You’ve Been Hacked or Spoofed—Now What?

Presented by Paul Bonapart

Typically, most of us don’t realize that our email accounts have been violated until we get a message or call from a friend asking why we sent that “spammy” email with a link to a miracle diet pill website. Have we been hacked? Spoofed? Whatever it was, can we prevent it from happening again?

Spoofing Vs. Hacking

Think of **spoofing** as something like falsifying a letter sent via the USPS. Anyone can write a letter, sign someone else’s name, and put that individual’s return address on the envelope. If you receive the phony letter, you probably believe that it came from the individual who supposedly signed it and the return address indicated. But, in reality, it could have been sent from anyone, anywhere.

Spoofers forge the header information on the emails they send (i.e., the To, From, and subject line fields, as well as the time stamp and path the emails took to arrive in your inbox) to make it appear as if their messages came from someone or somewhere you know (e.g., a friend or familiar organization, like Bank of America). **The spoofers’ goal is to get you to respond to their spam or to click on the malware-laden links or attachments in their phony messages.**

When an email address has been spoofed, the spammer doesn’t actually gain access to your email account. Hacking, however, is something quite different.

Hacking is when a criminal actually gets into your email account. He or she can do this in a number of ways—by sniffing out your activity on a public Wi-Fi network, through a phishing email, or via password-guessing software. Once in, **the hacker can access all of the information stored in your email account**, including your contact list, bank account numbers, credit card information, online transaction receipts, and emails from other organizations confirming changed passwords (making it easier to identify other accounts of yours that can be hacked).

How to Prevent a Second Hack

Unfortunately, there is no way to prevent spoofing. If your email address can be viewed publicly on the Internet, someone can spoof it. But there are steps you can take to mitigate the risk of a future hack.

- **Change your password.** This includes any passwords for other accounts that are the same or similar to the compromised password. When creating new passwords, don’t use dictionary words or anything personally identifiable, such as your birth date. Also, be sure that your passwords are *at least* 8 characters long and include upper- and lowercase letters, numbers, and special characters.
- **Change the answers to your security questions**. Either make up answers to the questions or add an extra letter or symbol to the real answers. That way, even if the hacker figures out the answers, he or she will still have a hard time accessing your accounts. For example, instead of answering “Jones” to the “What’s your mother’s maiden name?” question, add another symbol or character and make it “@Jones” or “JonesM.”
- **Set up multifactor authentication.** This feature requires you to provide more than a username and password to access your account. For example, an additional layer of authentication could be a passcode sent to your mobile phone that you need to input when you log in.
- **Review your email account settings.** The hacker may have altered your account settings so that copies of received emails will be automatically forwarded to his or her account. So even after you resecure your email account, the hacker can keep tabs on you. He or she could also have placed fraudulent links in your email signature and automatic replies, so check your settings and verify that these were not altered.
- **Run a virus scan.** It’s also possible that the hacker inserted malware into your system through your email account. This could enable him or her to conduct *recon*—meaning that all of your online activity would be automatically reported back to the hacker and allow him or her to collect even more of your personal information.
- **Don’t store financial or personally identifiable information in your email account.** If personal information was stored, such as your social security number (SSN), birth date, or account numbers, *strongly consider* getting the compromised account numbers changed. In addition, have the banks or other organizations report the new numbers to you over the phone, *not via email*. Also consider credit monitoring, especially if all or part of your SSN was compromised.

Protect Yourself
To sum things up, be wary about connecting to public Wi-Fi networks and the information you transmit over such networks, as this is one of the most common ways that cybercriminals obtain email addresses and passwords. In addition, be suspicious of unsolicited or spam emails. If you receive one from someone you know, let that individual know that his or her email may have been spoofed or hacked.

Rest assured that our firm is always looking out for your best interests and striving to keep your confidential information secure. If you have any questions about the information shared here, please feel free to call or email our office.

Paul Bonapart, JD, RFC, AIF®

Financial Security Planning Services, Inc.

520 Tamalpais Drive | Suites 103/104 | Corte Madera, CA 94925

415.927.2555 | 415.329.0071 fax | www.financialsecurityplanning.com | paul@financialsecurityplanning.com

Paul Bonapart (CA Insurance Lic. #0808412) is a Registered Representative and an Investment Adviser Representative with/and offers securities and advisory services through Commonwealth Financial Network®, Member FINRA/SIPC, a Registered Investment Adviser. He is also an Investment Adviser Representative of Financial Security Planning Services, Inc., a Registered Investment Adviser. Financial planning services offered through Financial Security Planning Services, Inc. are separate and unrelated to Commonwealth Financial Network®. Fixed insurance products and services are separate from and not offered through Commonwealth.