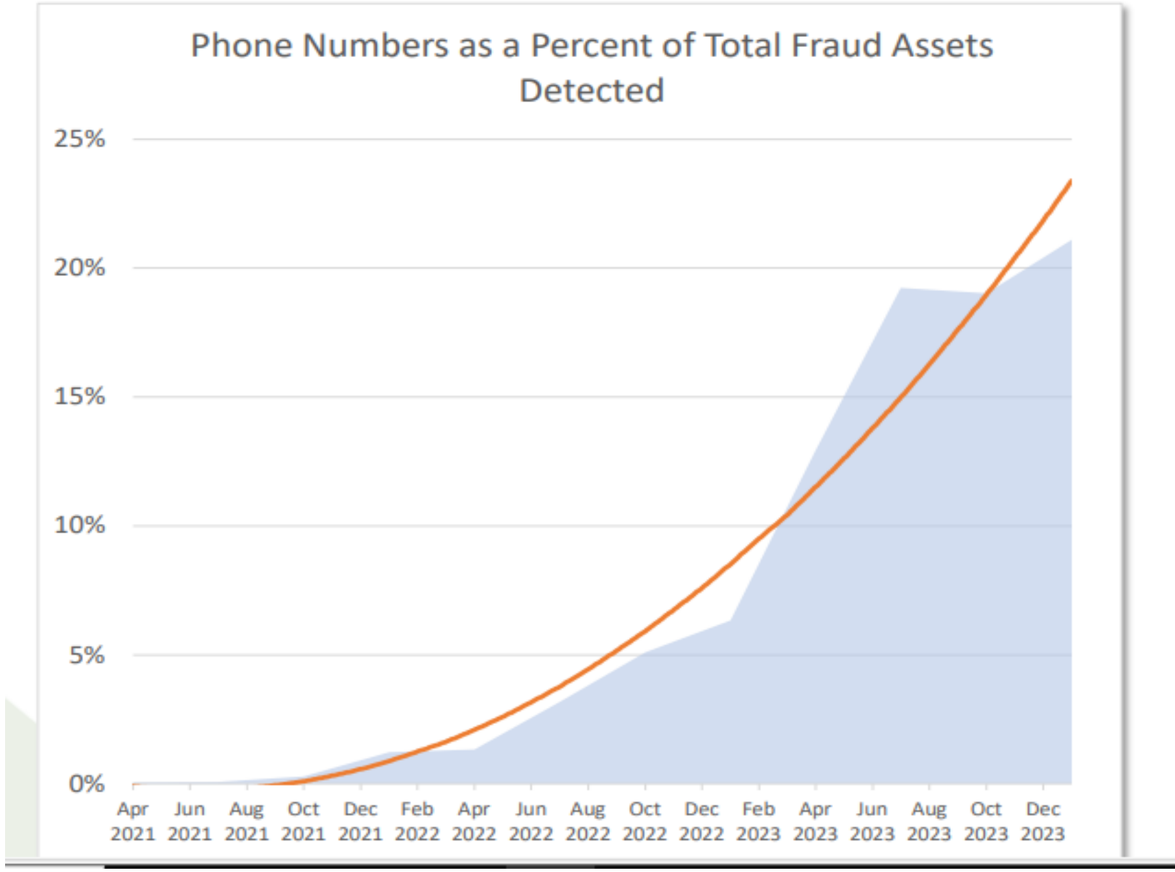
- Phone-based fraud is initiated by different methods. One is voice phishing or vishing -- where fraudsters call potential victims.



Cyber Attacks

- Social Engineering / Phishing:

