precision
CYBERTECHNOLOGIES & DIGITAL SOLUTIONS LTD

CYBER DIGITAL WORLD

NEWSLETTER

Volume: 25 September 2023

As we approach Cybersecurity awareness month in October, this month's issue of our newsletter is going to highlight "User awareness in cybersecurity". We will look at the importance of building and improving our awareness and how we can become more aware of our cybersecurity posture.

Dr. Ronald Walcott
Managing Director

INTRODUCTION

In an increasingly interconnected digital landscape, the importance of cybersecurity has never been more pronounced. As our lives become more intertwined with technology, the risks of cyber threats and attacks grow exponentially. One crucial aspect of safeguarding our digital lives and assets is building user awareness in cybersecurity. In this age of data breaches, ransomware attacks, and phishing scams, educating individuals about the ever-evolving threats they face is not just a necessity; it's an imperative. This month's issue of our newsletter will delve into the significance of building user awareness in cybersecurity, exploring its role in protecting personal and organizational data, as well as its contribution to creating a more resilient and secure digital ecosystem.

WHY IS BUILDING USER AWARENESS IN CYBERSECURITY IMPORTANT?

Building user awareness in cybersecurity is of paramount importance in today's digital age for several compelling reasons. Here are some of those reasons:

1) **Mitigating Human Error:** Human error remains one of the most significant contributors to cybersecurity breaches. Users who lack awareness are more likely to fall victim to phishing emails, click on malicious links, or download infected files. By educating users about the common tactics used by cybercriminals and how to recognize potential threats, organizations can significantly reduce the risk of breaches caused by inadvertent actions.

2) **Protection of Personal and Sensitive Data:** Individuals store an immense amount of personal and sensitive information online, from financial data to personal communications. Without proper cybersecurity awareness, users may inadvertently expose this information to malicious actors. By understanding the value of their data and how to protect it, individuals can play a pivotal role in safeguarding their privacy and preventing identity theft or financial loss.

CONTINUED ON PAGE 3

In this Issue:

Frequently Asked Questions:

DOES BEING AWARE MEAN THAT I AM NO LONGER AT RISK OF BECOMING A VICTIM OF CYBER-ATTACKS?

While cybersecurity awareness significantly reduces the risk of falling victim to common cyber threats and enhances one's ability to recognize and respond to potential dangers, it should be viewed as one layer of a comprehensive cybersecurity strategy. Users should complement their awareness efforts with robust cybersecurity practices, such as using strong passwords, keeping software up-to-date, and employing security tools like firewalls and antivirus software.

HOW DO I ENSURE THAT PEOPLE AROUND ME USE WHAT THEY LEARNED FROM AWARENESS TRAINING?

Here are some strategies to help ensure that people put their knowledge into practice:

- **Lead by Example:** Be a cybersecurity role model. Demonstrate good cybersecurity habits in your own online activities, and share your experiences and insights with others.
- **Regularly Reinforce Key Concepts:** Cybersecurity is not a one-time lesson but an ongoing process. Periodically remind people of the essential principles they've learned, such as the importance of strong passwords, safe browsing habits, and recognizing phishing attempts.
- **Provide Real-World Examples:** Share news articles or case studies of cybersecurity incidents to illustrate the real-world consequences of lax security practices. These examples can make the potential risks more tangible and relatable.

ISN'T HAVING STRONG PASSWORDS AND ANTIVIRUSES ENOUGH PROTECTION?

Having strong passwords and using antivirus software are essential components of cybersecurity, but they are not enough on their own to provide comprehensive protection against a wide range of cyber threats. Cybersecurity is a multi-faceted discipline that requires a layered approach to effectively safeguard your digital assets and data.

Headline News

DarkGate Malware Operators on a Phishing Spree

Advertising on Russian-language criminal forums is paying off for the author of the DarkGate malware as reflected by a spike in infections, including an unusual phishing campaign on Microsoft Teams to deliver the loader through HR-themed social engineering chat messages. Cyber defenders first spotted the DarkGate commodity loader in 2018. Researchers from Deutsche Telekom in late August said the commodity loader's coder this summer began renting out the malware to a limited number of affiliates. "Before that, the malware was only used privately by the developer," the researchers said to explain the intensified email spamming campaign to lure victims into downloading DarkGate.

