How to Know If You've Been Hacked

Christine M. Palmiere, RICP®
Vice President, Financial Advisor
Sage Rutty & Co., Inc.

100 Corporate Woods
Suite 300
Rochester, NY 14623

585-512-2324

cpalmiere@sagerutty.com
SageRutty.com

–Devin Kropp

Cyber-attacks are launched at us every day. Do you know the warning signs that your security has been compromised?

With cybercriminals constantly prying at your door, it can be tough to know if one of them had gotten through your cyber-defenses.

Weekly, we hear news of data breaches exposing our personal records and putting our accounts in danger. In a recent year, the Identity Theft Resource Center estimated that 170 million records were stolen. A study by Bankrate found that 41 million Americans have been victimized by identity theft.

Those numbers underscore the necessity of taking protective measures against those cyberscams. Dealing with a hacked account is time consuming and stressful. But the sooner it is caught, the better. Here are some warning signs that you may have been hacked.

1. Strange charges on your debit or credit cards

If you notice charges on any of your financial accounts that you did not make, close those accounts immediately. Hackers will often "test" your account by making small charges, so look out for strange charges on any amount.

Sign up for text or email alerts on your debit and credit accounts so you can know instantly when a charge is made. If you did not make the charge, you can contact your bank or credit card company immediately to report the fraud and cancel your account.

2. Emails you did not send

If there are emails in your sent mail that you did not send, chances are a hacker did. Often these emails will be sent to all your contacts and say that you are in trouble and need money right away. The hackers set up an account where your contacts can send money that they think is helping you, but it's really going straight to a cybercriminal.

To avoid this, choose a strong and unique password for your email account. A hacked email is one of the most dangerous hacked accounts because from your email, hackers can get into other accounts by resetting passwords. Remember to use numbers, characters, and uppercase letters in your password to increase its strength. You could also set up two-factor authentication, which will protect you even if a hacker gets your password. This security measure requires you to enter an additional code (usually sent to your phone) after you enter your regular password in order to access your account.

3. Items appear on your social media accounts that you did not post

If you log on to Facebook, Twitter, Instagram, or any other account and see posts that you did not make, be on alert. Chances are a hacker got into your account and made the posts. Generally, the posts are spam and the hacker gets paid for every click. Sometimes, the posts will have malware that can put your followers and friends at risk.

Again, strong passwords and two-factor authentication can keep hackers out of your accounts.

4. No access to your own accounts

You try to log in to your online account and your password doesn't work. There's a good chance a hacker got in and changed it. In this case, report it to the online service. They will help you regain control of your account.

If the hacked account uses the same passwords as any of your other accounts, change those immediately.

5. Your computer acts slow, strange

Hidden malware on your computer (or device) can cause your machine to slow down and not work as well. You may also notice strange popups.

Hackers usually trick you into downloading malware through phishing attacks. Often this malware can actually detect your keystrokes, which puts all your passwords and sensitive information at risk.

Run an antivirus and antimalware scan on your devices regularly, and be sure to update your software and browser to close security holes.

There are many antivirus software programs you can buy, such as Bitdefender Antivirus Plus, Norton Security, Webroot Security Anywhere AntiVirus, and Kaspersky Anti-Virus. They cost about $40-$80 per year.

There are also some free antivirus software programs available that security experts recommend. AVG AntiVirus Free is the most highly rated. Other options are Avira Free Antivirus and FortiClient 5.2.

6. Ransomware hits your computer

One of the newest and worst forms of malware is called "Ransomware." It encrypts all of your files and makes your computer unusable until you pay a bitcoin ransom to the hackers. If you are hit by ransomware, a screen will pop up saying that your computer is locked, the price to get your files back, and a deadline for payment.

Ransomware is usually spread by phishing emails, so do not click on any suspicious links or attachments in an email. Remember that most companies will not ask you for personal information via email. If you are unsure, it is best to call the company directly and check. Make sure to delete any suspicious emails immediately.

7. Your browser looks different

Another common form of malware installs malicious toolbars on your Internet browser. These toolbars may be disguised with names that seem real. If you did not download the toolbar yourself, remove it or restore your browser to the default settings. Running antivirus scans can help you detect this sort of malware quickly.

The best way to prevent being hacked is to be proactive about your cybersecurity. But knowing the warning signs that your device may have been compromised is the first step. Then acting immediately when you notice any of these signs can protect your data and time from hackers.

Devin Kropp is a writer based in New York City.