H E A D Q U A R T E R S
P H I L I P P I N E A R M Y
OFFICE OF THE ASSISTANT CHIEF OF STAFF FOR
COMMAND AND CONTROL COMMUNICATIONS, AND CYBER SYSTEMS, G6
Fort Andres Bonifacio, Metro Manila

6/CMB 27 January 2017

CYBERSECURITY BULLETIN

Cybersecurity Bulletin: #17-04

SOCIAL MEDIA SECURITY

What is the problem with social media?

The most recent and profound development in cyberspace is the global migration to social media. As of January 1, 2016, Facebook had 1.59 billion monthly active users, larger than the population of China. In a single minute of the day, 350,000 tweets are posted to Twitter, 300 hours of video are uploaded to YouTube and users like 1.75 million photos on Instagram.

Not only is this new social media landscape growing rapidly, it represents one of the most dynamic, unstructured and unregulated data sets anywhere in the digital world leading to the emergence of Digital Risk Monitoring.

The rise of social media has introduced a new security paradigm, one that puts users - employees, customers and partners - squarely in the attacker's crosshairs. Social media has become the new cyber battleground, presenting one of the largest, most dynamic risks to organizational security in decades. Attackers leverage social media for three main reasons:

1. **The scale of social media**

With 2 billion people on social media worldwide, attacks can spread like any other viral trend. The adversary can use trends, clickbait, and hashtags to

broadcast their attack, either to general population or to a certain group of people. This poses a monumental challenge for security teams to overcome manually.

2. **The Trusted Nature of Social Media**

Well, over one third of people accept unknown friend requests on social media, making it one of most effective vehicles for gaining the trust of a target. Once an attacker has entered one of their target's trusted social circles, it is much easier to entice the target to click a malicious link or file.

3. **Invisibility to Security Teams**

According to Computerworld, the average American spends over ¼ of their online time on social networks. InfoSec teams have no existing tools in their arsenal to extend their visibility beyond the perimeter into the social media realm, where employees are dangerously vulnerable to compromise.

Why must the Army care about Social Media Security?

Due to consumers' migration to social media channels, organizations that create brand value through social media reputation have vastly outperformed the market (growing 103% in market value vs. 63% for the S&P 500 and 30.3% for the MSCI World Index) since the launch of Facebook in 2004. Social media has also become a medium for Army personnel to communicate with their loved ones, friends, and acquaintances. It has also been a effective tool for the Army to reach out to stakeholders thru information dissemination and engagement. However, the parallel migration of hackers and scammers to social media is a growing problem: ZeroFOX Research Team found that for every 1 scam post remediated, 3 new ones are created.

Tips to Strengthen the Organization's Social Media Security

1. **Educate personnel**

Enterprises often place a heavy emphasis on SaaS solutions and high-tech tools to help secure the organization, but forget the simple practice of raising awareness and educating personnel about cybersecurity. Social media has evolved to become a fabric that connects society and a pervasive business communication tool in the digital age. There is a level of trust between users and the platform that fosters a presumption that all information shared via social platforms is safe. With personnel on the front lines of the latest cyber threats, it's important to spotlight the risks lurking at their fingertips with every tweet, snap, post and click.

Informing personnel of best practices can help move the needle not only for the overall security of the business, but overall security knowledge at the business level. Awareness through seminars, workshops, and other programs help educate how attackers use social media to target a brand via individual personnel.

2. **Encourage personnel to change passwords regularly**

While using the same password across multiple social media accounts is easy, it is a huge threat to personnel and the oragnization's security. Once a hacker decodes a "favorite" password, they can easily use it to gain access to other platforms and accounts. Encouraging personnel to diversify passwords across their

social platforms makes it infinitely more difficult for a hacker to breach accounts. This is also true for Army-branded accounts.

3. Utilize two-factor authentication

Make sure personnel and all Army accounts utilize two-factor authentication, which requires a password, username and something unique that only the user will recognize or know. Many of the larger social networks provide two-factor authentication, commonly in the form of a code sent to their smartphone or email each time a new device or browser attempts to login to the account.

This ensures that personnel's identity is legitimate to permit access to the desired account. Having this as a second layer of protection makes attackers' lives harder and reduces the vulnerability of attack.

4. Avoid engaging with suspicious content

Stress the practices of carefully reviewing URL links before clicking to make sure the company and site name are spelled correctly. Cybercriminals will often blast out links that are very similar to a real address adding, subtracting or rewording parts to differentiate them. This is further obfuscated by social networks URL shortening platforms. While these appear safe when quickly scrolling, if you stop and really look, it's difficult to determine if the link is safe. Another common hacking tactic is prompting a user to download an application via social media links outside of curated stores, such as the Apple App Store or Google Play, in order to view information. This is never a good idea and personnel need to be aware of the dangers of downloading third-party applications on work devices, especially from unfamiliar sources, which can render the company vulnerable.

The general rule of thumb in today's threatening digital landscape is that if a link or website looks suspicious, don't click.

5 . Install antivirus and security software

This is one of the most important, but often overlooked, practices among organizations. Preventing malware from breaching a corporate system is extremely important and the solution can be as simple as installing an antivirus software.

With the numerous phishing scams and malware-embedded links floating around social media, having an extra layer of protection is crucial. No matter how careful a user is, there's always the risk of accidentally engaging with a malicious link – and just one unfortunate click can lead to months of recovery time.

Once antivirus software has been installed, it's important to remind employees to update it frequently to protect against new, evolving threats.

6. Beware of fraudulent friend requests

Many hackers gain access to company information by creating fraudulent accounts and connecting with “colleagues.” Personnel may accept this request without vetting legitimacy and can ultimately fall victim.

Offices should encourage personnel to thoroughly vet a friend request before hitting “accept”. They should check to see if other colleagues are also connected to the account. If the account seems suspicious or you don’t know the individual, ignore or report the user, and refrain from clicking on any links they may have sent.

7. Validate and Verify

A common hacking technique is to cast a net that encompasses followers, connections, and mentions. For example, a hacker might post a non-descript image with many people tagged or mentioned. Before clicking, personnel must remember to validate the authenticity of the individual who tagged or mentioned them, ensuring that it is a trusted friend or colleague.

Similarly, hackers tend to create accounts impersonating celebrities, politicians, athletes or large companies. The larger social networks have added “verified accounts” indicated with a checkmark to note their legitimacy. However, many companies have yet to pursue this validation.

If a personnel receives a request, it’s important that they do their homework and search for the individual’s name or company online. If they find a verified account that doesn’t match the request, it’s most likely an impersonator. If this occurs, the personnel should flag the account to their internal IT department so that other colleagues can become aware of the situation and avoid any interaction.

Reference:

This was cross posted from:
http://www.csoonline.com/article/3148301/social-networking/7-ways-to-tighten-enterprise-social-media-security.html#slide8

https://www.zerofox.com/social-media-security/