CCIG

CCIG's CYBER SECURITY GUIDE

6 CYBER SECURITY BEST PRACTICES
TO PROTECT YOURSELF

INTRODUCTION

How pervasive is cyber crime today? What makes cyber crime dangerous is how subtle it is, and how often it can occur without anyone's notice. Cyber crime in reality is vastly different from what takes place in movies.

Here are some facts to help you get acquainted:

The United States is currently the **MOST TARGETED NATION** in the world for phishing attacks.

Cybercrime is expected to generate at least **$1.5 TRILLION IN REVENUE** for bad guys this year.

Most individuals are not secure from typical attacks that can result in information and financial losses ranging from **$75,000 TO $1 MILLION AND UP.**

In 2017, ransomware resulted in **$5 BILLION IN LOSSES**, both in terms of ransoms paid and spending and lost time in recovering from attacks.

More than 1 billion records were exposed in **DATA BREACHES** in 2018.

MOBILE PLATFORMS are one of the fastest-growing targets for cyber criminals.

1. Beware of Public WiFi

A public Wi-Fi network is inherently less secure than your personal, private one, because you don't know who set it up, or who else is connecting to it. Ideally, you wouldn't ever have to use it; better to use your smartphone as a hotspot instead.

But if you must use a public Wi-Fi, then browse over HTTPS, so that people on the same network as you can't snoop on the data that travels between you and the server of the website you're connecting to. Over HTTP? It's relatively easy for them to watch what you're doing.

2. Siri is listening ...

Not all technology companies operate in the same manner. In fact, their business models and data collection and use practices are often radically different from one another. Still, if you’re concerned that Siri might be tuning in when you don’t want her to, here’s how to turn the digital assistant off:

- Go to Settings
- Tap Siri & Search
- Turn off the toggles for “Listen for ‘Hey Siri,’” “Press [Side or Home] Button for Siri,” and “Allow Siri When Locked”

This will turn off Siri. You could also tape over the microphones on your phone, as many have taken to doing for their laptop webcams.

3. Update Your Software

This is especially important with your operating systems and internet security software.

Cybercriminals frequently use known exploits, or flaws, in your software to gain access to your system. Patching those exploits and flaws can make it less likely that you'll become a cybercrime target.

In short, anti-virus and anti-malware software has become a security non-negotiable. Neglecting security updates will only leave the door wide open for hackers.

4. Cross-infection risks

Blame this on the rapid growth of Internet of Things (IoT) devices being added to home networks.

Network segmentation is a way to isolate devices on separate networks to achieve better sharing of throughput or bandwidth to the Internet, securing systems with more sensitive data, and separating systems from people and other systems that don't have a need to connect to them.

In the typical home, this can be achieved by using two more routers, so that when your kids' friends are over or a long-lost relative shows up, you're not suddenly opening your digital lives to them.

5. Password managers

Still using your kid's birthday as your universal password? You're asking for trouble. With a password manager, you can have a unique and strong password for every secure website.

A password manager servers many purposes, all of them helpful. It keeps all your passwords under one encrypted (and password-protected) roof. It generates strong passwords for you and automatically inserts them when you log into different sites.

It can even store payment information to simplify online shopping.

6. Two-factor authorization

Two-factor, or multi-factor, authorization, is an extra layer of security used to make sure that people trying to gain access to an online account are who they say they are.

The basic idea is that a single password for your important accounts simply isn’t enough. Two-factor authorization itself is simple: after you enter your username and a password, you'll then be asked to provide another piece of information to gain access to your account.

Two-factor authorization, however, isn’t foolproof. If you elected to receive your codes via SMS, for example, the code could potentially be intercepted by hackers. So it's a good idea to use an authorization app. Google Authenticator, for example, will generate a constantly-changing stream of codes. You then input the latest one to verify your logins haven't fallen into the wrong hands.

Insurance Solutions

Cyber coverage can be added by endorsement to a homeowner's policy. Typically, coverage limits of $100,000 and $250,000 are available. However, up to $1 million in coverage may be available if the homeowner subscribes to a cyber monitoring service that actively monitors their home network and devices.

Highlights:

Coverage for Online and Offline Fraud: Reimburses the homeowner for financial losses related to fraud, whether the crime is committed online or offline. Examples include social engineering of an authorized account user, criminal deception, unauthorized transfers, forgery or alteration of checks, acceptance of counterfeit money and more.

Coverage for Cyber Extortion: In the event of a cyber extortion incident — a type of attack in which a cybercriminal demands money to prevent the damage or distribution of content or to restore access to the functionality of a device — this coverage will afford immediate access to crisis management advice from a subject matter expert to help best respond to the threat, and in the event a payment is made, reimburses the homeowner for the amount of the payment.

Coverage for System Attacks: Provides coverage for the cost of a professional to reinstall damaged software, remove malicious code, reconfigure the device or system and replace electronic data that has been lost or corrupted as the result of a cyber attack.

ABOUT US

Your home, automobiles, the RV. CCIG can help protect you, your family, your assets and your prized possessions with customized policies that meet the changing circumstances of your life.

We start by understanding who you are, your lifestyle, your passions, providing you with the kind of personal, responsive service that addresses your ongoing, specific needs.

CCIG's experienced Personal Insurance Advisors will get to know you and your family and build an insurance program tailored to your specific needs. So, whether you're just starting a family, buying a vacation home or your teenager has started driving, CCIG has you covered.

Connect with us today to learn more!

THINKCCIG.COM