ACC DOCKET
INFORMED. INDISPENSABLE. IN-HOUSE.

Safe Driving

Technology, Privacy, and eCommerce

We are bombarded with stories about hacking, data breaches, and phishing. It’s hard enough to deal with such things as legal advisors to our corporations; we definitely don’t want to have to worry about them on an individual level too. Here are some suggestions for ensuring better data security.

Don’t forget physical access — Now that the internet is the preferred attack vector, we sometimes forget that protecting against physical access and not trusting insecure peripherals remains a critical part of individual data security. It amazes me how many intelligent lawyers still accept free USB thumb drives offered at trade shows and insert them into their computers without knowing whether they are infected. The fact that they come from a vendor you trust is not enough — there have been many reports of USBs purchased in bulk from overseas manufacturers that contained malware of which the vendors themselves were unaware. In short, make sure your devices are locked when you leave them and that you avoid using drives from unreliable sources.

VPNs — Public Wi-Fi is both a blessing and a curse. Although LTE connectivity is improving dramatically and is in many cases already faster than public Wi-Fi, we often still find it super convenient to hook into the Wi-Fi at our local Starbucks. Unfortunately, criminals find it even more convenient to hook into those same networks so they can hijack information from unsuspecting users. The good news is that this is pretty easy to avoid.

First, you could just use your LTE network and feel pretty safe from anyone except the most sophisticated hackers. If you have a Wi-Fi only tablet or laptop, most cellular plans these days allow

you to use your smartphone as a secure personal hotspot.

Second, you can use a VPN (virtual private network). A VPN acts something like a personal firewall by using dedicated connections, virtual tunneling protocols, or traffic encryption.

My guess is that while your corporations provide VPN access for your work laptops, many have not yet begun doing so for smartphones and tablets. And if you use any personal devices, you may want to have a VPN service of your own.

My current favorites are Cloak and TunnelBear. They are simple to use subscription services that work on Mac, Windows, Android, and iOS. They are pretty affordable, with plans ranging from free (for a very small amount of data) to US$3-$5/month. If you use a lot of public Wi-Fi, the price is well worth the resulting peace of mind.

HTTPS and Watering Hole attacks — Pay attention to the URLs of the pages you visit. First, you may want to avoid pages whose URLs begin with HTTP versus HTTPS. HTTP (Hypertext Transfer Protocol) is the older and unfortunately still more common standard. HTTPS takes HTTP and secures it using TLS (Transport Layer Security) or a similar security protocol. HTTPS authenticates the webserver and also provides bidirectional encryption between your device and the server, which helps prevent accessing and tampering with or forging the contents of the communication.

But criminal hackers are smart and have developed ways for end-running HTTPS, using things like “watering hole” attacks. An invisible layer of code over a legitimate website steals your log-in information or redirects you to a website that looks exactly like the legitimate site but isn’t.

To help try to avoid this, examine the URLs of the sites you visit. The simplified URLs commonly exhibited by most browsers these days won’t help because the bad guys have gotten good at displaying shortened URLs that look legit. However, most browsers will expose the complete URL if you hover your cursor over it (or in iOS or Android long-press the URL). I know many people are irritated by these pop-ups when they appear and have come to ignore or even disable them. Don’t. The relative inconvenience of a false-positive isn’t nearly as troublesome as the alternative.

Passwords, TFA, and Password Utilities — We have a love/hate relationship with passwords. But until biometrics get a lot easier and more reliable we need some way to authenticate who we are, and passwords are still the best option. And since you should *never* use the same password for two different sites, you need a password utility to generate complex passwords and remember and fill them in for you. For any important sites (banking, purchasing, email, etc.) that offer it, also enables Two Factor Authentication. Using TFA is way easier than the hassle of getting hacked, and all of the better password utilities have token generation systems to make it even easier.

Greg Stern

Former Global Integration Counsel

Chubb, Independent Consultant