Greetings everybody! I hope you are safe and healthy and doing as well as you possibly can. If you are working from home, I hope you have made that transition well, too. At this time, you may be wondering, “Am I doing everything I can to keep my work computer, college data and information systems, and my home network safe from hackers?” If that is you, here are a few tips for you to consider.

Keep all your devices up-to-date. This includes your work computer, your personal computers, your mobile phones, and even the router you use to connect to the Internet. Don't forget your IoT devices. What are IoT devices? “IoT” stands for Internet of Things. The Internet of Things includes devices like doorbell cameras, other security cameras, game consoles, digital assistants (ex. Google Home and Amazon Alexa devices), smart TVs, thermostats, etc. If there is a setting that will allow any given device to automatically update, it is a good idea to let it. That way, you can be confident that you always have the latest security patches applied to your device.

Keep your software up-to-date. It isn’t just the operating system of a given device that needs to be kept up-to-date. The various applications on your devices, especially your computers, can also have security vulnerabilities that are addressed with regular software updates. You will want to check that office productivity suites, Adobe products, and web browsers are at the latest version.

Keep your home wireless network safe. Make sure your home WiFi is password protected.

Run antivirus software on your personal computers. Although no antivirus product is 100% effective, it will still protect you from many known viruses and other types of malware. Many antivirus programs will also protect you against browser-based threats, such as web-based phishing and browser hijackers. There are a lot of good products in this space. Be sure to choose one that is reputable and well-reviewed. I can recommend AVG and AVAST. The basic version of each is free for personal use.

Watch Out for COVID-related scams. The bad guys will use any opportunity to scam a buck. Be on the lookout for COVID-related phishing messages. These may come in various forms.

1. Phishing messages claiming to be from a reputable source like the CDC or WHO. These will likely carry links to bogus sites. As always carefully inspect the address of any link that comes in an email message.

2. Spam messages promoting cures, treatments, or vaccines for sale.

3. Spam messages promoting investment opportunities in companies with alleged cures, treatments, or vaccines.

4. Solicitation of donations to bogus charities. Only make donations to charities you know or can confirm are genuine.

5. Some phishing messages will direct you to a website that requires a login. These are designed to steal your username and password. Don’t fall for it. Don’t try to log in.

6. Vishing (voice phishing) and smishing (text phishing). The scammers won’t only use email, they’ll call on the phone and send text messages as well.

For more information about COVID-related scams, consider these resources:
COVID-19 Exploited by Malicious Cyber Actors
Coronavirus scams: guard against fraud cures and other cons

Use the VPN. There is good reason to use the VPN even if the resources you need to do your work don’t technically require using the VPN. First, the VPN is behind a firewall that inspects traffic in both directions looking for traffic patterns and signatures that are consistent with malware or other malicious activity. Secondly, we have network monitoring in place that alerts us when a machine communicates with a

known malicious domain or Internet address. You only benefit from these capabilities if you are on a Carleton network which includes the VPN networks.

Data Classification. Now is a good time to review our college data classification and data handling policies:
Data Risk Classification Guidelines
Data Management and Access Guidelines

A couple of things to keep in mind when working with high-risk data:

1. Only use a college-owned machine to access high-risk data.

2. Don't send high-risk data by email.

App security review. As you are looking for ways to make working or teaching from home easier, you may come across new applications and browser plugins. You might wonder if these are safe to install and use on your college computer. I will gladly help. Let me know which apps or plugins you are considering, and I will perform a security review.

The best way to request an application security review is through our help desk ticketing system. There are two ways to do this:

1. Send an email to helpdesk@carleton.edu

2. Use the Helpdesk portal at https://stolafcarleton.teamdynamix.com/TDClient/2092/Carleton/Home/ and select “Open a Ticket”.

Do you like videos? (Carl) Consider taking a few minutes to watch one of our student-produced PSAs covering the topics Multi-Factor Authentication, Password Managers, Browser Highjackers, and Social Networking Privacy. Or check out the Academic Technology channel for more videos covering a variety of topics.

And as always, be safe out there and, if you ever have any questions, don't hesitate to contact me or the Helpdesk.

Kendall George
Information Security Officer | Information Technology
Carleton
Pronouns: he/him/his
Office: 507-222-7079
One North College Street, Northfield, MN 55057
carleton.edu