7 Simple Things You Can Do To Protect Yourself From Bank Fraud

How To Stop Cybercriminals, Rogue Employees and Unethical Vendors From Robbing You Blind

By Bob Jenner and Michael Reuben, Ph.D.

A Collaboration of The Network Doctor, Inc. and LA Computer Works.

7 Simple Things You Can Do To Protect Yourself From Bank Fraud

There are many ways that criminals try to separate you from your valuable, often hard-earned assets. One of the costliest and most prevalent is bank fraud. ABA research has shown that fraud against bank deposit accounts amounted to $25.1 billion in 2018, up from $19.1 billion in 2016 and there has been a steady rise for decades. A significant part of that rise can be attributed to the world becoming more connected through the internet. Although there are non-internet related ways for bank fraud to occur including bank card skimming at gas stations, check washing, check forgery, etc the fastest growing forms of bank fraud are related to identity theft and various forms of scamming. Many of the best ways of protecting yourself from being a victim of bank fraud is to be aware of the problem and to stay vigilant. Here are 7 of the best ways to protect yourself from becoming a victim.

1) **Monitor your accounts**. Part of being vigilant is to regularly monitor your accounts either by viewing them for unusual activity through online banking or by using monitoring services provided by your bank or third-party services.
2) **Guard your online information**. Think twice before sharing your information. Don't go handing out you're your personal information like social security numbers, street addresses, your mother's maiden name, etc. Minimize the information you give to online or in store merchants. Corrupt merchants may turn around and sell your information to others who are equipped to take advantage of your personal information to steal from your bank account one way or another.
3) **Go paperless and shred your documents**. Mail theft has become rampant. Thieves aren't just looking for checks to intercept in the mail, but also personal information that can be found on bank statements, credit card statements, financial and loan documents and much more. Going paperless helps secure your information from people who would use that information if not to directly impersonate you in some way, but to also social engineer additional information about you from others who know you. The thief gains trust from someone you know because they appear to have personal information about you and they cleverly manipulate your friend to reveal additional information you. We save paper to recycle, but in many neighborhoods your recycle bins are searched for refundable cans or bottles, but also intact paper with personal information on it.
4) **Check your online credit report**. When your identity is stolen the thieves steal your money by impersonating you to the bank, a mortgage company or other financial institution. Often, they can do that online and are never seen by the loan officer or bank teller. Even the process of depositing your checks over the internet, while providing a great convenience in your not having to go to your bank to make a deposit, creates another opportunity for thieves to steal from you and not once but repeatedly. It used to be that when a thief cashed a washed check, they lost the check to the bank when they deposited the fraudulent check. Now with remote deposit via their cell phone the thief retains the check to be washed and used again. If you aren't monitoring your account, they may steal from you multiple times, redepositing the same fraudulent check over and over again.

   (***Tip:*** You can get a free copy of your credit report from each of the three major credit-reporting bureaus every year. By getting one of these reports every four months, you'll never have to pay to check your report.)
5) **Create strong passwords and use 2-factor authentication wherever possible**. Using your pet's name or your children's initials or your birth or anniversary dates as your passwords to online services like you bank or with online merchants is just asking to be stolen from. That information is easily obtained from any number of sources and practiced thieves know all the easy ways to get that information. Posting on Facebook where you went on your 20th anniversary or the cute pictures of your dog "Spot" provides clues to those simplistic passwords that all too many of us use because a strong password is way harder to remember. Consider using a password manager so you can use strong passwords and not have to worry about whether you will remember them.
6) **Beware of phishing scams**. Phishing scams are abundant. They can range from thieves posing as bank officers contacting you via email to ask you to update your account information

or even a scammer posing as an IRS agent, again, asking for your personal information. Phishing scams are not just perpetrated over the internet. Scammers can call your phone claiming your account is overdue or your grandson has been arrested and needs to be bailed out. Since phishing scams are so common and at times, so professionally done, it's important that you never give your personal information via the phone or through email. (Unless you're the one who has made the call to the number you know is legitimate.)

7) **Put a Password on your phone.** How much of your personal information is stored on your phone? Probably a lot – just ask yourself if you have a banking or finance app that you use. With all the apps, a stolen phone could be a gold mine for an identity thief. Put some type of password on your phone so that if it's lost or stolen nobody can access it. Remember, mix it up here as well, or add TouchID on an iPhone so you can have your fingerprint as your passcode.