precision
CYBERTECHNOLOGIES & DIGITAL SOLUTIONS LTD

CYBER DIGITAL WORLD

NEWSLETTER

Volume 7: Issue No. 1 March 2022

Today, we look at one of the most important aspects of cybersecurity that is usually overlooked; staff training.

Dr. Ronald Walcott
Managing Director

A NEED FOR A MORE ROBUST CYBER SECURITY

Small businesses are as much of a cyberattack target as large enterprises. But investing in enterprise cybersecurity alone is not going to cut it. small businesses need to invest in regular training for their employees in order to fully address this threat. This will help in adding yet another layer of protection for the company's sensitive data.

For this reason, it is important to assess the knowledge of your employees when it comes to cybersecurity. This is because more often than not, employees are the soft targets that scammers use to access your organization. With employees connected to the internet round the clock, businesses are more vulnerable than ever to attacks.

Almost every successful cyberattack reported in the media exploits the human factor. Fortunately, IT decision makers are increasingly aware of this. The most conscientious security chiefs are placing greater emphasis on staff training to secure their organization's perimeter.

SOME KEY POINTS REGARDING TRAINING

Responsibility for Company Data

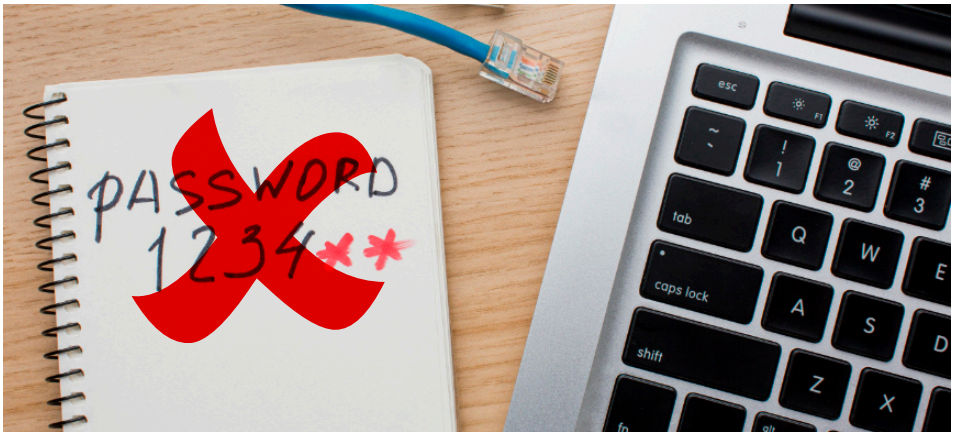
Continually emphasize the critical nature of data security and the responsibility of each employee to protect company data. You and your employees have legal and regulatory obligations to respect and protect the privacy of information and its integrity and confidentiality.

Document Management and Notification Procedures

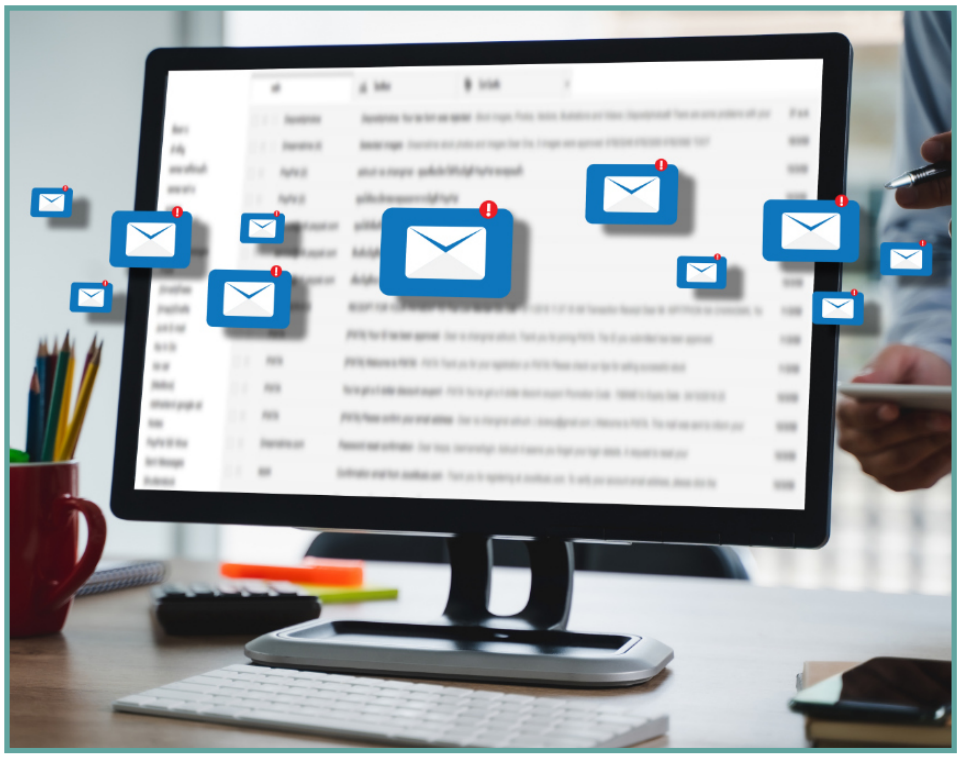
Employees should be educated on your data incident reporting procedure in the event an employee's computer becomes infected by a virus or is operating outside its norm (e.g., unexplained errors, running slowly, changes in desktop configurations, etc.). They should be trained to recognize a legitimate warning message or alert. In such cases, employees should immediately report the incident so your IT team can be engaged to mitigate and investigate the threat.

