Prevention tactics and Strategies

There are simple ways to avoid falling for phishing scams:

- Verbally, in person, confirm requests such as requests for money.
- Some AI-related scams clone the voice of a loved one to ask for money.
- Check the sender email and the contents of the message for any irregularities.
- Hover your mouse over the link provided to see if it links to somewhere different.
- Never clink on a link you're not 100% sure is legitimate.
- Never install programs onto your computer that another party tells you to do.
- If you've been phished, you can file a complaint with the Federal Trade Commission.

Effectiveness of Phishing Training and Awareness

Phishing awareness and training in businesses can be effective in reducing the risk of falling victim to phishing attacks. However, its success depends on various factors, including the quality and frequency of training, employee engagement, and the evolving nature of phishing tactics. Regular updates to training content and simulated phishing exercises can enhance effectiveness of anti-phishing measures by keeping employees informed about new threats. Being a victim to one of these

Statistics

Phishing is a field of study that merges social psychology, technical systems, security subjects, and politics. Phishing attacks are more prevalent: a recent study (Proofpoint, 2020) found that nearly 90% of organizations faced targeted phishing attacks in 2019, 88% experienced spear-phishing attacks, 83% faced voice phishing

(Vishing), 86% dealt with social media attacks, 84% reported SMS/text phishing (SMishing), and 81% reported malicious USB drops.

A study by Ke epnetLABS in 2018 confirmed that more than 91% of system breaches are caused by attacks initiated by email.

Participants with an age range between 18 and 25 are more susceptible to phishing than other age groups (Williams et al., 2018). The reason that younger adults are more likely to fall for phishing is that younger adults are more trusting when it comes to online communication, and are also more likely to click on unsolicited emails (Getsafeonline, 2017).

Moreover, older participants are less susceptible because they tend to be less impulsive (Arnsten et al., 2012).

Some studies confirmed that women are more susceptible than men to phishing as they click on links in phishing emails and enter information into phishing websites more often than men do.

In 2017, a report by PhishMe (2017) found that curiosity and urgency were the most common triggers that encourage people to respond to the attack. Later, these triggers were replaced by entertainment, social media, and reward/recognition as the top emotional motivators to click on a phishing link.

https://www.frontiersin.org/articles/10.3389/fcomp.2021.563060/full

What makes a good phishing campaign?

Phishing campaigns are an extremely effective way to make employees more aware of possibly deceitful emails or websites. Simulated attacks are designed to portray a realistic and informative example on how people are truly misled within business and personal life.

Some examples of this are:

Social Engineering: Phishing emails often rely on social engineering techniques to manipulate recipients into taking action. This could involve creating a sense of urgency, exploiting curiosity, or playing on emotions to prompt the recipient to click on a malicious link or download an infected file.

Spoofed Identities: Phishing emails may appear to come from trusted sources such as banks, government agencies, or well-known companies. The sender's email address might be spoofed to closely resemble a legitimate address, increasing the likelihood that recipients will trust the email.

Personalization: Phishing emails may include personal details about the recipient to make the message appear more legitimate. This could include using the recipient's name or referencing recent interactions to create a false sense of familiarity.

Professional Appearance: Phishing emails often mimic the design and formatting of legitimate emails to make them appear more credible. This could involve using company logos, professional language, and formatting that closely resembles official correspondence.

Malware and Exploits: Some phishing campaigns may involve malicious attachments or links that, when clicked, install malware or exploit vulnerabilities on the recipient's device. These payloads can compromise sensitive information or give attackers control over the victim's system.

URL Manipulation: Phishing emails may contain links that appear to lead to legitimate websites but actually redirect users to fraudulent sites designed to steal login credentials or financial information.