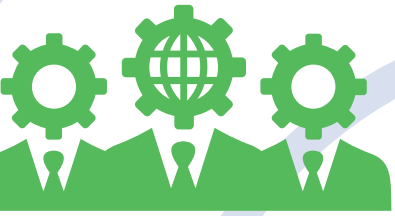
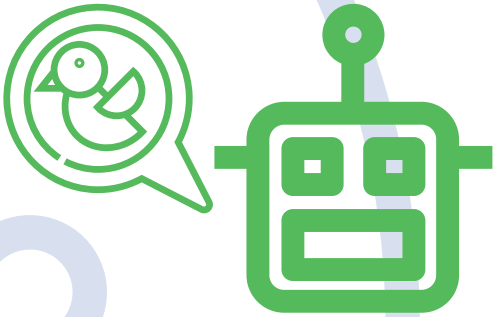
7 RULES FOR MONITORING *Digital* IDENTITY



IDENTITY is a valuable commodity. Not only is it the key to your personal, professional, and financial success, but also to your digital identity and safety. Knowing how to protect your online information, i.e., your digital identity, is a must as a 21st century digital citizen. Below are seven rules to protect yours!

AVOID HYPER-POSTING: Sharing your every activity, position, or emotion on social media makes an impression that revolves around your digital identity and digital life. For potential employers, if a candidate is always on social media outside of work, then they most likely will also be at work. Make sure your Digital Identity posts and participates at a healthy level and is balanced with real life interactions and experience.



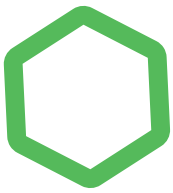
BEWARE OF THE BOTS: Botnets are a category of computer program scripts created to emulate a real person. Used in social media, it's traditionally a fake profile, fake person, or account. Bots & Fake News are common bedfellows because bots' sole purpose are to mislead, and spread fake news stories via a fake person or profile, i.e. a "robot." BOTS gain traction on a mass scale very quickly. What is even more dangerous is that BOTS bring mass media attention to topics and behaviors that typically wouldn't receive any publicity–meaning, their fake rhetoric is amplified and seems relevant, legitimate, and real in minutes!

FLASH COOKIES or **LOCAL SHARED OBJECTS (LSO)** are files stored by a website you've visited using Adobe Flash Player or similar technologies. Adobe phased out Flash Player in 2020, but some older browser versions may still support it. Flash Cookies may replace other browser cookies used for tracking & advertising. They also store your browser's settings and preferences. Companies can attach unique HTML5 cookies within your browser to identify you over time. When you "delete" or "clear cookies" from your browser, IT MAY NOT HAVE deleted the FLASH COOKIES also stored on your computer. Current versions of Google Chrome, Mozilla Firefox, and Microsoft Internet Explorer offer more control to delete Flash Cookies through the browser's settings. However, older versions do not.

LIMIT AD TRACKING or turn off in your Privacy settings– for new iPhone users, you may have been prompted to turn off, recently. Turned-ON, "limit ad tracking" reduces advertiser tracking on your iOS device, and similarly on Android devices will prevent targeted advertising within some installed apps– disrupts functionality of certain apps if on, so test this feature on your device.

CHECK IN WITH YOUR DEVICE ID: Depending on the mobile device, your DEVICE ID will identify which advertisers, marketers, and other services are tracking you when looking for a particular type of device, or for services in apps used on that device. Monitor and access within your device's Settings menu under 'Google - Ads,' as well as reset the ID, and/or opt-out of ad personalization. ~iOS, a device ID is: IDFA, IFA or *"Identity For Advertisers"* ~Android, a device ID is: GPS ADID or *"Google Play Services ID for Android"*.

DEVICE FINGERPRINTING technologies are evolving and can be used to track you on all kinds of Internet-connected devices that have browsers, such as smart phones, tablets, laptop, and desktop computers. Since device fingerprinting uses the characteristics of your browser configuration to track you, deleting cookies won't help.



MONITOR WEB BROWSER COOKIES: Websites request to store a cookie so it can recognize your device in the future. Later, if you return to that website, it can read that cookie to remember you from your last visit. By keeping track of you over time, cookies can be used to customize your browsing experience, or to deliver ads targeted to you.

UTSA LIBRARIES