An OPCUG Fraud Watch Article

Non-technical safeguards

by Chris Taylor

Most of my security articles focus on technical safeguards. Often, these are the easiest to put in place. Once you understand and implement them, many quietly go about their protection duties. Safeguards such as antivirus, firewalls, replacement DNS services that block access to malicious sites, and malicious-code-blocking browser extensions do their jobs largely by themselves without a lot of work and intervention on your part.

But there are times when technical solutions fail to deliver needed protection. In those cases, protecting your system falls to non-technical—or behavioural—safeguards.

Be suspicious

First and foremost, expect that there are people out there who are trying to trick you. Attackers often try to entice or scare you into doing something that will put your computer or your privacy at risk.

Email

Most malicious emails urge you to click a link in the email or download and run an attachment. The email might promise a windfall or it might offer to prevent something bad from happening such as closing your account or a big charge on your credit card. First, don’t react quickly. Pause and think. Don’t click links or open attachments. If it seems to be related to a service you actually use, open your browser and manually go to the site in question or use a trusted bookmark to verify the issue.

It is important to realize that email is unauthenticated. Email may appear to come from a known and trusted address, but that is not guaranteed. Although some email authentication standards have been developed over the years, there are problems which significantly limit effectiveness and use.

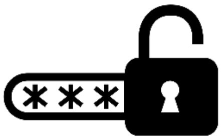
If you think your email account may have been compromised, change the password and make sure the attacker has not set up an auto-forwarding on your email. They may do this so they can force password resets at other sites and, even if they lose access to your email, any password resets sent to your email address will go to them as well.

Phone calls

Phone scams are common. Often, they warn of a unauthorised charges on your credit card. Hang up the phone and call the toll-free number on the back of your credit card to verify if the phone call is legitimate. Scam calls might purport to come from an authority such as the police or Canada Revenue Agency threatening arrest if you do not comply with their demands. Hang up the phone and use another method to contact the service in question. If you get a phone call from someone who claims to be a loved one in trouble requiring your money to bail them out, hang up and find another method of verifying the information. Notice a common thread? Start by hanging up!

Or better yet, stop answering the phone for numbers you don't recognize. My answering machine message says, "Due to the high number of scam and spam phone calls, I don't answer my phone. If you are not a scammer or spammer, leave a message. If I believe you, I will call you back." Scammers never leave a message.

Passwords



Make sure you use a different, strong password for every service/website you use. That way, if your account is compromised at one site, the same password can't be used to compromise your accounts at other sites.

Use two-factor verification wherever you can. If an attacker manages to get your password, they still have to get past the second factor before they can compromise your account. While some second factors, such as SMS messages containing a one-time code, have been criticized for having inherent weaknesses, they are still *far* batter than having no second factor.

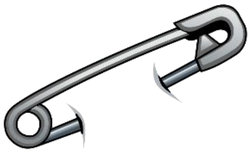
If you use an email address as a recovery mechanism for your password on websites, be sure to give extra attention to protecting that email account. If it gets compromised, you could open up the compromise of other services. Your mailbox may have emails from other online services you use. This gives an attacker known sites they can go to and request a password reset, which then gets sent to your email address, to which they have access.

Many websites allow you to set up security questions in order to recover a forgotten password. It is possible that the answers can be found online. A better approach is to give nonsense answers and record them in a password manager.

Oh…and use a password manager. I wrote about them 2018 https://opcug.ca/Reviews/ProtectPasswords.html. Alan wrote a review KeePass in 2013 https://opcug.ca/Reviews/KeePass.htm. We have talked about password managers multiple times at Q&A. Password managers makes separate, strong passwords for every service/website feasible.

Many people are not fans of frequently changing passwords, especially if they are strong and unique on every website. Even the National Institute of Standards and Technology (NIST) in the States no longer recommends periodic changing of passwords. But if you suspect a password may have been compromised, be sure to change it as soon as possible and change the answers to password recovery questions at the site. You can check at https://haveibeenpwned.com/ to see if your email address has shown up in data breaches. You can also sign up at the site to be notified if your email address shows up in future data breaches.

Other non-technical safeguards



Keep in mind Brian Krebs's 3 rules for online security (https://krebsonsecurity.com/2011/05/krebss-3-basic-rules-for-online-safety/): If you didn't go looking for it, don't install it; if you installed it, update it and; if you no longer need it, remove it.

Change Windows's default behaviour of hiding file extensions for known file types. And then watch for files sent to you with double file extensions. In many cases, this will be someone trying to trick you into thinking their malware is a benign file type. Don't trust the icon displayed for files. It is trivial to have any program display any icon.

Don't trust computers that are not in your control. They could have a keystroke logger installed, collecting usernames and passwords from unsuspecting users.

When you dispose of electronic devices or media that could contain sensitive data, sanitize them first.

Know your critical resources and pay special attention to their protection. If a file is really important, make sure you have multiple copies of it. If a file contains sensitive information consider encrypting it.

Be sure to check out the *Fraud Watch* page at the OPCUG website - https://opcug.ca/fraud-watch/ for a wealth of information on avoiding scams.

There is a security saying at places like airports, “If you see something, say something.” So it is with your computing devices. If something seems odd, don't shrug it off. Look into it. If you are unsure, have a trusted helper check it out.