Carnegie Mellon
INFORMATION SECURITY OFFICE

I Might Have Been Phished, What Do I Do?

Last Updated: August 10, 2016

"Phishing" is the practice of sending emails which often look legitimate and encourage recipients to click a link or respond via email and inadvertently provide information, often a username and password, to an unauthorized third party.

Don't Panic

Phishing messages, especially spear phishing, where a malicious message is sent targeting specific individuals or a group of individuals, have become more and more sophisticated over time, and appear like legitimate e-mail messages. Along with the attackers becoming craftier, we are all busy – constantly checking email on our computers and cell phones while juggling multiple responsibilities. It is difficult for even very experienced and computer savvy users to carefully review every message they receive to avoid falling for a phishing attack.

Today's scammers study their intended victims via public information like websites and directories to personalize their messages and better impersonate the alleged sender. Gone are the days when phishing emails were easily diagnosed by misspellings, grammatical errors, and commands like "Reply your password IMMEDIATELY or lose access". Now-a-days, scammers clone login screens and even redirect victims to their intended destination after stealing their login id and password.

The bottom line is that anyone can fall for a phish. The important thing is to detect it and recover quickly.

Move Your Hands Away from Your Keyboard

Some phishing messages will attempt to install malicious software onto your computer. Once you believe that you may have fallen victim or opened an attachment taking any actions on the computer may be risky. Keystrokes can be captured and sent to the attacker, or the system can be modified to cause damage or remove data. Use your phone or another computer to contact the ISO.

Leaving your computer running, without taking any other action on it, will preserve critical information for subsequent forensic investigation if necessary.

Disconnect Your Computer from the Network

If malicious software has been installed, removing the computer from the network will protect other systems on the network, and will mitigate potential data loss. Do not shut down the machine – if it is connected by cable, disconnect the cable. If it is connected on wireless many systems have a switch or button allowing you to manually disable the wireless card.

Based on the specific phishing message, the ISO will help to determine if any additional actions need to be taken to restore your computer to safe operation.

Report the Phishing Message to the Information Security Office

The ISO can block phishing e-mail messages to prevent others from receiving or responding to the same message. Phishing messages can be reported to the ISO via e-mail at iso-ir@andrew.cmu.edu or by phone at 412-268-2044. When e-mailing, please include the full headers of the message (instructions for doing so can be found at http://www.cmu.edu/iso/aware/email-headers.html)

ISO will walk you through evaluating the possible repercussions of responding, and will advise you of any other steps you should take in addition to the ones listed here.
Be prepared to answer the following questions, but don't delay contacting ISO if you are unsure of the answers:

- Did you click on the link in the email message?
- Did you provide your Andrew userID and password to a link in the email message?
- Do you work with PII or University Restricted data? (see http://www.cmu.edu/iso/governance/guidelines/data-classification.html)
- Do you have PII or University Restricted data in e-mail?

Change Your Password

If you think that you may have responded to a phishing message with your username and password please take the following steps:

1) Change your password immediately at https://identity.andrew.cmu.edu (login required). This should be done from a different computer than the one that you used to access the link in the phishing message.
2) Make sure to also change the passwords for any accounts where you may have reused the same password. For example, if you used the same password for your Andrew account and your Dropbox account (not recommended!), change the

password on both your Andrew account and your Dropbox account – preferably using a different new password for each!

To Learn More About Phishing

The Information Security Office licenses Anti-Phishing Phil (http://www.cmu.edu/iso/aware/phil/index.html) and Anti-Phishing Phyllis (http://www.cmu.edu/iso/aware/phyllis/index.html) to provide a fun way to help you spot phishing messages.

Revision History

Version	Date	Author	Description
1.0	04-AUG-2016	Laura Raderman <lbowser>	Initial Document