Social Engineering

“Social Engineering” is any method of theft that manipulates your human nature in order to gain access to your online financial accounts. Here are a few ways you can protect yourself from thieves using Social Engineering techniques:

1. Don't respond to ANY email or social network post or message that asks for money or confidential information. Thieves can hack email and social network accounts, and then pose as a friend or family member in order to gain your trust.
2. Don't assume that an unsolicited phone call or email is actually from a trusted source. Thieves can research your purchases or donations, then pose as a business or charity you trust. Or, they may pose as law enforcement, a bank officer or another trusted authority figure. Just because they have bits of information about you or your past activities doesn't mean they are legitimate.
3. Verify, verify, verify. If someone on the phone, or a message in your inbox, is telling you there is a problem with your online banking account, online auction account or credit card account, don't give them additional information to “fix” the problem. Instead, hang up the phone or delete the email and check those accounts directly by logging in normally or calling a published customer service number.
4. Be conscious of what can be learned about you. Many kinds of online accounts, including online banking, use challenge questions as part of their security. Make sure you don't choose responses that can be found online. For example, don't use your mother's maiden name if it is mentioned on a social network profile; or the model of your first car, if you discussed it on a forum. Thieves are very good at digging out those details from online searches.
5. Remember, even the most innocent email attachments can be infected with computer malware. Common and popular files like PDFs, JPGs and spreadsheets can provide a platform for installing viruses or keystroke-logging malware on your computer. If you aren't certain the file came from a legitimate business, charity or person, don't open it without verifying. Call them and ask if they sent an email with an attachment.

The thieves are smart and very good at exploiting your honesty and natural cooperation. They can send email that looks like it came from a family member, or hijack your best friend's social network account. Don't let your good nature become your downfall.

The best way to avoid Social Engineering schemes is to be cautious and suspicious of ANY request for money, passwords, account numbers or other confidential information – no matter where it seems to be coming from.

Remember: Your identity is one of the most valuable things you own. It’s important to keep your identity from being stolen by someone who can potentially harm your good name and financial well-being. Identity theft occurs when someone uses your name, address, Social Security Number, credit card or financial account numbers, passwords, and other personal information without your knowledge to commit fraud or other crimes. While the words may sound like a foreign language -- Phishing, Pharming, Vishing, Spyware, Dumpster Diving — they are actually techniques used by thieves to put your identity and finances at risk. And their attacks grow more frequent and sophisticated every year. Identity theft is the fastest growing crime in the United States. According to US Department of Justice statistics, it’s now passing drug trafficking as the number one crime in America.