# PREVENTING CYBERCRIME

*By Debbie Yokota, ARM, Chief Risk Officer, SDRMA*

In a technically driven society, people use various devices to make life simple. The increasing access to and continuous use of technology has radically impacted the way people communicate and conduct their daily lives. Nevertheless, the internet and computer can pose threats which can negatively impact civilization.

Cybercrime is a hazard against different organizations and people whose computers are connected to the internet and particularly mobile technology. Cybercrime basically is defined as any criminal activity that occurs over the internet. There are many examples; such as fraud, malware such as viruses, identity theft and cyber stalking. Earlier, cybercrime was committed mainly by individuals or small groups. Today, criminals that indulge in cybercrimes are not motivated by ego or expertise. Instead they want to use their knowledge to gain profits promptly.

**What is cybercrime?**

Cybercrime is a hazard against different organizations and people whose computers are connected to the internet and particularly mobile technology. Cybercrime basically is defined as any criminal activity that occurs over the internet.

Cybercrimes are broadly categorized into three groups, such as crime against:

1. Individual
2. Property
3. Government

### INDIVIDUAL

This type of cybercrime can be in the form of cyber stalking, trafficking and "grooming." Law enforcement agencies are considering such cybercrime very serious and are joining forces worldwide to reach and arrest the offenders.

### PROPERTY

This type of cybercrime involves offenders stealing a person's bank details to drain off money; run a scam to get naïve people to part with their hard earned money; use malicious software to gain access to an organization's website or disrupt the systems of the organization. The malicious software can also damage software and hardware, just as vandals damage property in the real world.

### GOVERNMENT

Crimes against a government agency are denoted as cyber terrorism. If criminals are successful, it can cause devastation and panic amongst the citizenry. In this class, criminals hack government websites, military websites or circulate propaganda.

High-profile data breaches at companies

like Twitter 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.

In today's increasingly complicated environment, all companies need to know what to look for and how to handle cybercrime. Everyone should know the basics of how to protect themselves and the groups or organizations they are a part of. Here is a brief look at some of the cybersecurity best practices every public agency should be considering:

### 1. KEEP EVERYTHING UP TO DATE

Many breaches, including the 2017 breach 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.

### 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 passwords 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 MULTIFACTOR 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 multifactor authentication makes it much harder for a hacker to break into your accounts. Whenever you have the option, enable multifactor 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 financial information, or irreplaceable, like family photos, it's

*continued on page 36*

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

### 6. BEFORE MAKING ANY ELECTRONIC FUNDS TRANSFERS VERIFY REQUEST

We are seeing more and more financially related cybercrime against public agencies. An email will be sent to an agency from a vendor partner requesting funds with new banking information. After the funds are transmitted, the public agency discovers the email was fraudulent and sent by an unknown party who copied an email from one of their vendor partners.

Another ruse is to copy an email by an officer or other employee within the agency that is then sent to the finance person asking for funds to be transmitted to a bank account. Verify all emails requesting funds be transferred or payments sent even if you recognize the sender.

### IN SHORT: BE CAUTIOUS, PROACTIVE, AND INFORMED

Of course, there is much more a person or organization can do to protect private data. 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. 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 and your organization will be a victim.