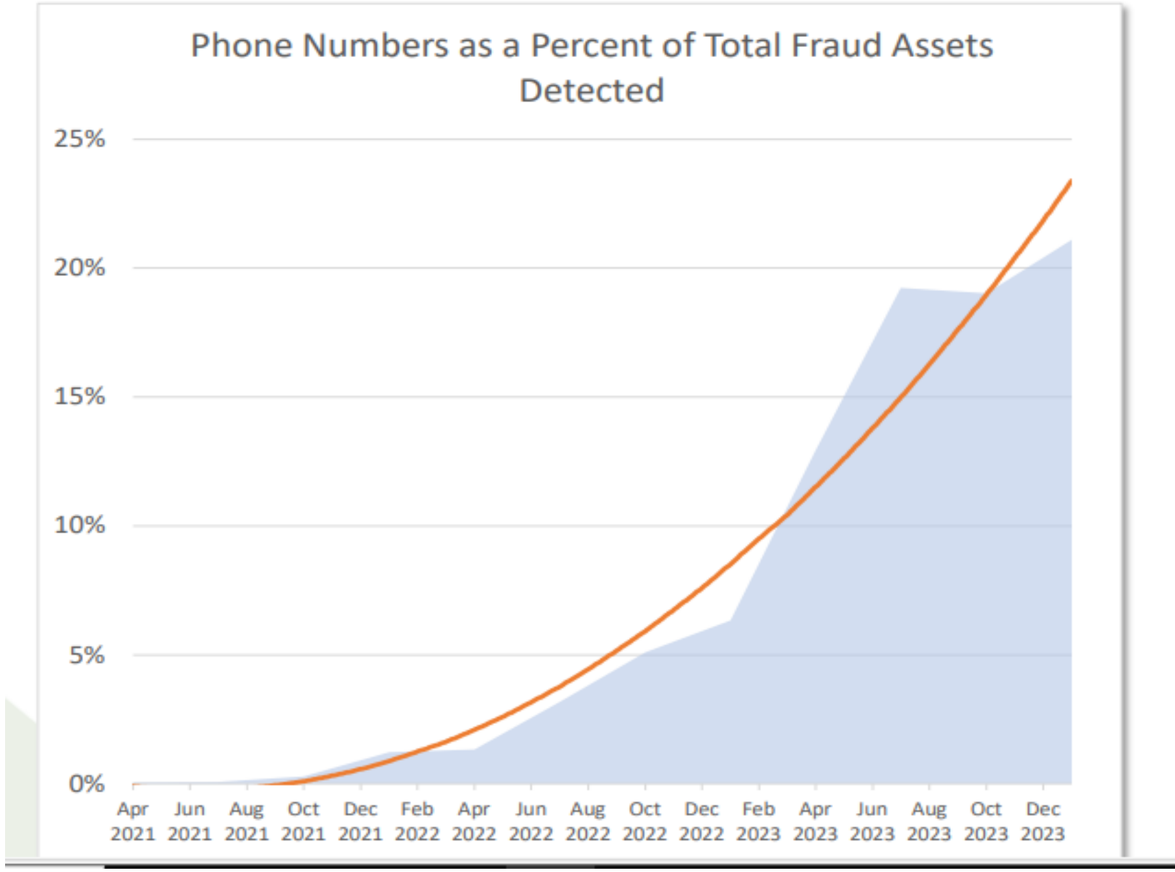
- Another is SMS-based phishing or smishing – in which fraudsters advertise the URLs of phishing sites within SMS (Short Message Service) messages



