We believe that data privacy and protection don't need to be expensive to be effective. This document lists many trusted sources, most of which are completely free! We hope you find them useful.

You can access the latest version of this document (with clickable links) at www.riskevolves.com/resources. If you can suggest another resource to add, please email us at info@riskevolves.com.

Please get in touch if we can help you protect your business further.

Helen & the Team

RESOURCES

riskevolves

We offer a range of services to suit every business, from training and Cyber Essentials certification to phishing protection that starts at just 10p per user per day.

We publish the latest threats, trends and signpost to new content on social media. Please follow us on Twitter (at #riskevolves), on LinkedIn (@riskevolves) and visit our website. These pages will be useful to you:

www.riskevolves.com/phishing-protection

www.riskevolves.com/cyberessentials

www.riskevolves.com/training

TAKE FIVE TO STOP FRAUD™

This **website** is focused on preventing financial fraud. It has free training materials and great advice to pass onto your team which will help them avoid cyber crime both at work and at home.

ActionFraud
National Fraud & Cyber Crime Reporting Centre
0300 123 2040

Action Fraud is the National Fraud & Cyber Crime Reporting Centre. If you become aware of a successful cyber attack on your organisation, make **Action Fraud** your first point of contact.

Action Fraud also offer **free services** that stop you from visiting malicious websites and protect you from email fraud whether at home or at work. We even use these ourselves!

National Cyber Security Centre
a part of GCHQ

The NCSC **website** includes a wealth of information that's easy to understand. Simply select 'Information for' from the top menu to find the information that's right for your needs or go straight to the **SME** page.

The site includes free training and tools to help you protect your business.

Your staff are the weak point in your organisation's defences. We recommend asking all employees to complete the **free cyber security training**, regardless of their level or experience. We are all vulnerable especially when we are busy.

Exercise in a Box is an online tool to help find out how resilient your organisation is to attack. It also lets you practice your response in a safe environment.

Larger businesses can also benefit from its advice for Board members. The **Board Toolkit** helps encourage essential cyber security conversations between a Board and its technical experts.

If you have some technical knowledge in house, you can use the NCSC's tool for **logging activity**.

Phishing attacks are on the increase but you can now forward phishing emails to the NCSC for investigation. The email address to use is **report@phishing.gov.uk**. You can find out what happens after a report on the NCSC's **phishing page**.

RESOURCES CONT...

GLOBAL CYBER ALLIANCE

The **Alliance** uses the proceeds from crime to fund tools to prevent cyber crime.

These tools, developed by major IT companies for business use, are completely free and are recommended by Action Fraud! The site also includes a wealth of publications and research.

GET RID OF OLD EQUIPMENT SAFELY

Devices with storage media need to be disposed of carefully to ensure that your data doesn't get into the wrong hands. The **NCSC** has some helpful guidance on the topic.

In our area, the **Air Ambulance** provides free and safe hardware destruction.

Don't forget to ask for a CESG certificate for your records and confirmation of the assets destroyed. These should be kept on file for several years.

CHECK IF YOU'VE BEEN COMPROMISED

To find out if your security details need changing pronto, visit the **Have I Been Pwned** website. This will tell you if one of your online accounts has been compromised in a breach, such as those which affected Canva and Adobe users.

If your email is on the list, but your password hasn't been changed in a long time, now's a good time to change it.

You can practice building safer passwords on the **Kaspersky** website. Never use your real password on this site!

We recommend using a password that doesn't contain words, so steer clear of passwords like dogcat77 and plump for sentences instead, e.g. IWTBIBB7OF (I want to be in Barbados by 7 on Friday) or IATAG98IMBER (I am terrible at golf, 98 is my best ever round).

Pick something that's easy to remember but not obvious to anyone else.

OTHER ONLINE RESOURCES

The **Information Commissioner's website** has free resources including a section on your **personal data rights**.

Other useful websites include **Get Safe Online**, **Cyber Aware** and the **University of York's** cyber security and data protection resources.

You can download an audiobook and PDFs from the **Met Police site** to help you prevent fraud and cyber crime.

The **Secure Book** PDF features step-by-step guides to securing smart phones, Zoom meetings and social media accounts (including LinkedIn).

TRAINING

OTHER ONLINE TRAINING

As well as the NCSC training, see overleaf, we recommend Bob's Business training. Modules, which include cyber security and some aspects of GDPR, are as low as £9 per user.

Videos are also a great source of education. The Met Police site has some useful ones on phishing, wifi, passwords and payment fraud.

Everyone should watch this video from the BBC about ransomware. Although the company in question is a large international organisation, there are learning points for every business.

Cisco's short video showing inside the mind of a hacker challenges damaging preconceptions about hackers.

CERTIFICATIONS

CYBER ESSENTIALS

Cyber Essentials is a government-backed accreditation which gives your customers peace of mind. It's cost-effective and includes free cyber insurance. You can find out more about the scheme on the NCSC website.

IASME is the certification body for Cyber Essentials. There are some useful resources on IASME's website.

We've helped clients from a range of sectors achieve Cyber Essentials.

Please see www.riskevolves.com/cyberessentials or contact us to explore how Cyber Essentials can help you grow your business.

DIGITALLY AWARE

Designed to meet the needs of smaller (or less risky) businesses, Digitally Aware costs just £50.

It has great credentials as it was developed in conjunction with the Police Digital Security Centre and British Standards (BSI).