VMGROUP

Tips for Good Cyber Security Hygiene

Cyber Security Awareness

1/9

www.vmgroup.ie 01 524 1630 info@vmgroup.ie D15 N28X

VMGROUP

01

Train your Employees

Employees and emails are a leading cause of data breaches for businesses because they are a direct path into your systems. Training employees on basic internet best practices can go a long way in preventing cyber-attacks. Does the email look suspicious? Don't click on it. The ABCs of cybersecurity are Always Be Cautious. Double-check where emails come from before responding, especially if something sounds off.

Training topics to cover include:

- ***Spotting a phishing email***
- ***Using good browsing practices***
- ***Avoiding suspicious downloads***
- ***Creating strong passwords***
- ***Protecting sensitive customer and vendor information***
- ***Maintaining good cyber hygiene***

VMGROUP

02

Use Antivirus Software and keep it Updated

Ensure each of your business's computers is equipped with antivirus software and antispyware and updated regularly. They should all be controlled centrally. It is recommended to update the database daily to have the latest protection against malware.

03

Secure your Networks

Safeguard your Internet connection by using a firewall and encrypting information. If you have a Wi-Fi network, ensure it is secure and hidden.

To hide your Wi-Fi network, set up your wireless access point or router, so it does not broadcast the network name, known as the Service Set Identifier (SSID).

Password-protect access to the router.

04

Use Strong Passwords and Multifactor Authentication

Using strong passwords is an easy way to improve your cybersecurity. Be sure to use different passwords for your other accounts.

A strong password includes:

- **12 characters or more**
- **At least one uppercase letter**
- **At least one lowercase letter**
- **At least one number**
- **At least one special character**

Enforce MFA on all systems. Do not use a single password on multiple systems.

05

Employ Device Encryption

While most companies automatically have data encryption processes in place, you also may want to encrypt your devices and other media that contain sensitive data — including laptops, tablets, smartphones, removable drives, backup tapes, and cloud storage. In fact, many devices use encryption as the default for data stored on smartphones. Some apps are using end-to-end encryption, and other services encrypt data on your devices and back them up in the cloud. Another option is to use an encrypted USB memory stick for protecting sensitive data.

06

Vulnerability Management Program

Ensure that your systems are patched regularly and avoid using legacy systems. Legacy systems are often at the heart of cyber breach incidents. Depending on the size of the network, run a *weekly scan* to identify vulnerabilities. Always stay updated with your vendors on critical vulnerabilities and address them accordingly. Review vulnerability reports and ensure that patching is running correctly. It is recommended to *Pen test all internet-facing servers at least once a year.*

07

BCP and Incident Response Plan

Have an incident response plan. Identify the types of incidents that may occur and have a plan on how to address them. Identify who will be required in the event of an emergency and have them documented in the plan. Update the plan at least annually. Keep a copy offline in case of emergencies.

Test the plan.

Firstly, perform a tabletop test. Decide what is working and what is not. Invite different departments to participate.

VMGROUP

08

Backups

Backups are a vital part of cyber security. Should you be infiltrated, it is the best way to recover. Back up regularly and keep the backup segregated.

Test the backups frequently. Ensure that the backup process is working correctly. Perform a full DR at least once a year of key systems. If the backups have not been tested, they may not work.

At VMGroup, we emphasise the critical role of proactive measures in safeguarding your business from cyber threats. By training employees to recognise and respond to potential threats, implementing strong password policies and multifactor authentication, securing networks, and keeping systems updated with the latest antivirus protections, you lay a solid foundation for cybersecurity.

LEARN MORE