Your Email's Been Hacked!! …*Or Maybe Not*

A Tutorial on Email Exploits

By Denise Mayhan, PhD
April 2014

Spamming. Spoofing. Phishing. Hacking. There's a whole new lexicon of labels to deal with the things people do to our computers to take our money and confidential information. It's almost enough to make you want to turn your computer off and take a trip back to the good ol' days when using the United States Postal Service (USPS) and Ma Bell were practically the only ways to communicate. Um, wait…well maybe we're not *that* scared. Truth is, we are ***never*** going back to using those methods of communication exclusively, so we all need to make an effort to keep up with Internet security issues.

Lest we forget, in "the good ol' days," we used to get inundated by phone or mail-order scams by unscrupulous people who would show us beautiful photographs, charts and graphs and make promises to entice us to send our checks or give our credit card numbers for something that, deep down, we knew was too good to be true. In return for our naiveté, we got none of what was promised, lost our money and perhaps a little bit of our pride. When we complained to the authorities, we learned that the P.O. Box to which we sent our payment is no longer in service and that there was no physical address for the company. Poof! The company and its promises, like our money, vanished into thin air.

The mail scams we experience today are really quite similar – except instead of using the USPS, the scammers are exploiting the features of technology and the difficulty of enforcing cybercrimes to exponentially increase their ability to reach many more people with less effort via email.

Spamming

To be effective, the mail scams of the "olden" days had to have access to valid street addresses so that their mail actually reached a person. Those addresses could be gathered by buying valid mailing lists, stealing email lists from legitimate companies or even using the phone book. Email scams of today are quite similar – scammers have to have valid email addresses. They get them in a variety of ways by using the addresses in group emails they have received, gaining access into the email servers of large email providers like AOL or Yahoo and stealing them, or even by buying legitimate email lists. Email addresses may even be stolen from computers (hacking) with absent or out of date Internet or network security software. These email addresses are used to send "**Spam"** – unsolicited and often irritating email – to the valid email addresses. It's like getting junk mail in your postal mail box – only there's usually a LOT more of it on your computer.

How do I recognize Spam?

1. Spam is often easy to spot without opening it as it will come from an unrecognized email address, the subject line with be empty or simply contain "RE:", relate to something you are not familiar with or contain nonsensical or misspelled words.

What to do if you're getting a lot of Spam:

1. Use the Spam (Junk Mail) filtering features on your email client to block out most of the Spam. Remember to check your Spam Folder on a regular basis to be sure your filters are set at an appropriate sensitivity to block most Spam while allowing legitimate emails to go through. If you find legitimate email in your Spam folder, be sure to "allow" messages from that domain or sender so that they don't get caught in your Spam folder again. For Spam that is getting through your filters, be sure to "block" the sender so that you don't get it from that sender again.
2. If the Spam is from a legitimate source that you don't want to receive information from and there is an "unsubscribe" link in the message, copy the link and paste it into your browser and then unsubscribe from the email list.

Spoofing

The next thing scammers need is to entice you to open their Spam email. In the old days, mail order scammers made their mailings look "official" as though they were from a legitimate business. How do email scammers do this? They make the email appear as though it came from someone or a business that you know. This is called ***"spoofing."*** A spoofed email address is one that is used to "mask" an unfamiliar email address so that the received thinks the mail came from a reputable source and is more likely to open it. How do you know if you are the recipient of "spoofed" mail? Many times, the mail looks like Spam. More sophisticated spoofers go to greater lengths to make their mail look official and will actually use official logos from popular businesses like AOL or Bank of America to make you think their mail is legitimate. In some instances, however, you may be the "spoofee" – your email address is being used to send spoofed email.

How can I tell if I'm being spoofed?

1. You see mailer-daemon error messages (returned emails) in your inbox that do NOT match any messages you sent out (as if someone sent a letter to another person and wrote <u>your</u> return address on the envelope instead of their own.)

2. You get messages from people who received email from you that you did NOT send.

What should I do?

While there isn't a way to stop whoever is spoofing your account right now, you should use this event to take steps to strengthen your account protection and reduce the likelihood that you will be spoofed again by:

1) Changing and strengthening your email account passwords. Generally, longer passwords with multiple character types are more difficult to guess.
2) Use the blind copy (Bcc) field in your emails when sending group mail.
3) Inform people in your email contact list that you are not sending those emails.
4) Identify the service from which the email is actually being sent and inform that company that people are using their email service to send "spoofed" email. You can identify the server that the email is actually coming from by looking at the Internet header located in the email properties. If you're not sure how to interpret the header information, copy and paste it all into an email to send to the email service provider along with the content of the spoofed email.

