UTHSC G.U.A.R.D.

May 2018

Google™ Yourself - Know What is Out There

by Chris Madeksho, Information Security Coordinator

In the cyber world, who are you? Google yourself. Go ahead and do it. What is the first search result? Is it your place of employment? Is it one of your online social media pages? An estimated 90% of your personal information is somewhere "out there". Knowing what information is available publicly is the first step in managing that data.

Organizations search social networking sites as part of background checks. Embarrassing or incriminating posts, no matter how old, can prevent you from getting hired or promoted.

Cyber criminals can harvest your personal information and use it against you. For example, they can use your information to guess the answers to your "secret questions" to reset your online passwords, create targeted email attacks known as spear phishing, or apply for a credit card using your name. These attacks can move into the physical world, such as identifying where you work or live.

How many people have their birthday posted to their social medial accounts? An easy target is to send a phishing email to recipients close to their birthday offering a special deal or birthday wish. As soon as you click on the link to see the deal, they got you.

The best protection is to limit the information you post. The privacy of your information is only as secure as the people you share it with. The more friends or contacts you share private information with, the more likely that information will become public. Ultimately, the best way to protect your privacy is to follow this rule: if you do not want your mother or boss to see your post, you should not post it.

Social networking sites are a powerful and fun way to communicate with the world. If you follow the tips outlined here, you can enjoy a safe online experience. For more information on how to use social networking sites safely or report unauthorized activity, be sure to review the security pages of the sites you are using.

For more information, contact the UTHSC Information Security Team at (901) 448-1880 or itsecurity@uthsc.edu.

Google Yourself
Find out what information about yourself is readily available

Information Footprint
Learn what steps you can take to reduce the amount of information available about you

Reducing Your Information Footprint
by Thomas F. Duffy, MS-ISAC Chair

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.

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 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. 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!

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.

Remember MySpace? LiveJournal? Do you still have that old email account or an account on an old dating website? 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!

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.

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.

For more information, contact the UTHSC Information Security Team at (901) 448-1880 or itsecurity@uthsc.edu.