What is a phishing email?

Q: What is a phishing email?

On this page:

Answer

Phishing is the fraudulent practice of sending emails pretending to be from reputable sources in order to steal passwords or sensitive personal or financial information, or to install malware on the target’s computer.

It’s common for attackers to make it seem like the message is coming from the IT department of your school or employer, your manager, friends, or companies that you do business with. These emails are successful because they manipulate our sense of urgency, fear, curiosity, greed, and desire to please.

Things to watch out for:

- Are you being asked to urgently do something? (log in to verify an account, retrieve messages, call IT support)
- Are you being asked to do something you don't normally do? (buy giftcards, change bank account numbers)
- Does this involve a password, money, or opening an attachment?

> ℹ You can help us protect others at the Institute: If you receive a phishing email please report it (using the Phish Alert Button or forward it as an attachment to phishing@mit.edu). If you receive an email you aren't sure about, please don't hesitate to ask. If you report using the Phish Alert Button, please leave a comment with your question. If not, please forward the email as an attachment to security@mit.edu and include your question.

Phishing examples

Recent phishing emails targeted at MIT are often shared on the MIT Phish Bowl. Also see Common Email Scams for examples and explanation of scams we often see over email.

If you've fallen for a Phishing scam

If you think you've fallen for a phishing scam please follow these steps to recover. It's important to change your password ASAP if it is compromised.

What can I do to protect myself?

MIT's Information Protection recommended tasks to protect low risk information can help protect your devices and data from malware that might be spread through phishing. The tasks include: running Sophos Anti-Virus and CrowdStrike security agents, enabling automatic updates in your browser and operating system, backing up your computer regularly, and enabling operating system firewalls to protect your computer.

Security Awareness training is also helpful to learn more about techniques used in phishing messages. Security Awareness Foundations (25 minutes) and Phishing Foundations (15 minutes) courses are available in the KnowBe4 Training Library.

See also

- Reporting Phishing Email
- MIT Information Protection