Protecting Yourself Against Internet Fraud

Phishing and Pharming
Internet scams are now a part of everyday life. It's important that you know how to spot one and how to avoid becoming a victim.

What is Phishing?
Phishing scams are just another attempt to get valuable information. Scammers often use an unsolicited phone call, email, text message or social media request from an individual claiming to be a representative from a financial institution, credit card issuer or other "trusted" source. Emails often state you should update your information for one reason or another, and they usually provide a link to do so.

While this may sound reasonable and look legitimate, the link provided does ***not*** take you to the financial institutions' website. Instead, you'll be submitting your sensitive information to a website run by scammers.

What is Pharming?
Similar to phishing, pharming seeks to obtain personal information by secretly directing you to a copycat website where your information is stolen, usually with a legitimate-looking form.

Why Phishing and Pharming Scams?
Lots of sensitive information can be gathered by phishing and pharming scams; account numbers, passwords, SSN, date of birth, etc. Gaining this personal information may help a scammer try to hijack your assets, steal your identity and open credit accounts in your name.

Don't Fall for Phishing and Pharming Scams.
Simple scams are easy to spot, but anybody can be tricked by a sophisticated phishing or pharming scam. Graphics and company logos along with links that look like a financial institution's website can be deceiving. The best way to avoid becoming a victim of a scam is to use your best judgment. No financial institution should contact you and ask for all of your sensitive information.

Protect Yourself:

- If you are contacted and asked to confirm confidential information, **do not** click on any link provided or provide any information. If the individual contacting you is legitimate, they should have your information and not need to ask you to provide such confidential details. If you believe the contact could be legitimate, use a phone number or website you know is legitimate for any necessary follow-up.
- Before submitting any financial information through a website, look for the "lock" icon on the web browser status bar, or look for "https" in the web address.
- Report suspicious activity to your financial institution or government agencies.
- Install anti-virus and anti-malware ("spyware") software on your computer. Update the software regularly; including operating system patches and updates.

If You Become a Victim of a Phishing or Pharming Scam
If you have been snagged by a phishing or pharming scam, you need to be vigilant.

1. Let your financial institution know what happened. They will likely want to pursue the scammer and will monitor your account more closely.
2. Victims should put a fraud alert on their credit report by contacting one of the major credit agencies.
3. Keep a close eye on your mail and accounts. If statements stop showing up or if you see unusual activity, call your bank immediately.