You've Been Hacked or Spoofed: Now What?

Typically, most of us don't realize that our e-mail accounts have been violated until we get a message or call from a friend asking why we sent that "spammy" e-mail 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

Spoofing. 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 from the return address indicated. But it could have been sent from anyone, anywhere.

Spoofers forge the header information of the e-mails they send (i.e., the To, From, and Subject lines, as well as the time stamp and path that the e-mails 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 e-mail address has been spoofed, the spammer doesn't actually gain access to your e-mail account. Hacking, however, is something quite different.

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

Tips for preventing a second hack

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

1. **Change your password** and any passwords for other accounts that are the same or similar to the compromised password. In creating new passwords, don't use dictionary words or anything personally identifiable such as your birthdate. Also, be sure that your passwords are *at least* 8 characters long and include upper- and lowercase letters and special characters.
2. **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."
3. **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.
4. **Review your e-mail account settings.** The hacker may have altered your account settings so that copies of received e-mails will be automatically forwarded to his or her account. So even after you resecure your e-mail account, the hacker can keep tabs on you. He or she could also have placed fraudulent links

in your e-mail signature and automatic replies, so check your settings and verify that these were not altered.

5. **Run a virus scan.** It's also possible that the hacker inserted malware into your system through your e-mail 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.
6. **Ensure that there was no financial or personally identifiable information** stored in your e-mail account. If personal information was stored, such as your social security number (SSN), birthdate, 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 e-mail*. Also consider credit monitoring, especially if all or part of your SSN was compromised.

Protect yourself from future issues

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 cyber criminals obtain e-mail addresses and passwords. In addition, be suspicious of unsolicited or spam e-mails. If you receive one from someone you know, let that individual know that his or her e-mail may have been spoofed or hacked.

Questions?

Rest assured that our firm is always looking out for your best interests and to keep your confidential information secure. If you have any questions about the information shared here, please feel free to call us at 610-280-9330.