Safe Persona

Your digital footprint refers to the content on the Internet that can be associated with you and available to anyone performing a search on you. That information can be used by hackers for identity theft; make sure you create a Safe Persona.

Follow these tips to help manage your digital footprint:

- **Map your footprint** - To know what your footprint 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 will 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. Most social networking sites have varying levels of privacy controls, so you can change settings and restrict access, as necessary.
- **Manage your interactions with others** - Be careful about how you interact with others online. Be cautious about referencing your place of employment or your job function .
- **Use caution on social media and networking websites** - Use privacy controls to limit and control access to your information. Think before you post.

Take Precautions on Social Networking Sites

Social networking sites are a convenient means for sharing personal information with family and friends. However, this convenience also brings a level of risk. To protect yourself, do the following:

- **Avoid posting personal information** such as address, phone number, place of employment, and other personal information that can be used to target or harass you.
- **Limit access to your information** to “friends only” and verify any new friend requests outside of social networking.
- **Review the security policies and settings** and opt-out of exposing personal information to search engines and applications.
- **Protect your location data.** Using a mobile device can potentially expose location data. Disable location services settings on the device/application and don’t voluntarily give your location away by using social media platforms to geo-tag or “check-in” at various public locations. Additionally, apps should be given as few permissions as possible, especially social media apps.

Deloitte.

For questions and additional resources, please contact safecircle@deloitte.com.

Safe Persona

SAFE CIRCLE

Your digital footprint refers to the content on the Internet that can be associated with you and available to anyone performing a search on you. That information can be used by hackers for identity theft; make sure you create a Safe Persona.

- **Enable strict privacy settings that block data sharing between apps**. Opt out of saving login passwords within application settings. Disable all error/debug reports. Review settings quarterly.
- If you need to connect to a public wireless hotspot, **use a virtual private network (VPN) to encrypt your web traffic**. Don't connect to networks if you're not familiar with them or can't verify their authenticity.
- Search for yourself online. It is critical to know what information can be found by a free search. Disallow tagging, as friends may not be as diligent with their location settings. **Photos and information they post about you may reveal your critical information. Do not post pictures while still on vacation or traveling. Don't let those you trust tell hackers what they want to know.**
- **If your account has been compromised**, contact social media tech support immediately. They can help you get access to your account. If friends or family may be compromised, reach out to them another way and have them verify posts you think might be fraudulent. **A compromised account can be used to hack other accounts, so be aware of "friends" posting suspiciously.**
- **Be wary of surveys, shared posts, or quizzes** that ask for personal information that could lead to an answer for a security question. Also, don't forward posts without verifying the truth. Fact check scams at a site like www.snopes.com
- **Hackers also use professional networking sites** to try to lure users to click a malicious link. If anyone is asking for personal information, be cautious and think who might use that information.
- **Narrow down connections to reduce threats**. Be wary of individuals and entities that you are connecting with on social media. Carefully review every connection, and don't connect with those that appear suspicious.
- **Check your browser for cookies.** Cookies make online browsing more convenient, however, some types of cookies can compromise your privacy. Make sure to delete your browser cookies every few months and set your cookie preferences to block third-party cookies.
- **Always update your software.** Outdated software can give hackers a backdoor for accessing your private information. You can set programs and apps to auto-update so you're sure you have the latest software installed.

Change your social media profiles to PRIVATE

These links will explain how to change your privacy settings:

- Twitter
- Facebook
- LinkedIn
- Instagram
- YouTube

Deloitte.

For questions and additional resources, please contact safecircle@deloitte.com.

Deloitte.

For questions and additional resources, please contact safecircle@deloitte.com.