Your Guide to Fighting Identity Theft

Protect YOUR Personal

Financial Information

How to Protect Yourself

1 **Never provide your personal information in response to an unsolicited request**, whether it is over the phone or over the Internet. E-mails and Internet pages created by phishers may look exactly like the real thing. They may even have a fake padlock icon that ordinarily is used to denote a secure site. If you did not initiate the communication, you should not provide any information.

2 **If you believe the contact may be legitimate, contact the financial institution yourself.** You can find phone numbers and Web sites on the monthly statements you receive from your financial institution, or you can look the company up in a phone book or on the Internet. The key is that you should be the one to initiate the contact, using contact information that you have verified yourself.

3 **Never provide your password over the phone or in response to an unsolicited Internet request.** A financial institution would never ask you to verify your account information online. Thieves armed with this information and your account number can help themselves to your savings.

4 **Review account statements regularly to ensure all charges are correct.** If your account statement is late in arriving, call your financial institution to find out why. If your financial institution offers electronic account access, periodically review activity online to catch suspicious activity right away.

LINCOLNWAY Community Bank ™

1000 East Lincoln Highway, New Lenox, IL 60451
815/462-4300 - www.LWCBank.com

What does it look like?

In a typical case, you'll receive an e-mail that appears to come from a reputable company that you recognize and do business with, such as your financial institution. In some cases, the e-mail may appear to come from a governmental agency, including one of the federal financial institution regulatory agencies, such as the FDIC.

The e-mail will probably warn you of a serious problem that requires your immediate attention. It may use phrases, such as "Immediate attention required," or "Please contact us immediately about your account." The e-mail will then encourage you to click on a button or a link to go to the institution's website.

In a phishing scam, you could be redirected to a phony website that may look exactly like the real thing. Sometimes, in fact, it may be the company's actual website. In those cases, a pop-up window will quickly appear for the purpose of harvesting your financial information.

In either case, you may be asked to update your account information or to provide information for verification purposes: your Social Security number, your account number, your password, or the information you use to verify your identity when speaking to a real financial institution, such as your mother's maiden name or your place of birth.

What to do if you fall victim:

- Contact your financial institution immediately and alert them to the situation.

- If you have disclosed sensitive information in a phishing attack, you should also contact one of the three major credit bureaus and discuss whether you need to place a fraud alert on your file, which will help prevent thieves from opening a new account in your name. Here is the contact information for each bureau's fraud division:

Equifax	**Experian**	**TransUnion**
888-766-0008	888-397-3742	800-680-7289
P.O. Box 740241	P.O. Box 4500	P.O. Box 2000
Atlanta, GA 30374	Allen, TX 75013	Chester, PA 19022

- Report all suspicious contacts to the Federal Trade Commission through the Internet at **www.consumer.gov/idtheft**, or by calling **1-877-IDTHEFT**.

A message from the federal bank, thrift and credit union regulatory agencies.
Board of Governors of the Federal Reserve System, Federal Deposit Insurance Corporation, National Credit Union Administration, Office of the Comptroller of the Currency and Office of Thrift Supervision