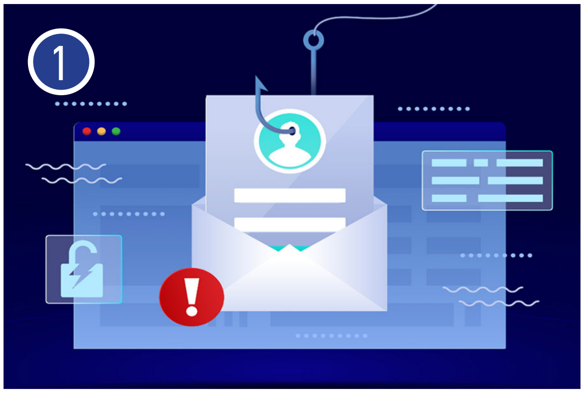
Cyber Talk's
10 Top Phishing Narratives to Share

These shocking stories and expert insights can help you build a winning business case for leadership support of phishing-prevention technologies and best practices.

Discover the best, the worst, the most deceptive, and the most dangerous attacks. These are our notable picks.



TITLE: The latest phishing kits are bypassing multi-factor authentication

DESCRIPTION: These kits use a transparent reverse proxy (TRP) to present an authentic website to a potential victim. The victim retains the illusion that he/she is logging into a safe online portal. In reality, cookies save the information, which hackers can exploit at a later point in time.

READ THE ARTICLE

TITLE: NFT owners lose $1.7M in OpenSea phishing attack

DESCRIPTION: A smart-contract migration email enabled an attacker to obtain 250 high-value NFTs from a mere 17 individuals. In order to successfully phish NFT investors, an attacker designed and deployed sophisticated social engineering techniques.

WHAT TO KNOW

TITLE: This tiny font phishing campaign could fool your O365 filters

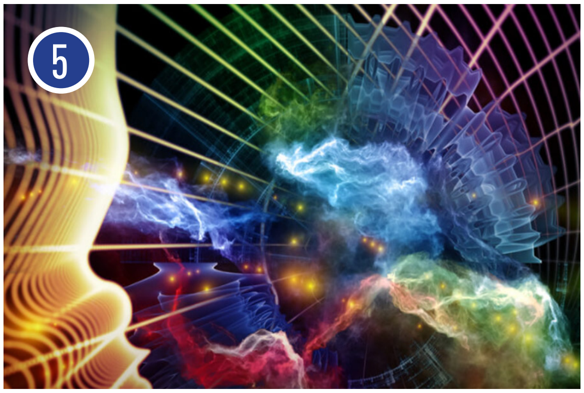
DESCRIPTION: The name of the campaign, One Font, derives from the fact that the scheme hides text in one point font within malicious messages. This is an example of an 11-point font – a one-point font is very, very tiny. The campaign leverages a variety of obfuscation techniques that help attacks skate past natural language processing filters.

READ THE ARTICLE

TITLE: Password attacks, malicious 0365 phishing campaign

DESCRIPTION: Microsoft warns that 0365 users should beware of new, email-based, malicious links that collect user credentials and lead to password attacks.

READ THE STORY



TITLE: How email AI fools humans into falling for attacks

DESCRIPTION: Technology researchers have discovered that the deep learning language model (GPT-3), combined with additional AI-as-a-Service platforms can make crafting spear phishing campaigns at-scale easier than ever.

READ ABOUT AI AND PHISHING

TITLE: Global energy suppliers facing spear phishing and spyware

DESCRIPTION: Energy sector trends show that spear phishing and other sophisticated social engineering techniques are at work in disrupting energy suppliers. For more than a year, cyber criminals have attempted to leverage these tactics to spread common remote access trojans (RATs). The RATs enable hackers to carry out cyber espionage activities.

READ THE STORY

TITLE: Chipotle's email marketing platform used in phishing campaign

DESCRIPTION: Chipotle Mexican Grill, an American "fast casual" restaurant chain, fell victim to a cyber attack. According to the report, attackers compromised one of Chipotle's email marketing accounts to access the service known as MailGun.

SEE WHAT HAPPENED

TITLE: Global phishing attacks deliver never-before-seen malware

DESCRIPTION: A well-resourced and sophisticated threat actor launched an advanced global phishing campaign, featuring three never-before-seen malware families. The attack is believed to have affected more than 50 firms worldwide, which range in geography and industry type. While the US appears as the main target, EMEA, Asia and Australia also experienced compromise through this campaign.

DETAILS HERE

TITLE: Inside a phishing attack gone wrong

DESCRIPTION: These hackers bungled their mission. They accidentally dumped their stolen loot on the public internet, enabling every hacker to access them free of charge. For the original hackers, these credentials no longer held value on the dark web.

LEARN MORE

TITLE: : Office 365 phishing attack, financial executives key targets

DESCRIPTION: Via this campaign, hackers hoped to harvest Microsoft Office 365 data and to catalyze more business email compromise (BEC) attacks.

READ THE STORY

Phishing prevention is a journey, rather than a destination. Arguably, the largest success factor in driving an anti-phishing program forward is management buy-in. Selectively share these phishing-related deceptions, threats, attacks and their real or potential consequences with your stakeholders to clearly communicate the need for a more resilient anti-phishing program. All it takes is one phishing email to bring an organization down.