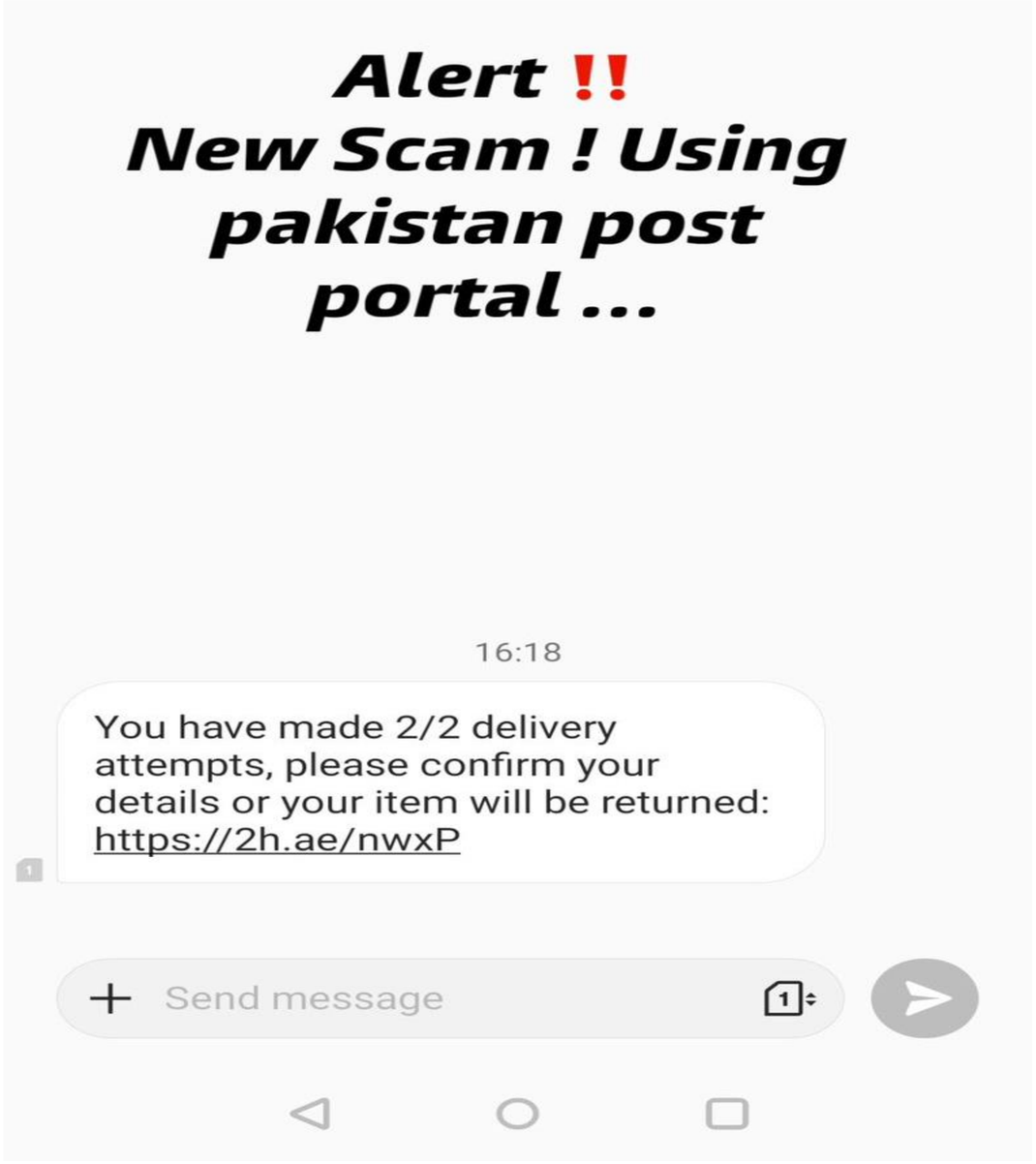
Cyber Attacks

- Social Engineering / Phishing:

  - Hybrid phishing. Sending the victim a fake purchase receipt via email, which requests that the recipient call a support phone number to dispute the charge. This “urgent call to action” is a common social engineering tactic. Once on the phone with the victim, the scammer collects the victim’s personal and financial information,



Alert !!
New Scam ! Using pakistan post portal ...



Your shipment has been put on hold due to a missing street number. Verify and update the correct address: https://qrco.de/bf566d

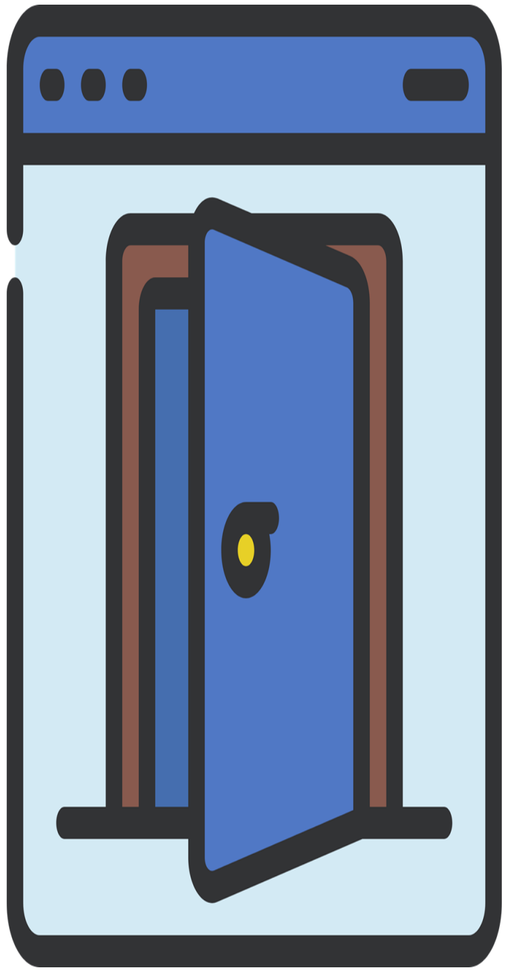
We regret to inform you! Unable to deliver due to wrong address. Please update your address or the package will be returned https://ep.gov-pk.top/a