Phishing

The third, and most important thing scammers need may happen only if you open the email and click on a link provided in the email. Depending on what the scam is, clicking on the link could take you to a website featuring porn or some other unscrupulous or offensive content, take you to an official-looking webpage that asks for confidential information such as password or log in ID, or activate an executable program, such as a virus, worm, Trojan horse, keylogger, malware, adware, etc. that could attack your computer. **"Phishing"** is when email scammers try to get sensitive information from you to use it to gain access to your private accounts like credit cards, bank accounts, PayPal accounts, etc. Remember, legitimate businesses will NEVER ask you for sensitive information, like passwords, log-in ID's or account numbers via email. As a general rule, don't click on any links in an email that you are suspicious of – delete it. Better safe than sorry.

How do I recognize Phishing?

Even though the email may look "official" with official logos or taglines, there are a couple of dead giveaways:

1) Any email that tries to scare you into doing something is suspicious.
2) No reputable service will provide links to a webpage within an email to enter sensitive personal information.

3) The email suggests that the only way to respond to their message is to download a file or click on a link provided.
4) There are a lot of misspelled words
5) THE EMAIL SCREAMS AT YOU IN ALL CAPS or has lots of !!!!!! at the end
6) The email is signed by some vague title, like, Customer Support, with no name or contact information.

What to do about Phishing

1) Recognize the Phishing scam and don't take the bait! Block the email sender and delete the message.
2) If the Phishing scam appears to be from a company that you do business with, forward the email to the appropriate authorities at that company for investigation.

Hacking vs. Spoofing

The good ol' days equivalent to hacking is simply stealing your mail out of your mailbox to get your personal information, sending mail to people you know using your return address and/or using your existing or creating new accounts in your name using the personal information stolen from your mailbox (or trash cans if you didn't shred it!). Let's say you get a message from a friend who says that they are getting Spam email from you that you know you didn't send. How do you know if your computer has been hacked or that your email address has simply been spoofed? Check your sent email folder. If you don't see these messages are being sent from your computer, chances are that your email address has simply been spoofed. On the other hand, if you do see the messages are being sent from your computer, you have been hacked and should take steps immediately to clean your computer and inform any persons or accounts you have that may be affected to limit your liability. The exact steps you need to take to protect your computer depend on the type of hacking attack. Consult a computer professional or check online (using a different computer!) for information on what to do.

How do I know if my email has been hacked?

1. You check your "sent" mail folder and discover that your computer is sending email that you are not writing.

What do I do about it?

1. Do not take this situation lightly. In all likelihood, it's not just your email that has been hacked. Take steps to immediately update your Internet Security software and run a complete scan and delete or quarantine any suspicious programs on your computer. You

can check to see how serious any identified infections are by using a different computer to look them up on your Internet Security software's website. After your Internet Security software scan and clean-up is completed, find your back-ups and restore your system to a date in the past you are sure your computer was not infected. DO NOT attempt to make a back-up of your currently infected files – it's too late.

2. Log into your computer as an administrator and review all of the User Accounts on your computer. If there are User Accounts that you don't recognize, they were most likely created by a hacker. Delete the unknown accounts. Step by step instructions:
   a. Log in to your computer as an Administrator.
   b. Click the Windows Start button, type "cmd" into the search box and press "Enter" to open a command-line window.
   c. Type "net user" without quotes at the command prompt and press "Enter." Windows lists all existing accounts on the computer.
   d. Verify that all accounts in the output of "net user" are legitimate. If there are additional accounts, those accounts were likely created by a hacker.
3. Log in to all of your external accounts with confidential/sensitive information that may have been compromised to change and strengthen your passwords and inform them that your computer was hacked (e.g., email /website accounts, credit cards/banking, facebook, etc.) Check the accounts regularly for any suspicious or unrecognized activity.
4. Check your credit report and then check it regularly for several months to identify any unrecognized activity.

More information

Several reputable websites offer good step-by-step information on computer technology issues, such as: the help section of your email service provider's website (e.g., http://help.aol.com), www.pcmag.com , or www.ehow.com. PCMag.com's most recent review of the best Internet Security software can be found here: http://www.pcmag.com/article2/0,2817,2369749,00.asp

Author

Denise Mayhan, PhD, is the President and Owner of Inspired Solutions, an education, management and technology company. She has served as the National Baptist Convention, USA, Inc. Technology Program Manager and Website Content Manager for nationalbaptist.com since 2003. You may contact Dr. Mayhan by email at dmayhan@nationalbaptist.com.