SBS INSIGHT HUB

SHARD Business Services

INTRODUCTION TO CYBER SECURITY - A QUICK REFERENCE GUIDE

WHAT IS CYBER SECURITY?

Cyber security is how individuals and organisations reduce the risk of cyber attacks. It focuses on protecting:

- The devices we use (phones, laptops, tablets, computers)
- The services we access (email, cloud, networks)
- The personal information we store online

WHAT IS A CYBER ATTACK?

A cyber attack is a deliberate attempt by an individual or organisation to breach another's systems for financial, operational, or reputational gain.

Example Scenario: Phone Scam

A caller posing as a **bank manager** claims to have found suspicious activity and asks for account details via a "secure link."

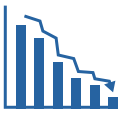
Key takeaway: Never share sensitive information or click on links from unknown sources.

RISKS OF CYBER ATTACKS

Financial loss

Confidentiality breaches

Reputational damage



Operational disruption

TYPES OF CYBER ATTACKS

Viruses: Spread when an infected program runs.
Worms: Self-replicating code that spreads across networks.
Trojan Horses: Disguise malicious intent in seemingly useful programs.

HOW TO PREVENT CYBER ATTACKS

- ✓ Be vigilant
- ✓ Don't ignore updates
- ✓ Scan your device regularly
- ✓ Follow security policies
- ✓ Use 2FA
- ✓ Create robust passwords
- ✓ Report suspicious activity
- ✓ Check your digital footprint

CYBER SECURITY

Social Engineering

Manipulating people into revealing confidential information or granting access. Common forms:

- **Spear Phishing** – Targeted fake emails
- **Baiting – T**empting offers or free downloads
- **Spear Phishing** – Targeted fake emails
- **Phishing –** Scam emails requesting login or payment info

Firewalls	**Antivirus protection**	**Filtering malicious content**	**Regular system updates**
Device encryption	**Data backups**	**Robust passwords**	**Two-factor authentication**

CYBER SECURITY AT WORK & HOME

Common Risks:

- Using public Wi-Fi
- Losing devices or credentials
- Ignoring software updates
- Relaxed security habits when remote working

Stay safe by:

- Using secure networks
- Keeping devices updated
- Following company IT policies

PASSWORD BEST PRACTICES

Don't: ✗

- Write passwords down
- Reuse the same password
- Share your passwords
- Use pet names or simple words

Do: ✓

- Use long, complex passwords
- Use a password manager
- Enable **two-factor authentication (2FA)**

shardbusinessservices.co.uk
07714651415
office@shardbusinessservices.co.uk
shardbusinessservices
shardbusiness
@shardbusiness