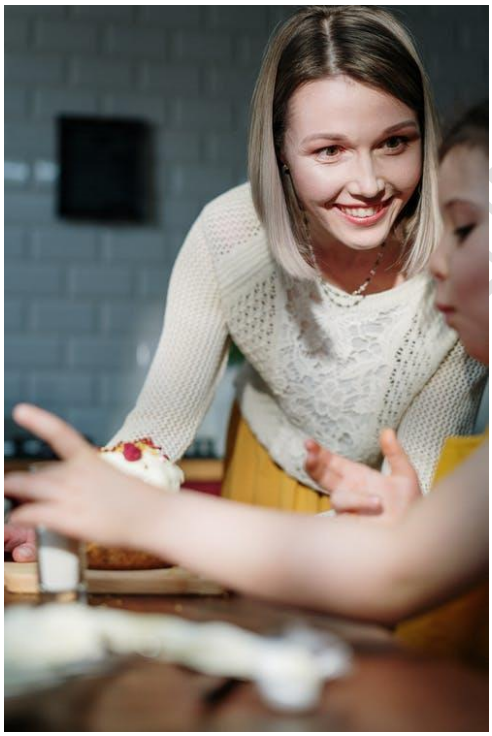
Cyber Security Guide for Small Businesses

Updated 2nd May 2020

Introduction

This is a brief but executable plan to cyber security for companies to stay secure online. It has a concise 25 step action plan to follow.



Who is this for

This is for any business who wants to administer their own cyber security plan without the need to outsource. It is ideal for any business that has the knowledge and expertise to do so, and this provides a concise list that will help protect against a vast majority of cyber security flaws in the market today.

Steps to undertake

Here we outline five very simple areas of security that you can implement to protect your business

STEP 1: PASSWORDS

Passwords should be used right across the business, from websites, emails, servers, accounts, banks, computers, tablets etc etc.

1. Password protect everything, including screen locks on devices. Simple but highly effective
2. Implement 2FA where possible.
3. High Password quality required – here's a good formula [Capital Letter + Something Memorable + Date + character]. For example: Minnesota1930?! or 1930Minnesota?!
4. Password Overload – use password managers to avoid overload on you or your staff
5. Change default passwords

STEP 2: MALWARE

Malicious software infects your devices and can steal, delete or encrypt your company's data.

1. Anti-virus software – install, and turn on, on all devices.
2. App management – approve all use of apps on company devices
3. Patching – keep all IT equipment up to date
4. USB stick management – approve what USB sticks are allowed in company devices
5. Switch on your firewall

STEP 3: PHISHING

Phishing is communication sent by email, text (smishing) or on the phone (vishing) that lures the

recipient into replying with sensitive information, clicking a link with malicious content, or downloading email attachments that contain malware.

1. Restrict staff access to sensitive data as much as possible – that way if they do succumb to an attack the attacker is unable to gain access
2. Train your staff – make them aware of common phishing tactics, how to avoid, and what to do if they are victims. Honestly is absolutely critical here.
3. Install spam filtering software
4. Report all phishing attacks to your security providers, or to the authorities, who in turn hunt down the culprits – report@phishing.gov.uk
5. Manage your digital footprint – more sophisticated attackers use data from social media to make phishing attempts more genuine.

STEP 4: DATA

Backing up your data, so if it is lost, stolen or encrypted, you have another readily available copy

1. Identify the critical data to your business
2. Store the data on a separate device that is not connected to the internet
3. Update your backup weekly (this is the only time this device should be connected to the internet/cloud)
4. Secure your separate device remotely – this can be a separate laptop at home, a USB stored in a safe.
5. Use a cloud provider to store data
6. Evaluate the cloud storage's security

STEP 5: WEBSITE SECURITY

The most visible part of businesses today is generally their website, so make sure it is secure

1. Patching – check for security weaknesses and update software where appropriate

2. Domains – update the privacy of your domains
3. Hosting – make sure that your hosting provider has upgraded the servers to minimise the security threat of a hack.
4. Install an SSL certificate – this keeps communication to and from the website secure.
5. Backups – take regular backups of your website content

Need Further Help?

For help with implementing any of the techniques above, or for a free check of your website please contact the team on the details below.

www.websitesecuritychecker.co.uk

Blue Ocean Media Limited
27 Market Street,
Hoylake,
Merseyside
CH47 2BG

Tel: 0800 002 9936
sales@websitesecuritychecker.co.uk