Wealth Planning **Update**

Best practices for your online safety

Tips to avoid scams and other online security threats.

The Internet has become a common feature of daily life, with nearly 90% of American adults saying they go online.[1] Unfortunately, anyone using the Internet can be the potential target of online scams and security threats. From email scams to malicious websites, it's more important than ever to protect your personal information and financial accounts online. Whether you're a baby boomer or younger adult, understanding the potential threats and taking some basic precautions can help keep your information safe and help you to make the most of your digital life.

Protecting yourself from email scams

Hackers and scam artists are usually after one thing: they want your personal information so they can steal your money or your identity. Personal information includes your bank or investment account numbers, credit card details, online passwords and other private data, such as your social security number. These threats may surface in your email, perhaps disguised as an offer to "click here" for a free prize or a vacation. It may appear that the emails were sent from a trusted place, such as the Social Security Administration, Medicare, the IRS, your bank or a charity. They may also threaten an action unless you reply quickly.

Don't be fooled. Websites or emails that ask for your personal information are typically not legitimate. Banks and other institutions will never request your personal information through email. Never enter your social security number, account number, date of birth or your mother's maiden name online unless you have verified that you are on a legitimate site that has a genuine need for that information.

It can be difficult to identify a malicious email or other online scams. Here are some tips that can help:

- **Read your emails carefully before you reply.** Typographical errors or phony-looking logos are a sure sign that the email is not trustworthy and likely does not come from a legitimate source.
- **Don't open an email if you don't recognize the person or organization that sent it** as it could contain a dangerous computer virus. Move the email directly to your trash folder or recycle bin without opening it.
- **Be wary of any offers that sound like they are too good to be true.**

Reducing your vulnerability to hackers

Hackers are people who use computers to gain unauthorized access to data. They've made national news headlines by attacking major institutions and stealing millions of people's credit card details, addresses, and other personal information. While large organizations are often the victims, even your personal computer is a potential target.

When your computer is not protected, hackers can wreak havoc in a number of ways. For example, they may install a keylogger to copy your usernames and passwords as you type them, then log in to your account later to transfer money out of your account and into theirs. They may also tap into your email and send malicious emails to all of your contacts in order to spread computer viruses and malware. In the worst case, hackers have accessed computers to deal in or hide the true origin of illegal activities.

Continued

You can limit the possibility that a hacker will gain access to your computer by safeguarding your system passwords, including both your modem and Wi-Fi passwords. Most people might only be familiar with their Wi-Fi password settings, but your modem security settings connect your computer to the Internet through your Internet Service Provider (ISP). It's a good idea to change these passwords periodically. Tip: You may need to contact your ISP to learn how to access and change your modem password.

Here are some other ways to protect your computer from hackers:

- **Never allow someone access to your computer remotely.** One exception might be your ISP if you've called them to fix a specific problem.
- **Keep your software up-to-date.** Operating system updates typically include the latest security features.
- **Use anti-virus software.** Although most operating systems have built-in security protection, such as a firewall, it's usually a good idea to supplement with anti-virus software that is specifically designed to detect and destroy computer viruses. Unix-based operating systems, such as those used by Apple, may be less vulnerable but determined hackers may still find new ways to exploit users.
- **Don't save your credit card details on your computer** for later use. It's worth the effort to enter them each time you make an online purchase.
- **Create strong passwords** with a combination of letters, numbers and special characters, and change them often.
- **Never store your passwords in a file on your computer** or in your browser unless you use a secure password management system that you trust.

