Let's Talk Finances

Protecting Your Personal Information and Money

By Charles Schmalz
President of
East Wisconsin Savings Bank

Last week we covered several common scams used to target bank customers. Here are some basic precautions you can use to help keep yourself from becoming a victim of financial fraud.

- Avoid offers that seem "too good to be true." If someone promises "opportunities" that are free or with surprisingly low costs or high returns, it is probably a scam. Be especially suspicious if someone pressures you into making a quick decision or to keep a transaction a secret.

- No matter how legitimate an offer or request may look or sound, don't give your personal information, such as bank account information, credit and debit card numbers, Social Security numbers and passwords, to anyone unless you initiate the contact and know the other party is reputable.

- Remember that financial institutions will not send you an email or call to ask you to provide account numbers, passwords or other sensitive data because they already have this information. To verify the authenticity of an email, independently contact the supposed source by using an email address or telephone number that you know is valid.

- Be cautious of unsolicited emails or text messages asking you to open an attachment or click on a link. This is a common way for cybercriminals to distribute malicious software, such as ransomware. Be especially cautious of emails that have typos or other obvious mistakes.

- Use reputable anti-virus software that periodically runs on your computer to search for and remove malicious software. Be careful if anyone (even a friend) gives you a thumb drive because it could have undetected malware, such as ransomware, on it. If you still want to use a thumb drive from someone else, use the anti-virus software on your computer to scan the files before opening them.

- Don't cash or deposit any checks, cashier's checks or money orders from strangers who ask you to wire any of that money back to them or an associate. If the check or money order proves to be a fake, the money you wired out of your account will be difficult to recover.

- Be wary of unsolicited offers "guaranteeing" to rescue your home from foreclosure. If you need assistance, contact your loan servicer (the company that collects the monthly payment for your mortgage) to find out if you may qualify for any programs to prevent foreclosure or to modify your loan without having to pay a fee. Also consider consulting with a trained professional at a reputable counseling agency that provides free or low-cost help. Go to the U.S. Department of Housing and Urban Development website for a referral to a nearby housing counseling agency approved by HUD or call 1-800-569-4287.

- Monitor credit card bills and bank statements for unauthorized purchases, withdrawals or anything else suspicious, and report them to your bank right away.

- Periodically review your credit reports for signs of identity theft, such as someone obtaining a credit card or a loan in your name. By law, you are entitled to receive at least one free credit report every 12 months from each of the nation's three main credit bureaus (Equifax, Experian and TransUnion). Start at AnnualCreditReport.com or call 1-877-322-8228. If you spot a potential problem, call the fraud department at the credit bureau that produced that credit report. If the account turns out to be fraudulent, ask for a "fraud alert" to be placed in your file at all three of the major credit bureaus. The alert tells lenders and other users of credit reports that you have been a victim of fraud and that they should verify any new accounts or changes to accounts in your name.

To learn more about how to avoid financial scams, visit the website for the Financial Fraud Enforcement Task Force at www.stopfraud.gov/protect.html.