Phishing

Key Actions

**Report any suspicious email** using the Report Phish to Duke found in all Outlook email clients. Report any suspicious calls or text messages to your local IT support or security@duke.edu.

Remember that **phone numbers can be spoofed**. If a call seems suspicious, hang up. If you don't recognize the incoming number, consider not answering the call. A legitimate caller can leave voicemail.

**Links in text messages may be malicious.** If you don't know the sender or weren't expecting it, don't click any links.

What is phishing and how to spot a potential attack

Scammers use email, phone calls or text messages to trick you into giving them your personal information. They may try to steal your passwords, account numbers, or Social Security numbers. If they get that information, they could gain access to your email, bank, or other accounts.

*Phishing emails and text messages may:*

- Look like they’re from a company you know or trust.
  - Tell a story to trick you into clicking on a link or opening an attachment. They may say they’ve noticed some suspicious activity or log-in attempts, claim there’s a problem with your account or your payment information, or say you must confirm some personal information.
  - Contain spelling mistakes and poor grammar.
  - Use threats or a sense of urgency.

Spear phishing is targeted phishing, often aimed at executives and employees with access to confidential data. Be wary of any email asking you to reply with account information or click on a link, especially if the message is written to sound urgent. Be especially suspicious if you receive urgent requests for money from a colleague or friend, as well: Confirm the legitimacy of such a request by a different communication method. (For example, if you receive an email requesting
funds, call the supposed sender to verify.)

Source URL: https://security.duke.edu/phishing