PHISHING ATTACKS

Phishing attacks are cyber-attacks in which malicious actors attempt to trick individuals into divulging sensitive information such as usernames, passwords, credit card numbers, or other personal data. These attacks typically occur via email but can also happen through other communication channels like text messages, social media, or phone calls.

True cases and examples

Bait: The attacker sends out fraudulent communications, often impersonating a trusted entity such as a bank, social media platform, or a reputable company. These messages are designed to appear legitimate and may include logos, branding, and other elements to deceive recipients.

Hook: The message contains a call to action, such as clicking on a link, downloading an attachment, or providing personal information. The goal is to lure the recipient into taking the desired action under pretenses.

Deception: The linked webpage or downloaded file may lead to a fake login page, a malicious website, or a malware-infected attachment. If the recipient falls for the deception and interacts with the malicious content, their sensitive information could be compromised, or malware could be installed on their device.

Phishing attacks can vary in sophistication, ranging from simple, generic emails to highly targeted and personalized messages known as spear phishing. Spear phishing attacks often involve extensive research to craft convincing messages tailored to specific individuals or organizations, making them harder to detect.

Recent attacks

A legitimate-looking Google search advertisement for the crypto trading platform Whales Market impersonates Whales Market to push wallet drainer malware. The advertisement redirects visitors to a wallet-draining phishing site that steals all their assets.

LabHost phishing service with 40,000 domains disrupted, 37 arrested: The **LabHost** phishing-as-a-service (PhaaS) platform was disrupted in a year-long global law enforcement operation that compromised the infrastructure and arrested 37 suspects, including the original developer.

FIN7 targets American automaker's IT staff in phishing attacks: The financially motivated threat actor FIN7 targeted a giant U.S. carmaker with spear-phishing emails for employees in the IT department to infect systems with the Anunak backdoor

Chrome Enterprise gets Premium security, but you have to pay for it: Google has announced a new version of its browser for organizations, Chrome Enterprise Premium, which comes with extended security controls for a monthly fee per user.

Hackers impersonate U.S. government agencies in **BEC** attacks: A gang of hackers specialized in business email compromise (BEC) attacks and tracked as TA4903 has impersonated various U.S. government entities to lure targets into opening malicious files carrying links to fake bidding processes.

A new phishing attack steals your Instagram backup codes to bypass 2FA: A new phishing campaign pretending to be a 'copyright infringement' email attempts to steal the backup codes of Instagram users, allowing hackers to bypass the two-factor authentication configured on the account.

How to prevent your organization from Phishing attacks?

The use of innovative solutions that can find any unwanted footprint before exiting by multi-sophisticated log-in credentials and identify any anomaly if planted from inside. CyberGhost uses Artificial intelligence and Machine learning to connect all endpoints in a neural network that interfaces with the two layers of authentication and authorization to prevent unauthorized users from getting to the data. In simple language, it acts as an investigator to investigate each attempt to temper or get access to the data to make data visible to them; otherwise, the data disappears.

In addition, the following steps may help additional guidelines to avoid falling into a phishing trap.

Be cautious: Be skeptical of unsolicited emails, especially those requesting personal information or urging urgent action.

Verify: Double-check the sender's email address, look for spelling or grammatical errors in the message, and scrutinize any links or attachments before interacting with them.

Use security tools: Employ email filtering, antivirus software, and web filters to detect and block phishing attempts.

Educate: Provide cybersecurity awareness training to employees and individuals so they can recognize phishing red flags and respond appropriately to suspicious messages.