President's Corner

Security is Important - Why Does it Take So Long (and Cost So Much)?

Author: Greg Skalka, President, Under the Computer Hood User Group, CA
October 2019 issue, Drive Light
www.uchug.org
president (at) uchug.org

I am a technology user. I use all sorts of tech products, applications and services. I have laptops, desktops and Chromebooks. I have mobile devices - smart phones and tablets. I have home Internet access and I access the web from other places as well. I have a home network and I have smart home devices (cameras, TVs, voice-controlled assistants, smart lights and appliances). I use lots of software. I search the web, bank and buy things online and send emails and texts. I'm not much for social networks, but I do appear in posts by others, especially my wife. I've got a lot of the things a typical middle-class American would have.

I use a lot of technology, but all I want to do is use it. I don't want to have to struggle to make it work, fix it or spend a lot of time and money keeping it working safely. I want it all to work every time as I expect it to work. Unfortunately, there is a lot more to our tech lives than that. None of the tech revolution we have seen in the last decades would have been possible without money. It is commerce, capital and the desire to make a profit that brought us most of this, including Microsoft, Google, Uber, Tesla and all the rest. Some key government investments in technology, in the space program, DARPA and the military-industrial complex helped with fundamental research, but the capitalist entrepreneurs filled in the rest. Money made tech great, but money also made it unsafe.

Entrepreneurs take legal risks to gain rewards; criminals try to find the least risky ways to make money, legal or not. Each new tech device, app or service that comes out is studied for vulnerabilities by the criminal elements intent on exploiting it for monetary gain. Now that technology has interconnected the world, we can be the victims of crime originating from all over the globe. Even nation states can get in the game, trying to steal information for economic and political purposes.

All this leaves the poor tech user vulnerable. The rapid rate of change, the ease of use and ubiquitousness of these product and services just add to the risk. How does a user evaluate the threat and defend against it? Is it all worth the cost?

The criminals are out there, ready to hack, snoop, steal and deceive. They want your personal information to steal your identity and your passwords to steal your money. They want to trick you into sending them gift cards and Bitcoin. Who is going to protect the tech user from all the cyber threats? Can the government protect us? Laws may be passed, regulations put in place and enforcement attempted, but citizens are still victimized. Unfortunately sometimes the government is part of the problem, not protecting the sensitive data we entrusted to them.

Can the companies we buy products and services from protect us? Their desires for profit over all else have created some of our tech problems. They will sell us devices that are not secure if they think it makes business sense. They'll collect and monetize our personal information and then often fail to protect it adequately. It seems we as tech users must find ways to protect ourselves, as no one else will take responsibility for our security. Unfortunately, that means additional costs in terms of money and time are required to keep our assets (money, identity, personal safety) secure when using all these tech items and services in the new global digital electronic world.

There is no practical way to remain 100% secure in our modern connected world. Even if you turn off all of your devices, disconnect them, put them in a box and seal it up (and cancel all your related services), you are not safe. The government still has your personal information, and even if you are not on Facebook, others could post about you. You will have to go back to paying with cash, shopping and banking in physical locations and communicating through personal visits and letters. Unless you want to step back into the 1950's, you will have to adopt some additional safeguards with every new tech item you acquire.

Safety as a tech user is not an absolute, but a matter of degree. More time and money spent to safeguard our activities will provide more relative safety and security, but trade-offs will need to be made. More security comes at a higher cost and usually a greater inconvenience as well. A user can make their tech life more resistant to attacks by cyber criminals and become more resilient should bad things happen, but it will require more time, money and effort on their part. Lots of articles are written about protecting ourselves online and describing precautions we all should take, yet cybercrime is still prevalent.

I think I take care of my tech household pretty well, though there is always more that can be done. The things I value most (finances, identity, property) I protect the most, while things of a lesser consequence I am a bit looser with. In some ways I probably go overboard in caution, but there are probably some risks I don't take as seriously as I should. I'm pretty careful with physical security, using strong passwords, encryption, a VPN and two-factor authentication where appropriate.

I'm pretty resistant to social engineering threats and am very careful with my personal information. Exercising care and vigilance online is good, but it requires effort and some investments. I have several laptops and desktops that my wife and I use, as well as a couple of Chromebooks. All the computers we regularly use run Windows 7, so I am presently working towards replacing at least some of them with Windows 10 computers ahead of the Windows 7 security sunset in January 2020. This considerable cost in new hardware and software and in time to set everything up is strictly due to Microsoft's desire to make Windows 7 obsolete; I would be perfectly happy staying with Windows 7 otherwise. I'll be spending money on new systems, probably buying new software and spending time teaching my wife how to use the new OS. I'll probably compromise by keeping a couple of old Win7 computers or laptops to run software I can't convert to Win10 or don't want to spend more on. I still have a Windows XP computer that I keep off-line to run certain programs. I'm actually writing this article on it; I've yet to find a Microsoft Word version I like overall as much as version 6.

Even when security updates are provided for free, our time is usually required to oversee their installation. If nothing else, the time required to install updates represents time we are unable to use our devices. While Windows 10 may force automatic security updates, they can wind up being applied at the most inopportune times. I don't mind as much the automatic updates my Chromebook gets from Google, as they are downloaded in the background and quickly applied on the next power-up.

In addition to computer updates, our network items often require security patches. Few users may pay much attention to updates for their routers, however, unless they are alerted somehow. I have a Netgear Orbi mesh Wi-Fi router, which I love for its performance and ease of use (but not so much for the initial cost). Because I'd registered the product and downloaded their app, I recently received an email that an update was available for my router's firmware. I initially tried to apply the update through the app (on my smart phone) but was unsuccessful. I was able to enter into an online chat through the app with their tech support, and thus began a two-hour process to finally get my router system updated.

I assumed I would be able to easily update through the Orbi app, but the support tech told me my installed firmware version was too old, and I instead would need to download and install an intermediate version from a web link. I find the small screen of a phone too difficult to use for this kind of activity, so pulled out a Chromebook, logged into my Orbi router and went to the web link. This also allowed me to keep the support chat going separately through the app on my phone.

Once I got to the web link, I found I would be downloading a zip file. There may be ways to unzip on a Chromebook, but I don't know them, so I switched again and logged in with my Windows laptop. The support tech said to apply the update first to the satellites (my mesh system consists of one router and two satellite units) and then to the router. The update page was a bit confusing, and I inadvertently updated the router first. Fortunately I was still connected to the tech support person, so after a number of additional steps, I successfully updated all components.

It is almost time to renew my anti-virus, and I need to make some decisions about it. I've been using ESET Internet Security for many years and really like it (and think it protects me, but who really knows). I'm not sure what I should use going forward on Windows 10, as I've heard that Microsoft's Win10 built-in protections are as good as anything else, and obviously are at no extra cost. I always buy ESET on sale ahead of when I need it, so I already have new copies to put on my Win7 computers. That seems like a waste, as I won't have these computers on the Internet past January. Still, I shouldn't cut corners on protecting my online banking computer, at least until I am switched over completely to Windows 10.

Though I may be spending a lot of time and money getting my new computers set up, it hopefully will increase the odds that I’ll have secure systems that will help protect my data.