What You Need to Know About Phishing

What is Phishing?

Phishing is a tactic cybercriminals use to gain your personal information. Their ultimate goal is to use your information to gain access to your identity and your money. Often, emails, websites and text messages with malicious software attached are downloaded to your computer or device and can steal your information.

How Does it Work?

There are three steps cybercriminals use:

1. Lure – They send out an enticement that encourages you to follow a link to a malicious website or to open an attachment that launches a malicious process on your computer.

2. Hook – Once you have clicked on the link to the malicious website, you will be asked to disclose personal information. Often these malicious websites look and feel like a legitimate site.

3. Catch – The cybercriminal uses the information they have collected to steal your money and identity.

Think Before You Click!

For more information visit
www.fdic.gov/consumernews

How Do You Protect Yourself?

1. Keep your software up to date. Manufacturers are constantly updating their products to fix any weaknesses in their security. Before installing any update, however, verify the update is valid. Criminals have imitated software venders saying they are providing a security update, when really they are distributing malware. Once you confirm it is legitimate, install the update as soon as possible.

2. Install anti-virus software. Criminals will often use links or attachments in an email to download malware to your computer. Anti-virus software will search for and help remove any malware. Also, it is best to only use security products from reputable companies.

3. Only shop online with reputable companies. Anytime you are inputting personal or financial information within a website, such as online shopping, make sure you are dealing with a reputable company. Look for a padlock symbol on the webpage and that the web address starts with "https://." The "s" stands for secure, so you can be confident that the website you are on is a secure page.

4. Be careful where and how you connect to the internet. Don't use public computers or public Wi-Fi when doing any kind of online shopping or banking. Criminals can use Wi-Fi in public areas to intercept your device's signals and collect your information.

Sources: FDIC Consumer News &
The Counter Intelligence Awareness Library