5 Simple Security Tips Everyone Should Know

By Martin F. Hengst

We live in a connected world, where everything, your phone, your car, and possibly even your refrigerator, are connected to millions of other machines in an ever expanding “Internet-of-Things.”

With all of those machines out here waiting to be tinkered with, it’s no surprise that there are bad people hidden in plain sight, just waiting to get their hands on your information.

Think that connected criminals are only interested in your bank account? Guess again. There’s a booming economy in information sales and everything about you, from your shopping patterns to your medical history has the potential to put money in an attacker’s pocket.

So how do you protect yourself from the dangers of this digital new world? Here are five simple tips that you can take action on right away to protect yourself from some of the most prominent dangers.

Passwords: Don’t just make them strong, make them long.

The traditional wisdom about passwords is to make them complex, which means including both upper and lower case letters, numbers, and the various symbols located around your keyboard. These days, strong passwords just aren’t enough to stop sophisticated brute force attacks.

For instance, a password like **H!z075a4**, which is a combined-case password including symbols and numbers would take a single PC about three days to figure out. That’s just one PC. Consider that people who break passwords for a living have hundreds, if not millions of computers at their disposal. When you factor that in, a password that might seem okay actually isn’t very secure at all.

On the other hand, a password like **37-Frogs-!n-A-Parade#** would take about 32 sextillion years for a single PC to crack. To put that in perspective, that’s the number 32 followed by 21 zeros (in the United States).

While no password is 100% crack-proof, you can see that a longer password takes more effort to break and is therefore a more secure option.

Treat Email Attachments like Abandoned Luggage

If you’ve been in an airport recently, you’ve probably heard the pre-taped announcements to be aware of abandoned luggage or parcels and report them to the authorities if you see something suspicious.

You would be well served to treat email attachments the same way. Unless you personally know the person sending you the attachment, take a moment to call and confirm that the attachment did, in fact, come from the party you think it did.

If you receive an email with an attachment from someone you don’t know, don’t open it. Report it to the authorities. In this case, the appropriate authority would be your Managed Service Provider, like Choice Technologies. They will be able to advise you if the attachment is safe to open or not.

It may seem like a bit of extra hassle, but it could be well worth the effort in avoided downtime and loss of productivity.

If you have doubt, check it out.

Anti-Virus: The Smoke Alarm for Your PC

While we're on the subject of downtime and lost productivity, nothing brings a screeching halt to your day faster than a virus infection running rampant over your PC, or worse, all the PCs in your organization.

While there is no "silver bullet" for virus and malware infection, a good anti-virus software that has been kept up-to-date is the most effective method of stopping the problem before it does too much damage.

You can think of anti-virus and anti-malware software as a smoke alarm for your PC. While no software is 100% effective at stopping all types of threats, most will give you advance warning of a problem and help to mitigate the damage done. Then your IT professionals can step in and ensure that your PCs are free of dangerous viruses and annoying malware.

Plan B(ackup): When Things Go Horribly Wrong

No one likes it when our things break and when our technology stops working, it often has a direct impact on our lives. The pain and frustration of a broken computer or smart phone can wreck your entire day. That pain will be much worse if you don't have a plan to fall back on.

Backups are vitally important. You can never know when a virus might encrypt all your data, a hard drive might fail, or a laptop could be stolen. Without a backup of your data, you could lose both your personal files and business related documents. Are you prepared to have to recreate all that information from scratch?

A popular family of computer viruses, the CryptoLocker variants, take advantage of the fact that many people don't back up their data. These viruses encrypt the data on the computer and then force you to pay $300 or more in order to get the keys to unlock your own data.

If you have a good backup, you don't have to worry about losing your data or having it stolen from you.

Big Brother is probably watching…and so is Your Future Employer

While the other tips have been related to your computer, this tip concerns you and how you use your computer and the services it is connected to. With the explosion of social media popularity like Facebook and Twitter comes the threat of data exposure.

It's natural to want to share your life with your friends and family. However, consider that anything you post on the Internet, to social media or other sites, is never 100% secure. Hackers, disgruntled employees, and even jilted friends can lead to your personal information ending up on the very public Internet, which data never dies.

A recent study found that 57% of hiring managers, when asked if they checked out potential hires online prior to making an offer, responded that not only did they do an online search of employees, but that the information found directly related to the possibility of getting an offer.

A good rule of thumb is that if you wouldn't want your grandmother to see it, avoid posting it online. You might save yourself some hardship later.