ACC DOCKET
INFORMED. INDISPENSABLE. IN-HOUSE.

Leading Practices in Personal Technology

Technology, Privacy, and eCommerce

The technology we use daily is becoming more capable and, therefore, more complex. In our modern landscape, we have a somewhat confusing mixture of (1) company-issued and maintained devices, (2) bring-your-own devices that often have company-imposed and technologically enforced requirements and restrictions, and (3) personal and independently owned and maintained devices. It is sometimes hard to know what best practices should be followed to maintain your personal tech. Here is some general advice.

Keep the operating systems of your devices updated — Almost every OS update addresses particular security flaws identified in the preceding system. There is a never-ending arms race between the black-hat hackers who want to exploit us and the white-hat hackers who are trying to defend us. I know that many people are wary of installing updates because they may have bugs or may change features we like. However, most updates are pretty stable and provide some worthwhile new features. More importantly, as soon as an update comes out, there are malevolent hackers who reverse engineer the security fixes in that update to try to take advantage of people who have failed to install it. If your device is issued or controlled by your company, you may not be able to install updates until they permit it, but try to do it as soon as possible.

By the way, I don’t recommend authorizing automatic OS updates because there will be the occasional kerfuffle when an update may brick your particular device. You should wait to install an

update until enough time (perhaps a day or two) has passed so that the very early adopters can serve as canaries in the coal mine.

Keep your apps updated — Some of the worst malware takes advantage of flaws in garden variety apps you use every day, like MS Word, Excel, or Outlook, or Adobe Flash or Acrobat. The better companies that issue these apps, like MS and Adobe, know this and make a sincere effort to eliminate any security flaws as quickly as possible. So please, pay attention to updates and install them as soon as it's safe to do so.

Be wary of using public Wi-Fi networks — Public Wi-Fi networks are dangerously convenient. Hackers use things like man-in-the-middle attacks and packet sniffers to steal your data and, potentially, install malware on your devices. Most of your work devices likely have virtual private network (VPN) software installed that will protect your device from these threats by creating virtual private networks that lock hackers out. You can install VPNs like Encrypt.Me or Tunnel Bear on your own personal devices too, although the better ones charge a subscription fee.

In the past several years, modern LTE cellular networks have become fast enough — and data plans cheap enough — that they have become a viable alternative to using public Wi-Fi for many people. Although these too can be hacked, doing so requires a great deal more sophistication and equipment than hacking Wi-Fi, so you generally are much safer using cellular than unprotected public Wi-Fi.

Study your devices — Most people I know treat their devices like those who refuse to read the owners' manual for new cars or appliances, and therefore don't learn either the advantages or the hazards that accompany them. There are a ton of settings in most devices that can not only make your devices more tailored to your preferences, but also much safer and more private. Our devices have become very powerful and feature-rich. They also often contain certain kinds of information that we should be terrified to expose, like identity, bank, and credit card information, the location of our homes and family members, etc. Whenever I get a new device (which I admit is far too often), I devote considerable time to learning the new features as well as the settings and other things I need to adjust to feel comfortable that I have it as locked down as I prefer.

Use a good password management system — The way hackers attack passwords these days relies on three basic approaches. First, they maintain a dictionary — a very big dictionary — of commonly used passwords. Those dictionaries contain (among many, many other things) most words in most dictionaries in most languages as well as a list of all the human and pet names followed by every conceivable list of short numbers. (So, if you have been relying on a password like Fluffy214, don't.) The second method uses highspeed computers to conduct what is called a brute force attack. This is basically trying a long series of random strings of letters, numbers, and characters to "guess" your password. At the current time, even a very powerful computer can take a relatively long time to generate random strings longer than six to eight characters; generating strings longer than 10-12 characters would likely take months or years. Third, they use social engineering to try to trick you into disclosing your password or trick a third party (like your bank) into changing your valid password into one of their own choosing.

You should take advantage of knowing these hacker techniques by (1) not using any words or phrases in any language, (2) making your passwords at least 12 characters long, and (3) being alert and using two-step verification to prevent anyone from changing your password without some kind of independent verification that you are you. You should also try not to use the same password for more than one login, because if one password is somehow discovered, you don't want that password to become the key to your whole kingdom.

Unfortunately, most humans don’t have the kind of memories that would enable them to easily remember a multitude of random passwords. That’s why I recommend using a good password management system, which can either be an app like 1Password or LastPass, or a physical notebook that you keep under lock and key.

These are just a few of the leading practices to manage your personal technology. Please let me know if there are other things you’d like me to address.

Greg Stern

Former Global Integration Counsel

Chubb, Independent Consultant