



# Cyber Security Tool Kit

Level 1 • Email Security  
Securing your business.

0330 174 9996  
[info@start-digital.co.uk](mailto:info@start-digital.co.uk)  
[start-digital.co.uk](http://start-digital.co.uk)

 **Start Digital**

Ver.2.1



# **What is This Document?**

## **What is this document?**

This **Level 1 Cyber Security Tool Kit** is a step-by-step guide to help you implement the measures and processes covered in the **Level 1 Health Check**.

Not all fields or groups of boxes will need to be filled in. We expect you to only fill in the ones you plan on implementing based on your health check audit results. You can always go back later to complete any additional modules if necessary.

The **Level 1 Cyber Security Tool Kit** is a **living document**, which means that you will be continually editing and updating the document. Cyber security is an on-going process, and sitting still is not a position you want to be caught in. Most of this document's tasks cannot be completed in a single sitting, or a short period of time. This means you will be coming back regularly to make updates and changes.

## **Policy Implementation:**

Certain topics within the **Level 1 Cyber Security Tool Kit** may be covered by existing policies you have implemented within your business. You may find that you can improve your existing policies with the help of the **Level 1 Health Check** and this **Level 1 Tool Kit**. If your existing policies are working as they should though, rather than repeating yourself, you can add supporting documents to the relevant policies and redirect towards the documents with the necessary information.

## **What you will achieve by completing this document:**

The goal of this document is to support your on-going cyber security journey, no matter how small each step is. Any step you take in the right direction is an important improvement to your business's cyber security, as well as establishing your business's digital culture.

## **Establishing a digital culture:**

Advancements and the reliance on digital technology coupled with classic business models have accelerated business disruption. In an increasingly global marketplace, the pandemic has further accelerated this trend, making the digital transformation critical for a business's success. However, it takes more than just technology and policies; the business leaders must also look at the human side of their organisations.

The culture within the business around the way your employees interact with technology is a significant factor in staying secure, and being successful. Developing a strong digital culture from the top down is an extremely important element to ensuring the policies you develop become second nature to all employees. Without the right culture of behaviour, the policies you implement have limited impact.

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



# Completing Task Sheets

## Completing Task Sheets:

This document's task sheets are laid out in a very simple, user-friendly table format. A task sheet has 2 primary elements: the **topic table**, and the **question** and/or **task box**. Some task boxes may include a **tick box** to indicate you have completed that specific task or full topic.

### Topic Table:

This is a table at the start of each module with each topic categorised. Once you have completed a full task, you can tick it off to keep track of the tasks you have carried out.

1: Topic Number	2: Module Topic	2: Tick Box
<b>Example Number:</b> 1	<b>Example Topic:</b> Cyber security policy	
This is just a simple box to denote the number of topics within a module.	This box names the specific topic of the module you are currently working through.	Tick this box to show you've completed the named topic.

### Answer Table:

Answer tables are set out in two different formats: **question boxes** where you are asked specific questions that require specific answers; and **task boxes** where the goal is for you to carry out a specified task, and then mark it as complete when you have finished. Some tasks will be multiple choice, where you choose one task or another.

### Question Box:

<b>1: Example Module Question:</b> What processes do you have in place for email safety?
<b>Example Answer:</b> Our current processes are...
This is where the question is asked, and you fill in the lower boxes with your answers.

### Task Box:

<b>1: Example Module Task:</b> Explain below what situations you should _____ data storage devices:	
<b>Example Prompt:</b> Re-use	<b>Example Task Answer:</b> I would re-use a data storage device when...
This is where a task might be <b>broken down</b> into a <b>sub task</b> , a <b>specific prompt</b> , or a <b>multiple choice</b> task.	This is where you record <b>your response</b> to the task using either the <b>prompt</b> or <b>sub task as a guideline</b> for your answer. <b>Don't forget</b> , not every box needs to be completed. <b>Multiple choice tasks</b> will only require <b>relevant</b> boxes to be <b>filled in</b> or <b>ticked off</b> .



# Email Security

## Business Email Security:

Establishing protocols for best practices amongst employees can help increase your team efficiency and productivity, whilst implementing email security best practices can help you prevent and mitigate the risk of email-related cyber-attacks. Email is such an important part of any business, but also such a common attack vector . It's worth taking the time to secure it. The module topics below will help you protect against business email account compromises:

Number	Module Topic	✓
1	Business Email	
2	Spam Filters	
3	Multi-Factor Authentication (MFA)	
4	SMTP Protection (SSL)	
5	Trusted Email List	

## Module Notes:

You can use this box to add any notes you feel are necessary to help you work through this module.

