Hacks for Outwitting Hackers and Avoiding Scams

Kirkland was skeptical and pressed him on his role, but Davis responded credibly and knew a lot about her relationship with the bank. He told her the fastest way to stop the unauthorized transaction was to give him access to her computer, which she reluctantly allowed.

Davis then wired $15,000 from Kirkland's bank account to an individual in the United Arab Emirates via a wire transfer set up in her name. By the time Kirkland's nagging doubts got the better of her, it was too late. The money was gone.

Fraud on the Rise

Cybercrime is how most money is stolen these days. "It's a $10.5 trillion global industry that's larger than the sale of all illegal drugs worldwide, combined," says Mark Hurley, founder and chief executive officer of Digital Privacy and Protection (DPP). "It's far easier to steal money with a computer than with a gun, and it's far harder to catch the bad guys."

Hurley, a serial entrepreneur in the financial services industry, saw a business opportunity in helping the clients of wealth managers guard their assets. He founded DPP in 2020.

According to a 2023 Gallup poll, 15 percent of U.S. adults said at least one member of their household had been the victim of a scam in the last year.

Karen Denise, head of wealth client service at CAPTRUST, says the Gallup data matches what she sees among clients. "Unfortunately, we're hearing from more and more people that they have responded to a fraudster who appeared to be contacting them from a legitimate financial institution,"

she says. “We work with them to try to recover their funds, but that can take time, and it’s very stressful.”

These sophisticated cybercriminals constantly innovate new tactics, making it difficult to stay ahead of them. To make matters worse, many such criminals work from outside the U.S., often placing them out of the reach of law enforcement. In the event they’re identified, they’re rarely prosecuted.

You’ve Been Hacked

According to Hurley, one of the most common tricks in recent months has been the “your account has been hacked” call.

Cybercriminals have become much more aggressive lately. In the past, they relied on text messages or emails to bait victims. Increasingly, they pose as company representatives and cold call their potential victims, ostensibly to help them address a hacked account.

“They’ll tell victims that their account has been breached and that they need to take certain steps to protect themselves,” says Hurley. “Typically, they’ll ask for specific personal information and direct the victim to open one of their apps and insert a code.”

Once the code is entered, the criminals can access the victim’s device and online accounts. They can move money or send a wire to themselves, as in Kirkland’s case. In one variation on this scam, the criminal convinces the victim to move the money themselves to protect the funds.

Losing money is bad, but that’s not always the extent of the issue. “When an investment or retirement account is involved, the damage can be compounded with taxes and tax penalties,” says Denise.

Someone’s Been Kidnapped

Another common fraud is the fake kidnapping scam, which seems even more frightening.

Criminals download videos from unprotected social media accounts and use artificial intelligence software to clone voices and images of people. They then call a victim and say they’ve kidnapped their loved one—often a child or grandchild—threatening to hurt them unless money is immediately sent to them either via wire transfer or cryptocurrency.

In the background, the relative will be screaming for help, and the call will appear to be from that person’s phone. To avoid detection, criminals may intercept the person’s calls. “As farfetched as this might sound, these criminals are very convincing and have a high success rate,” says Hurley.

These are only two of today’s dozens of scams. Enterprising cybercriminals are busy evolving their strategies and inventing new forms of stealing.

Danger Ahead

It's important to be on alert for potential frauds. "Successful ones tend to include two common aspects," says Hurley. "They're trying to get you to act urgently, and the parties involved will sound genuine, maybe even like authority figures."

These scams work because the criminals do their homework by collecting unprotected personal information on the internet. They know a lot about each victim before contacting them, so they sound especially convincing.

"A surprising amount of personal data is available online via public records and social media," says Denise. This can include a person's address, property value, phone number, email address, voter registration information, employer, job title, age, gender, race, and more.

Even worse, the information in unprotected social media accounts is effectively in the public domain, and anyone who wants to can access it.

Cybercriminals also regularly hack into people's personal email accounts, so they know what's going on in a potential victim's life. "For all these reasons, the criminals will sound like they're the real thing and can be very persuasive, even to sophisticated individuals," says Hurley.

