MCM | WEALTH
COMPREHENSIVE
WEALTH MANAGEMENT

25 YEARS

Cybersecurity: Are You Protecting Your Technology—and Yourself?

Key Takeaways:

- Multifactor authentication is a critical but underused tool to protect against bad guys.
- Phishing attempts have gotten very sophisticated and require a discerning eye.
- Businesses need recovery plans for their data in the event of a cybercrime.

We're more connected by technology today than ever. Ubiquitous laptops, tablets and smartphones mean we're always online. And increasingly, we spend that time dealing with critical communication and troves of sensitive data about our lives, businesses and finances.

All those devices and data have greatly expanded what cybersecurity experts call "attack surface" — touch points where cyber-criminals can try to enter and affect or extract data from. In other words, the bad guys have a whole lot more opportunities to harm you online. Worse, they're getting better and better at what they do, honing and innovating their techniques.

The good news: Fighting back can be easier than you may think. So says Lisa Plaggemier, executive director of the National Cybersecurity Alliance, which promotes awareness of smart and safe tech usage. She offered a helpful primer on crucial cyber hygiene for individuals, families and businesses.

HARDENING YOUR HARDWARE

Start with the laptops, tablets and smartphones themselves. Securing hardware generally comes down to a few very simple but vital moves. For example:

- **Lock your devices.** Use a passcode, PIN or facial recognition tool to prevent unwanted users from accessing your technology. Yes, it slows you down. But it also prevents catastrophes like one Plaggemier cites: An organized crime gang in Austin, Texas, was stealing people's phones at nightclubs and bars. Many of the phones were permanently logged into Venmo accounts, which are linked to bank accounts. The criminals were able to quickly drain people's checking accounts using Venmo via the unlocked phones.
- **Cover your camera.** It's easier than you might want to believe for a bad actor to hack and gain remote access to your laptop camera and spy on you. A pack of slidable laptop webcam covers will cost you only a few dollars.

MULTIFACTOR AUTHENTICATION, A NEW MUST-HAVE

By now, we should all be familiar with the need for "table stakes" cyber protection such as antivirus software and complex passwords. Add to that list the latest must-have for safeguarding our data: multifactor authentication.

You may have used MFA without even realizing it. For instance, when a web site texts your phone with a numeric code to enter online, even after you've typed your password on the computer, it's MFA. It works because even if one credential becomes compromised, unauthorized users should be unable to meet the second authentication requirement. It's a simple approach, says Plaggemier, but one whose effectiveness cannot be overstated.

The problem: Not nearly enough of us are enabling MFA on accounts where it's configurable. For consumers, MFA should be deployed on any software or web programs dealing with anything financial—but really, it should be in place for all accounts. For business organizations, it already should be *de rigueur*, deployed long ago.

Multifactor authentication is one thing you can do to protect yourself against most cybercrimes.

"One of the big tech companies came out last year and said they haven't had a single credential-based account compromise since they enforced it on their user base," explains Plaggemier. "When you think of just one thing you can do that can make a massive dent in global cybercrime, it's multifactor authentication."

PHISHING VARIANTS EMERGE

You're likely familiar with the online criminal activity known as phishing, when cyber thieves create phony (but legitimate-looking) web sites, emails and texts designed to compromise the data or identity of an unsuspecting user with a single trusting click.

Unfortunately, cybercriminals have gotten extraordinarily good at phishing. That fact, coupled with the seemingly endless increase in the number of emails and texts we get every day, requires us to redouble our efforts to stay secure.

Boost your awareness by understanding the variants of phishing that have emerged in recent years. For example, there's "vishing"—a social engineering scheme that entices victims to call a number and divulge sensitive information—as well as "smishing," delivered via SMS text messages. Add to that list "phushing," which takes advantage of the trend toward MFA by disguising malware or other exploits as unsolicited push notifications to unsuspecting users' smartphones.

Plaggemier's newest tips to help sniff out phishing attempts include the following:

- Read the sender address of an email very closely. Is it spelled correctly? Is it formatted accurately?

- Hover over any link in an email to see whether it will clearly send you to a legitimate web site. If you're unsure, navigate to the web site by entering the URL in your browser rather than clicking. Once there, see if you can find the content that the email is promoting.

- Be extremely careful with attachments that accompany a message. In particular, steer clear of file extensions such as ISO, which denotes files that can copy everything on your drive, or EXE, which denotes executables that can install malware (more on that later).

Important: Even legitimate files like word processing documents can contain macros—programmable shortcuts to automate certain tasks—that are hiding malware in email attachments. Plaggemier says to consider disabling macros in your Microsoft Office software. Also turn off auto-forwarding in your email so bad actors can't use macros to set up rules that enable them to send their scams to all your contacts (or all the contacts of your entire staff, if you own a business).

