Cyber Security Health Check

Level 1 • Email Security

Securing your business.

0330 174 9996
info@start-digital.co.uk
start-digital.co.uk

Start Digital

What is this Document?

What is this document?

This document is a cyber security audit; you will filter through and answer each question to improve your business's cyber security one easy step at a time.

We describe **what to do**, as well as **what not to do**. This is labelled as **Good Practice** and **Bad Practice**. You may find that some of your current practices or behaviours fall in to the **Bad Practice** category. This cyber security audit will be a key part of your cyber security journey, and show you what you are missing to secure and protect your business online.

This document's core topics will help you know how to answer questions similar to:

> *How do I avoid losing control of my social media accounts?*
>
> *How do I avoid email breaches?*
>
> *How do I recover compromised accounts? (Social/Email)*
>
> *How can I secure my website?*
>
> *Am I doing well with keeping my data safe?*
>
> *Do I have contingency plans ready in case anything goes wrong with my social media/email/website/data?*

Why these core topics are Important:

This document will cover the core topics listed above, as some of them can be easily overlooked by many people. From unskilled all the way up to people who are very skilled with technology. This document will help give you and understanding of your goals and aims regarding these topics. Using the topics covered in this document is a good baseline to help you plan your business's future cyber security plan of action.

What you hope to achieve by completing this document:

The goal of this document is to get you started on your cyber security journey, no matter how small or big the first steps are, any step in the right direction is important.

This is a document you may want to refer back to before and after you've implemented your business's new cyber security policies and procedures.

Performing an Audit

How to Use this Document:

This document is laid out in a very simple user-friendly way, with four core columns to focus on. The four columns are set out for you to follow from left to right in the following way:

1: Do You Have?	2:Yes/No	3: Good Practice	4: Bad Practice
Example Question: Do you have a secure password?		**Example Good Practice** A combination of the below: • Capital Letters • Lower Case Letters • Numbers • Special Characters. • Minimum 12 characters • Long Phrases	**Example Bad Practice:** • Names • Dates • Numbers • Predictable Sequences • Short Single Words • Short Phrases
This is a question to **assess** if you have a **specified cyber security** practice in place Some of these questions may have a simplified version which may be easier to understand.	You will answer with a **Yes/No** in this box	This will be **our recommendation** of what you should do to solve your lack of cyber security labelled as a **Good Practice**. A **Good Practice** is a behaviour that is **identified** as an **industry standard way** of doing particular things.	This is a section where we go over common **Bad Practices**. If any of your **current** behaviours are listed in the **Bad Practice example,** then you should put a **no** in the **Yes/No** box and look at the **Good Practise** for an idea of what you should be doing instead.

How to Use the Total Score Table:

At the end of every module, there is a **Total Score** table. This table is where you **total up** all your **yes/no** answers **for each module** you complete:

Total Score:	*Y:* *N:*	*Notes:*
This is the **total number** of **yes/no** answers in the boxes to the **right**.	This is where you will put the **amount** yes and **no answers** you have **totalled** up per section.	You can use this box for any **additional notes** you want to make for each unit you have covered.

Email Security

Email Security :
Email security is important as email is the core to many businesses. The reason emails are so important is due to the communication they can provide and the accounts that can be connected to your emails. This section will go over different ways to protect your emails, from logging into accounts, to interacting with others through emails.

Do You Have?	Yes/No	Good Practice	Bad Practice
Do you Have a **Secure Password?**		A secure password usually comprises of a combination of: • Capital Letters • Lower Case Letters • Numbers • Special Characters • Minimum 12 characters • Long Phrases You want a secure password to be difficult to guess, as well as being difficult to crack using software called "brute force" password crackers.	Personal information as the entire password, such as; • Names or birthdays of relatives • Names/birthdays of pets • The place you live • Your home address • Phone numbers • Any single words that appear in a dictionary, even if it's in a different language • Predictable number or letter sequences like **12345** or **qwerty** • Repeated numbers or characters like **99999** or **ZZZZZ**
Do your email accounts have a **Spam Filters?**		Spam filters are a great way to automatically remove unwanted emails. There are many lists online to help with creating a spam list and there are also different version of spam lists. Some automatically update the list when you mark an email as spam, while others you may need to do manually. Different email services have different ways to set up spam filters look for settings similar to: • Spam filter • Junk Email/filter • Filters and blocked addresses • Rules Change these setting for your business needs. Remove any spam you get.	Not sorting through your emails and keeping spam emails inside your main inbox of your emails . This can mean that your spam filter isn't kept up to date with the current trends of spam emails.

Email Security

Do You Have?	Yes/No	Good Practice	Bad Practice
Does each employee have **Separate Business email accounts** from their personal email accounts?		Each person should have a separate business and personal email accounts. This reduces the risk of any personal emails having vulnerabilities or dangers (viruses/malware) that may affect work. It also allows for reading work emails easier. You can get an email service hosted just for your business, here are some examples of email hosting providers: • **Google workspace** • **GoDaddy** • **IONOS** • **Office 365 outlook** • **Mailgun** You can join a free email service like (a hosted service is better as a business gets bigger): Outlook Gmail	Having employees use their personal email account for business related tasks.
Does your business have a system to monitor how staff uses their emails?		Knowing how staff are using their email is important when it comes to reducing possible risk to a business and its network. Some email hosting services allow for built in monitoring. Other times you can get tools to help, such as: • **Teramind Email monitoring** • **Boomerang** • **Microsoft viva** • **EmailAnalytics** Buy/use a service that fits your business.	Having no monitoring systems/rules in place for email usage in the workplace.
Using a service that protects your emails through encryption when sent/received?		To be good at keeping safe while using emails, practice is generally needed, and training allows this in a safe manner. One of the main types of staff training when it comes to emails is phishing training. Some phishing training services includes: • **Phished** • **Hook Security** • **Barracuda**	Having employees use their personal email account for business related tasks.

Email Security

Do You Have?	Yes/No	Good Practice	Bad Practice
Do your networked devices have an anti-virus or anti malware software package installed?		Anti-virus/anti-malware software packages are a good way to counter and stop malware/viruses before they can get into effect. They can also be used to remove malware/viruses if devices/network are affected by known malware/viruses. Anti-virus and anti malware software has gotten better and some have the capacity to scan emails/attachments before you open them. Here are some examples of anti-malware/anti-virus packages: • **ESET endpoint security** • **Avast business antivirus pro plus** • **AVG business** • **Bitdefender gravityzone business security** Some may scan email; some may not, look for what you need from it.	Having no security features on devices installed/enabled. OR Not knowing what security features you have installed/enabled
Do you have regular Staff Training sessions?		To be good at keeping safe while using emails, practice is generally needed, and training allows this in a safe manner. One of the main types of staff training when it comes to emails is phishing training. Some phishing training services: • **Phished** • **Hook Security** • **Barracuda**	Not training staff to have an understanding of what they should or shouldn't do in regards to their emails.

Email Security

Total Score:	Y:
	N:

Notes:

Now that you have completed your email security audit, you should have an improved understanding of your current level of email security. The more **yesses** you have, the more your chances of having an email related security breach are reduced.