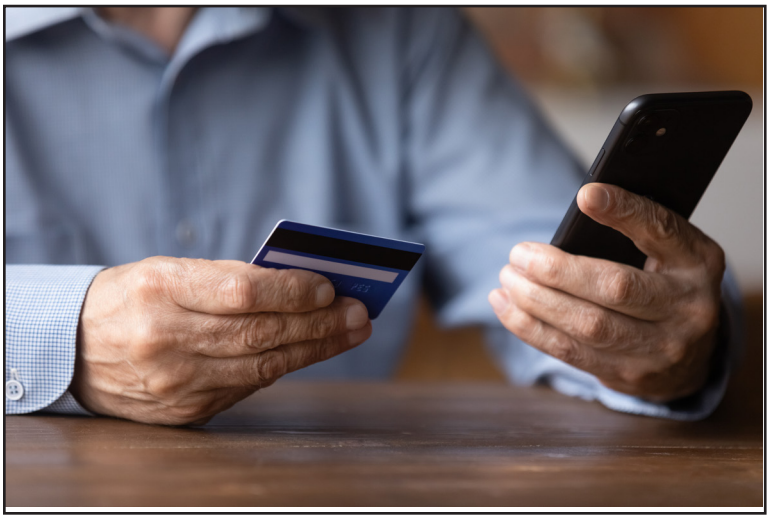
Are You an Informed Investor?

SENIORS' GUIDE TO STAYING SAFE ONLINE

May 2024



The stress of financial fraud can be life changing, especially for those in their retirement years. Losing money in an online investment fraud or financial scheme can severely affect your physical, mental and social health. To avoid online scams, it is important to keep on top of the web services, subscriptions, and passwords that you are using. This investor advisory explains how you can take a proactive role in staying more secure online.

Overwhelmed by your online presence? You're not alone

People of all ages are feeling exhausted and overwhelmed by the sheer amount of online services we use, so it's not a just a case of being older that may be making you feel like you can't keep up.

It seems like whenever we go online, a website or app is asking us for our email address, phone number, or both. Over the past few years, we've been increasingly asked to depend on online services for almost everything we do. To access these web-based services, people generally need to sign up by creating an online profile through an app or website, or they use an existing web or social media account to sign in, creating a digital footprint that is ever expanding. With convenience comes risk. The more services and subscriptions you use, the greater your chances of being hacked and scammed.

Benefits of Streamlining Your Online Presence

It's a good idea to take a yearly review of the online services you use, and to eliminate any that you don't need. There are many reasons for streamlining your online life. Benefits to consider:

- A clearer, less cluttered picture of your digital footprint;
- More control and less risk, because you will have a comprehensive, up-to-date knowledge of the services you are using;
- More likely to recognize a scam if you receive information related to a service or app you have deleted already;
- Eliminating unnecessary subscriptions, newsletters, and accounts means less risk of your personal or financial information being hacked and shared online; and
- Easier for family members to assist you with managing your affairs if you need help.

How to manage your online services

Start by setting time aside to do an in-depth review of the online services that you are using, including your home internet and Wi-Fi services. If you need help, ask a friend or family member to work with you so that you have a comprehensive list in the end. If you have a spouse or partner, it's a good idea to get them involved in the process too.

Collect information from your home computer, phone, tablet and any other connected device. Here are some suggestions of things to look for:

- List all of the online financial service apps or websites that you use for investing, financial transactions, banking, and insurance;
- Check your connected devices and browsers for apps and bookmarked websites that require sign-ins using login information such as a username and password;
- Write down all of the websites, online vendors, and apps you think you used in the past year;
- Check your email for newsletters and notifications that you signed up for; and,
- Confirm that your email address has not been compromised in known data breaches

  (there are services such as https://haveibeenpwned.com that allow you to search known data breaches to determine whether your information may be at risk).

Continued

How to declutter your online services and accounts

Now that you have a list, it may look too daunting to tackle. Don't despair. You'll feel much better once you've simplified things. Give yourself a deadline to complete this task.

Approach decluttering your online life the way you would clean a spare room, garage, or shed. Ask yourself these questions:

- Do I use this app or website often, or at all?
- Do I know what this app or website does?
- Does this app or website make my life better or more convenient?
- Is this online service useful or informative to me?
- Do I read this email newsletter or subscription?

If the answer to most or all of these questions is a "no," consider unsubscribing from the service, closing your account, and deleting the app from your device. If you need help, contact the service directly, making certain that you are interacting directly with the company or website. If you are uncertain or wary about the website or app, ask for help from a trusted friend or family member.

How to secure the services and devices you use

If you use the same (or similar) passwords for different services, there's an increased probability that a hacker can find a way into one or more of your accounts. Once you've decided on the services you want to keep, take steps to secure them:

- Verify your password reset processes for financial services sites (banking, investing, pay services, etc.);
- Be cautious when using biometric recognition or automated sign-in features, especially for financial services sites;
- Sign into your financial services websites directly, and avoid storing your password in a browser on your phone or computer;
- Don't use the same password for more than one site and follow the guidelines from the service provider to create a strong password;
- Use two-factor authentication for accounts that permit it;
- Ensure that your connected devices are password protected or secured by a lock screen and their operating systems are routinely updated; and
- Store your essential passwords (email, banking, payment services, etc.) securely and update them regularly.

Stay informed and be careful online

Now that you've simplified and streamlined your online life, be cautious about signing up for new services, promotions, or downloading new apps. Before you do, think about how much you will use them, and if they will improve your life. If not, avoid using them to keep things simple and safe.

Here are some other things to consider going forward:

- Restrict the personal information you put online – hackers may be able to use personal information to guess a password or spoof your identity;
- Keep a running record of websites you are visiting that store your personal financial information and store the record securely;
- Be wary of public Wi-Fi connections – hackers set up public Wi-Fi spots and use them to steal data
- Be careful of what you open and look at online – cyber-attacks are often triggered by people who click on a malicious link in their email or on a website;
- Lock your devices before putting them down or walking away – leaving your device open may allow someone to access your accounts and apps;
- Follow the news for data breaches – check the news for data breaches or hacks;
- Consider signing up for a credit monitoring service – some financial service providers will offer this service for free; and,
- Act quickly on data breaches – if a website, service, or app you use has been hacked immediately change your password or delete the account.

The bottom line

Remember, you are the first line of defense in protecting your personal information online. Staying on top of the websites and apps you use can help protect you from financial fraud. Investing online is easier than ever which, while convenient for you, also provides fraudsters with opportunities to access your information and accounts. Taking the simple steps outlined above can reduce your risk of experiencing a loss to an online scam. Apps and websites that provide investing services generally must be registered with state or provincial securities regulators. Contact your state or provincial securities regulator for help. These agencies can provide information about whether the app or website is registered to buy or sell securities or offer investment advice, and whether they have any regulatory actions or other disciplinary events in their past.

To learn more, contact the Department of Financial Institutions

500 Mero St., 2SW19, Frankfort, KY 40601 | (800) 223-2579 | KFI.ky.gov

TEAM KENTUCKY
PUBLIC PROTECTION CABINET
Department of Financial Institutions