Defending Yourself Against Identity Theft

As technology advances, you can be sure that identity thieves are not far behind. Here are some common methods cyberthieves use to steal your personal information and how you can increase your security while shopping or banking.

Phishing/vishing

Your email messages may not be quite what they appear to be if you're targeted by a phishing scam. Phishing is the act of sending fraudulent emails that seem to come from familiar businesses. These messages contain links to phony websites designed to steal personal information either directly or through malware and keyloggers. Often you'll see a problem referenced with a request to click on the link provided to correct it. Once you've entered your information, ID thieves can access your accounts.

Vishing is the telephone version of phishing. Callers are sometimes bold enough to suggest the victim call back to verify authenticity. But the vishers don't actually hang up; instead they play a recorded dial tone to make the victim believe he's making a call.

Debit and credit card fraud

Most shoppers love the convenience of plastic, and identity thieves use this to their advantage whether it involves skimming, phishing, vishing, malware, mail theft or just looking over a victim's shoulder to steal account numbers. Someone running up debt in your name can ruin your credit score. When debit cards are compromised, it's particularly alarming because fraudulent purchases drain your checking account instantly.

BEC scams

Business email compromise, or BEC, scams have cost companies more than $1.2 billion. A phony email from a CEO requesting that funds be transferred per attached instructions is sent to an employee. Because the email appears to come from the employee's superiors, and because the message so closely resembles requests this employee receives regularly, the transfer is often made without question. The money then ends up in overseas accounts that are almost impossible to trace.

Tips to protect yourself

To even further reduce fraud risk:

- Install the latest editions of antispyware, antivirus, firewalls and browsers to all devices, and password-protect them.

- Use strong passwords for all accounts and change them frequently.
- Monitor accounts and credit reports to detect fraud early
- Don't use public Wi-Fi networks for financial transactions.
- Keep cards away from public view, and shred personal documents before discarding.
- Opt in for two-factor authentication on accounts.
- Turn off bluetooth and near-field communication when not in use.
- Don't click on email links. Type full web addresses to access business websites.
- Never share sensitive information in response to an unsolicited call or email.
- To verify calls, hang up for at least one minute to ensure the first call is disconnected. Call the customer service number listed on your bank's website or the back of your credit card, not a number provided by an unsolicited contact.
- To protect your business from BEC scams, use a two-step verification process for all money transfers. Verbal confirmation is also wise.

Staying informed and adopting smart fraud prevention practices will go a long way toward protecting your identity. Between your efforts and your bank's security, you should be able to stay a step ahead of identity thieves.

© Copyright 2016 NerdWallet, Inc. All Rights Reserved