Online Security

The Internet is a great source for information and has made everything from shopping to managing your money a lot more convenient. Unfortunately, the Internet also provides a rich avenue for thieves looking to steal your personal information and commit fraud at your expense. While nothing provides full-proof protection, it is essential that if you use the Internet you take steps to protect your personal information.

Common Types Of Online Fraud

To begin, you should know that no representative of Central Credit Union Of Illinois will ever request your account numbers, PINs, social security number or other personal information via email. Neither will most other financial institutions, credit card companies, government agencies or reputable businesses.

Below are a few of the most common online scams designed to acquire your personal information.

Phishing

With phishing, identity thieves distribute email designed to look like it was sent from a financial institution, government agency, credit card company or retailer with whom you may or may not have a relationship. The purpose of the email is to get you to enter personal information, which the thieves may then use to obtain credit in your name, drain your bank accounts, secure identification in your name, open bank accounts in your name from which they can write bad checks, and more.

Phishing emails often look authentic even containing corporate logos. Such emails request that you enter some type of personal information such as an account number, Personal Identification Number (PIN), social security number or your mother's maiden name. Usually, you are told that the information is being requested to update an account, reactivate an account, furnish you with something you've won, avoid a penalty of some type or to resolve a problem. You may be asked to enter the information in the email and send it back or you may be directed to a site via a link in the email where you can enter your information.

To protect yourself:

- Do not respond to unsolicited emails. Never send your personal information in response to an email request. In general, you should not send personal information via email as email is not secure. If you must send such information by email, make sure that you have encrypted the information before you send it.
- Do not follow links embedded in unsolicited emails. While they may lead you to sites that appear to be legitimate, it is very possible they are not.

Spoofing

Spoofing is when thieves create a web site that appears to be legitimate but is in fact a fraudulent site designed to fool consumers into entering their personal information. A "spoofed" site may be one that you are directed to as a result of a link in a phishing email. It could also be a site that you come across online that appears to be a legitimate retailer or other business.

To protect yourself from entering personal information on a "spoofed" site:

- Do not connect to retailer sites through email links. Instead, obtain the official URL through an online search and type the address into your browser.
- Before making a purchase online and entering your personal information, be sure that you are using a secure site. If you are at a secure site, a padlock will appear at the bottom of your window. Most secure sites also have URLs that begin with https: or s-http:.

Spying and Pharming

Thieves may be able to access your personal information even if you don't enter it online. Unsolicited emails, or spam, that you receive may contain viruses that can destroy your software, allow others to follow your online activity or view information that you may have stored on your computer. Other viruses can corrupt your browser and take you to fake web sites when you input the URL of legitimate sites that you use where you may input personal information.

To protect yourself:

- Do not open email or email attachments from people you don't know.
- Install a firewall on your computer to protect it from other computers while online.
- Purchase anti-virus and anti-spyware programs and install them on your computer. Be diligent in keeping your programs up-to-date. Most programs offer online software updates.
- Check periodically to see if your system software manufacturer has software security patches that should be installed on your computer.

Steps To Take If You Are A Victim

If you have been the victim of a phishing scam or other online fraud, you may become an identity theft victim and should take immediate action.

- Notify the company whose name the fraudulent email was sent in to let them know about the scam. Phishing emails should also be forwarded to spam@uce.gov.
- Notify your financial institutions and credit card companies, and close any accounts that you know are affected. Take security precautions with others by changing your passwords, logins, etc.
- Contact local law enforcement and file a complaint at www.ftc.gov.
- Place a fraud alert with the credit bureaus to help prevent thieves from using your credit and opening new accounts in your name. To place an alert on your credit report, contact one of the following agencies. The others will then add the alert to your file as well.
    - Equifax: (800) 525-6285; www.equifax.com
    - Experian: (888) 397-3742; www.experian.com
    - TransUnion: (800) 680-7289; www.transunion.com

For more information about identity theft, we recommend that you visit the Federal Trade Commission's web site. The Commission offers a comprehensive free online guide for those dealing with identity theft at www.ftc.gov/bcp/edu/pubs/consumer/idtheft/idt04.shtm.