Cyber Attacks

- Social Engineering / Phishing:
  - People have been reporting on social media platforms that they have been getting calls from a Tel number that begins with a different country code. These people ring once, then end the call. If you call them back, they can copy your phone call history and any bank or credit card information that is on it.

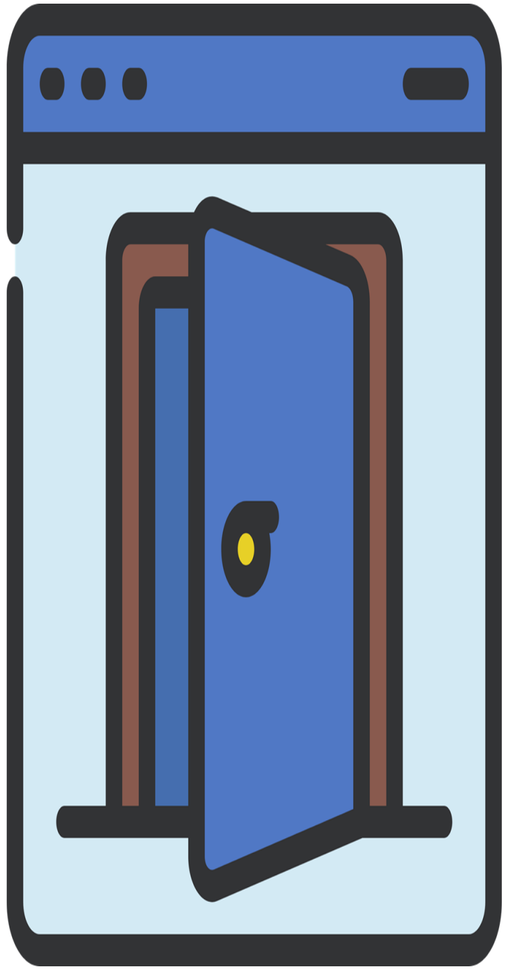
Cyber Attacks

- Malware
  - Backdoors: It refers to any method by which authorized and unauthorized users are able to get around normal security measures and gain high level user access on a computer system, network, or software application.