Small But Important

"While scammers today can be very sophisticated and convincing, there are some simple things you can do to protect yourself from them," says Denise.

Here are a few tips you can start using immediately.

- *Don't talk to strangers.* Don't answer calls from people who aren't on your contacts list. A legitimate person will leave a voicemail and callback number.
- *Approach with caution.* Most successful scams attempt to get you to act quickly and will sound like an authority figure. Be skeptical, and don't get swept up in their urgency.
- *Assume the worst.* Neither your bank nor government agencies like the Internal Revenue Service (IRS) will call you about a problem. The bank will freeze your account; the IRS will send you a letter.
- *Don't share PII.* Do not provide personally identifiable information (PII)—like passwords, and account, credit card, or Social Security numbers—to anyone who calls you on the phone. Legitimate service providers don't typically ask for this kind of information over the phone.
- *Call back.* If you suspect you're getting lured into a scam, hang up and call your bank, broker, or other service provider at a verified number.
- *Protect your social media accounts.* Criminals can use photos, videos, and check-ins shared on social media to target you unless you engage privacy settings on these accounts.

Key Defenses

There are a few important defensive actions that can also help immunize you against would-be scammers.

Privacy Settings

Managing the privacy settings in the apps, search engines, and browsers you use is critical. “Otherwise, you’re making it very easy for very bad guys to find you and steal your passwords and personal information,” says Hurley.

Each application has its own security settings, so you’ll need to dig in. Facebook, for example, has 80+ specific security and privacy settings to control who can see your profile, friends, posts, comments, and shares, and which apps and websites have access to your Facebook data. Beneath these categories lie many subcategories—and this is only one application.

Doing this yourself requires research and takes time, but it’s OK to lean on trusted experts. “For most people, it would take about 100 hours of work to figure out the settings and engage them,” says Hurley. “And companies regularly change them, so it’s not a one-time process.”

“We track privacy settings on the most popular applications and can implement

the right settings and set up password managers for our clients in a single three-hour appointment,” says Hurley.

Password Hygiene

Another key practice: Use long and complicated passwords. “AI systems can now correctly guess any eight-digit alphanumeric password in less than a second,” says Hurley.

To make your passwords effective and secure, use a minimum of 20 randomly generated characters—including uppercase and lowercase letters, numbers, and symbols.

Don’t use names, birthdays, or pet names, and never use the same password for more than one account.

Yes, this means you will have to juggle dozens of impossible-to-remember passwords. Thankfully, using a password manager, like LastPass, Keeper, or NordPass, can help you create, save, and manage passwords for your online accounts.

Device Security

The default settings on your personal computers and smartphones automatically record the passwords for every account that you access with them. That means if you haven’t turned on the

