DIGITAL SECURITY PRINCIPLES: HOW TO PROTECT YOURSELF AND WHAT TO DO IN A CRISIS?

In today's digital landscape, our online activities mirror real-life processes. Just as in the physical world, nobody is completely immune to fraud, theft, deception, and other threats on digital platforms. The evolution of digital technologies and services has paved the way for many inventive methods for dishonest individuals or organizations to access and exploit data for their own good. However, real-world security measures like locking doors and setting alarms, do have equivalents in the digital realm, so that we can identify risks and safeguard ourselves against cyberattacks.

What is a cyberattack?

A cyberattack refers to the deliberate efforts of cyber criminals, hackers, or other malicious actors to infiltrate a computer, phone, or system. The primary objectives of a cyberattack typically involve altering, stealing, or destroying information. These activities may be driven by financial, political, or even competitive business motives.

The most popular types of cyberattacks include:

- ***Malware.*** Any program or code intentionally designed to harm a computer, network, or server. It is the most prevalent type of cyberattack.

- ***Denial of Service (DoS) Attack.*** A targeted attack that floods a network with fake requests, aiming to disrupt business operations. During a DoS attack, users are unable to perform routine tasks like accessing email, websites, or other online resources.

- ***Phishing.*** A cyberattack that utilizes various channels such as email, SMS, phone calls, social media, and social engineering tactics to trick victims into sharing sensitive information like passwords or account numbers. Phishing is commonly used as a means to distribute malware.

Baltic Centre for Media Excellence
Google

- ***Impersonation attack.*** This involves attackers impersonating trusted sources, such as spoofing email or website domains, to deceive victims. These attacks are typically aimed at stealing information, extorting money, or installing malware or other malicious software on devices.

How to protect yourself?

An organization's digital security hinges greatly on its employees' awareness of various risks, the organization's resources, and its overall level of preparedness, including "cyber hygiene"—the practice of daily habits that mitigate the risk of cyberattack. Cybersecurity relies on the organization's information and communication technologies system being in place and familiar to its users. Remember – only the equipment and protocols established before a crisis will be available during one. Here are 9 questions to assist you in preparing and being ready for a cybersecurity crisis.

1. Has a risk assessment been carried out?

Every organization faces specific digital security risks, contingent on its scope, objectives, business partners, and the IT products and services it uses. It's crucial for the organization to evaluate the equipment and software employed in its workflows, determine who has access to them, identify the email service host, and ascertain how employees access their email. Additionally, the organization should identify areas of activity associated with potential threats to IT products and services, such as website server administration and maintenance—whether outsourced or handled internally. In order to reduce the likelihood of an attack and the potential severity of consequences, each IT product, service, and associated activity has to have a separate risk assessment done. Regular checks should be implemented, involving recurring risk analyses and reviews of existing security measures and protocols.

2. Are you storing data and is it backed up?

One of the most significant threats to digital security is the potential loss, corruption, or temporary inaccessibility of an organization's data. To mitigate this risk, implementing an understandable and trustworthy data storage and backup system is essential. The organization should outline what data is stored, its location, and which employees have access to it. It's noteworthy that cyber attackers often target corporate network backups, underscoring the importance of storing backups in a separate environment disconnected from the core network. Additionally, enabling remote access to necessary data for all employees, possibly through cloud technologies, is vital for maintaining operations during a crisis.

3. What is the staff's understanding of cyber hygiene?

Regardless of the investments made in information technology products and services, the security of an organization's data, systems, and equipment hinges on its employees' comprehension of cyber hygiene. Employees who can recognize threats at the user level contribute significantly to the organization's overall security posture. It’s important to organize regular staff training sessions to enhance cyber hygiene awareness. If the organization lacks resources to provide such training, there are various institutions that support public sector organizations in delivering education on IT security.

How to comply with cyber hygiene:

- ***Update the software.*** Stay current with software updates for your computers and phones as per the manufacturer's recommendations. Only download updates from verified sources such as trusted software stores like App Store or Google Play.

- ***Regularly delete unused apps.*** Delete apps and programs from smart devices and computers that are no longer in use to reduce potential security risks.

- ***Personalize app permissions.*** When installing a new app on your phone, review the data it requests access to and consider whether it's necessary. For instance, question why the Instagram app needs access to your contacts list or microphone function if you don't use these features.

- ***Be cautious with unknown emails.*** Verify the legitimacy of emails from unknown senders. If anything in the email seems suspicious, exercise caution.

- ***Beware of suspicious attachments and links.*** Avoid clicking on links or opening attachments from unfamiliar or suspicious emails, as they may contain phishing attacks. If you encounter such emails, switch from HTML to plain text in the email view settings to reveal the real source of the links and prevent automatic execution of third-party scripts.

