TechXplore

Five ways to protect yourself from cybercrime

July 23 2019, by Scott Shackelford

Have hackers driven us back to the age of the physical key? Credit: Bautsch/Wikimedia Commons

High-profile data breaches at companies like British Airways and Marriott get a lot of media coverage, but cybercriminals are increasingly going after community groups, schools, small businesses and municipal governments.

Just in the Midwest, hospitals, libraries, voter registration systems and police departments have fallen victim to one type of digital hijacking or another. Cybercrime is not just a concern for corporate technology departments. Schools, scout troops, Rotary clubs and religious organizations need to know what to look for and how to handle it.

As the academic director of a new cybersecurity clinic at Indiana University, I'll be helping to lead students and faculty members in teaching local, county and state government agencies, not-for-profit organizations and small businesses how to improve their cyber hygiene. They'll learn how to better manage digital systems, protect their intellectual property and improve consumer privacy.

Everyone should know the basics for how to protect themselves and the groups or organizations they're part of. Here is a brief look at some of the cybersecurity best practices we'll be teaching members of our communities to keep in mind as they go online for work, play or volunteering.

1. Keep everything up to date

Many breaches, including the 2017 one at the Equifax credit bureau that exposed the financial information of almost every American adult, boil down to someone leaving out-of-date software running. Most major computer companies issue regular updates to protect against newly emerging vulnerabilities.

Keep your software and operating systems updated. To make it easy, turn on automatic updates when possible. Also, be sure to install software to scan your system for viruses and malware, to catch anything that might get through. Some of that protection is free, like Avast, which Consumer Reports rates highly.

2. Use strong, unique passwords

Remembering passwords, especially complicated ones, isn't fun, which is why so much work is going into finding better alternatives. For the time being, though, it's important to use unique passwords that are different for each site, and not easy-to-hack things like "123456" or "password."

Choose ones that are at least 14 characters long. Consider starting with a favorite sentence, and then just using the first letter of each word. Add numbers, punctuation or symbols for complexity if you want, but length is more important. Make sure to change any default passwords set in a factory, like those that come with your Wi-Fi router or home security devices.

A password manager program can help you create and remember complex, secure passwords.

3. Enable multi-factor authentication

In many situations, websites are requiring users not only to provide a strong password but also to type in a separate code from an app, text message or email message when logging in. It is an extra step, and it's not perfect, but multi-factor authentication makes it much harder for a hacker to break into your accounts.

Whenever you have the option, enable multi-factor authentication, particularly for crucial log-ins like bank and credit card accounts. You could also consider getting a physical digital key that can connect with your computer or smartphone as an even more advanced level of protection.

4. Encrypt and back up your most important data

If you can, encrypt the data that's stored on your smartphone and computer. If a hacker copies your files, all he'll get is gibberish, rather than, for instance, your address book and financial records. This often involves installing software or changing system settings. Some manufacturers do this without users even knowing, which helps improve everyone's security.

For data that's crucial, like medical information, or irreplaceable, like family photos, it's important to keep copies. These backups should ideally be duplicated as well, with one stored locally on an external hard drive only periodically connected to your primary computer, and one remote, such as in a cloud storage system.

5. Be careful using public Wi-Fi

When using public Wi-Fi, anyone nearby who is connected to the same network can listen in on what your computer is sending and receiving across the internet. You can use free browsers like Tor, which was originally developed to provide secure communications for the U.S. Navy, to encrypt your traffic and camouflage what you're doing online.

You can also use a virtual private network to encrypt all your internet traffic, in addition to what goes through your browser—like Spotify music or video in the Netflix app—to make it more difficult for hackers, or even casual users, to spy on you. There is a wide range of free and paid VPN options.

In short: Be cautious, proactive and informed

Of course, there is much more a person or organization can do to protect private data. Search engines like DuckDuckGo don't track users or their searches. Firewall software built into both Windows and Mac OS – or downloaded separately—can help stop viruses and worms from making their way into your systems.

To protect yourself against data breaches at places where your information is stored, you should consider freezing your credit, which blocks anyone from applying for credit in your name without your personal permission. It's free. If you have already received a notification that your data has been stolen, consider putting a free "fraud alert" on your credit reports.

There are plenty of other places to learn more about cybersecurity, too, including some very good podcasts.

No person, organization or computer can ever be 100% secure. Someone with the patience, money and skill can break into even the most protected systems. But by taking these steps, you can make it less likely that you'll be a victim, and in the process help raise the overall level of cyber hygiene in your communities, making everyone safer both online and off.

Provided by The Conversation

Citation: Five ways to protect yourself from cybercrime (2019, July 23) retrieved 6 May 2024 from https://techxplore.com/news/2019-07-ways-cybercrime.html