BANK OF AMERICA

PRIVATE BANK

Digital defense: Keeping your family safe online

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.

The digital landscape continues to grow at an exponential rate. From personal technology, like computers, mobile phones and smart watches, to the Internet of Things (IoT), such as doorbells, connected appliances and digital assistants, the innovations make our lives easier and allow us to be more productive as we go about our daily routines. These conveniences also introduce our families to greater cyber risk. This landscape continues to grow as more objects and devices connect and those connections become smarter, faster and easier. Throughout your day, you probably don't go anywhere that you're not part of the framework, which includes applications (apps), email, the Internet, social networks and mobile devices. Pacemakers, doorbells, insulin pumps and refrigerators are now part of this landscape, too.

The numbers are staggering: Estimates suggest 4.4 billion people are now using the Internet.[1] Equally astonishing, almost 3.5 billion are social media users, and more than 5.1 billion are using a mobile phone.[1] There's no question the framework provides convenience and plays a growing role in our lives, but it also allows for increasing financial risks.

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.

[1] "Digital in Around the World in April 2019" We Are Social, April 2019.

Trust and fiduciary services are provided by Bank of America, N.A., Member FDIC and wholly owned subsidiary of Bank of America Corporation (BofA Corp.).

Investment products:

Are Not FDIC Insured	**Are Not Bank Guaranteed**	**May Lose Value**

Please see back for additional important disclosure information.

The family contacted Tania Neild, a cyber security consultant, to analyze and diagnose what had happened. In the process they learned some key preventative measures. A Ph.D. in database integration who spent five years at the National Security Administration (NSA), Neild says family members usually have little idea about how much their daily online activities may be putting their assets at risk. This family in particular was victimized because they weren't following some of the basic guidelines of cyber security.

"We worked backward to find out what happened," says Neild. "Were they on a public Wi-Fi? Yes. Were they conducting a transaction? Yes. Were they successfully processing the consequences? No." Neild said it was helpful to have the whole family in the room so they could work on the issue together. "This was a four-generation family," she says, noting that different family members had very different skill sets when it came to technology. "I had everyone from an infant to a great-grandfather in front of me, and although I had my work cut out for me, in the end, it was helpful to work as a team."

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.

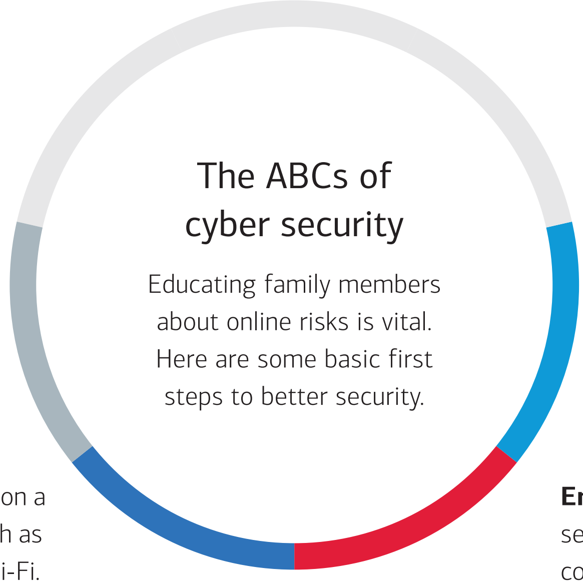
What is it? A VPN extends a private network across a public network, and enables users to send and receive data across shared or public networks as if their computing devices were directly connected to the private network. Your information is encrypted, making it difficult to steal or corrupt.

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, according to cyber security consultant Tania Neild, 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. "There's no added complexity, so you can just apply it across the board," Neild says.



The ABCs of cyber security

Educating family members about online risks is vital. Here are some basic first steps to better 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.

A protection checklist for your devices

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

"We are just in the early innings of the Digital Age," says Brad Deflin, founder and president of Total Digital Security. With the technology (and threats) constantly evolving, Deflin recommends six ways to protect your devices.

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

They open your accounts, 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 cowboysmilingmoonpalm is a good example, Deflin says. The image of a cowboy on the moon smiling 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.

Thinking through vulnerabilities

While cyber crime increased by 38% in 2016,[2] this doesn't mean families can't use email and social networks. Roughly 96% of Americans now own a cellphone of some kind, and 84% of those adults are smartphone Internet users.[3] Kids, especially, want to participate because so many of their friends are online. An independent study found 45% of teens are online "almost constantly" via smartphones and almost 95% of teens have smartphones.[4]

Neild says rules are important, but the real key is balance. "I try to move everyone to the middle," she says. "If it gets too strict, then it's not practical. But if it's too loose, you open yourself up to great risk." **Neild begins with the basics:**

1 Connect to websites to access sensitive information via a secure Internet connection (see "Always use a VPN (It's easier than ever)" on page 2 for more).

