

The Three Ps of Online security

The ability to connect anonymously is one of the Internet's great opportunities, but in many ways, false feeling of absolute anonymity and creates a sense of distance from our words and actions. News headlines confirm the disconnect between the online and offline worlds in terms of behavior. The large number outrageous comments and voracious BLOG entries submitted daily illustrate this phenomenon. Many people write things in BLOGS that they would never say in face to face conversations.

The disconnect is also clear in the rise in explicit pictures sent via the internet and cell phones. The Navy times recently had a front page headline detailing the large number of sailors and marines facing UCMJ action for sending explicit texts, despite the fact that it is, flashing publicly. The disclosure that former Congressman Anthony Weiner posted photos via Twitter, illustrate the dangers of online behavior having dire consequences in the physical world. His behavior is a disappointment for his constituents but also carries lessons for all. Even basic online interactions and behavior must be planned and monitored to avoid malicious exploitation or embarrassment. Online security does not just happen: it takes real effort, knowledge and skill to achieve a reasonably secure level of anonymity (or pseudonymity sic) online.

A few tips can help you become a cyber-savvy citizen and make the smartest, most effective use of the internet. An article in the Harvard Business Review provided the best way to manage the personal and professional risks of internet usage is to observe, "The Three Ps of online indulgence" insure your actions are Principled, Private and Planned. Some practices you may want to consider:

Principled:

- . Identify the ethical principles or standards you're going to adhere to in your private activities
- . Avoid sites or people that you consider unhealthy or wrong.

Private:

- . Talk with family about what information is important for you to keep private online, and make sure you are both taking the same precautions to keep your private activities shielded from the world.
- . Cut off communications if an online contact insists on asking for (or giving you) permission to indulge in behaviors that are unhealthy, hurtful or against your conscience.
- . Create a private online identity without links to any identifiable information (i.e. don't connect it to your Facebook account, main email address, social security number or credit card). This reduces your risk of exposure, and prevents you from inappropriately exploiting your professional status or privileges.
- . Choose a web browser that offers enhanced privacy options, and use it along with a proxy server.
- . Use an anonymous proxy server to keep the web sites you're visiting from tracking your IP address
- . Automatically delete your search history, cookies, logins etc. whenever you log out and/or at the end of every day, or erase your tracks manually.
- . Read up on the basics of Internet privacy by visit the web sites: Electronic Privacy Information Center and the Electronic Frontier Foundation
- . Be careful when using WI-FI hotspots turn on the settings on your Laptop to alert you when a computer attempts to connect to your computer

Planned:

- . Identify core principles for online behavior for yourself and your family
- . Think carefully about any private activities, information or photographs that, if exposed, would affect your reputation or have significant consequences for your organization.
- . Anticipate the possibility of exploitation because of whom you are and where you work. If you cannot handle the professional and emotional consequences of revelation, don't put it online.
- . Research the latest news on technology or policy changes that could affect your online privacy
- . Do not employ these practices for behavior that is hurtful, unethical or illegal, or to avoid the consequences of bad decisions.