SWCP Portal
January 2015

Starting the year off right

Security Tips for 2015

Every January over the past seven years since this newsletter started, we've begun the new year with a review of what users can do to stay safe online. Good password practices, the need for firewalls and antivirus programs, keeping software up to date, and being ever alert to dangers have all been discussed repeatedly. And each year, warnings of hackers and cyberwar have become more urgent and dire.

Nowadays, you might be tempted to give up trying. With the websites that offer the most useful services treating you as a product, government agencies able to track and hack at will, and criminals waiting to pounce on your slightest mistake, it's easy to feel completely overwhelmed and totally outclassed.

No substitute for vigilance

However, online security is now far too important to be lackadaisical about it; your virtual life has become so entwined with real life that serious consequences can result from a simple mistake. One recent **horror story** was about a tech-savvy fellow who wanted to store some photos with Amazon Web Services through GitHub. He accidentally uploaded an account key. And though he took it down within minutes, it wasn't fast enough. Hackers were watching and used his account to mine bitcoins. Within several hours, *$2,375* in fees had been rung up. Luckily for him, Amazon dropped the charges, but the incident points out that **users cannot assume obscurity, poverty, innocence, or insignificance is any kind of protection against modern hackers**.

What the man should have done was change his app key even *before* deleting the post. For what the bad guys crave most is **access** – the keys to the kingdom. Unfortunately, in most cases, all that stands between them and your correspondence, bank accounts, and everything else is just a string of letters and numbers. And not just you. *Any* security breach nowadays endangers *all* who use the same site or resources.

Sadly, it's virtually impossible to be 100% secure these days. The recent **Sony hack** shows just how vulnerable even the biggest corporations are. But the reason to lock up your accounts is the same reason you have deadbolts on your doors. They won't keep criminals out if they are truly intent on causing you harm, but if they are merely seeking entrance to an ungaurded house by rattling doorknobs, they'll likely pick on your less-secured neighbors first.

Remembering passwords made easy

Experts now generally agree that passwords are poor security. Better forms of authentication need to be found, but every suggested method has drawbacks. Biometrics can change somewhat with age and health; **fingerprints can be scanned** even from a photo, and more passwords complicate the problem.

All kinds of methods have been proposed: mixing letters, numbers, and other characters is one popular solution, but easily forgettable. **Password manager programs**, touted for their ability to keep track of all your passwords are particularly liable to attack, too.

Any password can be broken with enough attempts, so the longer and more complicated the password is, the harder it will be to crack. However, one easy trick to generate and recall such combinations, called "**the memory palace**," has been around for centuries.

Before he was burned at the stake in 1600 for his outrageous belief in an infinite number of inhabited worlds, **Giordano Bruno** got internationally famous

Continued on back

Continued from front

for teaching the **art of memory**. He devised techniques to allow a normal person to recall huge amounts of unrelated abstract information, like lists of numbers or words, both easily and accurately.

The same methods can devise memorable, nearly-unbreakable passwords. Basically, you first come up with a striking image – the more unusual the better. Describe the picture in a phrase that you can associate with whatever account you wish. So, for example, in my office, I see a hat, a postal scale, and a photo of an astronaut. If I visualize the spaceman on the moon wearing a cowboy hat and weighing a letter on the scale, I have an odd, hard to forget image easy to associate with email. So a good password might be "**cowboymoonmanscales**" – a string that's both long and very unlikely to be found in any text sample.

To make even more sure, I'd change some o's to zeroes or another substitution easy to recall. Then all I'd have to do to recall my password is to think of Neil Armstrong in a 10-gallon hat with a pair of scales.

Dangerous downloads

All of us are dependent on "free" software, from web browsers to content creation tools. Many of these are open-source software backed by a large number of developers, and are generally considered safe.

But not all are. In 2014, several tools the entire Internet has depended on for decades have been shown to have serious flaws. There was the **Heartbleed bug**, **Shellshock, and others**. While no evidence surfaced to suggest that most of these potential exploits had ever been used, they shocked developers into rethinking their reliance on legacy programs.

In any event, those kind of holes in servers are problems for service providers like SWCP (which has plugged them); ordinary users can do nothing. But there are plenty of things offered freely online for users that come with suspicious baggage.

All software and most big websites come with **Terms of Service**. Couched in dense legalese, their objectionable provisions deeply buried, they have to be accepted before resources can be used. But who has the time or patience to study them first?

Now there is an eye-opening site, **Terms of Service; Didn't Read**, that lists and rates them for you. You may be surprised at the various rights you give up – often to content you create – and the high-handed arbitrary ways they can treat you and your material.

An even bigger annoyance for most users are **drive-by downloads**. These are unintended downloads, either without users' knowledge, such as viruses and other malware, or that have been authorized but without their consequences and actions being understood. The latter often happens when getting free or shareware. They can be found bundled even with useful programs on well-known, respected sites such as **C|NET**. What happens is that a "search tool enhancement", or "free security scan" will be listed in very small type, usually on the page with the "Submit" button. If you do *not* uncheck it, the software will download automatically along with the other.

The next thing you know, you could be staring at advertising pop-ups, a different homepage, or with strange search engines that can't be changed. These "freebies" are thinly-disguised malware, and need to be removed *fast*, before the infestation grows.

Many of these cannot be detected or removed by antivirus tools such as **Malwarebytes** – or at least their free versions. There are plenty of websites that offer removal of these pests, but you need to be *very* careful not to make the situation worse.

Recently, when accidentally infected with an annoying advertising program called **Genius Box**, I found one site promising easy removal. However, it wanted me to download *three* separate programs – each of which then wanted payment by credit card to work.

Instead I looked further. I eventually found all I had to do was delete the program through the Windows Control Panel, and reset Firefox to its default settings.

Don't panic!

This advice for galactic hitchhikers is equally valuable for users. *Anyone* can fall for a scam – after all, the bad guys spend a lot of time and effort looking for the right psychological buttons to push. So be aware and take time to think, especially if you receive a message that you *must* do something right away. Get up, take a breather, and call Tech Support with your concerns.

Remember, Southwest Cyberport is on your side. We monitor general usage patterns for infected accounts, filter out viruses from the mailstream when detected, and keep our servers patched. For our customers, we offer one **free computer cleaning** per year, along with free antivirus software, as well as inexpensive hardware and software installation.

Southwest Cyberport

New Mexico's Expert Internet Service Provider since 1994
505-243-SWCP (7927) ⦿ **SWCP.com** ⦿ **Help@swcp.com**
5021 Indian School NE, Suite 600, Albuquerque, NM 87110

Portal *editor/chief writer, Jay Nelson* **jnelson@swcp.com**

Click on blue terms in PDF file to open links.