Eight simple steps to secure your devices and data

September 1 2016, by Troy Wolverton, The Mercury News

It's not easy protecting your devices and data these days. Ransomware, email scams, identity theft, hacking attacks, massive data breaches - the news is filled with stories of the security threats consumers, businesses and governments face. When even the National Security Agency can't keep its crucial information secure, you may rightly wonder what an average person can do.

It's definitely a challenge. The threats are evolving, becoming increasingly sophisticated and costly and affecting more people. What's considered to be the best advice can soon become obsolete as criminals develop new methods or the security researchers better understand the weaknesses in older strategies. And the more data we put online, the more devices we connect and the more things we do on the internet, the more we have at risk.

"I don't envy the average consumer who has to stay on top of these things," said Marcin Kleczynski, CEO of Malwarebytes, which makes anti-malware software.

But as difficult as it may be, it's important to try to protect yourself. Consumers and businesses have been bilked out of billions of dollars and lost access to valuable files and data thanks to malware and online scams.

And as daunting as it may seem, there are some relatively simple steps you can take to make your devices and data more secure. The top advice from security experts: Don't expect any one step to completely protect

you. Instead, think of the steps as lines of defense.

Here are some of the measures security experts recommend:

-Assess your risk. Someone working in the political opposition in Egypt is going to have a different level of risk than the average American. Someone who spends much of her life online is going to have more at risk than someone who goes online only occasionally to check his email. The more at risk you are or the more sensitive your data, the more steps you'll likely have to take to protect yourself.

-Backup your data. This is perhaps the most critical step you can take, because it helps ensure not only against security threats but also hardware failures. A malware infection becomes much more tolerable if you can just wipe out your computer and reinstall everything from a backup.

It's smart to backup regularly, so that you can restore the latest changes you've made to your device or the latest data you've added. But it's also important to ensure that the hard drive or service you use to backup your computer isn't always connected to it. The latest versions of ransomware, a type of malware that encrypts data and extorts users for money to unscramble it, can jump from a PC to attached drives, potentially affecting backups as well.

You can avoid such problems by disconnecting your hard drive after it backs up your computer; burning your data to DVDs; or using an online backup service like Carbonite that only connects to your computer periodically and keeps multiple versions of your data.

-Keep your software up to date. Much of the malware in circulation exploits security holes in operating systems, browsers and plug-in programs like Adobe's Flash. It's important to install security updates to

those software programs because they close those holes. And it's a good idea to install those updates right away or set your computer to automatically install them when they are released, because the release draws attention to vulnerabilities in the unpatched software, potentially leading to more malware designed to exploit them.

Just by keeping your software up to date, "you will be far less vulnerable to attacks," said Cooper Quintin, staff technologist at the Electronic Frontier Foundation, a digital rights advocacy group.

-Run anti-malware software and keep it updated. Anti-malware software is far from perfect. Research indicates that most programs do a pretty good job at catching viruses that have been in circulation for a while - and a pretty lousy job at identifying and eliminating novel threats. But anti-malware is usually better than nothing - as long as you don't rely on it as your sole means of defense.

-Be careful with your passwords. Doubtless, you've heard lots of advice on using better, more secure passwords. And undoubtedly, you've probably ignored that advice, at least on occasion. It's a good idea to heed it, at least when trying to protect things like your financial accounts or sensitive data. The more powerful computers become and the more sophisticated hackers get, the easier it is for them to crack simple passwords.

Some of the key advice from security analysts: Generally, the longer the password and the more random the characters used, the better. And don't reuse passwords, at least not with the accounts that house your most valuable information. If that password is compromised, it puts multiple accounts at risk.

Of course, following such advice can make it difficult or impossible to remember passwords. One thing that can help is a password manager.

Programs like LastPass and 1Password can store all your complicated passwords, help you create new ones and allow you to access your list on different devices.

-Be careful with social media. What you say on Facebook doesn't necessarily stay on Facebook. Scammers can use information they glean about you from your social media posts to impersonate you to scam money from your friends and relatives or your company. They can also use that information to crack your passwords or the security questions that many companies use to authenticate users who want to reset their passwords.

That doesn't mean you should close your Facebook and Twitter accounts. But it does mean you should think about what you post and who has access to it.

-Think before you click. One of the most common sources of malware is through email links and attachments. Scammers have gotten pretty good at sending out email the looks like it legitimately came from your bank, and hackers have frequently been able to use malware to hijack consumers' accounts to send out emails in their name to family members and friends. That's why it's a good idea to be skeptical of any link or attachment you receive, even if it appears to be from your spouse or most trusted associate.

Instead of clicking on a link that appears to come from your bank, go to the bank's website directly. Rather than open the attachment that appears to come from your friend, text or call the friend to make sure they actually sent it to you.

-Be skeptical. You should develop a "suspicious mindset" when you're online, said Eugene Spafford, a professor of computer science at Purdue University who focuses on security issues. This extends beyond being

skeptical of email links and attachments to being careful about clicking on advertisements you see or visiting websites.

Advertisements for free software or notifications that urge you to download anti-virus programs can be vehicles for malware. And the internet's pornography and gambling sites can be havens for malicious software.

"Moral issues aside, there are solid technical reasons why to not visit the seedier sites on the internet," said John Dickson, principal at the Denim Group, a security consulting firm.

—-

HOW TO KEEP YOUR INFORMATION SECURE

1. Assess your personal risk

2. Backup the information on your devices

3. Be sure to keep your software up to date

4. Run anti-malware software (and keep it updated)

5. Don't ignore advice on creating strong passwords

6. Watch what you share on social media

7. Think before you click

8. Be cautious online