Fevruary
2020

Cybersecurity Newsletter

2d Marine Division G-6

Cyber Attackers and Response Actions

Overview

Most people believe they are not a target for cyber attackers; that they, their systems, or accounts have no value, but they are misteken. The truth is, if you use technology in anyway, whether at work or at home, bad guys are trying to get your information. No matter how secure you are, sooner of later they may get in. Below are some clues that you have been compromised, and things you can do to fix the problem.

Types of Attackers

Cyber Criminals: These guys are out to make as much money as possible. What makes the Internet so valuable to them is they can now easily target everyone in the world with just the push of a button. And there are a lot of ways they can make money from you. Examples include stealing money from your bank or retirement accounts, creating a credit card in your name and sending you the bill, using your computer to hack other people, or hacking your social media or gaming accounts and selling them to other criminals. The list is almost endless how bad guys can make money off you. There are hundreds of thousands of these bad guys who wake up each morning with the goal of hacking as many people as possible every single day.

Targeted Attackers: These are highly trained cyber attackers, often working for governments, criminal syndicates, or competitors targeting you at work. You may feel your job would not attract much attention, but you would be very surprised.

- The information you handle at work has tremendous value to different companies or governments.
- Targeted attackers may target you at work not because they want to hack you, but to use you to hack one of your co-workers or other systems.
- These types of attackers may target you at work because of what other companies you work with.

Clues You've Been Hacked

- Your anti-virus program generates an alert that your system is infected. Make sure it is your anti-virus software generating the alert, and not a pop-up window from a website trying to fool you into calling a number or installing something else.
- You get a pop-up window saying your computer has been encrypted and you have to pay a ransom to get your files back.
- Your browser is taking you to all sorts of websites that you did not want to go to.
- Your computer or applications are constantly crashing or there are icons for unknown apps or strange windows popping up.
- Your password no longer works even though you know it is correct.
- Friends ask you why you are spamming them with emails that you know you never sent.

How to Respond

If you suspect you have been hacked, the sooner you act the better. If the hack is work related, do not try to fix the problem yourself; instead, report it immediately. If it is a personal system or account that has been hacked, here are some steps you can take:

- Change Your Passwords: Change the passwords on your computers, mobile devices, and online accounts. Do not use the hacked computer to change your passwords; use a different system that you know is secure. If you have a lot of accounts, start with the most important ones first. If you can't keep track of all your passwords, use a password manager.
- Financial: For issues with your credit card or any financial accounts, call your bank or credit card company right away. Use a trusted phone number to call them, such as from the back of your bank card, your financial statements, or visit their website from a trusted computer. Also consider putting a credit freeze on your credit files.
- Anti-virus: If your anti-virus software informs you of an infected file, follow the actions it recommends. Most anti-virus software will have links you can follow to learn more about the specific infection.
- Reinstalling: If you are unable to fix an infected computer or you want to be surer your system is safe, reinstall the operating system. Do not reinstall from backups; your system may have been hacked before the backup. If you feel uncomfortable reinstalling, consider using a professional service to help you. If your computer or device is old, it may be easier to purchase a new one. Finally, once you have reinstalled your OS or purchased a new one, make sure it is updated and enable automatic updating whenever possible.
- Backups: A key step to protecting yourself is to prepare ahead of time with regular backups. Many solutions will automatically back up your files daily or hourly. Regardless of which solution you use, periodically check that you are able to restore those files. Quite often, recovering your data backups is the only way you can recover from being hacked.
- Law Enforcement: If you feel in any way threatened, report the incident to local law enforcement. If you are the victim of identity theft and are based in the United States, then visit https://www.identitytheft.gov.

But I Have Anti-Virus

"I'll just install anti-virus and a firewall on my computer and I'm protected". Unfortunately, that's not always true. Many people feel if they install some security tools then they are secure. Cyber attackers continue to get better and better, and many of their attack methods now easily bypass security technologies. They often create special malware that your antivirus cannot detect. They bypass your email filters with a customized phishing attack or call you on the phone and trick or scam you out of your credit card, money, or password. Technology plays an important role in protecting you, but you are your best defense.

Being secure is not that hard; common sense and some basic behaviors are your best defense. If you get an email, message, or phone call that is extremely urgent, odd, or suspicious, it may be an attack. To ensure your computers and devices are secure, keep them current and enable automatic updating. Finally, use a strong, unique passphrase for each of your accounts.

Contact your Cybersecurity Personnel

If you have additional questions, comments, or concerns, please contact the 2d Marine Division G-6 Cybersecurity personnel at commercial 910-451-0083 or email 2mardiv_g-6_ia@usmc.mil.