Habits That Threaten Your Identity and Pocketbook

Article Highlights

- What's In Your Wallet Or Purse
- Your Fear Of The IRS
- Using Public Internet Connections
- Not Screening Your E-Mails
- E-Mailing And Texting Sensitive Information
- Being Free and Easy With Passwords
- Using Identical Passwords

They're just old habits. You likely to do them without even thinking. But these habits could be making you vulnerable to hacks, scams, ID theft and Internet phishing schemes out to separate you from your hard-earned money.

1. **What's in Your Wallet or Purse?** Does it contain items that include your Social Security Number (SSN) and birth date? For instance, does it contain your driver's license and either your Social Security card or Medicare card? If it does, and the wallet or purse falls into the wrong hands, the thief will have both your SSN and birth date, the two key items that can be used to compromise your identity. If your ID gets hacked, you are in for a long-running and expensive nightmare. Make sure your wallet or purse isn't a jackpot for an ID thief.
2. **Your Fear of the IRS**. It is common for most folks to have a natural fear of the IRS. Get a letter in the mail from the IRS, and the adrenalin kicks in and your pulse rate quickens. Scammers play on that emotion to ply their scams on the unsuspecting who don't want to have any problems with the IRS. These range from e-mail messages to personal calls threatening arrest, property seizure or other dire consequences. But wait a minute! The IRS only initially communicates by U.S. mail, so any other form of communication is fake, and you can hang up on the caller or delete the e-mail without fearing you'll incur the IRS's wrath. Still unsure? Call your tax preparer. **Don't be a victim!**
3. **Using Public Internet Connections.** These days you can find public Internet connections almost anywhere – at the airport, your favorite coffee house and even shopping malls. Getting work done or taking care of financial dealings while you are out and about may seem like a good idea, but remember the cyber thieves also have access to that Wi-Fi and they have the know-how to access your computer through that Wi-Fi connection. Only use secure Internet connections to get work done or conduct financial transactions, and save public connections for personal browsing purposes.
4. **Not Screening Your E-Mails**. ID thieves send out e-mails trying to entice you into clicking on an imbedded link within the e-mail, which will then allow them access to your computer and whatever is on it. They will try to sucker you into clicking on the imbedded link by promising free this and that, or even telling you that you have won a monetary prize and need to go to a website to claim it. Don't be tempted; just remember, if it's too good to be true it probably isn't true. Just delete the e-mail!
5. **E-Mailing and Texting Sensitive Information.** What we all forget is how easy it is for e-mail and text messages to get hacked. You have to worry not only about your end getting hacked but also about the one to whom you are sending the message. Never send documents that include sensitive

information. A common error is to inadvertently send a document with your SSN, birth date, passwords, or other information. The best practice is to always assume your e-mails and texts can be seen by others and act appropriately.

6. **Being Free and Easy With Passwords.** It may not seem like a big deal to share your password with a family member that you're close to, but even if that person is completely trustworthy, they may not be as safety conscious as you and may accidently leak the password. You should always keep your passwords completely confidential to ensure that they don't fall into the wrong hands.
7. **Using Identical Passwords.** It is easier to remember one password than several, and in today's digital world just about everything needs a password. But if you use just one and it gets compromised, then all your accounts are compromised. It is a best practice to use a different password for every account. In addition, it is a good idea to periodically change your passwords.

Bottom line, stop and think before you act, always be skeptical of unsolicited and unexpected communications, guard your sensitive information like you are guarding Fort Knox and when in doubt call this office for assistance.