



For Immediate Release

May 19, 2005

Phishing, ID Theft Crimes Begin Targeting Wisconsin Banks

By Kurt Bauer, president/CEO of the Wisconsin Bankers Association

Phishing – pronounced fishing – is when thieves e-mail hundreds of thousands of people stating that they represent a bank or another financial institution and ask you to provide your personal account information. Basically, the crooks are “phishing” for information from a randomly selected group of individuals in hopes that someone will fall for the scam and provide their personal account data.

The Wisconsin Bankers Association has noticed an increase in the number of phishing scams that are targeting Wisconsin-based banks. Consumers should note that a bank would never e-mail or call their customers asking for their account information because they already have access to it.

These e-mails can look quite convincing, with company logos and banners copied from actual Web sites; however, when looked at closely, many of these e-mails are poorly written with grammatical mistakes. Often, these scammers will tell you that a security procedure has changed at the bank or that they need to update (or validate) your account information, and then direct you to a look-alike Web site. If you respond with your personal account information, the thieves use that information to order goods and services or obtain credit.

Consumers should note that with your account information, Social Security number, PINs, credit card numbers, passwords, mothers’ maiden name and other personal information, these con artists can do some serious damage to your account and steal your money. They can also ruin your good credit.

To avoid becoming a victim of a phishing scam, the Wisconsin Bankers Association offers these tips:

- If you don’t initiate the call or e-mail, never give out your personal financial information. If someone calls you or e-mails you asking for your personal information, never give it out. Banks would never call or e-mail their customers asking for that information.
- Do not respond to e-mail that may warn of shutting down your account or other dire consequences unless you validate your information immediately. Contact the company to confirm the e-mail's validity using a telephone number or Web address you know to be genuine.

- Check your credit card and bank account statements regularly and look for unauthorized transactions, even small ones. Some thieves hope small transactions will go unnoticed. Report discrepancies immediately.
- When submitting financial information to a Web site, look for the padlock or key icon at the bottom of your browser, and make sure the Internet address begins with "https." This signals that your information is secure during transmission.
- Report suspicious activity to the Internet Crime Complaint Center, a partnership between the FBI and the National White Collar Crime Center. You can file a complaint at www.ifccfbi.gov/cf1.asp.
- If you responded to an email, contact your bank immediately so they can protect your account and your identity.
- For more information on phishing, visit the Federal Deposit Insurance Corporation at www.fdic.gov, the Federal Trade Commission at www.ftc.gov or the Anti-Phishing Working Group at www.antiphishing.org.

Phishing is fast becoming one of the most common forms of identity theft and it's been called the hottest, most troubling new scam on the Internet. A total of 43.4 percent of adults have received a "phishing" contact and it's estimated that nearly 5 percent of all "phishing" attempts are successful, according to First Data Debit Services. It's now the fourth most common Internet scam, based on complaints to the National Consumers League's National Fraud Information Center/Internet Fraud Watch database.

-30-

For more information, please contact Cheryl McCollum at the Wisconsin Bankers Association at 608/441-1216 or cmccollum@wisbank.com.

The Wisconsin Bankers Association represents 310 Wisconsin banks of all sizes.

Wisconsin Bankers Association, 4721 S. Biltmore Lane, Madison, WI 53718, 608/441-1200