Badger Bank

Especially during the holiday season, there are a number of things you should do, both as an individual and as a business, to prevent identity theft. Here are tips to follow in case you aren't sure if something is phishy or legit.

1. Be stingy with your SSN.

Always remember that the only people who have the legal right to demand your social security number are government bodies, like the motor vehicle department, welfare department, tax department and organizations such as banks, brokerages and your employer. The Social Security Administration provides specific guidelines on who is and who is not deserving of your SSN.

2. Don't brush aside the small bits.

Your SSN is a goldmine, but it's not the only factor that matters. Seemingly innocuous information – your full name, address, date of birth, etc. – can be pieced together by fraudsters, materializing enough of your identity to do damage.

3. Protect your trash.

Tear up or (preferably) shred all documents that contain personal information once you don't need them anymore. Fraudsters are not too proud to dumpster dive.

4. Opt out.

Just say no to unsolicited mailers/email, preapproved credit card applications and telemarketing calls. The FTC provides guidelines to secure and customize your opt-out – by mail or online, for five years or permanently, etc.

5. Be aware of your surroundings.

Whenever you're writing down personal information or typing it on a computer, check to ensure that there are no "shoulder surfers" around who are trying to take a peek. Never enter personal information on a public computer.

6. Require the photo ID.

Instead of putting your signature behind your credit cards, write: Ask for Photo ID. It's not a perfect solution, but it certainly adds an extra line of defense by requiring that your identification be verified each time you or anyone else presents your credit card.

7. Dispose digital data diligently.

Before you throw away any digital equipment, make sure it's completely wiped clean of all data. Deleting the data alone is not enough. Do an online search for data sanitizer software – they're not expensive, and the data fumigation is priceless.

8. Scrutinize your statements.

Review all statements with diligent eyes each month, making sure you recognize all purchases and transactions.

9. Check up on your credit report.

The Fair Credit Reporting Act (FCRA) requires that each of the nationwide consumer reporting companies (e.g., Equifax, Experian and TransUnion) provide you with a free copy of your credit report, at your request, once every 12 months. The FTC provides easy instruction on how to tackle this process.

10. Don't leave it to the mailbox.

Personally mail all bills or documents that contain your personal information either at the post office or through a service mailbox. Leaving them in your unguarded mailbox at the end of the driveway is just another invitation for fraud.

11. Check your receipts.

It's very rare, but some vendors are still printing receipts with your full credit card number and expiration date. If this happens to you, scratch out the details before signing. Then let the vendor know that they are violating the Fair and Accurate Credit Transaction Act (FACTA), which requires businesses to shorten credit/debit card numbers on electronically printed receipts –exposing no more than the last five numbers of your account – and forbids them from printing the expiration date altogether.

12. Be careful when opening attachments and downloading files.

You can obtain a virus, worm, or Trojan simply by opening e-mails and attachments, and by accepting files from your friends, family, or others. If you choose to download files, make sure your security software is enabled and pay close attention to any warnings provided. Use e-mail wisely. E-mail is a great way to keep in touch with friends and family, and as a tool to conduct business. Even if you have good security software on your PC, your friends and family might not have the same protection. Be careful about what information you submit via e-mail. Never send your Social Security number, credit card information, or other private information via e-mail.

13. Do not reply to spam e-mail.

If you don't recognize the sender, don't respond. Even replying to unsubscribe could set you up for more spam.

14. Respect the padlock.

We all got a lesson in browser protection when Heartbleed hit the fan. When making purchases online, always look for that "https" and padlock symbol in the website address, indicating that your information is encrypted before transmission. Click the padlock to get the details of the website's digital certificate and, of course, always keep a close eye on your online purchases.

While the padlock is now commonplace, things like Heartbleed remind us how additional lines of defences are essential. There is also an additional line of security added with the "Verified By Visa" and its MasterCard equivalent where you need to enter an additional password whenever you use your card online. You should actively seek this even if your card company hasn't offered it yet. Basically, when you make a purchase online, key in your card details, you're then taken to another page where you need to enter the credit card password that only you know.

15. Be social with caution.

Social networking sites like Facebook, LinkedIn and Twitter are information goldmines for crafty social engineers. It's easy to seem credible, professional, familiar, charitable, affable and harmless in the social sphere. Don't be an open e-book.

16. Respond with caution.

Don't respond to emails or texts asking you for personal information, even if the sender seems credible (e.g., the government, a bank or your favorite e-commerce site). And remember: It's incredibly rare to win lotteries, drawings and awards. Don't be an easy target.

17. Act with urgency.

If you think you've become a victim of identity theft, follow FTC guidelines immediately.