January
2020

Cybersecurity Newsletter

2d Marine Division G-6

Securely Using Social Media

Overview

Social media sites, such as Snapchat, Facebook, Twitter, Instagram, and LinkedIn, are amazing resources, allowing you to meet, interact, and share with people around the world. However, with all this technology comes risk, not just for you, but your family, friends, and fellow Marines and Sailors. This has never been more with the rise of TikTok and other live social media platforms.

Posting

Be careful and think before posting. Anything you post will most likely become public at some point, impacting your reputation and future, including where you can go to school or the jobs you can get. If you don't want your family or boss to see it, you probably shouldn't post it. Also, be aware of what others are posting about you. You may have to ask others to remove what they share about you.

Privacy

Almost all social media sites have strong privacy options. Enable them when possible. For example, does the site really need to be able to track your location? In addition, privacy options can be confusing and change often. Make it a habit to check and confirm they are working as you expect them to.

Passphrase

Secure your social media account with a long, unique passphrase. A passphrase is a password made up of multiple words, making it easy for you to type and remember, but hard for cyber attackers to guess.

Lock Down Your Account

Even better, enable two-factor authentication on all of your accounts. This adds a one-time code with your password when you need to log in to your account. This is actually very simple and is one of the most powerful ways to secure your account.

Scams

Just like in email, bad guys will attempt to trick or fool you using social media messages. For example, they may try to trick you out of your password or credit card. Be careful what you click on: if a friend sends you what appears to be an odd message or one that does not sound like them, it could be a cyber attacker pretending to be your friend.

- Urgency: The message has a sense of urgency that demands "immediate action" before something bad happens, like threatening to close your account or send you to jail. The attacker wants to rush you into making a mistake.

- Pressure: The message pressures you to bypass or ignore policies or procedures at work.

- Curiosity: The message invokes a strong sense of curiosity or promises something that is too good to be true. No, you did not just win the lottery.

- Sensitive: The message includes a request for highly sensitive information, such as your credit card number or password, or any information that you're just not comfortable sharing.

- Official: The message says it comes from an official organization, but has poor grammar or spelling. Most government organizations will not use social media for official communications directly with you. If you are not sure if the message is legitimate, call the organization back, but use a trusted phone number, such as one from their website.

- Impersonation: You receive a message from a friend or co-worker, but the tone or wording just does not sound like them. If you are suspicious, call the sender on the phone to verify they sent the message. It is easy for a cyber attacker to create messages that appear to be from someone you know. In some cases, they can take over one of your friend's accounts and then pretend to be your friend and reach out to you. Be particularly aware of text messages, Twitter, and other short message formats, where it is more difficult to get a sense of the sender's personality.

You must be your own defense against scams, cons, and attacks like these. If a post or message seems odd or suspicious, simply ignore or delete it. If it is from someone you personally know, call the person on the phone to confirm if they really sent it.

Current Cybersecurity Concerns

With tensions raising in Iraq and Iran, consider how what you post can be used by foreign intelligence services and hacker groups to gain intelligence and profile you, your fellow Marines and Sailors, and your unit.

- https://www.militarytimes.com/off-duty/military-culture/2020/01/08/for-the-love-of-opsec-put-away-your-phone/

- https://whnt.com/2016/08/15/general-marines-put-down-those-cell-phones/

- https://www.c4isrnet.com/intel-geoint/2020/01/03/dont-expect-an-invasion-of-iran-to-be-tiktokd/

- https://www.sentinelone.com/blog/how-hackers-use-social-media-profile-targets/

- https://www.zdnet.com/article/fbi-warning-foreign-spies-using-social-media-to-target-government-contractors/

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.