NORTH Dakota | Securities
Be Legendary.

Investor Advisory: Seniors' Guide to Staying Safe Online

The stress of financial fraud can be life altering, 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 track of the internet services, subscriptions, and passwords 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 they use. 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. Accessing these web-based services usually requires signing up or creating an online profile through an app or website, or using an existing internet 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 or scammed.

Benefits of streamlining your online presence

It's a good idea to make a yearly review of the online services you use, and to eliminate any that you don't need. Benefits to consider are:

- A clearer, less cluttered picture of your digital footprint;
- More control and less risk by having comprehensive, up-to-date knowledge of the services you are using;
- Ability to recognize a scam if you receive information related to a service or app you have discontinued already;
- Eliminating unnecessary subscriptions, newsletters, and accounts means less risk of your personal financial information being hacked and shared online; and
- Family members can more easily 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 you use, including your home internet and Wi-Fi services. If you need help, ask a trusted friend or family member.

Collect information from your home computer, phone, tablet, and any other connected device:

- List all 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 usernames and passwords.
- Write down all 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.
- Confirm that your email address has not been compromised in any known data breaches.

How to declutter your online services and accounts

Approach decluttering your online life the way you would clean a spare room, garage or shed. Give yourself a deadline, and ask 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 is “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 sure you are interacting directly with the company or website. If you are uncertain or wary about the site 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, payment services, etc.)

- Be cautious when using biometric recognition or automated sign-in features, especially for financial services sites.
- Sign in to 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.
- Store your essential passwords 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. Going forward:

- Restrict the personal information you put online. Hackers may be able to use personal information to guess a password or steal 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 WiFi connections. Hackers set up public WiFi spots and use them to steal data. If using public WiFi, consider using a personal VPN (virtual private network) to keep your data safe.
- Be careful of what you open and look at online. Cyber attacks are often triggered by clicking on a malicious link in an 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.
- Consider signing up for a credit monitoring service. Some financial service providers will offer this for free.
- 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 and taking the simple steps outlined above can help protect you from fraud.

Contact the North Dakota Securities Department

Phone: 701-328-2910

Email: ndsecurities@nd.gov

Website: www.securities.nd.gov