CYBERSECURITY AWARENESS

Stop employees from being the weak link

learn how to spot and avoid cyber dangers

Cybersecurity awareness training can help employees learn how to spot dangers and give them the tools needed to avoid being exploited by criminals for access to business and client data.

One of the most common types of cybersecurity threats is phishing, where attackers try to trick people into giving them sensitive information. Ransomware is another type of threat that can be particularly damaging to businesses.

Why cybersecurity awareness training? To help employees:

- **Understand and recognize cybersecurity risks**
- **Know how to protect themselves and their company from these risks**
- **Know what to do if they suspect or experience a cybersecurity breach**
- **Stay up-to-date on the latest cybersecurity threats and trends**

Train your employees so they become your first line of defense against cyber attacks.

Three of the common cyber dangers causing businesses pain and costing them money are:

- **Phishing scams**
- **Ransomware**
- **Malware and viruses**

Preparation is key in any endeavor, but it's even more critical in protecting your business from cyber attack.

Cybersecurity awareness training can help employees learn how to spot and avoid these threats. Additionally, having a cybersecurity plan in place can help minimize the damage if a business is hit by a cyberattack.

1. **Awareness -** In order to protect your company from cyber threats, all employees should be aware of best practices for cybersecurity.

2. **Links -** Employees should never click on links or attachments from unknown senders, even if the email looks legitimate.

3. **Email -** If an employee receives a suspicious email, they should report it to their IT department or security team immediately.

4. **Credential sharing -** Employees should never give out their username or password to anyone, even if they seem trustworthy.

5. **Credential strength -** Employees should practice good password hygiene by using strong and unique passwords for each account.

6. **Multi-factor Authentication -** Employees should enable two-factor authentication (2FA) whenever possible to add an extra layer of security to their accounts.

7. **Public platforms -** Employees should be careful about what information they share on social media or public places.

8. **Reporting -** If an employee suspects that their account has been compromised, they should report it to their IT department or security team immediately.

The business benefit of being cyber aware

- **Lower your cyber risk profile**
- **Improve your uptime potential**
- **Reduce financial risk to the company**
- **Help meet cyber awareness training requirements for insurance**
- **Help guard employee, customer, and business data**

Need more information?

MF Telecom Services

www.mftelecomservices.co.uk

ben.capas@mfts.uk

01892 577577