OLD NATIONAL® INVESTMENTS

PRIVATE WEALTH MANAGEMENT

5 Ways to Protect Yourself—and Your Assets—Online

The rise of everything digital has created a lot of opportunity and convenience. But it's also come with the increased risk of cybercrime, which is criminal activity that involves a digital device or computer. In fact, 47% of Americans have had their personal information exposed to cybercriminals, according to the Federal Cybersecurity & Infrastructure Security Agency.

Individuals are often easier to attack than a business because they don't have the IT security in place to thwart suspicious activity. What's more, you may have an online presence, such as a Facebook or Twitter account, that makes it easier for criminals to learn more about your activities and whereabouts and use that information against you.

So how can you reduce the risk of cybercrime and protect your assets and reputation? Here are five important actions that help limit your digital danger.

1 Keep your software, apps, and devices updated.

The companies providing most of the software and mobile devices you use for business and life likely have cybersecurity teams monitoring their solutions for trouble and creating patches that fix problems or vulnerabilities. Updating your software, apps, devices, and online browsers such as Google or Safari ensures that you benefit from any new security improvements. Also, most experts agree that anti-virus software is now optional because most of these updates provide that security.

If remembering to update your digital solutions is a challenge, don't worry. You can make the updating process easier by turning on automatic updates for your phone and other mobile devices. Regular updates give you access to the latest and greatest features of your devices and apps. But more importantly, they are key to protecting yourself from large-scale breaches, the ones that impact thousands or even millions of accounts at a time. Stay on top of your updates, and you'll reduce your risk considerably.

2 Use a password manager.

The average person has more than 100 passwords to various online accounts. Not only is it hard to remember this many passwords, but it's likely that many of them are the same. That means that a breach of one company could give criminals access to multiple accounts.

A password manager solves this problem. This tool creates unique passwords for all of your online accounts and stores them in a secure spot. You can then access your accounts with one login and one password via the password manager. These tools also make it easy to change passwords and create complex passwords for accounts that are unrelated to your personal information (no more birthdays or pet names required).

3 Utilize additional security layers.

In addition to passwords, there are other security steps you can take to ensure that only you have access to your important accounts and financial information. For example, you may want to take advantage of two-factor authentication, which requires you to login to your account with your password and then provide an additional piece of identifying information—usually a text-message security code.

You might also consider using facial recognition or other biometrics such as a fingerprint to access your devices. That way, if someone steals your phone or laptop, they can't log on and get into your banking or other accounts. Multi-factor authentication makes it much more difficult for a fraudster to impersonate you or get into your account than with a password alone.

4 Watch the Wifi.

Try to avoid public Wifi networks—they're more apt to be unsecured and create opportunities for criminals to intercept and steal your information or gain access to your accounts. This is where a virtual private network (VPN) can come in handy. A VPN encrypts data moving between a router and your devices, hiding your identity and any other personal information from anyone in the area trying to steal it. Using one while in public ensures that criminals can't access your sensitive information and use it for their own purposes.

However, while VPNs are helpful, the best idea is to avoid accessing your financial accounts in public. Conduct your financial activity in secure spaces such as your home or office to prevent your information from getting into the wrong hands.

5 Limit your social media sharing.

This is especially important for individuals and family members who want to reduce their chances of being targeted. Criminals can use the information you share on social media to impersonate you or create convincing phishing campaigns targeting your interests. For example, if you post a lot of information about your children and where they go to school on Facebook, someone could pretend to be from the school and send a fraudulent email asking for money.

If you do share on social media, consider posting information about your location and activities after the fact. This way, criminal don't know your real-time location or the details of where you're going or what you're doing. You might post your vacation pics to Facebook after you get home or photos from a restaurant meal a few days later. In addition, keep personal details to a minimum and create a private account to control who is following you.

Having a digital life does come with the threat of cybercrime. But by following the tips above, you can greatly reduce your risk of becoming a victim.

First Name Last Name

Address
Phone Number
1834.com

2329657-0823-125 | 472229