10 Steps to Protecting Your Identity and Safeguarding Your Privacy

When it comes to online security, an ounce of prevention truly is worth a pound of cure. Have fun online, enjoy the social aspect, but also be careful what you reveal publicly, and guard your identity.

BY CHRISTINE PILCH MANCINI

Reputation management used to be a lot easier before the age of the Internet, where things are documented permanently. You can delete something, but search engines have become so adept at grabbing information instantly that nothing ever really goes away.

Protecting your online privacy requires persistence and diligence, but you can do it if you have a healthy dose of common sense and a pinch of skepticism.

ANTIVIRUS/ANTI-MALWARE

First and foremost, run antivirus/anti-malware software on your computer. If you have an unprotected PC, you're asking for trouble. Malicious hackers can grab your personal and financial information right off your hard drive. They can also use your computer as a server to send out spam email and perform other malicious tasks. Antivirus/antimalware software can catch problems before they become major headaches.

> Facebook is ultimately in the information collection business, so it's in their interest to encourage you to share as much personal information as possible, so they, and their advertisers, can better market to you."

FACEBOOK

Adjust your Facebook privacy settings. Facebook is ultimately in the information collection business, so it's in their interest to encourage you to share as much personal information as possible, so they, and their advertisers, can better market to you. Unfortunately, this quest is relatively incompatible with locking down privacy. Facebook offers the perception of safety through proliferation of the widely held belief that the "Friends Only" setting restricts the flow of your information exclusively to your friends

Unfortunately if you look no further than that, you are still doing things such as using Facebook through an unencrypted connection, sharing your information on search engines, sharing information about your activity on partner sites, allowing your friends to reveal detailed personal information about you whenever they use an application, and opening up your pictures publicly.

LINKEDIN

LinkedIn also has privacy settings, although they are not nearly as detailed as Facebook's, so you can decide such things as who can see your photo and activity. Perhaps most important here though is to maintain a constant awareness that LinkedIn in a professional network as opposed to a primarily social one. All of your activity here should be sifted through an internal filter of, "Is this something that I want a prospective client to read?" LinkedIn is such a huge and powerful database that oftentimes your LinkedIn profile appears above anything else when someone Googles you. Your activity here is likely to greatly affect your professional reputation, so it's in your best interests to refrain from doing anything questionable, like attacking others in Groups and Answers or writing unprofessional status updates.

YELP/GOOGLE/YAHOO

Yelp is a powerful social network that acts as a peer reviewing service. It's most popular within the hospitality industry now, but pension and financial services providers are starting to appear there and on similar sites, like Google and Yahoo, so you would be wise to keep tabs on the opinions that people are sharing about you there. If not, you're ignoring client feedback and missing out on opportunities to thank loyal customers and deal with unflattering reviews.

PASSWORDS

Social media has also made it easier for hackers to guess passwords. Information like your mother's maiden name may now be accessible to your entire network if she is connected to you on social sites. Addresses, home towns, pets and phone numbers are also sometimes available there. This information is popular fodder when creating passwords or security questions, so it may be wise to revisit them.

WIRELESS NETWORK

It's not smart to neglect password security on your home wireless network either. Not only can people use the connection that you're paying for, but hackers can monitor your online usage and gain access to your personal habits and information. They can also use your network for illegal activities that can cause trouble for you. Lock down your network.

GOOGLE ALERTS

It's easy to set up Google Alerts on your own name and your company's. You can choose how often you want to be notified of web-wide mentions of the phrases you select. This provides you with an opportunity to see new information shortly after it is posted online and react accordingly.

APPLICATIONS

Facebook, LinkedIn, Twitter and smartphones all have applications developed by third-party vendors that are fun, informative or enhance productivity. But what really happens when you sign up for those applications? There are no free rides in life, so when you use a free application, they take something from you in return—your personal information. Details are described before you click on the agreement link though, so take a minute to read them and balance the value of the application against the surrender of your information. After a while, you may decide that an application isn't what you thought it would be, or you're just not using it like you expected, so feel free to clean house from time to time. The fewer applications you use, the more you safeguard your privacy.

SANITIZE

On About.com's HR section, according to Rob Pickell, senior vice president of customer solutions at HireRight, "76% of companies said that they do use or are planning to use social media sites for recruiting." So if you're a job seeker, you'd better sanitize your online identity. Remove anything that is unflattering, such as photos and comments, and be careful about your affiliations as well.

DOMAINS AND USERNAMES

Domains are cheap to register, and it's a good idea to own your name. That helps guard against somebody muddying up the rankings when someone Googles you, and it also assures that you control what is displayed when someone types your name into the URL box. It's also a good idea to snap up your username and vanity URL across as many sites as possible. You might want to own your name on LinkedIn, Facebook, Twitter, and YouTube at the very least. Also, you might want to grab your name with popular web-based email providers as well, like Gmail, Yahoo, and Excite, even if you don't yet intend to use them.

Ultimately, a lot of online security comes down to common sense. In this case, an ounce of prevention truly is worth a pound of cure. Have fun online, enjoy the social aspect, but also be careful what you reveal publicly and guard your identity. PC

Christine Pilch Mancini is a partner with Grow My Company and a social media marketing strategist. She trains businesses to utilize LinkedIn, Twitter, Facebook, YouTube, Pinterest, blogging and other social media tools to grow, and she collaborates with professional service firms to get results through innovative positioning and branding strategies.