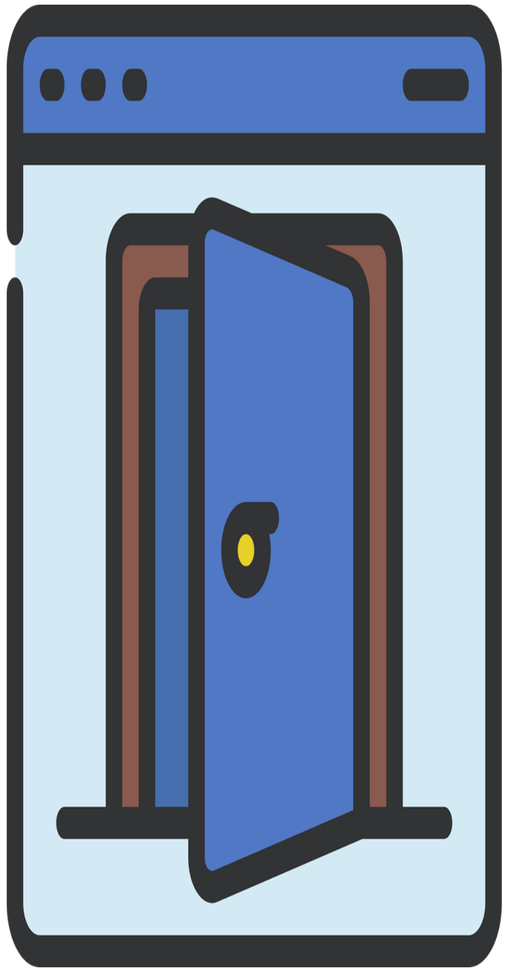
Cyber Attacks

- Malware (Backdoor)
  - Sony Pictures Hack: In Nov 2014 executed by a group calling themselves the "Guardians of Peace," leaked sensitive information, including unreleased movies, personal employee data, and emails. This resulted in damaging Sony's reputation and financial losses.



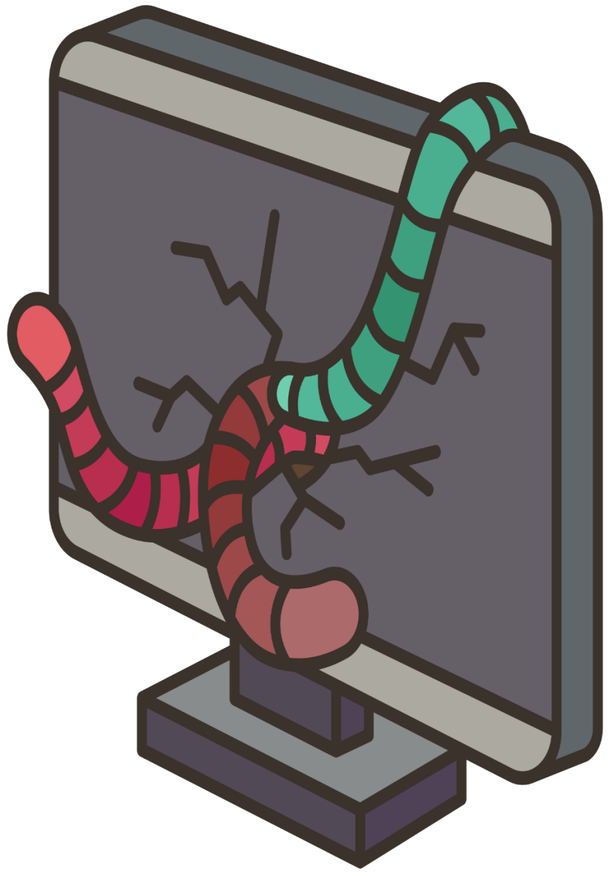
Cyber Attacks

- Malware (Backdoor)
  - Solar Wind Supply Chain Attacks: In Dec 2020 Compromised SolarWinds' Orion software updates, allowing attackers to insert a backdoor known as SUNBURST into the systems.
  - Impact : US Government Agencies, Microsoft, FireEye.



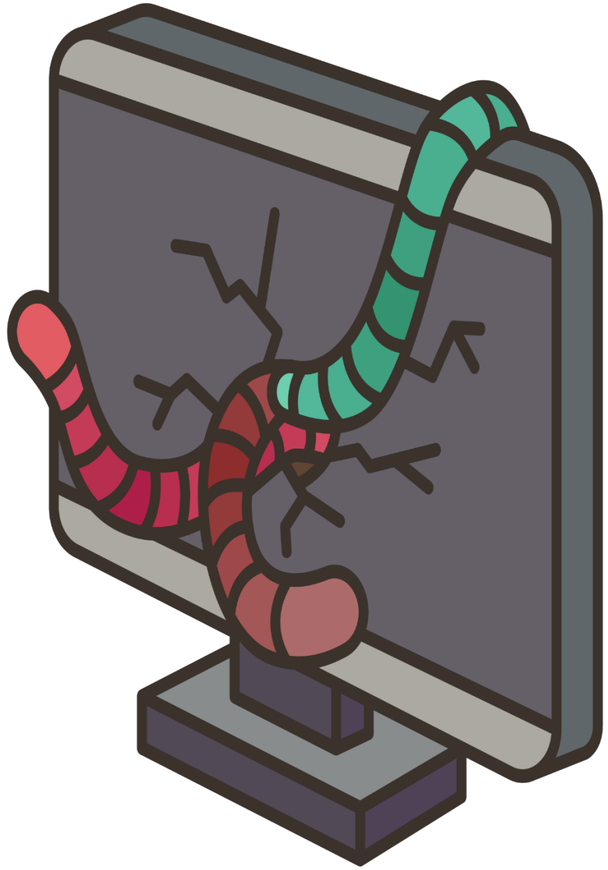
Cyber Attacks

- Malware
  - Worms: A self-replicating, self-propagating, self-contained program that uses networking mechanisms to spread itself..



