The New Rules of Cybersecurity

Ten tips for staying ahead of increasingly sophisticated scams.

ILLUSTRATION BY AHRA KWON

Cyber fraud may be as old as the internet itself, but it's also a growth industry. In 2020, the FBI recorded 792,000 cybercrime complaints in the U.S. alone—a 69% increase over 2019. Losses from those frauds totaled $4.2 billion.

"The pandemic has given bad actors *a lot* of new opportunities," says Peter Campbell, a managing director in Schwab's Financial Crimes Risk Management division. "More of our lives are being conducted online than ever before, without our having thought through the security implications of that change."

While the best practices for keeping your accounts safe are ever evolving, they boil down to common sense and a healthy dose of suspicion when living and working online. With that in mind, here are 10 tips for keeping cyber criminals at bay.

1. Think before you click

More than 3 billion emails pretending to be from individuals or entities that recipients know and trust are sent every day, according to the cybersecurity firm Valimail. One wrong click could drain a financial account, expose you to identify theft, or install malware on your device.

"These so-called phishing scams successfully trick too many people into revealing highly sensitive information, including credit card information and passwords," says Joel Sauer, director of senior and vulnerable investor investigations in Schwab's Financial Crimes Risk Management division. "If you get an email you're not expecting, don't click on any links or accept any offers."

Rather, confirm the legitimacy of the source, says Victoria Thomas, senior manager of cybersecurity awareness and IT risk culture at Schwab:

- Double-check the email address, which can differ by just a single character from an account you know.
- Hover your cursor over any links—without clicking—which will reveal the underlying URL (that may or may not jibe with the one it's purporting to be).
- Activate your email program's spam filters, which have become adept at separating out suspicious and unsolicited emails.
- "Above all, call the company back at a known or publicly listed number rather than risk responding directly to a fraudster," Joel says.

Beyond email, be aware of other forms of attack—including fraudulent SMS texts (a.k.a. "smishing"), voice calls ("vishing"), and "spear phishing," or the practice of mining social media posts for personal information to create more targeted and potentially convincing emails.

- If you suspect an email that appears to be from Schwab is a phishing email, forward it to **phishing@schwab.com**.

2. Step up your security

Financial firms, in particular, have implemented security features aimed at preventing cybercrime. Chief among them:

- **Security alerts** via email or text that can notify you of everything from individual transactions to changes to your password and other vital information.
- **Two-factor authentication**, which typically involves sending a randomly generated number to your phone or email, which you must enter before you can access the account. "That extra step alone can be critical to preventing unauthorized access to your accounts," Peter says.

- Sign up for security alerts and two-factor authentication for your Schwab accounts at **schwab.com/securitycenter**.

- **Voice identification**, which allows you to access your account securely by speaking a simple phrase—such as, "At Schwab my voice is my password."

- Enroll in Schwab's voice ID service by calling **800-435-4000**.

3. Be password smart

"The first rule of passwords is: Never share passwords," says Joel. And while most people know not to use simple passwords like "1234" or their birthday, consider creating strong, hard-to-guess passwords that don't use personal information. Password managers can create, store, and even autofill unique passwords for as many sites as you choose. Whether you opt for a password manager or not, be sure to password-protect your laptop, phone, and tablet, as well. "These days, there is no greater repository of personal information than our devices," Joel says.

4. Keep your devices up to date

Most desktop and mobile operating systems—as well as individual applications—offer periodic updates, which frequently include security patches as new vulnerabilities are discovered.

"You can typically sign up to install these updates automatically through the application's or operating system's settings," Victoria says. Failing to do so can be costly—as up to 143 million customers of one credit reporting agency learned the hard way in 2017 when their Social Security numbers, birthdates, and home addresses were exposed though a security hole for which a software patch had been issued months earlier.

And finally, when it comes time to discard old gear, don't forget to restore the device to factory settings in order to securely remove all personal data.