In June 2023, ZeroFox reported that someone claiming to be the original author of DarkGate had promoted access of the malware to just 10 people for an annual price of $100,000.

Researchers from TrueSec now said they've spotted threat actors abusing compromised Office 365 accounts to send phishing messages containing a DarkGate Loader malware on Microsoft Teams to an unnamed organization. The bait was a link to a SharePoint-hosted file named "Changes to the vacation schedule.zip." Microsoft Teams security features such as Safe Attachments and Safe Links did not detect or block the malicious attack, said TrueSec.

Researchers from Kaspersky said DarkGate's capabilities include hidden VNC, Windows Defender exclusion, browser history stealing, reverse proxy, file management, and Discord token stealing. The features "go beyond typical downloader functionality," they wrote.

Malwarebytes in late August uncovered an additional vector of DarkGate infection: malvertising. Bad actors behind the dropper bought ads on the Google search engine. Victims who clicked on the advertising saw a fake webpage masquerading as a popular network scanning tool offering a download containing the legitimate app "but also some extra files," i.e., DarkGate.

3) **Securing Organizational Assets:** Within a business or organizational context, employees are often the weakest link in the cybersecurity chain. Ignorance or negligence can lead to data breaches, ransomware attacks, and other security incidents that can have devastating consequences for the organization. Building user awareness ensures that employees understand their role in maintaining a secure digital environment, which is crucial for protecting sensitive corporate data and maintaining business continuity.

4) **Preventing Social Engineering Attacks:** Social engineering attacks, such as phishing and pretexting, rely on manipulating human psychology to deceive individuals into divulging sensitive information or taking harmful actions. When users are aware of these tactics and know how to recognize and respond to them, the effectiveness of such attacks is significantly reduced. This knowledge acts as a robust defense against tactics that prey on human trust and emotions.

5) **Enhancing Incident Response:** In the unfortunate event of a cybersecurity incident, users who are aware of best practices can play a crucial role in mitigating the damage. They can report incidents promptly, follow established incident response procedures, and avoid actions that might exacerbate the situation. This proactive involvement can help organizations recover more swiftly and minimize the impact of a breach.

HOW CAN USERS INCREASE THEIR CYBERSECURITY AWARENESS?

Users can increase awareness through a combination of education, training, and adopting best practices. Precision Cybertechnologies has partnered with KnowBe4 to provide security awareness training to users that will educate them and teach them best practices. Here are some key steps and strategies for individuals to enhance their cybersecurity awareness which Precision/Knowbe4 amplifies:

1) **Participate in Cybersecurity Training:**
   - Attend cybersecurity workshops, webinars, or seminars offered by reputable organizations, both online and in person.
   - Seek out free or low-cost online courses and tutorials that cover cybersecurity fundamentals.
   - Take advantage of training resources provided by your employer or educational institution.

2) **Stay Informed:**
   - Keep up-to-date with the latest cybersecurity threats, trends, and news through reputable sources such as cybersecurity blogs, news websites, and official government websites.
   - Subscribe to cybersecurity newsletters and mailing lists for regular updates.

3) **Understand Common Threats:**
   - Educate yourself about common cybersecurity threats, including phishing, malware, ransomware, social engineering, and identity theft.
   - Learn how these threats work and the tactics cybercriminals use to exploit vulnerabilities.
   - Learn how to identify possibly suspicious or malicious emails, files, programs, etc.

4) **Secure Your Devices:**
   - Keep your operating systems, software, and applications up-to-date with the latest security patches.
   - Use antivirus and anti-malware software on your devices and keep them updated.
   - Enable device encryption and use screen lock or password protection.

5) **Encourage Cybersecurity Awareness in Your Community:**
   - Share cybersecurity tips and best practices with family members, friends, and colleagues.
   - Promote a culture of cybersecurity awareness within your social and professional circles.

By actively engaging in these practices and continuously educating themselves about cybersecurity, users can significantly enhance their awareness and reduce the risk of falling victim to cyber threats. Additionally, promoting these habits within their communities can contribute to a safer online environment for everyone.

Upcoming Events

LONDON CYBERSECURITY SUMMIT
September 19th, 2023
London

AMCHAM HSSE CONFERENCE
October 31st, 2023
Trinidad & Tobago

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