PRIVATE BANKING &
INVESTMENT GROUP

Viewpoint

Timely Insights from the Private Banking & Investment Group

Protecting Your Family in the Digital Age

As our lives become more and more digital, families face increasing threats of cybercrime. Here are some ways to avoid becoming a victim.

There's little doubt the next generation of today's families will grow up with open and continual access to technology. This generation, more than any before, will be "digital natives," meaning they won't have ever lived without applications (apps), email, the Internet, social networks and mobile devices.

The numbers are staggering: Estimates suggest an additional 1 billion people will have access to the Internet over the next five years, and they will be doing so almost exclusively via smartphones.[1] There's no question these devices provide convenience and play a growing role in our lives, but they also allow for increasing financial risks. Because people accustomed to constant online access may not fully understand these risks, never before has it been more important for everyone to protect their assets and identity from cybercrime and those who commit it.

Attacks can come from anywhere. For example, a family noticed, during a routine check of a credit report, someone had purchased over 100 gift cards—each worth $150—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. (See "Shop Smart," on page 6 for more.)

Think You've Been Hacked?

Do these **5 things** immediately.

Change all your passwords.

Disconnect your computer from the Internet.

Scan your computer for infected files or malicious programs.

Contact a security expert, and request that credit agencies put out a fraud alert.

File a police report.

[1] "Mobile Is Eating the World," by Benedict Evans, Partner of Tech, Mobile & Media at Andreessen Horowitz, 2015.

Merrill Lynch makes available products and services offered by Merrill Lynch, Pierce, Fenner & Smith Incorporated (MLPF&S) and other subsidiaries of Bank of America Corporation ("BofA Corp.").

The Private Banking and Investment Group is a division of MLPF&S that offers a broad array of personalized wealth management products and services. Both brokerage and investment advisory services (including financial planning) are offered by the Group's Private Wealth Advisors through MLPF&S. The nature and degree of advice and assistance provided, the fees charged, and client rights and Merrill Lynch's obligations will differ among these services. Investments involve risk, including the possible loss of principal investment.

The banking, credit and trust services sold by the Group's Private Wealth Advisors are offered by licensed banks and trust companies, including Bank of America, N.A., member FDIC, and other affiliated banks.

Investment products:

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

MLPF&S is a registered broker-dealer, a registered investment adviser, member SIPC and a wholly owned subsidiary of BofA Corp.

The family contacted Tania Neild, a cybersecurity 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 cybersecurity.

"We worked backward to find out what went wrong," says Neild. "Were they on a public Wi-Fi? Yes. Were they doing 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 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."

The ABCs of Cybersecurity

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.

Wi-Fi: Matters regarding assets should only be conducted on a trusted private Internet connection, never a public one. This means never when using mobile devices.

Social media: Avoid connecting with people you don't know on social networks. Social media can give away a family's whereabouts or allow a hacker inside their personal lives.

THINKING THROUGH VULNERABILITIES

While cybercrime has increased by 38% in 2016,[2] this doesn't mean families can't use email and social networks. Kids, especially, want to participate since so many of their friends are online.

Building Stronger Passwords

They open your accounts, so make sure they are unique, strong and complex.

There's more to building a password than keeping it a secret—for example, understanding the mathematics behind creating a password that is difficult to hack. Brad Deflin, founder and president of Total Digital Security, suggests three key elements to consider.

- **Length:** The primary driver to creating a password that is difficult to crack is length. So an eight-character password is far less effective than a 14-character one. Deflin notes a longer password—21 characters, for example—would take hundreds of years to crack, even at the rate of 1,000 guesses per second that today's hacking software is capable of.
- **Complexity:** One option is to create passwords by using the first letter of each word of a line from a favorite song. Another option, according to some experts, is interspersing passwords with numbers or special characters (e.g.,"@" or "&"). If you think the password is complicated, you're on the right path.
- **Randomness:** Because hackers feed password-cracking software with personal information to increase their odds of success, we can deduce the most effective passwords are long and random. Creating such a password can be approached by using random words to create a phrase that recalls a specific image easily drawn upon from memory. Remember the phrase should be a minimum of 14 characters in length.

Putting it all together

Start your thinking by using something longer 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. From there, you might add special characters and cases to further increase the password's complexity and strength.

[2] The Global State of Information Security® Survey, 2016.

Two is Better Than One

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

What. At it's 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 login into a particular website or online account.

Where. Using two-factor authentication is a good idea anywhere it's an available option, 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 hackers figured out your password, they would have to steal your phone in order to access your accounts," she says.

How. With cybersecurity 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 applications available for your smartphone, she says, noting LastPass and My Keeper as being particularly effective and easy to use.

A recent independent study found 24% of American teens are online "almost constantly" via smartphones and almost 75% of teens have smartphones.[3]

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." She begins with the basics:

1. **Access financial information** only via a private Internet connection—only with a mobile device if the site is secure.

