FOLLOW PROCEDURES KNOW THE THREAT STAY ALERT

"THE WARRIOR"

IRANIAN HACKERS TARGETED U.S. MILITARY VIA SOCIAL MEDIA

Don't think foreign governments are interested in obtaining PII from Soldiers? Think again… A social media spokesperson stated their company had recently identified and disrupted activities linked to an Iranian cyber group who targeted U.S. Soldiers and the global defense industry via its web site. The hackers used the social media outlet to identify potential victims and convince them to migrate conversations offline; malware identified by the social media company is linked to the Iranian military via a known Iranian IT company who the U.S. has currently placed sanctions upon.

https://thehill.com/policy/cybersecurity/563241-facebook-disrupts-iranian-hackers-using-platform-to-target-us-military?rl=1

THE PANDEMIC WAS A CASH COW FOR HACKERS AND CRIMINALS

Criminals, by definition, are opportunists who are quick to leverage bad news to make a quick buck. During the COVID-19 pandemic, the U.S. government instituted numerous assistance programs that quickly caught the attention of cyber criminals. The DOJ has charged at least 474 people for pandemic-related fraud – their ploys ranged from luring victims to 'snake oil' COVID treatments (via slick web pages) to spear phishing campaigns that promised financial assistance to individuals and companies. The dollar amount currently attributed to pandemic-related fraud is a staggering $569 million (translation: U.S. taxpayer money).

https://www.zdnet.com/article/us-charges-close-to-500-individuals-for-covid-19-fraud-criminal-activity/?&web_view=true

What is the purpose of our Newsletter? Quite simply it is to educate all of our Soldiers, Civilians and Contractors of the very real cyber, information, personnel and physical security threats to the DOD. We all have a responsibility to safeguard equipment, information and each other! Stay alert and stay alive!

STAY SAFE! STAY ALERT!

INSIDERS CAUSE 75% OF BREACHES

Just how dangerous are "Insider Threats"? The answer, extremely dangerous. So much so that between Nov 2019 and Oct 2020, 75% of security breaches within the legal sector was attributed to negligent and/or malicious employees who possessed access to the data. Roughly 57% of the loss of legal data was tied to human error, which included the employee's failure to redact document information and including the wrong (or unauthorized) email address within an outbound email that contained sensitive legal information. The impact to legal firms (and customers that entrusted them with sensitive legal matters) is huge – and places their firms in legal jeopardy for leaking sensitive information. Remember, always be aware of Insider Threats. It is the responsibility of all of us to be on the lookout for the warning signs. See something, say something is best way to combat this very serious threat! Report it! It is better to be safe than sorry!

EMPLOYER NETWORKS PLACED AT RISK FROM EMPLOYEE'S POOR INFOSEC

Most Americans have a basic understanding of Information Security (INFOSEC) "best practices" - for example, they typically know to safeguard their birth date and social security numbers. However, when it comes to their social media content, using a social media user account to automatically log into other websites, those same people unwittingly supply hackers with information that is highly useful to attack corporate networks via spear phishing attacks. Large scale database breaches and websites that fail to encrypt user names/passwords leak an *enormous* amount of useful information that hackers leverage to infiltrate company-owned websites. When employees exercise poor INFOSEC hygiene on their personal devices they can inadvertently provide a hacker with information that places their employer's computer systems at risk. Workplace photos posted onto social media websites (that sometimes show sensitive information laying on a desk or a sticky note stuck on a computer screen) are a common INFOSEC failure; reusing computer passwords (versus password management software tools) is also problematic.

https://beta.darkreading.com/endpoint/how-personally-identifiable-information-can-put-your-company-at-risk?web_view=true

Did You Know?

August is the eighth month of the year in the Julian and Gregorian calendars, and the fifth of seven months to have a length of 31 days. It was originally named Sextilis in Latin because it was the sixth month in the original ten-month Roman calendar under Romulus in **753 BC**, with March being the first month of the year.

More Allied ships were sunk by German submarines in the Gulf of Mexico during World War Two than were destroyed in the Japanese attack at Pearl Harbor. And the only German U-Boat lost during the conflict was sunk off the coast of Louisiana.

The Louisiana Purchase (1803) was eventually cut into all or part of 15 U.S. states (Arkansas, Colorado, Iowa, Oklahoma, Kansas, Louisiana, Minnesota, Missouri, Montana, Nebraska, New Mexico, North Dakota, South Dakota, Texas and Wyoming), plus small portions of land that would become part of the Canadian provinces of Alberta and Saskatchewan.

533 MILLION SOCIAL MEDIA PLATFORM USER ACCOUNTS LEAKED ONLINE

An Internet forum that caters to hackers/hacking activities recently shocked the world via a user account that posted a link to a file that contained Personally Identifiable Information (PII) for all 533 million user accounts of the world's largest social media platform. The data encompassed 106 countries (including the U.S.) and listed the user account + the user's full name, birth date, location, password reset phone number, email account, biographic data – the works. An independent study of the leaked file confirmed its legitimacy. The leaked data could be leveraged for future spear phishing campaigns and identity theft. The incident serves as a reminder that posting as little PII onto the Internet as possible remains the best Information Security policy.

https://www.businessinsider.in/tech/news/533-million-facebook-users-phone-numbers-and-personal-data-have-been-leaked-online/articleshow/81889315.cms?&web_view=true

HEALTH, SAFETY & SECURITY

Department of State Travel Advisories
https://travel.state.gov/content/travel/en/traveladvisories/traveladvisories.html/

You Are a Target

You may not realize it, but you are a target. Your computer, work, personal accounts, and your information are all highly valuable to cyber criminals. Be mindful that bad guys are out to get you.

Should you have any questions regarding;
CCRI or INFOSEC, call Chris Jackson
PERSEC or clearances, call Mayna Taylor
Foreign Disclosure issues, call Roland Huson
Physical Security, call Ben Iles

All of these Security Professionals can be reached at 337.531.9512