June 2018

Reducing your Information Footprint

noabank
Good People, Smart Banking Member FDIC

From the desk of Judy Allen, Information Security Officer

From the desk of Thomas F. Duffy, MS-ISAC Chair

While spring cleaning your home and, if you're like me, the top of your desk, consider also cleaning up your information footprint. Your information footprint is how much information about you is recorded and available in both digital and paper formats. Cleaning up your footprint can mean examining social media, online accounts, and even paper records containing sensitive information. While we may use a few key digital devices and services on a regular basis, they often contain more information about us than is necessary. It's also likely that devices and services we don't use anymore may still contain information. You might have that pile of paper you've been meaning to shred for a while, making this an opportune time to spring clean your information footprint. By spending a little bit of time and effort, you can better secure your information to safeguard against various forms of identity theft.

Disks, Hard Drives, and USB drives, Oh My!
Over the years, it's easy to accumulate a mass of CD's, DVD's, hard drives, and USB drives that are no longer needed or with data that is no longer needed stored on them. If you have hard drives or USB drives with old data but want to continue to use them, consider following US-CERT's guidance on how to securely clean the data off of these items before properly recycling them. Many shredders, including those rated for home use, can shred CDs and DVDs. If your shredder can't handle them, check your local community for shredding days as many towns, schools, and office supply businesses will sponsor shredding events.

Clean Up Your Paper Trail
Many of us have a large quantity of paper documents that may contain sensitive information about ourselves, financial accounts, government identification information, tax returns, and more. Take some time to go through these documents this spring and check whether it is something you truly need to hold onto. If the answer is no, be sure to securely dispose of it by shredding it and recycling the shredded pieces. Simply ripping up sensitive documents is not enough to guarantee your information is unreadable.

Not sure how long you should hold on to those old documents? The Federal Trade Commission (FTC) has a handy website – "A Pack Rat's Guide to Shredding" with information on how long you should hold on to those documents!

Closing Old Online Accounts
It is common for people to use many different shopping sites, social media outlets, online storage, clubs, and other online outlets that require you to enter, store, and sometimes share information from or about you. If you are no longer using any of these accounts, consider removing information that may be sensitive and consider closing them out if you do not plan to use them again. Sometimes, it is easiest to check out as a guest when shopping online at a place that you rarely, if ever, patronize. Checking out as a guest should minimize the data retained about you.

Old Social Media Accounts
Remember MySpace? LiveJournal? Do you still have that old email account or an account on an old dating website? As we move from Myspace to Facebook to Twitter, Instagram, and the other latest and

greatest social media platforms, our old accounts and information are left behind, filled with personal details. Consider closing out social media accounts that you no longer use, as it will reduce your digital footprint. Keep in mind that all social media platforms have different policies when deleting old accounts and content. Be sure to read the policy. And, don't forget to remove the app from your smartphone, too!

Oversharing on Social Media That You Do Use

If you frequently use a social media or online account but it contains lots of personal details or information that you now think should be safeguarded more closely, consider removing it from your profile or deleting the posted content. Think about if the information you continue to share could be used against you or combined with other information to be used against you. Enough pieces of personal information combined together can be very useful to cybercriminals.

Being aware of any information that you share that could be used to respond to "Challenge" questions, which are frequently used to reset passwords. What does that mean? How could information be combined to be used against you? Think about your online bank account. If you forget your password what types of questions do they ask? Probably something about the color of your car, your mother's maiden name, your birthday, or pets' names. Did you post a picture of your new car? Friend your mother or her brother on social media? Answer a meme about your birth month and day? Share adorable pictures of Fluffy? If you did, you've helped someone find out the answers to your bank's security questions!

This is the case for many of the pieces of information you may share online and many online accounts that use challenge questions to reset passwords. Information commonly used for challenge questions include the above examples and other details, such as your favorite sports team, vacation spot, fruit, ice cream, type of reading material, youngest sibling, elementary school name, and so on. As you clean up your data think about what information could be used to answer your security questions and try to remove that data from your social media accounts.

In closing, these short tips can make a world of difference in lowering your information's exposure to others. By questioning if you need to share or provide certain information online as you move forward, you can save yourself from many of the unnecessary overexposures we discuss here. Additionally, by taking a look at both your digital and paper trails to do these activities on a routine basis, you can be sure to keep overexposure in check.