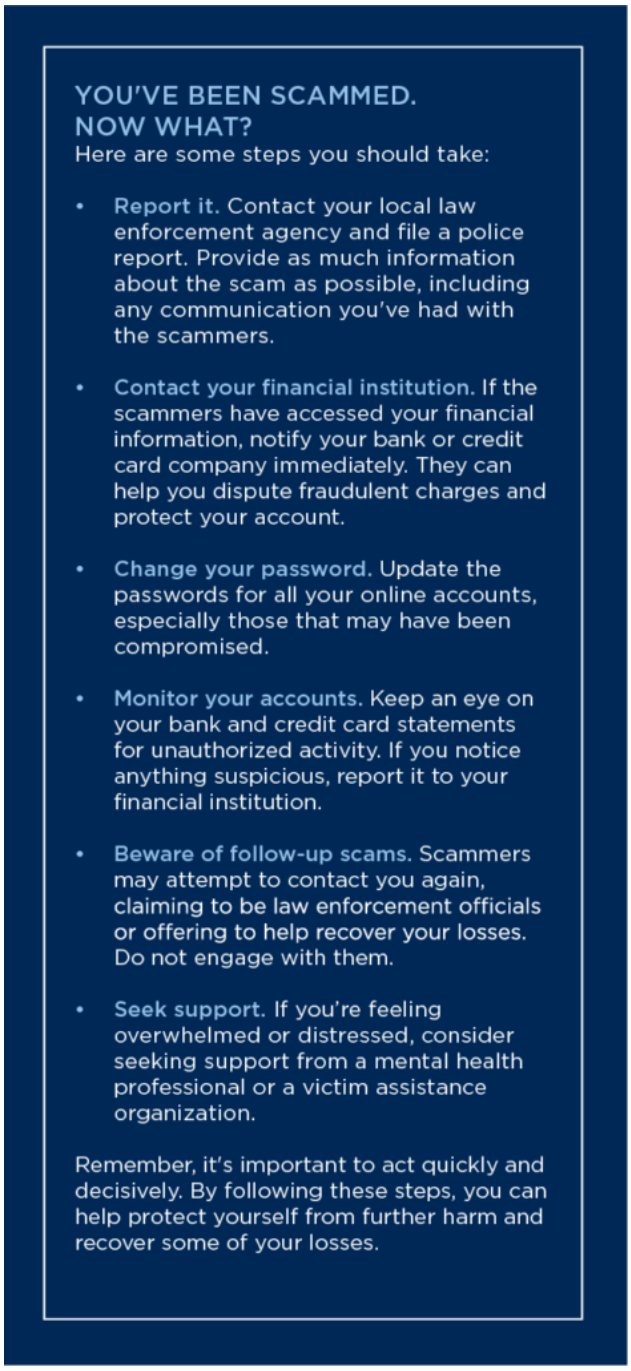
appropriate security settings on your devices and a cybercriminal breaches your device, they'll be able to access every one of your accounts.

It's no more difficult than a thief looking over your shoulder as you enter your smartphone passcode at a restaurant and then stealing your device.

To help reduce this risk, use a complex passcode, a fingerprint, or facial recognition to unlock your device; set your phone to automatically lock itself after a short period of inactivity; and enable functionality to erase all information on your phone if it's lost or stolen. Also, use multi-factor authentication (MFA) when it's available.

MFA is a security process that requires you to provide two or more verification factors to access a resource. This is what is happening when your online account wants to send a text to your phone, then asks you to enter a code from that text before letting you log in.

Yes, MFA can be frustrating and slow you down when you're trying to log into your accounts, but it is one of the very best defenses against scams and cyber threats.



“If you’ve been scammed, the quicker you take action, the less damage will occur,” says Hurley. “Once cybercriminals breach you, they quickly use the information they get to target every financial and social media account you have. This is how a single breach often leads to losing millions of dollars.”

After You’ve Been Scammed

What to do depends on how and what was breached. The first step is to figure out what happened and why and then take steps to minimize the damage.

This could be as simple as changing a password or as complicated as freezing your bank, custodial, and credit accounts, and making filings with the Federal Trade Commission, Federal Bureau of Investigation, and local law enforcement.

“Assume that, if you have been breached, the bad guys will soon return,” says Hurley. “Just as sharks regularly return to where they’ve been able to find animals to devour, cybercriminals return to target clients they’ve breached before.”

The Emotional Toll

Falling victim to a cybercriminal isn’t just a financial issue. Being scammed can erode the victims’ trust in others, and they may feel ashamed or embarrassed, especially if they lost a significant amount of money.

Also, scams can lead to feelings of anxiety and fear, as victims may worry about their financial security and the potential consequences of the scam.

These feelings can cause a victim to stay quiet or delay alerting the authorities about their situation. But it’s important to remember that acting quickly is the key to recovering lost funds and protecting oneself from future scams.

“Financial scams targeting older people can have a severe and long-lasting emotional impact,” says Denise. “It’s important to us to do everything we can to protect our clients and help them when they need us.”

By John Curry

CAPTRUST’s former Chief Marketing Officer, John Curry is now constructing his own second act and adjusting to unretirement in Spain. In the finance industry since 1986, Curry was instrumental in the launch of *VESTED* magazine, serving as its original editor in chief.