DigiKnow
CYBER SECURITY DEPENDS ON YOU

IS YOUR EMAIL ADDRESS SPAMMING PEOPLE?

August 2023| Issue 2023:6

SPOOFED OR HACKED?

It's an ordinary day. You check your messages and find that your friends and family are asking why you're stuffing their inboxes with hundreds of dubious emails. Several people suggest that your email account has been hacked, and you start to feel a little panicked.

Chances are that your email account was NOT actually compromised. Unfortunately, spammers can misappropriate your email address without actually hacking into your email account. It is relatively easy to "spoof" an email address so that it appears a message is coming from one address when it was really sent from another. The design of the Internet's email protocols allows anyone to put any address in the FROM line of an outgoing email.

Spammers use high-volume mail merge software that picks a name and address from a database and inserts it into the FROM line of outgoing emails. How do they get your email address in the first place? Massive data breaches are reported all of the time and millions of records and data are sold on the dark web. This is how cyber criminals get access to huge amounts of valid names and email addresses.

What's My Next Step?

Check your computer for malware. If your Internet security software has a scan option, run it. If it shows nothing unusual, if you can still login to your email account with your password, and you see nothing amiss in your Sent folder, then you can safely assume no breach has occurred. It is still a good idea to change your

HELP, I'VE BEEN HACKED!

An email account can be hijacked in several ways. Phishing attacks in which a hacker subtly persuades a user into revealing login passwords are one hijacking technique. Some forms of malware such as viruses and spyware, attack for the purpose of gaining access to your computer, to enslave it in a botnet, and use it as a spamming device. Keylogger spyware installed on your computer can record every keystroke you type and send the results to a remote operator who can then read your password from the log file.

It is possible for a hacker to change your email password so that you cannot log in to your own account. Then they can raid your contact list to harvest valid email addresses to add to their spam lists. Also, the hacker now has access to all your saved email, which may include sensitive personal and financial information. If you've been locked out of your own email account, contact your email service provider, or use the "can't access my account" link that appears on the login screen.

WHAT SHOULD I DO IF MY EMAIL IS HACKED?

1) Change your passwords:
Change your password for your email account if you can. Make it a strong, unique password—don't reuse a password from another account. Next, update the passwords for other accounts if you use the same or similar passwords for them.

2) Use your email provider's recovery service, if needed:
In the case where you've been locked out of your account because you think the hacker has changed the password, your email provider should have a webpage dedicated to recovering your account. This is a good reason to keep your security questions and alternate contact information current with your provider, as this is the primary way to regain control of your account.

3) Reach out to your email contacts:
As mentioned above, a big part of the hacker's strategy is to get their hooks into your address book and spread malware to others. As quickly as you can, send a message to all your email contacts and let them know that your email has been compromised. And if you've done so, let them know that you've reset your password so that your account is secure again.

4) Scan your device for malware and viruses:
Give your device a thorough virus scan with comprehensive online protection software to ensure your device is free

password, update security questions, and turn on two-factor authentication.

But what happens if your email account really was hacked? Check out the next column to learn how to handle a hack.

Solomon Adote
Chief Security Officer

from malware. Set up a regular scan to run automatically if you haven't already.

5) Check your other accounts:
Sometimes one bad hack leads to another. If someone has access to your email and all the messages in it, they may have what they need to conduct further attacks. Take a look at your other accounts across banking, finances, social media, and other services you use and keep an eye out for any unusual activity.

Information Sourced from "Ask Bob Rankin" and "mcafee.com"

READ MORE CYBERSECURITY NEWS at DIGIKNOW!

Delaware Department of Technology & Information publishes and sends this newsletter to all network users because we need YOUR help to keep our network secure. If you are having problems viewing this message, accessing the links or want to print a PDF copy, go to:https://digiknow.dti.delaware.gov/news/index.shtml?dc=newsletters

Department of Technology and Information
Contact us at **esecurity@delaware.gov**