precision CYBERTECHNOLOGIES & DIGITAL SOLUTIONS

CYBER DIGITAL WORLD

NEWSLETTER

Volume 1: Issue No. 1 **September:** 2021

Employee awareness – the "vaccine" against corporate cyber threats

Did you know that human error is one of the leading causes of data breaches within organizations? Employees are every company's most valuable set of assets, and the key to delivering the business strategy. Similarly, when it comes to cyber defenses, employees can contribute, often unwittingly, to the success or failure of your company.

Dr. Ronald Walcott
Managing Director

Welcome to Cyber & Digital World, Precision Cybertechnologies and Digital Solutions fortnightly newsletter. Every two weeks we will explore the world of cyber security and digital technology solutions. Through featured articles, tech updates and news digests we will bring to you the leading discussions, concepts, tools, and industry approaches to help you make informed technology decisions for your business.

It is important for you and your employees to understand how to identify and know what to do when faced with cyber threats. You also want your clients and key stakeholders to have the security of knowing that you are a secure and protected partner in business.

Our newsletter will help bridge the gap between the employee understanding and the cyber world. Every time they receive a new newsletter, employees will be reminded of their responsibility when accessing corporate systems and data. Most importantly, employees will learn how to effectively communicate with IT teams.

Ransomware

IN THIS FIRST ISSUE WE'RE TALKING RANSOMWARE: WHAT IS IT AND HOW DO YOU PROTECT YOUR COMPANY AND SYSTEMS FROM IT.

In response to the pandemic, many end-users are now working from home instead of going into the office. Homes are being used as workspaces, and computers and networks are being shared by family members. Families are using computers to take classes, do homework, and surf the web in addition to regular business functions.

The data created may be stored locally or in the cloud. Backups often do not happen until devices are returned to the office or the end-user manually backs up the work. This new environment is ripe for cyber-attacks.

In this Issue:

Ransomware is a type of cyber-attack that has been on the rise. In fact, Statista, a leading source for market and consumer data has stated that the annual share of ransomware attacks experienced by organizations worldwide has been on the rise since 2018, peaking at 68.5 percent in 2021.

WHAT IS RANSOMWARE?

Ransomware is a type of malware that is normally delivered through a phishing (email) message. The phishing message entices the reader to click on a link or open an attachment. When the recipient falls for the phish, the process of infecting the device is started. It initiates a connection back to the attacker's device to receive instructions for encrypting the device. Once the encryption is completed, the user is locked out of their data and the device. At this point, a ransomware note is displayed, and a ransom is demanded in cryptocurrency (e.g. Bitcoin) to regain access to their data and their system.

BEST PRACTICES TO PROTECT AGAINST RANSOMWARE

- Do not open email from anyone you don't know, or you aren't expecting.
- Do not click on links in messages.
- Avoid opening attachments in messages. If you must download the attachment, scan them for malware before opening.
- If it sounds too good to be true, it probably is. Don't give away any personal information that could allow an attacker to compromise your devices or steal your identity.
- Install anti-virus/anti-malware software on your device and keep it up to date.
- Apply patches to all applications and your device's operating system as they become available.
- Don't browse suspicious sites. Cybercriminals count on users mistyping the name of a legitimate site. These sites are made to look like the legitimate site but are used to deliver malware to the device.

MORE ON THIS IN OUR NEXT ISSUE

HEADLINE NEWS:

Aussie Researcher Fakes Digital COVID-19 Vaccination Proof

Australia is developing digital certificates to show when individuals have been vaccinated against COVID-19. (Photo: Service Australia)

Australian software engineer Richard Nelson is warning that he was able to create a fake digital COVID-19 vaccine certificate via the government's Express Medicare Plus app. He says the agency in charge of the app has so far failed to acknowledge his bug report.

Sydney-based Nelson was part of a team of independent security researchers that last year identified serious flaws in Australia's digital contact-tracing app.

On Aug. 18, he detailed the vaccine certificate problems via Twitter, noting that he'd failed to receive a response from Services Australia, which is the federal government agency that developed the app.

Three weeks later, the bug still isn't fixed. Nelson worries the issue could be embraced by anti-vaccination campaigners for nefarious purposes. There's also the question of how fake certificates might pose an increased risk to public health. "If they're going to use it to allow people to go to restaurants or bars or even eat, how is someone supposed to check if what they're seeing is real or not?" Nelson asks.

Showing digital proof of vaccination will grow in importance. States such as New South Wales and Victoria remain in lockdown, and other states are on a knife's edge due to growing Delta cases. Some states and the federal government have promised looser restrictions for those who are vaccinated after states hit 80% double-dose vaccination rates.

