State of Oklahoma
Monthly Security Tips
NEWSLETTER

July 2012 Volume 7, Issue 7

Managing Your Digital Footprint: Think Before You Post

From the Desk of CPT Jeff Elliott, Oklahoma Office of Homeland Security

If you're not familiar with the phrase "digital footprint", it's important that you become aware of what it is and how it impacts you. Digital footprint refers to the compilation of content on the Internet that can be associated with you and, thus, potentially available by anyone performing a search on you. The list of possible content visible online is endless: your family videos on YouTube, your comments on a news article or blog, vacation photos on Flickr, your posts on Facebook and Twitter.

Why should you be concerned about the information available online about you? While these pieces of information may seem innocuous on an individual basis, when pieced together they create a composite profile that could be used by cyber criminals. The more information out there, the more information that is accessible for social engineering and ID theft scams. Additionally, this content may be accessed at some point by an outside source doing an assessment of you, whether it be for college admissions or a new job.

With so much of your information in so many places online, can you do anything to manage your digital footprint? Yes. By reviewing the tips below, you can help minimize your online exposure and possibly reduce the risk of identity theft. Keep in mind, once information is posted on the Internet, sometimes it may be impossible to remove it.

Map Your Footprint
Before you can start reducing and cleaning your digital footprint, you should know what it currently looks like. Make a list of all the social networking sites that you've signed up for, any websites where you've had an account in the past, and all the usernames or aliases you have used on the web.

Using your name, other personal details, and the information from your list, do a few searches on multiple search engines and you'll get a good idea of how big or small your digital footprint is.

Take Control of Your Privacy
Once your footprint is mapped, you can start to clean it up. Perhaps you found a few social networking posts that were available to the public, or maybe a few photos that you would rather not have everyone see. Most social networking sites have varying levels of privacy controls, so you can change a few settings and restrict access. Think before you post.

Manage Your Interactions with Others
Don't forget others may be able to see whom you are associated with. Be careful about how you interact with others online. Be selective about which venues you participate in. If you regularly contribute to blogs or message boards, consider how your statements might be interpreted by others. Be cautious about

referencing your place of employment or your job function as this might be used for social engineering and other scams.

Use Caution on Social Media and Networking Websites
Use privacy controls available to limit and control access to your information. Do not post any inappropriate photos, comments, status updates or other content. Think before you post.

Recommendations
- Clean up your footprint. Remove any photos, content and links that are inappropriate or reveal too much information.
- Be selective about who you authorize to access your information.
- Monitor comments made by others.
- Consider using the "block comments" feature or setting your social networking profile to "private" so only designated friends can view it.
- Think before you post.

For More Information
MaximumPC: How To Erase Your Digital Footprint:
http://www.maximumpc.com/article/features/how_erase_your_digital_footprint

Washington Post: Beware of Privacy Policies: Time to Clean Up Your Digital Footprint:
http://www.washingtonpost.com/lifestyle/style/beware-of-privacy-policies-time-to-hide-your-digital-footprint/2012/01/31/gIQADI7PnQ_story.html

The information provided in the Monthly Security Tips Newsletters is intended to increase the security awareness of an organization's end users and to help them behave in a more secure manner within their work environment. While some of the tips may relate to maintaining a home computer, the increased awareness is intended to help improve the organization's overall cyber security posture. This is especially critical if employees access their work network from their home computer. Organizations have permission and are encouraged to brand and redistribute this newsletter in whole for educational, non-commercial purposes.

Brought to you by:

MS-ISAC
MULTI-STATE Information Sharing & Analysis Center™
A DIVISION OF CENTER FOR INTERNET SECURITY