Defend yourself from phishing, vishing and smishing attacks

Fraudsters use social engineering to persuade people to expose themselves to many types of fraud. Three common approaches are Phishing, Vishing, and Smishing.

Phishing—Email attacks

Phishing is a form of social engineering 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.

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.

Fraudsters are texting more often to scam people. Mobile phishing and smishing soared by 328 percent in the third quarter of 2020 compared with the same period of 2019.

Guidelines for defending yourself against phishing, vishing 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, or return unknown phone 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 and passwords, and financial information.
- **Report, block and delete phishing emails, smishing** texts, and vishing calls.
- **Consider registering** your phone number with a **donotcall.gov**.

90%

of data breaches within organizations in 2020 resulted from phishing attacks[1]

550%

increase in reported vishing cases in the first quarter of 2022 compared to the first quarter of 2021[2]

People open **98%** of text messages—nearly **5x** more than those who open emails. What's more, they respond to texts in 90 seconds—a stunning 60 times faster than emails.[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] Cisco: **2021 Cybersecurity threat trends - phishing, crypto top the list**.

[2] Agari and Phishlabs: **Quarterly Threat Trends & Intelligence Report**, May 2022.

[3] ClickSend: **Text messaging statistics: 32+ fascinating facts you should know**, July 2022.

2444325
P0355210

(10/22)