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

3. **Avoid social media posts** with personal information that could take a hacker inside a family's home or divulge their whereabouts on vacation.

4. **Establish passwords**—the most common security breach—no one can guess or decode (see "Building Stronger Passwords," on page 2 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," on this page for more).

6. **Minimize the use of "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 AOL, Gmail or Yahoo whenever possible. These personal email services are the first places hackers go to access your information, Neild says.

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 cybercriminals to individual

[3] Amanda Lenhart, "Teens, Social Media & Technology Overview 2015," Pew Research Center, April 2015.

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."

RECOGNIZING THREATS

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

Some cybercriminals are outsiders, digging up information on a family via 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 cybercriminals is paramount to a family's security, as is taking precautions.

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

- **Cybercriminals:** They use the Internet with the intention of monetary gain. Their targets may include companies, individuals and their families. Criminals go after capital, but also target assets with monetary value, such as music accounts, gift certificates and frequent-flier miles.
- **Cyber spies:** A growing number of cybercriminals steal information—such as passwords to music accounts or store credit, instead of capital—and sell it on the black cybermarket, an increasingly popular underground economy similar in function to the traditional black market.

> Recognizing different kinds of cybercriminals is paramount to a family's security, as is taking precautions.

- **Cyber activists:** A group seeking access to networks in order to disrupt them for political reasons, activists will often use hijacked accounts to hide their own identity as they breach an organization's security systems. Neild points to a recent email attack that affected 150 million users, including some of her clients whose accounts contained financial information. It was a wake-up call for all parties. "Nothing was stolen, because that wasn't the goal," she says, "but the cyber activists brought the network to its knees."

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 Information Age," says Brad Deflin, founder and president of Total Digital Security. With the technology (and threats) constantly evolving, Deflin recommends four 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 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 security for your network, and you may want to have it set up by an expert. With today's threats, make sure you have your firewall activated even when you're offline.

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.

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 five scams.[4]

Obituary scam: After finding a widow on the Internet, scammers will pretend to be a collection agency calling about the recently deceased's debts.

Magazine subscription scam: Companies send a few issues out, and then call and attempt to confuse seniors by saying the final deadline for payment is due right away.

Sweepstakes scam: Scammers will email requesting a shipping-and-handling fee and stating it's all that lies between you and a grand prize, but in reality (and in the fine print) the prize is worthless.

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.

WHAT ARE SOME BEST PRACTICES?

As the threat of cybercrime grows, so does the need to protect family assets. How is this done? Some suggest working with a web master 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 cybersecurity, 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.

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. "There is a vanity element to it," he says. "When they see their last name in the domain it somehow creates a different perspective and the kids are like 'well, that's kind of cool.'"

In addition, Neild suggests having a trusted technology (tech) expert help set up secure email and build a private server—or firewall. This server should be used when handling family assets, instead of public servers or Wi-Fi devices. The server design should include a desktop accessible to authorized family members with unshared passwords. The desktop should not have wireless capabilities, and should be hardwired via ethernet to the server. The firewall should be checked and reinforced in regular monthly installments, or at least once every quarter.

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 hacking software 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."

AFTER A BREACH

Despite all the precautions you can take, hackers still get around the cybersecurity 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 remembering these three steps:

1. **Don't disturb** any evidence. As with any other crime scene, cybercrimes leave a trail. Don't disturb anything, and let the investigators take it from there.

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

2. **Contact** the place from which the property was stolen, be it a from a bank, credit card company or retail store with a shopping app.

3. **Alert** your family's financial and legal advisors.

> With thorough preparation and a good understanding of the online world, all members of families should be able to enjoy the benefits of the Internet.

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. Taking these three actions can help you get back on the path towards peace of mind.

Shop Smart

When buying on the web, keep your guard up with these simple tactics.

- **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.
- **Credit trumps debit:** Your credit card generally has more built-in protection than your debit card. Either way, remember to always check your statements against your purchases.
- **Avoid the unknown:** If a small website is offering a deal that's too good to be true, it might be. Stick with brand-name sites and familiar e-commerce sites when possible.

Cybercrime 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. But with thorough preparation and a good understanding of the online world, all members of families should be able to enjoy the benefits of the Internet today and look forward to a safe and secure tomorrow.

Merrill Lynch
Bank of America Corporation

PRIVATE BANKING &
INVESTMENT GROUP

The opinions, assumptions, estimates and views expressed are as of the date of this publication, are subject to change, and do not necessarily reflect the opinions and views of Bank of America Corporation or any of its affiliates. The information does not constitute advice for making any investment decision or its tax consequences and is not intended as a recommendation, offer or solicitation for the purchase or sale of any investment product or service. Before acting on the information provided, you should consider suitability for your circumstances and, if necessary, seek professional advice.