It's still early days for exactly how people in Australia will show their vaccinated status. One method is via a government app on a person's phone. Another option is downloading a digital vaccination certificate and loading it into Apple's Wallet or Google's Pay apps, according to Services Australia.

The state of New South Wales has suggested it may incorporate digital proof of vaccination into its Service NSW app. The app is already used for checking into locations using QR codes, which then assist contact tracers.

Frequently Asked Questions:

WHAT IS CYBERSECURITY?

Cybersecurity refers to the specialization of computer network security that consists of technologies, policies, and procedures that protect networked computer systems from unauthorized use or harm. Broadly speaking, cybersecurity topics can be subdivided into two related areas: cyber-attacks, which are essentially offensive and emphasize network penetration techniques; and cyber defenses, which are protective and emphasize countermeasures intended to eliminate or lessen cyber-attacks. Cybersecurity Forum, 2021.

WHAT IS A CYBER-ATTACK?

Cyber-attacks are unwelcome attempts to steal, expose, alter, disable or destroy information through unauthorized access to computer systems.

In addition to cybercrime, cyber-attacks can also be associated with cyber warfare or cyberterrorism, like hacktivists. Motivations can vary, in other words. And in these motivations, there are three main categories: criminal, political and personal.

Cyber-attacks can take aim at the enterprise, government, military, and other infrastructural assets of a nation, companies, or its citizens, where these assets can include physical infrastructure (e.g., power grids, nuclear reactors) as well as computational infrastructure (e.g., computers, networks).

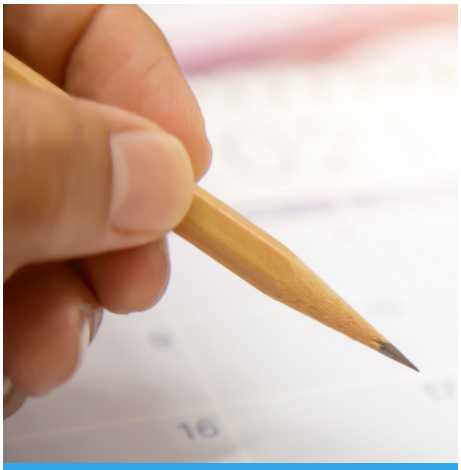
Cyber-attacks can be classified by their participating actors (states vs. non-states) and their attack mechanisms (e.g., direct attack, malware, exploits). Cyber-attacks can also be employed on end user devices such as mobile phones and tablets. Cybersecurity Forum, 2021.

WHY DO WE NEED CYBERSECURITY?

Cybercrime can disrupt and damage enterprise business. In 2021, for example, the average cost of a data breach was USD4.24 million globally and USD9.05 million in the United States. These costs include discovering and responding to the violation, the cost of downtime and lost revenue, and the long-term reputational damage to a business and its brand. And in the case of compromised Personal Identifiable Information (PII), it can lead to a loss of customer trust, regulatory fines, and even legal action.

Organizations can reduce cyber-attacks with an effective cybersecurity system. Cybersecurity is the practice of protecting critical systems and sensitive information from digital attacks, involving technology, people and processes. An effective cybersecurity system prevents, detects and reports cyber-attacks using key cybersecurity technologies and best practices, including:

- .Identity and access management (IAM)
- A comprehensive data security platform
- Security information and event management (SIEM)



Upcoming Events

A MASTER CLASS ON IT SECURITY: ROGER GRIMES TEACHES YOU PHISHING MITIGATION
Tuesday, Sep. 14, 2021
11:30 AM EDT

LIVE WEBINAR
THE STATE OF SECURITY 2021
Tuesday, Sep. 21, 2021
11:30 AM EDT

LIVE WEBINAR | SHAPING STRONGER SECURITY: HOW SECURITY LEADERS CAN MITIGATE AND RESPOND TO INSIDER THREATS IN A ZERO TRUST WORLD
Thursday, Sep. 23, 2021
2:00 PM EDT

ON-DEMAND | ENDPOINT SECURITY BREACH DEFENSE: CONNECTING THE MISSING DOTS, FAST
webinar is available On-Demand

IMPROVE CLOUD THREAT DETECTION AND RESPONSE USING THE MITRE ATT&CK FRAMEWORK
webinar is available On-Demand

868-610-7237
salesinfo@precision-cyber.com
www.precision-cyber.com
1st Floor, Brair Place, 10-12 Sweet Road
St. Clair, Port of Spain, Trinidad