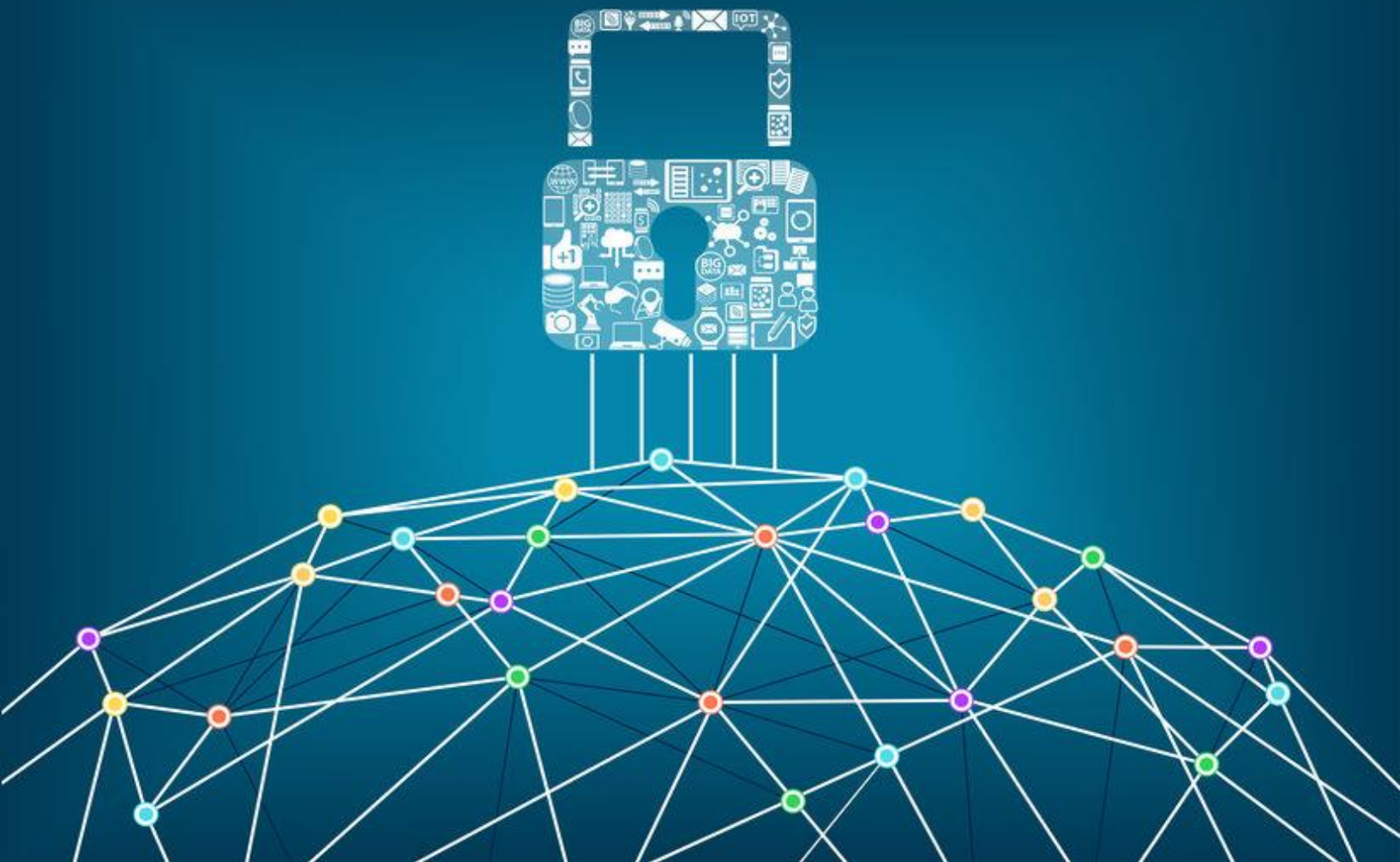


# IT SECURITY AWARENESS BRANCH GUIDELINES

---



LIVE ON 



## Introduction

There are many benefits of using technology, it makes administration easier and faster to complete and can connect people from across the globe with each other who wouldn't normally have the opportunity to do so.

However, the use of technology does come with its risks, these can be from website data breaches, \*cyber attacks or malicious emails. Cyber criminals see people as the weakest link and target them.

Cyber attacks can be prevented by recognising the threats and taking counter measures to deal with the increasingly sophisticated methods trying to compromise the IT systems, data and reputation.

Throughout these pages, we will highlight the key areas to increase awareness and promote best practice to protect IT systems.

\*cyber = involving, using, or relating to computers, especially the internet.



# Keeping your computer clean

Keeping your devices free from malware and infection makes everyone safer. Following these best practice tips will help you to achieve this:



Always use a virus or malware protection program – there are some free ones available.

Apply software updates on your computer regularly.

Never install an unlicensed software.

If you must save any personal details, make sure you protect the file with a strong password. (see 'How to make a secure password')



Do not plug an unknown USB into your computer

Do not store personal data on your personal devices (computer, smartphone, laptop, tablet, etc). We strongly recommend using O365 to access the details of your members.



## Signs of Cyber Breach

If the worst happens and your computer gets infected it is important to recognise the signs of a security breach. Here are some of the common symptoms:



Unexplained errors and crashes



Files missing



Slow or no response



Computer running slower than usual



Changes to configurations e.g. your desktop looks different



## Beware of Cyber Phishing

Phishing is the fraudulent practice of sending emails claiming to be from reputable companies or known contacts such as family/friends and people in your community in order to get individuals to reveal personal information, such as passwords and credit card numbers.