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

3 Avoid creating social media posts with personal information that could take a cyber criminal inside a family's home or divulge their whereabouts on vacation. Also, respect those around you, and consider their privacy too before posting.

4 Establish passwords — the most common security breach — no one can guess (see "Smarter passwords" on page 3 for more).

5 Use two-factor authentication whenever possible, especially when using banking and online marketplace sites that involve financial transactions and information (see "Two is better than one" to the right for more).

6 Minimize the use of the "Forgot your password?" function when logging into sites that involve financial transactions or store sensitive personal information. These may include your bank's website and online marketplaces used to make purchases. In the event you do need to use this function, remember to change the temporary password immediately and avoid using vulnerable email services such as Gmail or Yahoo whenever possible. These personal email services are the first places cyber criminals go to access your information, Neild says.

Two is better than one

Using two-factor authentication can strengthen your defenses and mitigate the chances of a breach. Below, Neild breaks down the basics of incorporating the process into your digital security plan.

What: At its core, two-factor authentication is a security tool that requires users to enter a numerical code — typically delivered to the user's cellphone via text message — after entering their username and password in order to successfully log in to a particular website or online account.

Where: Using two-factor authentication is a good idea whenever it is available, but it is particularly important when using accounts that involve financial transactions and information, Neild says. In addition to using it on the websites themselves, she also highly recommends users use the two-factor process when logging in to the actual email accounts connected with these types of websites.

Why: No matter how strong a password may be, it is still at risk of being hacked. With two-factor authentication, a second level of security is added, Neild explains. "Even if cyber criminals figured out your password, they would have to steal your phone in order to access your accounts," she says.

How: With cyber security such a primary concern in today's world, many companies and email providers either require two-factor authentication or at least offer it as an option to users, Neild says. There are also a variety of mobile apps available for your smartphone, she says, noting that they are particularly effective and easy to use.

[2] Pew Research Center, The Global State of Information Security® Survey, 2018.

[3] Pew Research Center, Mobile Fact Sheet, June 12, 2019.

[4] Pew Research Center, Teens, Social Media & Technology 2018, May 31, 2018.

Sometimes stating the obvious is necessary, Neild says, such as reminding kids they should never share their passwords. Likewise, children need to understand the dangers of posting photos and personal information. “They need to recognize what is and isn’t visible and act appropriately,” she says. A large public donation, for example, could end up in local media for positive reasons, but also could lead cyber criminals to individual family members’ work or social network accounts. From there, seemingly innocent public information can be used against a family. “It could be something as benign as a post like ‘Having fun in Cabo,’” she says. “But if someone recognizes your name because your family just donated $10 million to build a library, there you are in Mexico, where kidnapping is big.”

What are some of the best practices?

As the threat of cyber crime grows, so does the need to protect family assets. How is this done? Some suggest working with a webmaster to establish a family domain — a secure site accessible by a small number of approved family members, each with their own domain email (e.g., bob@familyname.com). While this is often fairly simple to set up, it can require engaging your children in discussions about cyber security, which is far easier said than done. “It’s the last thing they want to talk about,” says Brad Deflin, founder and president of Total Digital Security. “The private domain is like a fort from which the family is protected — a safe haven from the hostilities on the variety of vulnerable ‘free’ email services available.”

Though initially hearing from clients about the challenge in communicating the importance of security to their children, Deflin eventually observed that the idea of a family domain was an effective starting point to pique children’s interest and get them thinking differently about the subject. The private email approach demonstrates the importance of striving for more digital autonomy and protecting personal information.

Recognizing threats

Over 100,000 breaches in cyber security occur every day, Neild says. And there’s more than one kind of cyber criminal. Just like in the real world, different people want different things, and have different tactics to try to get them.

Some cyber criminals are outsiders, digging up information on a family through social networks or by accessing networks illegally. Others may have insider information about the family, or even be family acquaintances or on the family’s payroll.
Recognizing different kinds of cyber criminals is paramount to a family’s security, as is taking precautions.

The criminals behind these acts can be divided roughly into four categories:

Insider	Malicious or benign, an authorized user with access to a person or organization’s data or information assets.
Criminal	An individual or group who uses the Internet to commit theft, fraud or other criminal acts.
Hacktivist	A person or group who uses cyber activities to achieve political, social or personal goals.
Nation state	Government-backed actors with training, resources and offensive capabilities.

Manage your digital dossier

You may have your offline life, but everything you do online can be combined into one larger "digital dossier" by scammers. Sometimes people live multiple lives online. For example, you may have one persona for social media and another for online video games and a third for online dating. But a scammer can connect those personas and learn a lot about you by connecting the dots with all your data.

