Office of the Chief Information Security Officer
Risk Advisory: Phishing

BACKGROUND

Phishing scams are one of the fastest growing internet crimes. Cyber-criminals use phishing to steal personal information such as account usernames and passwords, social security numbers, or credit card numbers. In a typical scam, the cyber-criminal sends an email, SMS, or voice message with the intent to impersonate a person or business you know or trust. Phishing messages often include distressing or enticing statements to provoke an immediate reaction or they may threaten consequences if you fail to respond.

A common message asks you to reply with personal information or click on a link which takes you to a phony web page designed to look like the official website. The phony page may ask you to "update" or "confirm" information from a bank, internet service provider, government agency, or university office. Personal information may be abused to send spam via your email or social media account, obtain credit, or buy expensive items. To add insult to injury, cyber-criminals may then sell your information to other criminals for further misuse or to infect your computer with malware.

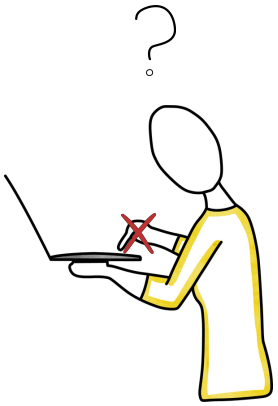
THERE ARE MANY TYPES OF PHISHING SCAMS, VARIATIONS INCLUDE:

- **Smishing** - cell phone text messages (SMS) that request personal information.
- **Spear Phishing** - messages that specifically target a particular individual. Cyber-criminals may spend considerable time researching their target in order to craft a convincing message. It usually includes information specific enough that the recipient may believe the message is authentic, and therefore be tricked into opening attachments that may contain malware.
- **Vishing** - phone calls made to potential victims by criminals who pretend to be from a person, business or financial institution and ask for personal information. Voice over IP (VoIP) technology makes this technique nearly untraceable while exploiting the potential victim's trust in traditional landline communication.

Office of the Chief Information Security Officer
Risk Advisory: Phishing

TIPS TO AVOID PHISHING SCAMS:

- Enable phishing filters or the safe browsing feature when available in your web browser.
- Keep an eye on the web browser address bar. Be cautious if the address changes unexpectedly or if you click on a link and are taken to an unfamiliar address.
- Exercise caution if a message sounds or a website looks suspicious, is out of the ordinary or unexpected, or contains an offer that is too good to be true.
- If you receive a message requesting personal or financial information, do not reply and do not click on the link in the message. Consider using a published or familiar phone number to contact the person or business referenced to determine the authenticity of the message.
- Don't use email to send personal or financial information, and delete any emails that ask you to confirm or divulge your personal or financial information.
- If you come across a phishing scam that specifically targets the University of Washington, please contact help@uw.edu.



This list is not exhaustive. For additional information, consult your department IT support person.

WHAT TO DO IF YOU HAVE FALLEN VICTIM TO OR SUSPECT A PHISHING SCAM:

- Advice on what to do from the Washington State Office of the Attorney General.
- If you suspect fraud, contact the Federal Trade Commission and the FBI's Crime Complaint Center.