A fraudster sends a fake or spoofed email that appears to be from a trusted source, e.g. a bank account or an online organisation, with links to fake websites.

They try to trick you to click on the link or attachment in the email to and disclose your username and password in order to gain access to your computer and steal data.



It is called phishing because the fraudsters are 'fishing' for your private account information.



If you are ever in doubt about an email, call the sender to check authenticity

### Can you spot a phishing email?

Phishing emails often have common traits. Here are some of their features below:

- Referring to you as 'Customer' or similar rather than your name
- Typos or spelling mistakes in the email
- Asking you to click on links or attachments
- The 'From' email address doesn't appear to be who it says it is from
- An odd message from a person known to you sounding distressed, needs help or is excited about a new opportunity that must be shared



# Phishing Scams Look Normal


Many phishing scams tend to look quite normal to the average internet user. Even more experience web-surfers may have a difficult time differentiating a phishing scam from something legitimate given the level of sophistication involved.

The more you know about phishing scams, the more you can be on the lookout for them to protect yourself.

You may receive an email that appears to be sent from a bank or government organisation. Their goal is to trick you into clicking the link or open the attachment in the email.

Below are examples of recent phishing scams. These are just examples from one organisation although there many different formats and identities will be used by scammers.

## 'Click a Link' Phishing

 HM Revenue Customs

---

### Income Tax rates and Personal Allowances

Dear TaxPayer ,

You are eligible to receive a refund of up to 425.58 GBP.  
In order to do so, you are required to submit an official claim application using the information you have registered with us.

[Claim your tax](#)

**Note:**  
If you will not complete the refund form now , you will not be able to claim your annual tax refund online

HMRC Customer - Secured E-mail -


Best Regards, Luke Sullivan.

**Why you got this email**

You registered for a refund Government Gateway.

From HMRC Government Gateway

## 'Download an Attachment' Phishing

Attached  [2018-HMRC-Notification.pdf \(95 KB\)](#)

---

**From:** "HMRC-Notification-IdReference-1389716@gkatak.com" <HMRC-Notification-IdReference-1389716@gkatak.com>  
**Subject:** Sign in and review recent transaction !  
**Date:**  
**Resent-From:** <jfrosemmary@hotmail.com>

Hi

[--We are pleased to confirm that your claim form has been successfully submitted.

[--Your unique claim reference is HMRC1938567124

[--Your claim form has been sent in you Email.

[--Once received, please complete the required boxes,to progress with your refund claim.

[--Please find and download the attached 2018-HMRC-Notification.pdf and follow the instruction.

[--We look forward to assisting you.

[--Thanks For understanding.  
 [--Issued by HMRC-Team. support office.  
 [--2018 HM Revenue Agency.

## Text message Phishing

< HMRCUK ⓘ

Sat 7 Apr, 13:29

You have a pending Tax Refund of 265.84GBP from HMRC. To proceed your application please complete your form via [hmrc.gov.signin-uk.com](http://hmrc.gov.signin-uk.com)



## How to make a Secure Password

Passwords are often the first line of defence. If a password is too simple or contains your personal information, people can break into accounts and use your details to conduct further attacks. It's important to strengthen the use of your passwords by following these tips:



Your password should be strong and long, do not use personal information such as your name or Date of Birth



Change your password regularly



Use different passwords for different accounts



Do not share your password with anyone



Choose a memorable password and do not write it down

### Create a Powerful Password

To make an original and completely randomised password, make three columns and write down the categories: Who, What, and When. Then fill in the blanks and remember that the crazier the idea, the better. Be specific with dates and times and develop it into a sentence with full punctuation.

Now simply take the first character of each word, and you end up with an incredibly strong password that's easy to remember and is virtually un-hackable.

Who	What	When
Me	Training with Superman	8am on Saturday



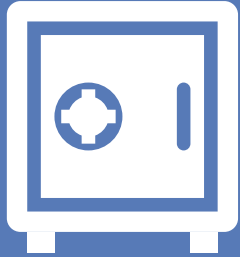
"I'm training with Superman at 8am on Saturday!"



Password: **ItwSa8oS!**



# IT Security – Our Top Tips



Lock up items, never leave your devices unattended. If you need to leave your computer, phone or tablet for any length of time, no matter how short, lock it up so no one can use it while your gone.



Be cautious of the information you share on social networks. Criminals can befriend you and easily gain access to a lot of information. Where you go to school, where you work and where you're on vacation. All this could help them gain access to more valuable data.



Sensitive browsing, such as banking or shopping, downloading reports that contain personal data should only be done on a device that belongs to you, on a network that you trust. Whether it's a friend's phone, a public device or a café's free Wi-Fi, your data could be copied or stolen.



## Summary

- Use Legion systems sensibly, professionally & lawfully. Store all your documents on O365 as they will not need backing up.
- Do not access inappropriate or unlawful material
- Malicious or inappropriate sites must not be accessed
- Be security conscious when working in public
- Passwords and login information must be secure, eight characters is not enough. Don't share your passwords or write them down.
- Be cautious when opening attachments or clicking links in emails and of what you plug in to your computer.
- Monitor your account for suspicious activity and report security incidents immediately to your MSO.

## MEMBERSHIP

The Royal British Legion  
199 Borough High Street  
London  
SE1 1AA

For further information on IT security for RBL Branches please contact  
**[membership.itsupport@rbl.community](mailto:membership.itsupport@rbl.community)**

Registered Charity Number: 219279

Registered Charity: The Royal British Legion, Haig House, 199 Borough High Street, London, SE1 1AA