MyDigitalSME x Cisco Umbrella Episode 1

Learn The 1-2-3s of Cyber Security

Know the steps you could be taking to help prevent cyberattacks on your business with Digi Business and Cisco Umbrella.

Malware

Malware is the collective name for a number of malicious software variants, including viruses, ransomware and spyware. And all these are designed to cause extensive damage to data and systems or to gain unauthorized access to a network.

How can the people of today protect themselves from Malware?

1. Secure your network by adding layers of security such as having a firewall in place to safeguard and monitor access to your network
2. Use multi-factor authentication to verify your user every step of the way, even on the go.
3. Encrypt your data to ensure that even in the event of an emergency, your data will not be exploited or be permanently lost.

Distributed Denial of Service (DDoS)

A distributed denial-of-service (DDoS) attack is a malicious attempt to disrupt the normal traffic of a targeted server, service or network by overwhelming the target or its surrounding infrastructure with a flood of Internet traffic.

What are some of the prevention methods to block DDoS attacks?

1. Secure your network by adding layers of security such as having a firewall in place to safeguard and monitor access to your network.
2. Use multi-factor authentication to verify your user every step of the way, even on the go.
3. Encrypt your data to ensure that even in the event of an emergency, your data will not be exploited or be permanently lost.

Phishing

Phishing attacks are fraudulent communications that appear to come from a reputable source and are commonly conducted over emails. The goal is to trick the recipient into giving away sensitive data or to install malware in the form of spyware on the victim's system.

How can businesses protect themselves from Phishing?

1. Never click links in an email that seems suspicious
2. Have a two-factor authentication system installed as an extra layer of protection
3. Conduct security awareness training so your own employees know the best practices to avoid phishing emails

MyDigitalSME x Cisco Umbrella Episode 2

Common Cyber Security Questions - Answered

Know the answers to all your cyber security-related queries as we unpack all the common questions SMEs are asking

Should my employees be cautious about clicking on suspicious links?

Yes. Employees need to be vigilant by not clicking any suspicious links or downloading attachments. Here are some best practices:

- **Avoid suspicious pop-ups, unknown emails,** and links
- Connect to **secure Wi-Fi** or use a virtual private network (VPN) if you're working remotely
- Embrace **education and training** and know the cybersecurity policies in your company

Is it important to encrypt databases and customer information in a company?

Yes. And here's why:

- It **prevents security attacks** and intruders will not be able to breach data.
- It helps to protect remote workers and **prevents cybercriminals from intercepting** unsecured public Wi-Fi connections
- It **increases consumer trust.** By complying to certain encryption standards, this could give you a competitive advantage.

Should my employees be required to change their passwords often?

Yes and here are some best practices:

- We recommend using **random words** rather than words from the dictionary.
- Remember to **avoid basic information** that cyber criminals can easily guess such as your birthday and your name.
- Make sure these **random words add up to at least 12 characters.** You can convert a phrase to an Acronym or choose a phrase you can remember and use the first letters of each word.

What is DNS layer security and how does this help my business?

Domain name system (DNS) layer security acts as the first line of defense. It **stops malware earlier** and **prevents callbacks** to attackers if infected machines connect to your network. It's the primary target of cyberattacks as people tend to pay less attention to it.

How to ensure employees can access what they need safely?

It comes down to access control. This means giving employees the correct level of access to match their responsibilities This will

- **Keep data** safe from remote access attacks
- Limit social engineering attacks
- **Prevents confusion** and streamlines responsibilities

Can my employees use personal devices for work purposes?

Yes. With the work-from-home culture, businesses should supply the necessary tools to enable their employees to function adequately from home. But we must understand, many businesses face a cash flow problem and can't afford the expenditure. Hence many resort to using personal devices.