Cyber Attacks

- Malware (Worm)
  - Stuxnet: In Jun 2010 a sophisticated worm specifically designed to target industrial control systems, particularly Iran's nuclear facilities. It caused physical damage to centrifuges by manipulating their operation.
  - Impact : Natanz Nuclear Facility (Iran), Siemens SCADA System



Cyber Threats

- Malware
  - Ransomware: Ransomware encrypts files or entire systems and demands payment (usually in cryptocurrency) for the decryption key.

Cyber Attacks

- Malware (Ransomware)
- Colonial Pipeline. In May 2021, a ransomware group known as DarkSide targeted the Colonial Pipeline Company, one of the largest fuel pipelines in the United States.

Cyber Attacks

- Malware (Ransomware)
- Colonial Pipeline. The attack resulted in the shutdown of the pipeline for several days, leading to widespread fuel shortages and a significant increase in gas prices. The company ultimately paid a ransom of approximately $4.4 million to regain control of its systems

Cyber Attacks

- Malware (Ransomware)
- WannaCry
  - Infected over 200,000 computers worldwide, causing massive disruption and financial losses.
  - Impacted: NHS (UK), FedEx, Telefonica, Renault

Cyber Attacks

- Cyber Espionage, also known as cyber spying or cyber intelligence gathering, is the covert acquisition of sensitive information from computer systems, networks, or electronic devices using digital techniques and technologies

Cyber Attacks

- Malware (Spyware)
- Pegasus: Pegasus is sophisticated spyware capable of infecting iOS and Android devices. It can secretly extract messages, photos, emails, call logs, and more, allowing for surveillance of targeted individuals,

Cyber Attacks

- Crypto AG Cyber Espionage 1950-2010:

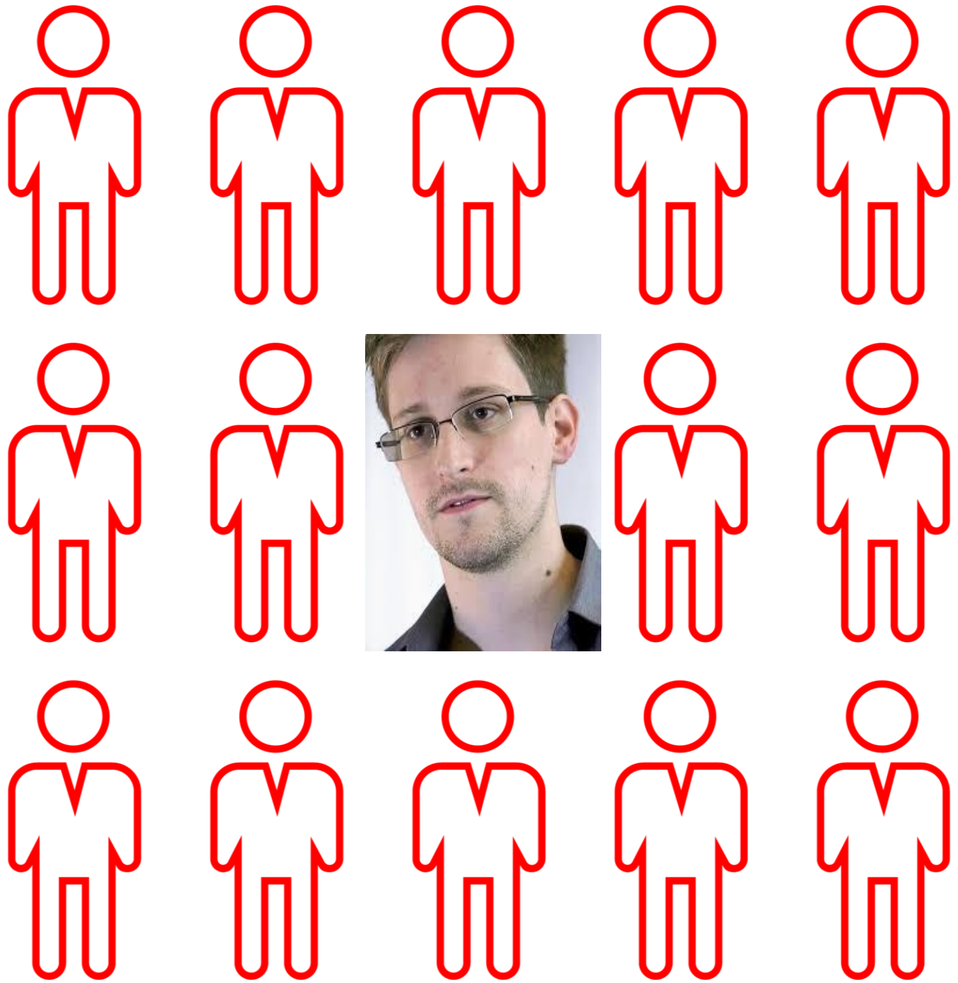
  Crypto AG, a Swiss company, produced cryptographic equipment used by governments and organizations worldwide. However, it was revealed in 2020 that Crypto AG had been secretly owned by the CIA (Central Intelligence Agency) in partnership with the BND (German Federal Intelligence Service).