Use these tactics to put your online presence into perspective:

Think of it as engraving: Everything you do online should be considered permanent, says Brad Deflin, founder and president of Total Digital Security. Thinking about each social post as engraved in stone will help you see the importance of it.

Make yourself proud: Would you be able to look back at comments you made on a video game message board in 10 years and feel happy about the content? Think about your future self when you do anything online.

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.

Stay out of dark alleys: If you are unsure about how an app or website is using your data, don't blindly submit your information.

"Just be really conscious of the activities you participate in," says Deflin. "And tell your children, 'We are really printing permanently here, so be sure it represents who you are and who you want to be. And aspire to make it great.'"

“There is a vanity element to it as well,” he says. “When kids see their last name in the domain it somehow creates a different perspective and they’re like ‘well, that’s kind of cool.’”

In addition, Neild suggests having a trusted technology expert help set up a safe email address and implement security controls on your private network(s), like a firewall. This network should be used when handling family assets, instead of public networks or insecure Wi-Fi, and the design should include a machine accessible to authorized family members with unshared passwords. This network could include access to secure cloud-based applications, but it is how you access those applications that needs to be included in the design. While that may sound super secret and technical, the cost is ~~low~~ and is usually one day of work for a network engineer. The firewall should be monitored and tuned as needed. It is just as important as having security on your devices and access points.

Neild says it’s also essential to choose the right tech expert, and that the person designing the system should be evaluated the way one would a mechanic. “References, references, references,” she says. “You want someone to be focused and very rigorous when setting this up.”

While complexity often plays an important role, simply increasing the length of a password can also help ensure a family’s online safety, according to Deflin. “Length is everything,” he says. “Certain criminal software programs can sometimes crack an eight-character password in less than a day, while a 14-character password could take a year and a half to crack using the same software.” Though ideal, committing multiple 14-character passwords to memory is unrealistic, “so using a password manager is essential,” says Deflin.

Watch out for these scams

Even if you’ve protected your computer and network, some scammers or companies will try to trick you into giving them money. Watch out for these top six scams.[7]

Computer support scam:

Even on a protected computer, the scammer remotely inserts a popup from the user’s browser with an alarming warning that their computer is infected and under an immediate threat. The scammer asks for a payment to fix it, and/or authorization to “remote in” to the user’s device. The scammers are typically very aggressive, intimidating and bullying, playing on the individual’s fear and emotions.

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.

Fake news:

Scammers will impersonate legitimate news outlets or other websites in order to influence your opinions or gain access to information about you.

[7] The True Link Report on Elder Financial Abuse 2015, True Link Financial, January 2015.

Four big takeaways

Reduce your digital footprint~~:~~

There is less risk when you have less information online. In the same way seatbelts weren’t used and then they were, VPNs should be used. “It’s like a cloak of invisibility,” says Brad Deflin.

Find the “s”~~:~~

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 into a site without the s.

Use a two-factor password authorization

Two-factor password authorization is essential. Two deadbolts on a door are better than one, so layer digital protection as well.

Privatize communication~~:~~

It’s time to get off of public email. Any information you send via unprotected email clients is potentially vulnerable. Set up a family domain for each email user.

After a breach

Despite all the precautions you can take, cyber criminals still get around the cyber security that’s in place and breaches do occur, reiterates Neild.

This, too, is something for which every family should prepare. Victims of cyber theft, like burglary, often feel violated and don’t know what to do next. A good start is to follow the five things you should do if you think you’ve been hacked on page 1:

1 Disconnect your computer from the Internet.

2 Change passwords depending on the type of attack.

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

4 Contact a security expert.

5 File a report with the police.

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.

Cyber crime is a fact of modern life, and it’s only becoming worse. While the benefits of instant online access are many, so are the perils. However, with thorough preparation and a good understanding of the risks, everyone should be able to enjoy the benefits of the Internet today and look forward to a safe and secure tomorrow.

Bank of America Private Bank operates through Bank of America, N.A., and other subsidiaries of Bank of America Corporation. Bank of America, N.A. and Bank of America Private Bank Company of Delaware (collectively the “Bank”) do not serve in a fiduciary capacity with respect to all products or services. Fiduciary standards or fiduciary duties do not apply, for example, when the Bank is offering or providing credit solutions, banking, custody or brokerage products/services or referrals to other affiliates of the Bank.

Neither Bank of America Private Bank nor any of its affiliates or advisors provide legal, tax or accounting advice. You should consult your legal and/or tax advisors before making any financial decisions. Bank of America, N.A., Member FDIC.

To learn about Bank of America’s environmental goals and initiatives, go to bankofamerica.com/environment.
Leaf icon is a registered trademark of Bank of America Corporation.

BANK OF AMERICA

PRIVATE BANK