mason
INFOTECH

An SME Owner’s Guide to Cyber Security

Contents

Threats Facing SMEs

Phishing Attacks: Phishing is a common tactic where attackers deceive individuals into revealing personal information or clicking on malicious links. This can lead to data breaches or financial loss.

Malware: Malware, including viruses, trojans, and spyware, can infect business systems, causing significant damage and data loss.

Ransomware: Ransomware encrypts a company's data, rendering it inaccessible until a ransom is paid. This can disrupt operations and lead to substantial financial loss.

Data Breaches: Unauthorised access to sensitive data can result in the theft of customer information, intellectual property, and financial records.

Insider Threats: Employees or contractors with access to critical systems can inadvertently or maliciously cause security breaches.

Where to start

Firstly, conduct a security risk assessment. Start by identifying potential risks and vulnerabilities in your business. A thorough risk assessment can help prioritise areas that need immediate attention. Mason Infotech's cybersecurity specialists can assist in evaluating your current security posture and recommending improvements.

Free Audit: Mason Infotech offers free, no obligation cybersecurity audits to all prospective new clients. This covers things like your network, hardware, and 3rd party apps.

Dark Web Scan: Also free of charge, you can scan the dark web to see if your credentials have been sold by cybercriminals. This takes a few seconds, and all we need is your email domain.

Our managed security services for small business bring enterprise-grade managed security to SMEs. We help businesses to stay safe and compliant through proactive management of bleeding-edge technology and a wealth of expertise.

Implement strong passwords

Ensure that employees use strong, unique passwords for all accounts.

Encourage the use of password managers to securely store and manage passwords.

Regularly update passwords and enforce multi-factor authentication (MFA) to add an extra layer of security.

Educate and Train Employees

Cybersecurity awareness training is essential for all employees.

Regular training sessions should cover topics such as identifying phishing emails, safe internet practices, and proper data handling procedures.

Educated employees are often the first line of defense against cyber threats.

Software

Utilise comprehensive security software to protect against malware, viruses, and other cyber threats. Firewalls, antivirus programs, and intrusion detection systems are fundamental components of a strong cybersecurity framework.

Shadow IT: Shadow IT is the name given to software used by employees that may not have been approved by management. This can be anything from productivity tools like Trello, or AI products like ChatGPT. It’s important that employees understand how shadow IT impacts your business’s cybersecurity posture.

3rd Party Apps: As with above, if you use a 3rd party application like Microsoft 365, Sage, or Hubspot, it’s important to understand where your data is stored. Larger providers usually map their solutions alongside regulations, but it’s always important to double check.

Cybersecurity Tools: There’s a whole world of specific cybersecurity tools available to help businesses improve their security posture. XDR, Firewall-as-a-service, and mail filters are all examples of these.

Backups

Regular data backups are essential to protect against data loss due to cyber attacks. Store backups securely and ensure they are tested periodically to verify their integrity and availability.

Microsoft 365: Microsoft are only liable for your data up to a point, it’s important to have external backups in case of emergency. Backing up your Microsoft 365 data can protect you from things like accidental data loss or deliberate attacks like ransomware.

Servers: If you’re running applications on your server, or storing things like customer information, backing up can protect you from downtime if you have an incident.

3rd Party: Lots of businesses supplement their main businesses apps with additional products like Google Drive. Take stock of where you store data, and if it’s business critical, back it up.

Incident Response Plan

Prepare for potential cyber incidents by developing a response plan. This plan should outline steps to take in the event of a security breach, including communication protocols and recovery procedures. Having a plan in place can minimise damage and ensure a swift response.

Collaborating with Mason Infotech's IT security experts is crucial for small businesses that lack in-house cybersecurity expertise. Our cybersecurity experts can provide valuable services such as:

- **Risk Assessments and Audits:** Identifying vulnerabilities and recommending tailored security measures.
- **Implementation of Security Solutions:** Installing and configuring advanced security tools and software.
- **Ongoing Monitoring and Support:** Continuously monitoring systems for threats and providing support to mitigate risks.
- **Compliance Assistance:** Ensuring that your business complies with relevant cybersecurity regulations and standards.

mason
INFOTECH

Found this content valuable?

Click the link in the post above to learn more about Mason Infotech's Cybersecurity solutions, or book your free dark web scan today.

T: 0115 940 8040
E: ask@masoninfotech.co.uk