Cyber Attacks

- Cyber Espionage: 1950-2010. This allowed the CIA and BND to manipulate the encryption devices, enabling them to eavesdrop on communications of numerous countries for decades. The scandal shook global trust in cryptographic security and had significant geopolitical implications, affecting diplomatic relations between nations.

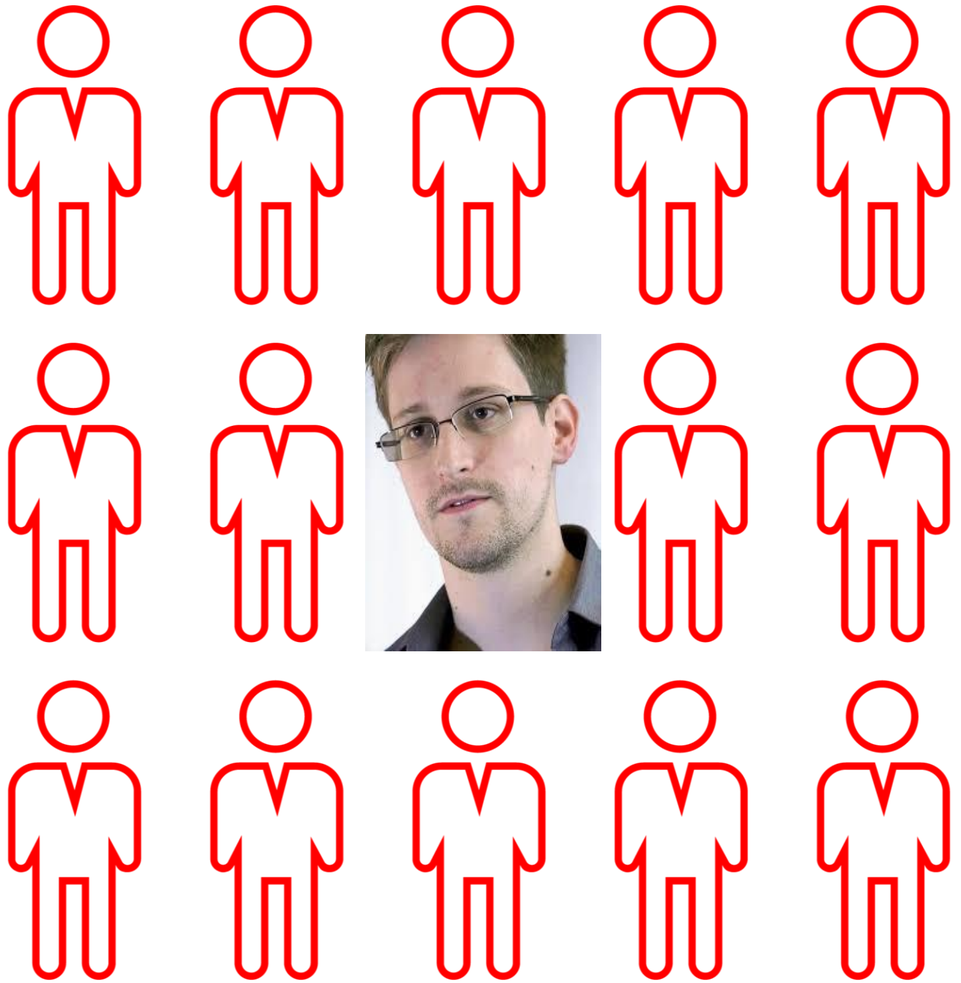
Cyber Attacks

- Insider Threat.
  - We all know the name, Edward Snowden (A former contractor to the CIA). Variously described as a whistleblower, hero, or even a traitor, in the security community, he is what is known as an 'insider threat.



Cyber Attacks

- Insider Threat.
  - Snowden copied and released thousands of classified documents to journalists, many relating to secret and controversial government surveillance activities in the U.S. and abroad. He has been living in Russia since, the subject of ongoing criminal charges from the U.S. government.

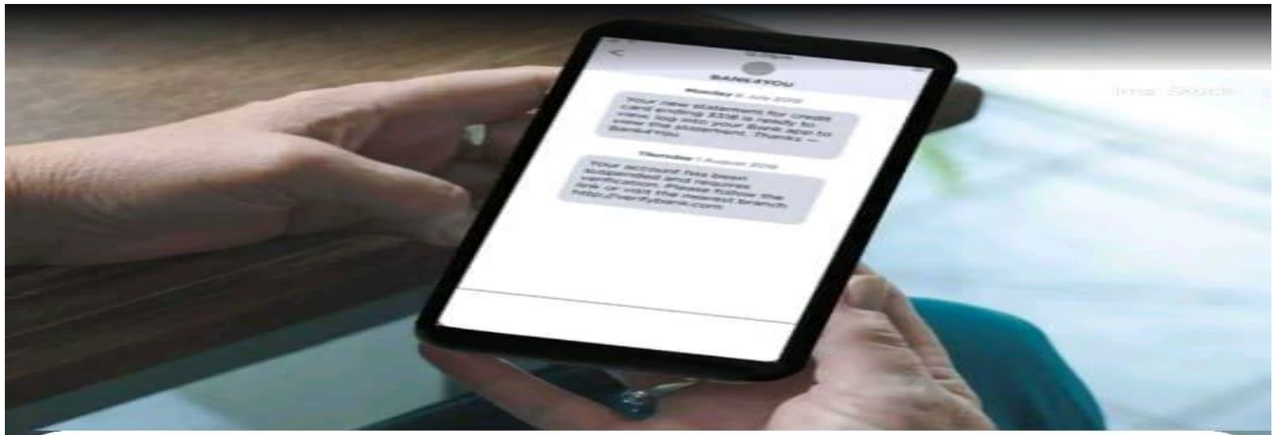


Cyber Attacks

- Sophisticated Cybercrime
  - Deep Fake. Video of a person in which their face or body has been digitally altered so that they appear to be someone else

Cyber Attacks

- Malware (Banking Trojan)
  - Zeus Trojan. A type of banking Trojan designed to steal banking credentials and financial information from infected computers and adding machines to a botnet. It targets Microsoft Windows.
  - It spread primarily through phishing emails and infected websites, leading to significant financial losses for millions of victims worldwide.



Beware! Now, hackers can transfer money without OTP

A new online fraud method involves a message that appears to be from a reputed bank, containing an APK link. Clicking the link downloads applications to your phone without your knowledge. These applications forward your SMS messages, including OTPs, to fraudsters, allowing them to access your device and steal money from your account without requiring you to provide an OTP.

Know more from **Udayavani** & others
Xpresso by 24x7 · 20 May 2024

Thanks