- ***Change your passwords.*** Update the passwords regularly and avoid using the same password across multiple platforms. Use a freely available password manager like Bitwarden or Keepass to organize your passwords securely. When creating a password, ensure it consists of a mix of letters, numbers, and symbols. For extra safety think of something unconventional and impossibly difficult to guess (e.g., MysteriousRaccoon21!).

- ***Enable two-factor authentication whenever possible.*** Use applications like Google Authenticator, that provide an additional layer of security by requiring a unique combination of numbers alongside the password when logging into your profile.

4. Who has the admin rights for different systems and devices?

The equipment, including computers, mobile phones, cameras, and software purchased by the organization, are the property of the organization. Therefore, these systems must be centrally managed and utilized solely for work-related tasks. To facilitate this, there should be one individual responsible for managing and overseeing the organization's information technology infrastructure. This individual should ensure regular maintenance and updates of the IT assets. Additionally, they are responsible for ensuring that staff members understand cybersecurity and adhere to established digital safety procedures. This includes enforcing password complexity requirements, discouraging password reuse, promoting the use of two-factor authentication where possible, and other relevant security practices.

5. How does the staff log in on social media platforms, and email?

In the media industry, engaging with various online communication and social media platforms is essential. These platforms are accessed not only from work computers but also from personal devices

like phones. It's crucial for each employee to create unique usernames and passwords for their accounts and to enable two-factor authentication for added security when logging in. Several apps and services, such as Google Authenticator or Microsoft Authenticator, offer two-factor authentication options. Selecting the most suitable tool or service provider that aligns with your organization's needs and capabilities is important.

6. How is data shared and exchanged?

Organizations often encounter cyberattacks through malicious emails aimed at accessing the organization's data and information. Implementing encrypted data exchange, particularly for emails, is advisable to enhance security. Encryption converts the content of an email from plain text into encrypted text, accessible only to the intended recipient. This functionality, provided by services like Microsoft 365 subscriptions, helps safeguard sensitive information. For instance, the American Cybersecurity Protection Agency has outlined guidelines for enhancing email security.

7. What communication channels are used for each purpose?

Organizations and their employees rely on various communication channels such as email, chat apps, etc., on a daily basis. When outlining plans to address different crises, it's crucial to determine and agree upon which communication channels will be utilized during a crisis situation in advance. Clear guidelines should be established regarding the assignment of channel administrator rights, preferably designated to at least two trustworthy individuals. During a crisis, it's advisable to maintain access to two communication channels for staff members: one primary channel that is typically used for daily communication and another backup channel on a different chat app. This ensures continuity of communication even if the primary channel encounters technical issues. The crisis action protocol should outline when and how each communication channel should be used to ensure swift and effective dissemination of information.

8. What should the employees do in the event of a cyberattack?

Cyberattacks manifest in various forms, often leaving individuals unaware that their computer, email, or mobile phone has been compromised. To foster employee awareness and responsiveness, organizations should cultivate an environment where reporting suspicious emails, unusual messages in communication apps, or strange device behavior is encouraged. It's essential that employees feel safe to report suspicions without fear of condemnation or ridicule, even if the concern turns out to be unfounded. Establishing a reporting protocol detailing how and to whom to report suspicions to

systematizes and organizes this process. The more freely employees can express their concerns, the better equipped the responsible person will be to identify risks and ensure the organization's cybersecurity.

RESILIENT BALTICS

9. **Are you ready to react?**

Create action protocols outlining the steps employees should take if the organization faces a threat to its IT products and services due to a cyberattack or other crises (e.g., like floods or fires). Regularly update this information and ensure that all employees are well-informed about crisis procedures.

Digital Security in a Crisis

When the crisis stems from a compromise of the organization's information technology products and services, such as a cyberattack or data leak:

1. Recognize the scale of the situation. Quickly assess the extent of the crisis and isolate the compromised information technology products and services to prevent further spread of the attack.
2. Inform employees. Communicate the crisis situation to employees and provide clear instructions on the necessary steps to resolve it.
3. Isolate compromised equipment. Disconnect the compromised equipment from the corporate network to contain the impact of the attack.
4. Analyze and develop a recovery plan. Investigate the attack or data leak to determine its cause and develop a comprehensive recovery plan. Activate the crisis protocol and adapt it to address the specific situation.

If the crisis is unrelated to the compromise of the organization's information technology products and services:

1. Activate approved internal communication channels. Use only the internal communication channels specified in the crisis protocol.
2. Follow the guidelines. Ensure adherence to the guidance outlined in recommendations 2, 3, 5, and 6.
3. Verify data security. Confirm the availability of necessary data on cloud platforms and ensure backup copies are accessible.
4. Protect critical resources: Take measures to safeguard the organization's critical resources amidst the crisis.

Author: Zane Štāla
Editor: Krista Priedīte

Baltic Centre for Media Excellence
Google