Greater Manchester | Greater Security | Greater Business
Cyber Foundry

21 Useful Cyber Security Terms for SMEs

A quick reference glossary of common terms

Audience: General   Reading Time: 5 Mins

In today's digital age cyber security is both relevant and highly important to small and medium sized enterprises (SMEs). With cyber threats evolving rapidly, it is crucial for SME owners and managers to be familiar with the fundamental concepts of cyber security.

Cyber Security is a field that is fraught with many different terms and acronyms that can be rather bewildering for those who do not work in the industry. Here we present a comprehensive list of 21 commonly used terms that SMEs need to understand to protect their valuable assets. From malware and phishing to encryption more, these terms will empower SMEs to navigate the complex world of cyber security, and fortify your SME against cyber threats with this essential knowledge:

Malware: Is a portmanteau of 'malicious software', and it is designed to harm computers. This malicious software encompasses things like viruses, worms, ransomware, and more. The programs are designed to infiltrate and damage computers without consent. To protect from these, it is crucial to have reliable, up-to-date antivirus software and to avoid downloading files or clicking links from unknown sources. Best practice is for businesses to invest in good antivirus software and educate their employees about the risks of downloading from untrusted sources.

Phishing: Phishing attacks are fraudulent attempts to obtain sensitive information. Cybercriminals attempt to trick people into sharing sensitive information such as passwords or credit card numbers by disguising themselves as trustworthy entities in email or other communication. SMEs can protect against this by training employees to recognise suspicious phishing attempt emails and never to disclose sensitive information. Technical solutions such as email filtering, can further help prevent phishing attacks.

Ransomware: is a type malware that encrypts files. This type of malicious software is designed to block access to

European Union
European Regional
Development Fund
The Cyber Foundry project is part funded by the European Regional Development Fund

Lancaster University

MANCHESTER 1824
The University of Manchester

Manchester Metropolitan University

University of Salford MANCHESTER

a computer system until a sum of money is paid. Regular backups of data can mitigate the effects of a ransomware attack, and strong security software can prevent it altogether.

Firewall: A firewall is a network security system that monitors and controls incoming and outgoing traffic. This digital barrier blocks unauthorised access to your computers and devices. Firewalls are usually included as part of a comprehensive security software suite and should be kept updated to guard against the latest threats. Good practice is for SMEs to have a robust firewall system and ensuring proper configuration.

Intrusion Detection System (IDS): This is a system that monitors network traffic for suspicious activity and known threats, sending out alerts when it finds something potentially dangerous. A good IDS can help catch threats before they cause damage.

Encryption: This is the process of converting data into a code to prevent unauthorized access. Businesses can use encryption to protect sensitive information like customer data, both at rest and in transit, ensuring it is unreadable to anyone who does not have the decryption key.

Two-Factor Authentication (2FA): 2FA is a security process where a user provides two different authentication factors to verify themselves. For instance, this might be a password and then a unique code sent to a smartphone. This adds an extra layer of security greatly enhancing the security of your accounts.

Virtual Private Network (VPN): A VPN provides a secure connection over the internet to keep data private. This is particularly important for anyone working remotely to ensure their internet connection is secure. Ideally, businesses should provide a VPN for employees accessing work systems remotely.
Security Patch: This is a software update designed to fix vulnerabilities that could be exploited by hackers. Regularly updating software ensures you have the most recent security patches, safeguarding your systems against known issues.

Security Audit: A security audit is a systematic evaluation of an organisation's adherence to regulatory guidelines. Audits may involve the review of physical security controls, IT and information handling practices, and the specific ins and outs of a company's network. Regular security audits can help SMEs find and rectify weaknesses.

Penetration Testing (Pen Test): A simulated cyberattack against a computer system to check for vulnerabilities. Regular pen tests can help SMEs find and mitigate against weaknesses.

Password Management: The practice of using, storing, and managing passwords securely. This includes techniques such as creating strong passwords, using a different password for each account, and using a secure password manager to keep track of them all. SMEs would ideally encourage the use of password managers and complex passwords.

Social Engineering: This is the use of deception to manipulate individuals into divulging confidential or personal information that may be used for fraudulent purposes. Training employees to recognise and avoid this is vital.

DDoS (Distributed Denial of Service) Attack: This is an attack in which multiple compromised computer systems attack a target and cause a denial of service for users of the targeted system, overloading a network to cause a shutdown. Implementing DDoS protection services can help mitigate this.

Access Control: This is a method of guaranteeing that users are who they say they are, and that they have the appropriate access to company data. In other words, determining who has access to what data. This could involve methods such as passwords, biometric scans, or physical or electronic keys. Regular audits of access controls can help prevent unauthorised access.

Security Operations Centre (SOC): A SOC is a centralised unit or team in an organisation that deals with security issues. It is responsible for monitoring and analysing an organisation's security position on an ongoing basis and for preventing, detecting, analysing, and responding to cybersecurity incidents. Given the potential cost to setup a full-time SOC, SMEs might consider outsourcing SOC services for continuous monitoring and response.

Incident Response: This is an organisation's process of handling a security incident. This includes the stages before, during, and after an incident, and involves planning, preparation, detection, analysis, containment, eradication, and recovery. Having an incident response plan can help SMEs respond effectively to breaches.

DNS (Domain Name System) Security: DNS security refers to the measures taken to protect a DNS from cyber threats. It includes measures like DNSSEC (DNS Security Extensions) that helps prevent DNS spoofing and attacks like DNS poisoning.

Cybersecurity Framework: This is a series of guidelines for private sector companies to manage cybersecurity risks and to be better prepared in identifying, detecting, responding to, and recovering from cyber-attacks. Adopting a recognised framework (like the NCSC framework) can help SMEs implement strong cybersecurity practices.

Managed Security Service Provider (MSSP): This is a third-party company that provides organisations with some amount of network security management, which may include virus blocking, spam blocking, intrusion detection, firewalls, and VPN management. For SMEs with limited resources, using an MSSP can be a cost-effective solution.

Identity and Access Management (IAM): This is the framework of business processes that facilitates the management of electronic or digital identities. With IAM technologies, businesses can control user access to critical information within their organisations.

Dark Web Monitoring: Dark web monitoring is the process of scanning the dark web to determine whether your data is present there. Using a dark web monitoring service can alert SMEs if their data is found on the dark web. This service can alert you if data, such as credit card details or login credentials, is found on the dark web, and thereby signalling a data breach.