Staying safe on websites

Many websites require you to enter sensitive information, including a username, password, account number or credit card details. With some diligence, you can minimize the risk that a hacker will uncover your data. Here are some tips:

- **Before you enter personal information on a website, be sure the URL begins with "https."** The "s" at the end stands for "secure" and means the data is encrypted and can't be seen by anyone but you.
- **Log out of your accounts before you leave a website or close your browser.** This ensures the account won't be visible to the next person who opens the browser.
- **Log in to your accounts only from your home,** where you know that your connection is safeguarded. Internet connections from public places such as coffee shops and airports may not be secure.
- **Use caution on social media.** Scam artists create fake profiles to entice you to follow links to malicious websites or to give up sensitive personal information.
- **Be careful on dating websites** where prowlers may try to gain your trust and then ask for a credit card number or money.
- **Beware of counterfeit drug scams** targeting people who search the web for better prices on medication.
- **Ignore pop-up windows that open automatically** when you're searching the web. They often simulate virus-scanning software and will try to fool you into either downloading a fake anti-virus program (at a substantial cost) or an actual virus that will expose whatever information is on your computer to hackers.

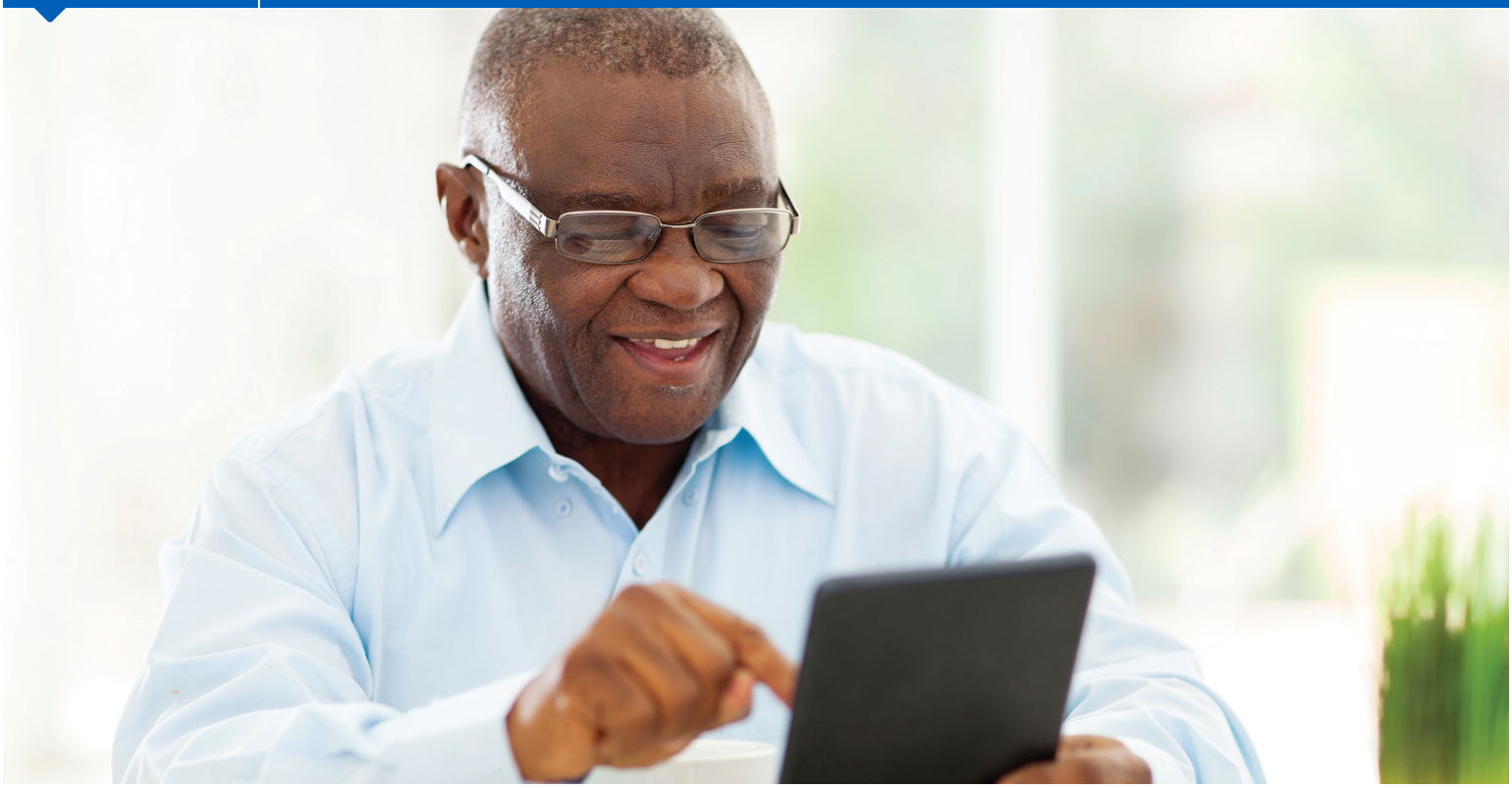
How data aggregation tools can help you monitor your financial accounts

