CYBERSECURITY AWARENESS BULLETIN

WHAT TO DO IF YOU SUSPECT YOUR EMAIL ACCOUNT IS COMPROMISED

Serial:	CI-AWA-2020-180-01
Date:	28 JUNE 2020

Scope

This bulletin provides background and guidance for responding to situations where your email account may be (or may appear to be) compromised.

Summary

Email compromises come in three scenarios as described in the graphic. Many of the indicators are similar, but the response required will vary. If you cannot verify the situation, you should respond as if Scenario 3 occurred to cover all of your bases. The steps listed in the details portion of this document should serve as a framework for your response in Scenarios 1 and 3.

There are many steps to take to respond. The exact steps vary based on your email provider. Simply changing your password isn't good enough. You'll also want to make sure the hacker has not configured your account to let them return or to keep spamming.

In other instances, people may be reporting that they have received email from your name or actual email address without your account being compromised. In that case, someone is spoofing - a fraudulent or malicious practice in which communication is sent from an unknown source disguised as a source known to the receiver - using your email address. Unfortunately, you can't do much about it, except to alert your contacts about it and ask them to verify the authenticity of the messages received from your address. You can however, in the case where it the email is coming from account that is not yours but is using your name, ask the various email providers from as Gmail and Yahoo to mark the account as spam using directions on their systems.

Finally, in the hybrid scenario, your account has been compromised, but the attacker has created a spoofed account to manage and use for follow-up actions.

Details

How do I know if my email account has been compromised? This can be determined by taking a look at the email headers. If you're not comfortable with performing this assessment, please contact your email provider's support team. The CGAUX CI Division may also be able to assist for Auxiliary related accounts. Review of headers is outside of the scope of this document.

If your email account has been compromised, there are many steps to take to respond. The exact steps vary based on your email provider (check your provider for instructions and report the incident). However, changing your password isn't good enough. You'll also want to make sure the hacker has not configured your account to let them return or to keep spamming.

Step #1: Perform a FULL Security Scan of Your Devices

Run a full scan of your devices with your anti-virus and/or anti-malware software. Do not simply perform a quick scan, if that's an option. Sending email to your friends and family isn't the end goal for hackers. They want to separate you from your money and that means that they'll try to install keyloggers to get your passwords and other malware.

Step #2: Change your Password and Other Security Questions

The very first thing you should do is keep the hacker from getting back into your email account. Change your password to a strong password that is not related to your prior password.

WHAT TO DO IF YOU SUSPECT YOUR EMAIL ACCOUNT IS COMPROMISED

In addition to your email password, change the passwords of any accounts that share the same password as your hacked email account and those that are variation of that password. As an extra security measure, also change the passwords for any sites that story your credit card information, like your Nextlix, Amazon and credit card company. Remember that the attacker could have used “forgotten password” procedures on these other accounts and reset them using your email account.

For accounts that require security questions, change those as well. And if the questions are generic, like what's your mother's maiden name, lie when answering and record those answers in your password manager. If you want to be extra careful, use a password generator to create a nonsense answer.

Step #3: Reclaim Your Account

The hacker may have changed your password too, locking you out of your account. If that’s the case, you’ll need to reclaim your account, which is usually a matter of using the “forgot your password” link and answering your security questions or using your backup email address. Check out the specific recommendations for reclaiming possession of your account based on your email provider.

Step #4: Check Your Email Settings

Sometimes hackers might change your settings to forward a copy of every email you receive to themselves so that they can watch for any emails containing login information for other sites. Check your mail forwarding settings to ensure no unexpected email addresses have been added. Check your "reply to" email address. Sometimes hackers will change your "reply to" email address to one they've created that looks similar to yours. So when someone replies to your email, it goes to the hacker's account, not yours. Last, check to make sure the hackers haven’t turned on an auto-responder, turning your out-of-office notification into a spam machine.

Step #5: Notify Your Contacts

Let the people in your contacts list know that your email was hacked and that they should not open any suspicious emails or click on any links in any email(s) that recently received from you.

Step #6: Prevention from Re-occurrence

Some recommendations for preventing repeat incidents include:

- Use a strong password that is difficult to guess but easy to remember.
- Use a unique password for your email account, your bank account and any other sensitive accounts.
- Use a secure password management program to do the work for you if you cannot manage them yourself.
- If your mail provider offers multifactor authenitcation, implement. This is the best protection from hackers.
- Limit the amount of personal information you share publicly on social media. Hackers use this publicly available personal information to help answer security questions that protect your accounts.
- Bookmark websites that you frequently use to access personal information or input credit card information to will prevent you from accidentally landing on sites hackers set up to catch people mistyping the address.
- Log in only using trusted systems and trusted networks. Computers in hotel lobbies, libraries and other public places are perfect locations for hackers to install key-logging programs to capture your credentials.