precision
CYBERTECHNOLOGIES & DIGITAL SOLUTIONS LTD

CYBER DIGITAL WORLD

NEWSLETTER

Volume: 10 June 2022

Today, we'd like to recap on our webinar, which took place on the 13th of June. With several speakers involved, we looked at cyber preparedness, awareness and surviving different attacks.

CYBER PREPAREDNESS

Dr. Ronald Walcott
Managing Director

With the current shift globally to a digital platform where we're always connected, be it for work or personal use, the clear need for cyber security is at an all time high. As the world becomes connected, more so than ever (even a modern fridge can connect to the internet) we provide a larger surface area for attackers to find vulnerabilities and backdoors into our networks and devices. With this in mind, as an organization scales with more connected devices, the security surrounding should also be scaled to suit. The key to corporate resilience does not only reside among being prepared (before an incident), but also the coordination and management during and after. With the evolving risk and dynamic landscape, the best option for many organizations would be outsourcing to a managed service to either work in conjunction with internal IT departments, or a fully outsourced solution.

For a more in depth look at cyber crisis management, a PDF document is available from one of our partners, Deloitte.

CREATING A CYBER AWARE CULTURE

The concept of cyber security culture speaks to the entire workforce of an organization and the way they act, react and engage or interface with the organization. Essentially cybersecurity should be second nature to all employees revolving around all access to company networks and data. This can range from opening E-mails or simply downloading a document. Through consistent training and keeping them engaged and updated, this can aid in ensuring cybersecurity is a priority.

We can look at Cultivating a cyber risk-aware culture a bit more here from Deloitte.

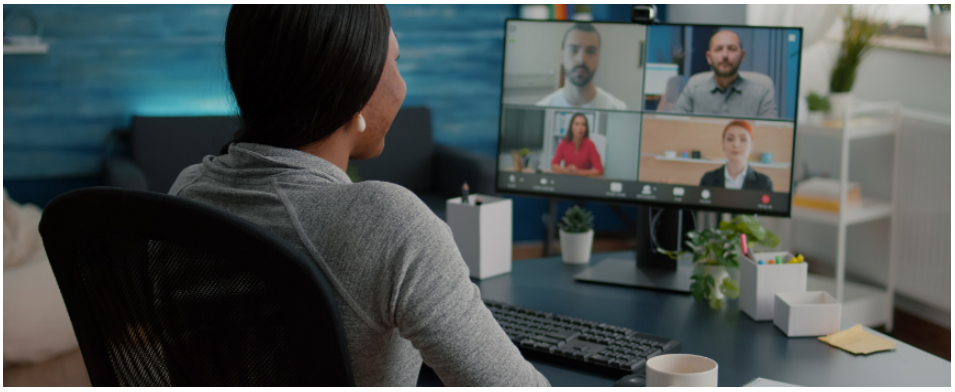
SURVIVING SOCIAL ENGINEERING & RANSOMWARE ATTACKS

We've spoken about ransomware at various depths within our past newsletters, so let's take another look at social engineering.

Social engineering attacks are used to gain control over a system or personal information. This attack relies solely on humans. An attacker will try to gain the victims trust so they can potentially reveal sensitive information.

Here are a couple types of social engineering attacks –

Baiting: it is a type of social engineering that uses a false promise to lure a victim into the trap. The trap could be in the form of a malicious attachment with an enticing name.



In this Issue:

Tailgating: it is a physical breach where an unauthorised person manipulates the way into a restricted area or an employee-only authorised area through the use of social engineering attacks.

Of course, there are also several ways to safeguard yourself –

Do not open any email or email attachments from suspicious sources.

1. Use Multi-Factor Authentication.
2. Protect your WIFI network.
3. Use VPN.
4. Install and update antivirus and other software.
5. Back up your data regularly.

While these are not the only ways to safeguard yourself, they are however crucial points to take understand and implement.

Our entire Webinar can be watched at your own pace via our YouTube channel!

Frequently Asked Questions:

IS SOCIAL ENGINEERING ILLEGAL, AND WHAT IS THE PENALTY?

Social engineering is illegal and is a form of fraud. There are severe legal penalties for people who are convicted, including fines and jail terms.

WHY IS SOCIAL ENGINEERING DANGEROUS?

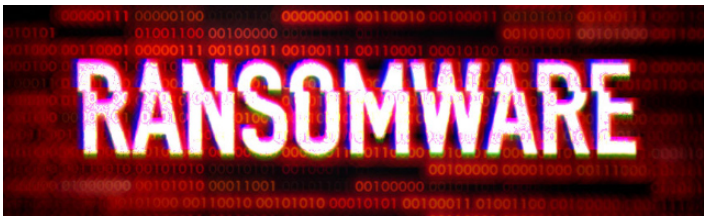
Social engineering is dangerous because it exploits human error rather than relying on finding a fault or weakness in software, applications, or networks. Cybercriminals are prepared to spend time and resources researching potential victims, looking for opportunities in their behaviours or the policies of the company that employs them.

HOW TO PREVENT SOCIAL ENGINEERING ATTACKS

The most effective defence against social engineering is education

Headline News:

Ransomware-as-a-Service Gang LockBit Has Bug Bounty Program



A ransomware group is taking a page out of the white hat hacker playbook to offer a bug bounty program for researchers willing to aid in cybercriminality.

The LockBit ransomware-as-a-service group says it will pay individuals who find exploitable vulnerabilities as well as bugs in the software it uses to maliciously encrypt files that would allow victims to rescue their data.

"We invite all security researchers, ethical and unethical hackers on the planet to participate in our bug bounty program. The amount of remuneration varies from $1000 to $1 million," the group posted on its website, according to malware repository vx-underground. Bug bounties are programs intended to incentivize responsible disclosure of vulnerabilities by enticing researchers to submit their findings to the responsible vendor.

LockBit's largest payout is reserved for anyone who reveals the real identity of the group's affiliate program boss.

The prolific ransomware gang tied the announcement of its bounty to the rollout of a new version of its presumably improved malware, LockBit 3.0.

"Make Ransomware Great Again!" the group says.

Source: https://www.databreachtoday.com/

Upcoming Events

HYBRID CYBERSECURITY SUMMIT: BENGALURU
July 7, 2022

HEALTHCARE CYBERSECURITY SUMMIT
JULY 12, 2022

GOVERNMENT CYBERSECURITY SUMMIT
July 26, 2022

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