Passwords

Train your employees on how to select strong passwords. Passwords should be cryptic so they cannot be easily guessed but also should be easily remembered so they do not need to be in writing. Your company systems should be set to send out periodic automatic reminders to



In this Issue:



employees to change their passwords.

Unauthorized Software
Make your employees aware that they are not allowed to install unlicensed software on any company computer. Unlicensed software downloads could make your company susceptible to malicious software downloads that can attack and corrupt your company data.

Internet Use
Train your employees to avoid emailed or online links that are suspicious or from unknown sources. Such links can release malicious software, infect computers and steal company data. Your company also should establish safe browsing rules and limits on employee Internet usage in the workplace.

Email
Responsible email usage is the best defence for preventing data theft. Employees should be aware of scams and not respond to email they do not recognize. Educate your employees to accept email that:

- Comes from someone they know.
- Comes from someone they have received mail from before.
- Is something they were expecting.
- Does not look odd with unusual spellings or characters.
- Passes your anti-virus program test.
- Social Engineering and Phishing

Train your employees to recognize common cybercrime and information security risks, including social engineering, online fraud, phishing and web-browsing risks.

Social Media Policy
Educate your employees on social media and communicate, at a minimum, your policy and guidance on the use of a company email address to register, post or receive social media.

Mobile Devices
Communicate your mobile device policy to your employees for company-owned and personally owned devices used during the course of business.

Protecting Computer Resources
Train your employees on safeguarding their computers from theft by locking them or keeping them in a secure place. Critical information should be backed up routinely, with backup copies being kept in a secure location. All of your employees are responsible for accepting current virus protection software updates on company PCs.

Frequently Asked Questions:

WHAT IS CYBER THREAT MITIGATION?
In the context of cyber threats mitigation refers to reducing the severity or damage caused by cyber-attacks. Compare with cyber threat remediation, which refers to a more effective counter measure.

WHAT IS A PHISHING EMAIL?
Criminals want to trick you into giving your information to them – this is known as phishing. They're hoping that you'll click on fake links to sites or open attachments, so they can steal data or install malicious software. Malicious emails account for nearly three quarters of security breaches or attacks. It's often a good idea to pass round screenshots of any phishing emails that have been received by staff to make sure everyone is aware of them and can more easily identify any future suspicious emails.

Upcoming Events

PACIFIC NORTHWEST US CYBERSECURITY SUMMIT
March 22, 2022

CLOUD DATA SECURITY SUMMIT
March 29, 2022

HEADLINE NEWS:

US Officials Push Collaboration, AML Controls for Crypto

High-ranking U.S. officials say that while it would be nearly impossible for Russia to "flip the switch" and convert to cryptocurrency to stabilize its sanctioned economy, they caution that Russian elites and entities may yet try to skirt the measures by transferring and obfuscating funds across the blockchain.

In an event hosted by the blockchain analytics firm TRM Labs on Friday, Todd Conklin, counselor to the deputy secretary of the U.S. Treasury Department, and Carole House, director of cybersecurity and secure digital innovation for the White House National Security Council, outlined the unprecedented federal activity over the past week that has hobbled Moscow and aims to choke Russia's economy as it continues its military campaign in Ukraine.

The experts discussed the growing threat of eventual cyber escalation in the conflict, with the sanctioned Russian President Vladimir Putin potentially lashing out at the U.S. or its Western allies by infiltrating critical infrastructure or government agencies. To allow Russia to make such manoeuvres, and as its currency - the ruble - falters, foreign policy experts have suggested the Russians may resort to bulk cryptocurrency transactions.

This aligns with previous reports of North Korea allegedly using ill-gotten crypto gains to fund its ballistic missile program, or Iran reportedly mining bitcoin to skirt sanctions and infuse its economy with hundreds of millions of dollars in cash

Source: https://www.databreachtoday.com

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