Social Engineering: What's the hype?

Taylor Kahny - 2025-03-12 - Data Privacy & Security

We often hear about “phishing” attacks in the news or in University security alerts. These attacks frequently use email messages to fool recipients into installing malicious applications (malware) or visiting fake websites through links or attachments. Phishing emails are just one of several social engineering techniques used by cyber attackers and criminals to exploit people’s inclination to trust. Other social engineering techniques to watch out for include...

Phone scam – If you receive a phone call requesting to verify your bank account, PIN, or a username and password, be wary. The caller may provide partial information to gain trust. When receiving such a call, refrain from providing sensitive information. Instead, call the entity’s officially published number to verify the legitimacy of the call.

USB flash drive – This often occurs when an infected USB flash drive is left in a place that is easily accessible to others. The victims insert this flash drive into their computers, resulting in the installation of malware. If you find a USB drive on a counter or the floor, hand it over to the ITS Service Desk in Fagin Hall Suite #202.

Scareware - This technique involves convincing the victims into thinking their computers are infected with malware or other issues. The victims are lured to “fix” the issue by clicking on a pop-up window button or on a webpage link. Malware is then installed once the victims click on the button or the link. If you

have clicked a suspicious pop-up window button, please contact the ITS Service Desk (servicedesk@nursing.upenn.edu) as soon as possible.

Security tip provided by the University of Pennsylvania Offices of Information Systems & Computing and Audit, Compliance & Privacy.