Terms of Service

Privacy rights for citizens have been gradually legislated over many years. Technology service providers are required to present the terms of service to prospective users at the time of enrollment, and they must be agreed to for the account to go live. In many aspects, agreeing to the terms of service essentially waives your privacy rights.

Account and Device Settings

Privacy Settings: If social media platforms must be used for personal communication, ensure accounts, conversations and images are set to ‘Friends-only’; never ’Friends-of-Friends’. ‘Everyone’ should be used only for business accounts.

App Permissions: From Settings… Permissions, review each for every app on your cellphone or tablet; consider if they are necessary for the app’s functionality, and if not, if it is appropriate that they surveil you. Disable the unnecessary permissions and uninstall apps you do not need.

Location Services: From Settings… Location, disable this at the operating system level, and Settings… Permissions… for every app that has this function. If needed for a specific app to provide value such as real-time traffic-reporting, enable it for the operating system and that app, then disable both when your need for the service has ended.

The Browser

Cookies. Small text files placed in the browser by websites. They are necessary to accept for logging into online accounts. Third-party cookies surveil your messages, visited websites and device apps and report this information to their authors. The Privacy & Security section of a browser’s Settings offers the ability to minimize surveillance of your online activities. Familiarize with this area and enable the Block Third Party Cookies setting.

Private Browsing. A feature where temporary internet files, cached web pages and most cookies are deleted when the browser is closed. Helps minimize the persistence of malware and other surveillance objects. Right-click a browser icon, or from an open browser’s main menu, select New Private/Incognito Window to begin using.

Browser Compartmentalization. A technique where multiple browsers are routinely used for different online activities. For example, use one browser exclusively for signing into accounts, a different browser is used for general and relatively safe browsing of reputable websites, while a third browser is used for visiting less-reputable, higher risk sites.

Records of Activity

Personal Messages: Text messages are not sent from personal device to personal device; the sender places it on the service provider's servers and a copy is forwarded to the recipient, whose reply then repeats the process in reverse. Over time, a huge record of a user's thoughts and sights accumulate on numerous hard drives around the world. Resist 'thinking out loud' through your electronic devices. **Search Engines**: Every visit to a website records the visitor's IP address, date and time. Most search engines records the same information plus the search text. As most accounts use the same modem or data plan for many years, an indisputable record of a user's searched content grows steadily larger. **Email Compartmentalization**: Using a single email address for each of personal, professional and obscure contacts can lead to a number of problems. Instead, create and use four email addresses — One for friends and family, one for professional contacts, one for suppliers like financials and utilities, and one for sites not qualifying as any of these but that require an address for you to engage with. Ideally they are not all with the same provider, and considerable thought should go into the selection of each username.

Encryption

Website Content: Information that is exchanged between users through a website can be intercepted by 3rd parties in several ways. This risk is minimized by reputable websites' usage of encryption, indicated by an *https* in the site's address. That is not enough, however. The website must also provide 'end-to end encryption' (check its policy wording on "encryption"), meaning its operators cannot access the contents of information exchanged between its users.

Confidential Documents: Sensitive files should only be attached to email and texts if they are encrypted with a password. Free document archivers have been available for decades through a web search. Sender and recipient each need one but doesn't have to be the same app. Steps: Sender creates the password-protected archive; closes then re-opens it with the password; sender notifies the recipient of the password through a communication method different from the pending message; sender delivers the message/attachment.

Virtual Private Network (VPN): A service and app that encrypts your internet traffic and replaces the IP address assigned by your service provider. For whole-computer protection, several 'free with limited functions' can be found by searching the web for 'best free VPN'. Familiarize with one of these for confidential, legal internet activities. If meeting your needs, use when needed, or consider upgrading to its paid subscription. Alternately, search the web again for 'best VPN' (will return other paid subscription offerings). Free browser-only protection is also available by searching for 'VPN' in the Add-ons/ Extensions section of any browser.

Any information in this handout is intended for general guidance only. Any reliance you place on the information in this handout is strictly at your own risk.

Udemy

Amazon