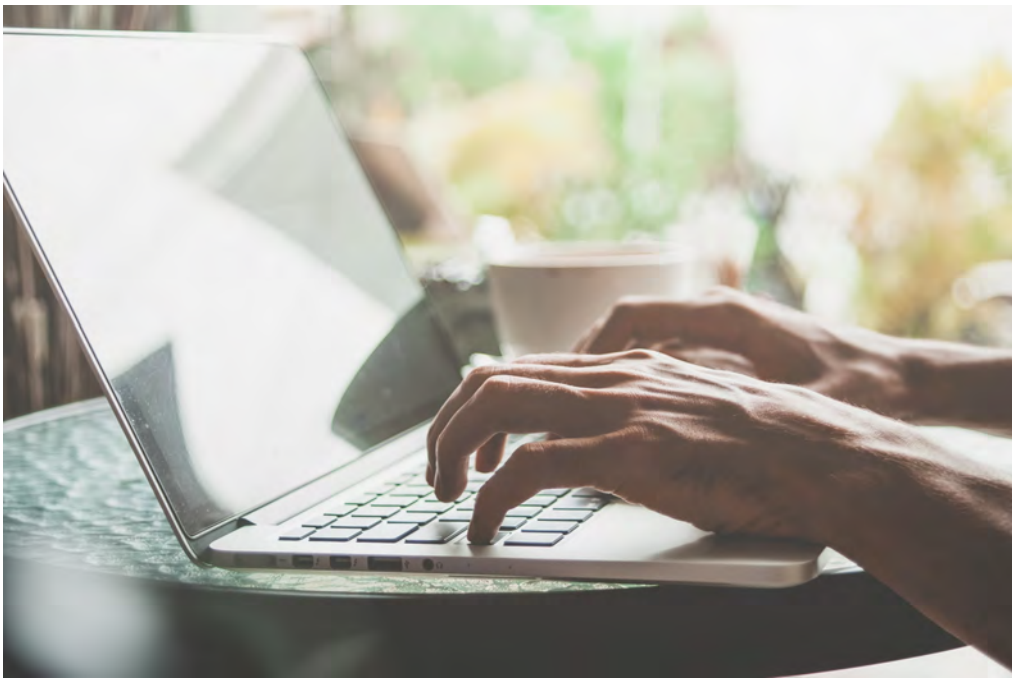
total Digital Security

Cybersecurity for Life.

Checklists and best practices

As our lives become more and more digital, families face increasing threats of cyber crime. Here are some ways to secure your online activities and avoid becoming a victim.



Think you've been hacked? Do these five things immediately.

Disconnect your computer from the Internet.

Change passwords depending on the type of attack.

Scan your computer and network then apply patches and software updates.

Contact a security expert, and request that credit agencies put out a fraud alert and ensure data is backed up to recover from future cyber attacks.

File a police report, including relevant notes and other documentation of the incident.

People have become accustomed to constant online access and may not fully understand the risks. Due to this, it has never been more important to protect your assets and identity from cybercriminals who wish to corrupt and steal.

Attacks can come from anywhere. For example, a family noticed, during a routine check of a credit card statement, that someone had purchased over 100 gift cards — each worth $500 — and had given them away to people whose names they didn't recognize. The hack occurred through a shopping app on a teenager's smartphone when an item was purchased through a store's Wi-Fi connection.

Family assets may be insured, but once trust is violated, it's not easily rebuilt. Even after a security breach during which nothing was stolen, families may feel like they've been robbed.

The ABCs of cyber security

Educating families about cyber risk is vital. Here are some basic first steps toward better privacy and security.

Texting: Avoid texting private information, such as birth dates, Social Security numbers and credit card information.

Social media: Avoid connecting with strangers on social networks. Social media can give away a family's whereabouts or allow a criminal inside their personal lives.

Wi-Fi: Matters regarding financial transactions should only be conducted on a trusted private Internet connection such as VPN to connect securely when using Wi-Fi. Cybercriminals often use public Wi-Fi to steal information from network users that are not using VPN encryption.

Email accounts: Avoid emailing sensitive information that could be compromised, resulting in transmission of malware, criminals eavesdropping on conversations, and criminals imitating you through a similar email address.

