CS
CYBER SECURITY & YOU
NOVEMBER 2022
LASERS

PROTECT WHAT YOU'VE EARNED:
7 Ways to Safeguard Your Financial Investments

The pandemic created economic disruption around the globe and served as a catalyst to amplify cyberattacks, compounding the issue of protecting wealth. Not only do investors need to find ways to avoid losing hard-won gains in a tough economy, they also need to protect their wealth from actual theft and fraud.

If you are worried about cybercrime, here is a quick reminder of some ways you can safeguard your financial investments:

1 Start with a willing mindset and acknowledge the value of cybersecurity. Commit to protecting your investments by staking real time, effort, and resources in a positive effort to protect your cash (and your peace of mind).

2 Vet your tools carefully because they can make or break your safety measures. Whenever you consider using a new financial tool to manage your wealth, start by asking the following questions:

- Is it well-established?
- Are the tool's purpose and benefit clear?
- What do others think of the tool?
- What affiliations does the tool have with reliable name-brand security solutions?

Building an arsenal of security tools is a foundational element to protecting your wealth. Make sure to select each item with care.

3 Choose good passwords and make them long and complex. When shopping for a password manager, vet each tool carefully when making your choice.

4 Embrace multi-factor authentication. Security measures, like a strong password, are a great single wall of protection. However, if you want to exponentially increase the effectiveness of your digital security, you want to add multi-factor authentication to the mix whenever possible.

5 Consider encryption. There are different ways you can do this, such as:

- Encrypting specific files within your computer or device;
- Encrypting whole devices so that everything on them is secure;
- Extending encryption to your home network (and, consequentially all of your online activity) through a VPN.

It can take a bit of work to set up proper levels of encryption. But the peace of mind that it creates is well worth the effort.

6 Familiarize yourself with phishing by becoming comfortable with identifying when an email or text message is trying to capture your personal information or gain access to sensitive data. There are a few obvious giveaways to look for when vetting a message to see if it's a phishing attempt.

- Does it have a link or attachment? Never click on links or attachments from any message unless you are absolutely certain you have verified the sender and the contents.
- Does it promise something odd? Research anything that seems to be unusually threatening or too good to be true.
- Does it come from an unrecognizable address? For example, if an email from "Shopify" comes from a sender whose address is "xdwwwfhen@trex.com," that's a good sign it's a fraud.
- Is it professionally written? Any business communication should be cleanly and legibly written with few grammatical mistakes.

Familiarizing yourself with phishing attacks is a great way to make sure you're doing your part to avoid putting your investments at risk.

7 Practice digital hygiene. Guarding against phishing is a good start, but ideally, you should practice good digital hygiene on every level. This includes:

- Updating your devices as soon as patches and updates become available;
- Avoiding public WiFi when accessing sensitive data;
- Using passwords, multi-factor authentication, encryption, and other recommendations on this list;
- Always being careful when giving out your personal information; and
- Creating an account to access your investments before someone else does. It is easier to compromise your account if you have not taken the time to set it up yourself. ■

Credit to: Deanna Ritchie, November 1, 2022
Much of this information originally appeared on *Due.com.*