by John Wunderlich

Protect Yourself First

Privacy is an integral part of your job as a payroll professional, and this column focuses on how you can best protect the privacy of personal information in the workplace. However, it is also important that you protect the privacy of your information in your personal life, especially as many of you may be booking travel or buying gifts online for the holidays.

We have all heard horror stories about identity theft, information breaches and similar. However, this is not inevitable. You have options and choices to protect your privacy online. It begins with critical thinking.

Let's use the example of a website or email offering something for free. With the exception of some open-source software, "free" likely means one of three scenarios. Exercise caution and remember the three privacy rules below.

1. Your personal information is being harvested for its commercial value. You, or your online behaviour, are the "product" that websites sell to advertisers. Sites like Facebook and Google are good examples. They provide "free" content or services, and advertisers get to present their ads on the resulting pages. The advertisers pay the site based on how successful they are at getting you to click on the ads or buy products. Both the site and the advertisers get to know what you are interested in and may be able to track other sites you frequent and transactions you have completed.

Privacy Rule 1: Do not post anything or search for anything online that you would not be comfortable sharing with your friends and colleagues. Think of this online presence as your public persona, not your private one.

2. The "free" offer is legitimate. Its purpose is to provide you with a preview of the product or service so you will be enticed to pay for the full version. In some cases, the free offer is accompanied by ads, in which case it also falls into the scenario above. In other cases, the full version of the free offer is priced such that it covers the free version as well, and you may feel comfortable buying the product or service. For example, Dropbox offers 2 GB of cloud storage for free, while the subscription models provide 50 or 100 GB. In this case, you are the customer, not a statistic for advertisers. However, keep in mind that if you are using "cloud" storage, the information you put there may be available to the administrators of that service.

Privacy Rule 2: The terms of the free product or service offer should make it clear how the service pays for itself. If it does not, it is not free—there are strings attached.

3. You are a potential victim of a scam. You are the target of an Internet fraud or are being driven to a website that will infect your computer with malware. Depending on how your computer's security program is set up, it may become infected with malware just by visiting a site. In general, you need to click on the hyperlink or email attachment to become infected.

Privacy Rule 3: Do not click on hyperlinks or attachments unless they are from someone you trust and you expected to receive them.

Once you have the right attitude toward protecting your privacy, you will be better equipped to determine which technology will help you. There are several anti-virus and Internet security products and services

to choose from, and you may already be using them. I cannot give specific recommendations that suit everyone but here are some good general tips:

- Purchase an Internet security package for your computer. See reviews from trustworthy sources and reputable websites to determine which package is best for you. Most of these packages require annual subscriptions. Pay them.
- Make sure that both your computer's operating system and your browser software are kept up to date. If you don't know how to do this, find someone in your professional or personal network who can help.
- Do **not** use the same password on every website. There are password managers that can help you to create, track and use secure passwords. KeePass is a good open-source option in this area.
- If you use USB keys, encrypt them. Better yet, encrypt your computer's hard drive. TrueCrypt is the leading open-source option here.

There is no such thing as perfect privacy or security. Only you can determine the balance between information sharing, open web surfing, and privacy protection that is appropriate for you. However, it is better to take action now while you have time to explore all the options. ■

John Wunderlich is an information privacy and security consultant, based in Toronto. For more information, check out his intermittently updated website at **http://compliance.wunderlich.ca**.

Notice: This column reflects solely the opinions of the author. Individuals are encouraged to seek qualified legal advice on points of law or matters of interpretation.