5. Fortify your home network

Don't overlook the internet connection that powers your home. Newer routers—devices that stream data from your internet provider to your various devices—tend to have stronger encryption settings and offer automatic updates, which manufacturers may discontinue for older models. Your router, too, should be secured with a strong password—as should internet-enabled doorbells, speakers, thermostats, and other smart devices, whose default passwords are often as simple as "password."

6. Protect yourself in public

Cyber criminals can easily set up a decoy Wi-Fi network containing the name of the airport, hotel, or restaurant from which you're trying to connect. "Instead, tether your laptop or tablet to a 'personal hotspot'—a feature of many smartphones," Victoria says. "That's one sure way to avoid falling victim to fraudsters when accessing the internet in public." In a pinch, you can safely use public Wi-Fi for innocuous tasks like checking sports scores—but avoid logging in to financial, shopping, and other sensitive accounts.

7. Talk with your children ...

While most children grow up with the internet, they may not be aware of its potential pitfalls or their own vulnerabilities to them. Start early—and be frank about the risks involved and your own experiences online.

"I have two teenagers and I'm constantly preaching the gospel of online safety," Peter says—including not giving anyone your name, the name of your school, or your home address, and never agreeing to meet anyone in person who you've only ever met online. "They're as susceptible as anyone else, if not more so," Peter says.

8. ... and elderly relatives, too

Cognitive decline and social isolation, in particular, can leave the elderly susceptible to scams. "Many people were more isolated during the pandemic than ever before," Joel says. "As a result, they were that much more vulnerable to scammers trying to form an emotional attachment over the phone or online."

Joel recommends framing conversations about cyber fraud in ways that don't question a loved one's judgment. "Talk about the steps *you* take, not the steps *they* should take," he says. Above all, offer a helping hand. "Everyone needs a family member, a friend, or even a trusted financial advisor they can call with questions," he says.

What's more, most financial institutions encourage all clients to establish a "trusted contact"—someone with whom your financial institution can discuss any signs of financial exploitation. "Even if you have a spouse listed on the account, a trusted contact can provide an additional person to contact in case of suspicious activity," Joel says.

- Add or change a trusted contact for your Schwab accounts at **schwab.com/trustedcontact**.

Fighting back

What to do if you're a victim of cybercrime.

- "Lock down the threat by reporting suspicious activity to all your financial institutions," Victoria says—including banks, brokerages, credit card companies, and the Social Security Administration if you suspect your Social Security number has been compromised.
- To report suspicious activity in your Schwab account, call **800-435-4000**.
- Change the password on all compromised accounts—and any accounts that share those passwords.
- Report the crime to your local police, whose report may be helpful in recouping any losses, as well as to the FBI's Internet Crime Complaint Center (ic3.gov/Home/FileComplaint).
- Request fraud alerts—as well as a credit freeze to prevent further fraud—from all three credit reporting agencies.
- Remain vigilant by reviewing account statements, scanning your devices for malware, and monitoring your credit reports, possibly with the help of a credit-monitoring service, which can help detect instances of identity theft.

9. Stay informed

Sign up for the latest consumer-fraud alerts from the Federal Trade Commission at consumer.ftc.gov/features/scam-alerts. "It's also a good idea to check your credit report for suspicious activity at least annually," Peter says. You are entitled to a free annual credit report from each of the three credit reporting agencies—Equifax, Experian, and TransUnion—with whom you can dispute any errors or unauthorized activity.

You might also consider instituting a "credit freeze" for you and your family members with each of the three agencies, which can prevent new accounts that require a credit check from being opened in your name without your express permission (learn more at consumer.ftc.gov/articles/0497-credit-freeze-faqs).

10. Follow your instincts

"If an offer seems too good to be true, it probably is," Peter says. And no reputable company will reach out electronically to request sensitive personal information, so that's another red flag.

"To my mind, you have to do all you can to prevent fraud—but you also have to be ready to mitigate the consequences," Joel adds (see "Fighting back," left). "The key is to remain vigilant so all this wonderful new access and technology isn't used against you." ■

See page 42 for important information. (0821-13SF)