SCAM SAFETY TIPS

Criminals are constantly coming up with new schemes designed to compromise computers, steal passwords, trick you into revealing personal, financial, and other valuable information, or con you out of money. Scams can lead to identity theft, regular theft, access to your accounts and personal information, and compromised computers. And a compromised computer can put all of your information and passwords at risk.

KEY INDICATORS

- Requests for personal or private information, such as your password, financial account information, Social Security number, or money.
- Unexpected/unsolicited emails with links or attachments.
- Scare tactics or threats stressing that, if you don't act quickly, something bad will happen.
- Promises of something too good to be true. This includes bargains, "great offers," or links to claim an award or reward.
- Requests that you forward emails, attachments, links, etc., to your friends, co-workers, or family.

SAFETY MEASURES

- Install **antivirus software** and all necessary security patches and updates — and make sure you know what to do, if anything, to keep them current.
- Do not respond to email, instant messages, texts, phone calls, etc., asking for your password. You should never disclose your password to anyone, even if that they say they work for the University of Utah, other campus organizations, or places you do business (like your bank).
- Do not give sensitive personal, financial, log-in, business, system, or network information to anyone you don't know or who doesn't have a legitimate need for it.
- Do not open files, click links, or call numbers in unsolicited emails, text messages, instant messages, Facebook posts, tweets, etc.
- Do not click on unknown links. Instead, look up the website by a method you know to be legitimate — or contact the sender separately by a method you know to be legitimate in order to verify it.
  - Malicious links can infect your computer or take you to web pages designed to steal your information, and malicious attachments can infect your computer. Even seemingly legitimate links and attachments can be harmful.
  - Cryptic or shortened URLs (e.g. tiny URLs) are particularly risky because you can't easily tell where they are supposed to go.
- Do not click on links in pop-up ads or windows. Use your web browser's pop-up blocker, if it has one, to help prevent these ads from getting through.

SUSPICIOUS EMAIL?

If you cannot tell whether an email is legitimate, please forward it to **phish@utah.edu** or call your respective central IT help desk: Main campus, 801-581-4000, option 1; University of Utah Health, 801-587-6000.