Notes:



# Email Security

Do you have an email service set up for your business?

Yes

No

If you have chosen **YES**, write in the box below which services you use, then skip the rest of this table.

If you have chosen **NO**, complete the rest of the table.

Typically, there are two methods of setting up an email account for your business:

1. Third party service, such as @outlook, @gmail, etc
2. Your own custom domain, this could be something like; yourname@yourrowndomain.co.uk

For this process, select only one. You can always return to this section if you change your mind.

## 1. Research and choose an email service that meets your business's requirements

Service:	Cost:	Pros:	Cons:	✓
Outlook	£			
Gmail	£			
Proton Mail	£			
Zoho	£			

Other:

## 2. Research these email hosting services that require your own domain to use.

**Note:** you need to make sure you are keeping your domains renewed each year to keep the accounts functional.

Service:	Cost:	Pros:	Cons:	✓
Google Workspace	£			
Office 365 Outlook	£			
Rackspace Email	£			
Zoho Mail	£			
Rackspace Email	£			
Zoho Mail	£			

Other:

Which service did you choose, and why?

Make a business specific email account for all employees. Tick the box when complete.

Tick the box once you have completed this topic.



Spam filters are a common tool that provide the vital service of protecting our inboxes from malware or phishing, while also making sure essential messages we want to see aren't drowned out by spam. There are different types of spam filters, but more common ones allow you to block emails and send them to a spam folder by giving the folder a set of criteria contained in emails.

Go to the email client's settings, and look for settings similar to:

1. Spam Filter
2. Junk Email/filter
3. Filters and blocked addresses
4. Rules (this is an option to sort your inbox, it can also help with sending stuff to spam)

List all relevant email accounts below, and configure spam filters for each. Tick each off when complete.

[illegible]



MFA is a great way to keep secure. Though some find it an inconvenient hurdle in their day to day work-flow, it's become a necessary step in establishing security. MFA requires all login attempts to be authenticated using additional means such as: text, email, or via an app. Make a list of the online services your business uses in the table below:

[illegible]

\_\_\_\_\_

**Start Digital**  *Cyber Security Tool Kit • Level 1 • Email Security*





# Email Security

## 4. SMTP protection (SSL):

Email cannot be relied upon as a secure communication channel unless you and your service provider implement a high level of security to protect your email client. That's where SMTP authentication comes in. SMTP authentication allows you to leverage the scalability and features of your SMTP service provider, while protecting you from unauthorised use of your email client or account.

Do you have an email encryption service set up for your business?

Yes

No

If you have chosen **YES**, write in the box below which services you use, then skip the rest of this table.

If you have chosen **NO**, complete the rest of the table.

Research and choose an email encryption service that meets your business's requirements

Service:	Cost:	Pros:	Cons:	<input checked="" type="checkbox"/>
SSL Checker (By SSL Shopper)	£			<input type="checkbox"/>
SSL Test (By SSL Labs)	£			<input type="checkbox"/>

With the service you've chosen above, use it to check your SSL certificate. Tick the box once done.

Research these SSL services, and assess their suitability to meet your business's needs. Tick off as you go.

Service:	Cost:	Pros:	Cons:	<input checked="" type="checkbox"/>
Comodo SSL	£			<input type="checkbox"/>
DigiCert	£			<input type="checkbox"/>
Entrust DataCard	£			<input type="checkbox"/>
GoDaddy	£			<input type="checkbox"/>
RapidSSL	£			<input type="checkbox"/>
SSL.com	£			<input type="checkbox"/>
AlphaSSL	£			<input type="checkbox"/>

Which service meets your business's needs?

Why did you choose this service?

Purchase your chosen SSL certificate from above. Tick the box when complete.

Following the SSL service's instructions, implement SSL on your mail server/s. Tick the box when complete.

Make a business specific email account for all employees. Tick the box when complete.

Tick the box once you have completed this topic.





A trusted email list is a list of “approved” email senders that have given you permission to send them updates and promotions. An email safe list tells your email client that you know and trust the messages that come from that email address. It can help build trust and confidence with your clients. Each email provider or security service has their own process for adding email addresses to a whitelist.

**Trusted internal email addresses** (these will be your colleagues within the same business or company.)

**Tick the box once you have completed this topic.**



**Tick the box once you have completed this topic.**