Defend yourself from phishing, vishing and smishing attacks

Fraudsters use social engineering to persuade people to expose sensitive personal information, opening themselves up to many kinds of fraud. Four common approaches are Phishing, Vishing, Quishing and Smishing.

Phishing—Email attacks

Phishing is a form of cyberattack that occurs when a fraudster sends people fake emails to trick them into clicking on a malicious link or attachment. If successful, the fraudsters access the person's username, password or other sensitive personal data, and use it for their financial benefit. Phishing attacks are widespread.

Vishing—Phone call attacks

Vishing is a form of social engineering that occurs when a fraudster makes unsolicited phone calls to individuals to trick them into sharing sensitive personal information—and the ploy often works.

Quishing—Camera based attacks

Quishing attacks take advantage of people's willingness to scan QR codes. An innocuous QR code in a text or a public place such as a restaurant routes the unsuspecting person to a malicious website where they are then tricked into revealing sensitive information.

Smishing—Text message attacks

A third type of social engineering is called smishing in which a fraudster sends phony text messages to people with malicious attachments and links. Their goal may be to steal and monetize data. Smishing is a serious threat.

Guidelines for defending yourself against phishing, vishing, quishing and smishing attacks

- **Verify the sender's information.** Email addresses used by attackers may be incorrect by a single letter. Caller ID should not be trusted since fraudsters can locate and spoof phone numbers of legitimate companies, government agencies and people with whom you do business.
- **Don't click on links and attachments, QR codes, or return unknown calls.** Instead, go to the company's official website to confirm whether the link or phone number is real.
- **Look out for grammatical or spelling mistakes** both in the subject and body of the message and the sender's information.
- **Avoid sharing personal information**, usernames, passwords, and financial information.
- **Report, block and delete** phishing emails, smishing texts, and vishing calls.
- **Consider registering your phone number** with a donotcall.gov.

71%

of organizations experienced at least one successful phishing attack in 2023[1]

260%

increase in reported vishing cases in the fourth quarter of 2023 compared to the fourth quarter 2022[2]

331%

increase in fraudulent QR code activity in 2023[3]

For more insights on how to prevent cyberattacks and the steps TIAA takes to protect your personal information, visit the **TIAA Security Center**.

[1] Proofpoint: 2024 State of the Phish Report

[2] APWG: Phishing Activity Trends Report Q4 2023

[3] Cofense: Annual State of Email Security Report 2024

GGN-3582442CR-E0524X (05/24)