# Cyber Security Health Check

## Level 1•Social Media 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:**<br>Do you have a secure password? | | **Example Good Practice**<br>A combination of the below:<br>• Capital Letters<br>• Lower Case Letters<br>• Numbers<br>• Special Characters.<br>• Minimum 12 characters<br>• Long Phrases | **Example Bad Practice:**<br>• Names<br>• Dates<br>• Numbers<br>• Predictable Sequences<br>• Short Single Words<br>• Short Phrases |
| This is a question to **assess** if you have a **specified cyber security** practice in place<br>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**.<br>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:*<br>*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. |

# Social Media Security

**Social Media Security:**
Most businesses have social media accounts, some use it for marketing, some of them rely on social media for business. This includes features/habits that you should have in place to make sure your security is up to scratch, and you are not in danger of losing any of your business social media accounts, or at least get them back easily if you do.

| Do You Have? | Yes/No | Good Practice | Bad Practice |
|---|---|---|---|
| Do you consider your password to be strong? | | A strong password requires a combination of:<br>• Capital Letters<br>• Lower Case Letters<br>• Numbers<br>• Special Characters<br>• Minimum 12 characters<br>• Long Phrases | Having a password that contains:<br>• Personal information<br>• Fewer than 10 characters<br>• Re-using passwords across different accounts |
| Do you have any multi factor authentication implemented where possible? | | Using multi-factor authentication is a must. Some methods of multi-factor authentication are:<br>• Authentication Apps<br>• SMS<br>• Email<br>SMS multi-factor authentication is often the weakest form, and can often be compromised easily. We recommend that you avoid using SMS where possible.<br>Tip: Have a dedicated device for multi-factor authentication that is kept in a secure location with limited access. | Not having any form of multi-factor authentication. |
| Do you have access control in place?<br>Do you limit what your employees can do on your devices/network based on their needs? | | Keep the minimum amount of people possible connected to a single account, this way it is easier to keep track of who does what. | Not having any control over what your staff or employees do, or what they have access to. |
| Do you have a social media policy for your employees? | | Having a social media policy is a must. It outlines how you expect your employees to conduct themselves when they are representing your business on social media. Some social media policies can also outline how your business expects your employees to conduct themselves on their personal accounts as well. | Not having a social media policy that outlines expected behaviour of your staff who might be in a position to represent your business online. |

# Social Media Security

| Do You Have? | Yes/No | Good Practice | Bad Practice |
|---|---|---|---|
| Do you have, and use, a password manager? | | Password managers are used to keep track of all your password, and you only need to remember one password. Some password managers support auto fill too so can be used to speed up processes.<br>Here are some password managers:<br>• Keeper<br>• Dashlane<br>• 1Password<br>• Last Pass<br>If you do not want a digital password manager, you can always keep track of password in a book. If you choose to keep a password book, it's best to keep this in a secure location known only to necessary staff.<br>Password managers are not required, it depends on your business's need. But they are highly recommended.<br>Once you have a password manager, it is recommended to change passwords, that it says is unsecured. | Writing passwords on notes left at a computer or device.<br>Having passwords stored in an unsecured location. |
| Do you have a policy to limit or remove any password sharing within the business? | | Limit the sharing of passwords unless strictly necessary. The more people in your business using a single social media account with the same access credentials, the chances of losing access to social media accounts through a security breach increase exponentially.<br>A better practice is to have dedicated staff who are responsible for social media posts and updates. | Freely giving out social media account passwords to any staff in the business rather than having staff dedicated to social media posts and updates. |
| Have you recently changed passwords? | | Change passwords every 6 months. Use a unique password every time.<br>When someone leaves the business change, passwords on accounts they have access to.<br>Changing passwords in most cases will log people off who are logged into the accounts, helping with removing old employees from access. | Having a password older than 6 months old.<br>Not monitoring whether any of your login details have appeared in data leaks. Password management services can do this for you. |

# Social Media Security

| Do You Have? | Yes/No | Good Practice | Bad Practice |
|---|---|---|---|
| Do you have separate email addresses you use just for your social media accounts? | | Make separate email accounts that have specified purposes for the whole business. In this case for just social media. By having a separate email address for each social media account in use by the business, you can reduce the chances of losing access to your business's social media accounts when employees leave the business. It also allows for more control from an executive position over the social media account, since they will have access to the social media accounts' emails. | Using personal emails to create work connected accounts.<br>Not documenting the email addresses and passwords associated with each different social media account in use with the business. |
| Do you have and use any password protection applications or settings on mobile devices used within the business? | | There are services that add an extra layer of protection on various social media applications. Having them on mobile devices will reduce the risk if a device is lost, stolen, or becomes faulty. It also does not need to be for only social media apps.<br>Here are some example apps that can be used to lock other apps on android:<br>• Norton App Lock<br>• IVY applock<br>• LOCKit<br>iPhones have a setting to do this on the recent builds of iOS. | Having no security on any portable device, such as:<br>• No passwords<br>• No biometric locks<br>• Sharing passwords |
| Do you have a policy to monitor direct messages on your business's social media accounts? | | Keep an eye on direct/personal messages frequently. For all social media accounts.<br>This allows you to keep an understanding of what type of communication is going on between employees and customers. It also allows you to see if anyone may have access to your account without you knowing and is using it in unintended ways. | Never looking over recent private messages on any of your social media accounts. |
| Do you have a social media account with all the large social media platforms? | | Create social media accounts on all popular social media services in your business's name.<br>Having an official social media account for your business allows you to reduce the chance of impersonation. It also allows you to more easily report impersonation accounts to social media services. | Only having social media accounts for the services you use actively use, and not getting social media accounts for services you don't currently use, but could use in the future. |

# Social Media Security

| Do You Have? | Yes/No | Good Practice | Bad Practice |
|---|---|---|---|
| Do you have a social media policy for your business? | | A social media policy is document that outlines what employees are expected to do and not do when representing your business on social media using the business's social media accounts.<br>Make a document that contains:<br>• How you want the social media to be used<br>• Who can access or post<br>• Who can reply on social media<br>• Guidance on what can be posted or shared on social media<br>• Supporting Documents<br>Sometimes social media policies cover how you expect your employees to conduct themselves using their own personal social media accounts. However, this is usually highly dependant on the sector your business works in, and isn't recommended for most businesses. | Not having a business policy that covers social media usage by your employees. |
| Do you have any of your social media accounts connected to third party services or applications?<br>Do you frequently remove any unused or unnecessary third-party applications? | | Third party applications are websites or software services you may have visited and/or you have connected to your business's social media accounts. The more third-part connections the more vulnerable the social media account is.<br>Remove unnecessary third-party apps/applications connected to social media accounts using social media settings similar to:<br>• Logged in with<br>• Apps and websites<br>• Connected apps<br>• Manage app permission | Having unnecessary apps/applications connected to your social media accounts. |
| Do you have a limit on what employees can do on your business's social media accounts? | | Reduce the amount of people that can do certain tasks on the business's social media accounts.<br>Example: posting, replying, providing customer service, etc.<br>This way you know who is responsible for what has been done on the social media account, which allows for better monitoring. | Not monitoring social media usage of your employees on the businesses social media accounts. |

# Social Media Security

|  |  |
|---|---|
| Total Score: | Y: |
|  | N: |

Notes:

After completing this section you, should have a good idea on where you need to improve your security when it comes to your business's social media accounts. The more of these processes you put in place, the more you lower the risk of you losing your business's social media accounts, which could harm your brand's reputation. But the real benefit of taking these precautions is that it makes account recoveries much more likely.