When it comes to recognizing phishing attempts, says Plaggemier, it's all about making sure the sender is really who you think it is and keeping a keen eye out for any changes in the regular process you're used to that don't pass the smell test. Example: A phishing scam might send out emails saying an account or routing number has been changed or that a new type of document is now being used for contracts. If that occurs, says Plaggemier, pick up the phone and call to make sure.

RANSOMWARE RUNNING RAMPANT

The global scourge of ransomware mainly targets (at the moment, at least) large businesses and organizations such as hospitals and health systems—big players that cybercriminals and state-sponsored bad actors assume are most willing to take the gambit of paying large sums in hopes of decrypting their seized data.

That said, owners of small and midsize companies should not presume they're immune to the exploits of these groups. Plaggemier's advice here:

1. Have all of your kids' baby photos and all other files that are important to you backed up to a cloud service that's safe from ransomware attack.

2. Don't pay the ransom, as it helps perpetuate more cybercrime. There's also no guarantee that you will get access to your data back again. The FBI and DHS echo this advice.

3. Instead, contact law enforcement—up to and including your local FBI field office.

> The feds have gotten a lot of practice dealing with these exploits in recent years. The bureau's Internet Crime Complaint Center, or IC3, is an important resource.

If you're a small to midsize business, you may be less likely to be targeted—but a lower probability doesn't mean zero possibility. Plaggemier suggests such business owners work with the Cybersecurity and Infrastructure Security Agency, a federal agency that has recently prioritized helping small and midsize businesses prevent and, when necessary, recover from cyberattacks. (See the sidebar for more tips for entrepreneurs.)

Of course, prevention starts with each of us. Ransomware is often delivered via a phishing email or a link in a message that is malicious. The advice above therefore can help you and your staff avoid getting scammed *and* having your data held hostage.

> If you don't use a manager tool, it's very likely that you're simply recycling a single password and using it across multiple accounts.

CYBER INSURANCE—A GOOD POLICY?

One hedge against potentially damaging cyberattacks would be to get cyber insurance. Such policies were first offered about two decades ago—which is essentially an eternity ago considering how technology has evolved and how significantly cyberthreats have intensified.

These days, with ransomware attacks on business a near-daily routine, and bad guys regularly seeking ransoms in the multimillions, the severity and cost of such attacks have risen significantly.

In turn, the relatively small pool of insurers offering cyber policies have raised their premiums significantly. According to a report by The National Association of Insurance Commissioners, the cost of policies offered by the biggest carriers increased by 92 percent year over year in 2021.

What's more, these companies are also becoming much more stringent about whom they'll insure and what they require from policyholders. Even if you decide to purchase cyber insurance, you can count on being expected to have a robust risk mitigation strategy and to dot every "i" and cross every "t" when it comes to cyber hygiene (such as patching, updates and access management).

WHAT'S THE PASSWORD?

The good news is that fewer and fewer people these days protect their data using flimsy passwords like "1234567" or "password."

But Plaggemier remains surprised by how few people and businesses still don't use password managers, which enable users to have unique passwords for each account that differ greatly from one another. It's likely that people are afraid to have all their passwords stored in one location—worrying that if someone breaks into their password manager, the thief will have access to everything.

The reality: If you don't use a manager tool, it's very likely that you're simply recycling a single password and using it across multiple accounts. That's far riskier than the chance that your password manager is going to be compromised, according to Plaggemier.

Similarly, to safeguard your home Wi-Fi network, the best move is to simply change the default password on your router (it's usually something like "admin") to one that's complex and unique. Keep the software updated and install any security patches that come out, and you'll greatly reduce the chance of unwanted visitors using your network or viewing your home and family through your smart security camera system.

CONCLUSION

Ultimately, there's no perfect guarantee that your cybersecurity efforts will thwart each and every online criminal. But given the risks to your wealth, your family, your business and your peace of mind that cybercrimes present, ignoring the issue is simply not an option. Get the basics in place, implement the more advanced solutions and be ready to stay on top of developments in this fast-moving area that impacts all of us.

MCM | WEALTH COMPREHENSIVE WEALTH MANAGEMENT 25 YEARS

P

We Are *The* Portfolio Second-Opinion Experts

- We learn about you first
- We build custom portfolios objectively
- We engage specialists for advanced needs

Contact our CEO and founder, Geoff Hakim, to experience our portfolio second-opinion process with no obligation

Click here for details

This report is intended to be used for educational purposes only and does not constitute a solicitation to purchase any security or advisory services. Past performance is no guarantee of future results. An investment in any security involves significant risks and any investment may lose value. Refer to all risk disclosures related to each security product carefully before investing. Securities offered through Marin Capital Management, LLC is not affiliated with AES Nation, LLC. AES Nation, LLC is the creator and publisher of this content.