Considering the various online threats, it's more important than ever to keep track of your accounts and be watchful of suspicious activity. This can be challenging if you have several bank, investment and credit card accounts. Data aggregation tools provide a way to view the transactions and balances in all of your accounts in a single, secure location. Using a dashboard-like interface, these tools provide a concise summary of your finances that you can access from your computer, smartphone or tablet.

Typically you cannot make a transaction from a data aggregation dashboard, so there is no risk of your money being accessed from these systems. Also, aggregators do not store your complete account numbers; they use truncated numbers, such as the last 4 digits. In addition, many data aggregation tools have alert features. For example, BMO Wealth Connection will notify you through email whenever a transaction in any of your accounts exceeds a dollar amount maximum that you have set.

At any age, it's important to understand online scams and threats, and to take precautions to protect your personal information and financial accounts. If you suspect you've been the victim of a scam or hack, don't be embarrassed. Tell someone you trust or seek help from your advisor or National Adult Protective Services (http://www.napsa-now.org/get-help/help-in-your-area/).

For more information about BMO Wealth Connection, please speak with your financial professional.



CASE STUDY »

Beware of bogus requests to wire money.

This past holiday season, Anna and others in her Florida retirement community received emails that appeared to be from a friend claiming to be stranded in India.

The message included instructions to wire money in order to help the person get back to America. Some of the residents, including Anna, were each duped into sending thousands of dollars to an unknown recipient.

Unfortunately, this type of scam is all too common. Many scam artists will try to convince you that they are a friend or relative in distress, a debt collector or government agency claiming you owe money, or a technology company trying to protect your computer from a virus. Make sure you take the time to verify the truthfulness of an email—perhaps by asking a relative—before sending money to anyone.

CASE STUDY »

Usernames can be just as important as passwords.

Michael used his first initial and last name as his username for his online bank account. He was unaware that hackers had figured out the username and were trying random combinations of characters to decode his password.

Every time the hackers entered an incorrect password three times, his account would be locked from online access. He would then need to reset his password in order to get back into it.

When he called the bank, he learned there had been numerous attempts to log in that he had not initiated. Michael immediately changed his username to something less obvious and also changed his password.

Stephen L. Williams, CFP®, CIMA® is Senior Vice President and Head of Financial Planning, U.S. at BMO Private Bank.

Steve oversees the strategic development and delivery of customized financial planning services to high net worth individuals and families throughout the United States. He earned an MBA in Finance from Kellstadt Graduate School of Business, DePaul University in Chicago, IL. Steve is a CERTIFIED FINANCIAL PLANNER™ and a Certified Investment Management Analyst℠ professional. He is also a Certified Retirement Counsellor.

Feel confident about your future

Stoker Ostler — its professionals, disciplined approach, and comprehensive advisory platform — can provide financial peace of mind. Call your Stoker Ostler Portfolio Manager today.

www.stokerostler.com

Stoker Ostler

BMO | A part of BMO Financial Group

[1] Tech Adoption Climbs Among Older Adults. Pew Research Center. May 17, 2017. Access online 1/26/18. http://www.pewinternet.org/2017/05/17/technology-use-among-seniors/