Use a VPN Every Day

Always use a VPN (It's easier than ever)

Make sure to use a virtual private network (VPN) to ensure privacy when accessing public networks. A VPN allows you to become essentially invisible on the Internet, whether using a computer or mobile device.

What is it? A VPN extends a private network across a public network, and enables users to send and receive data across shared or public networks as if their computing devices were directly connected to the private network. Your information is encrypted, making it difficult to steal or corrupt.

Can it be used anywhere? Users can be on any network anywhere in the world, and all communications are auto-encrypted and invisible to anyone on the outside.

How do you get it? Today, you can set up a VPN for your family's connected devices with an app, which costs a few dollars a month.

What app should I use? Use only name brands, or talk with a security expert to decide which service to use. Scammers have set up fake VPNs that can compromise the very information you are trying to protect.

In the past, VPNs were used for only the most crucial information. Social media and web browsing would be fine without it, but online banking required it. Today, it's so easy that you should be using it for all of your online activity.

Protect Your Devices

A protection checklist for your devices

Make sure you consider these technologies when you're connecting to the Internet.

Antivirus software: The tool is about prevention, and only the best providers should be considered. Look for software with automatic updates and fast responses.

Intruder malware and rootkit protection: Assume intruders are always trying to connect to your devices and collect personal data. Sometimes they use rootkits, which are assemblies of software enabling access while masking their existence. Make sure your security professional shields your network.

Firewall: A firewall is a gatekeeper for your network. Your firewall should be configured to ensure the right information enters and exits your network.

Router: All of your online activity flows through your router. Be careful to change the default router password to a unique one in order to guard against cybercriminals gaining access to your network and private information.

Software updates: Keeping software updated is a very effective measure against hacking. Turn on the automatic updates to your software, and be sure to download the newest operating systems and applications.

Smarter passwords

Passwords are the keys to our digital kingdom, so make sure they are unique, strong and complex.

Length

The primary driver for creating a password that is difficult to crack is length. So a four-character password is far less effective than a 14-character one.

Randomness

Because cyber criminals feed password-cracking software with personal information to increase their odds of success, we can deduce the most effective passwords are long and random. Randomize by using phrases, upper/lowercase letters, numbers and special characters.

Password manager

Use a software application to simplify the complexity of logging in. Committing 15 to 30 minutes to setting this up will make you more secure for the rest of your life. It encrypts and stores the user names and passwords for all of your online accounts. You gain access to your account using one long, more-secure master password.

Putting it all together

To create a more secure password, start by using a long word or phrase that's easy to remember. Something like cowboymoonpalm is a good example**.** The image of a cowboy on the moon while leaning on a palm tree is not only easy to remember, but it is also long and unique, making it very difficult to hack.

Double-bolt your passwords

Using two-factor authentication can strengthen your defenses and mitigate the chances of a breach.

Best Practices

1. Use good password habits: See “Smarter Passwords” on page 3

2. Use a two-factor password authorization:

   Passwords are the keys to our kingdom, so double-bolting with two-factor password authorization is essential.

3. Don’t email private information like birth dates, Social Security numbers or credit card information.

4. https: Websites that begin with https (as opposed to just http) have a layer of encryption called the secure sockets layer, or SSL. Never enter your card information or other sensitive data into a site without the “s”.

5. Wi-Fi: Matters regarding financial transactions should only be conducted on a trusted private Internet connection such as VPN to connect securely when using Wi-Fi. Cybercriminals often use public Wi-Fi to steal information from network users that are not using VPN encryption.

Remember the value of personal information:

Create a sense of value around personal information, and appreciate the fact that it’s increasing in value. Companies (and scammers) in the digital age are collecting personal information and engineering it in a way to exploit something or sell you something.

Current Scams:

Invoicing scam: Scammers will monitor personal news: births, deaths, new homes and more, and then send fake invoices for payment. For example, after finding a widow on the Internet, scammers will pretend to be a collection agency calling about the recently deceased’s debts.

Charitable donations scam: Beware of requests for money immediately after a disaster. Scammers set up fake websites with names similar to real charities and solicit donations. Investment scam: Scammers will set up seminars or websites where they suggest investing in specific funds or unusual assets has made them rich.

Personal scams: With so much information available online — through social media or online dating apps — scammers may be using blackmail or personal scams in addition to just economic scams.