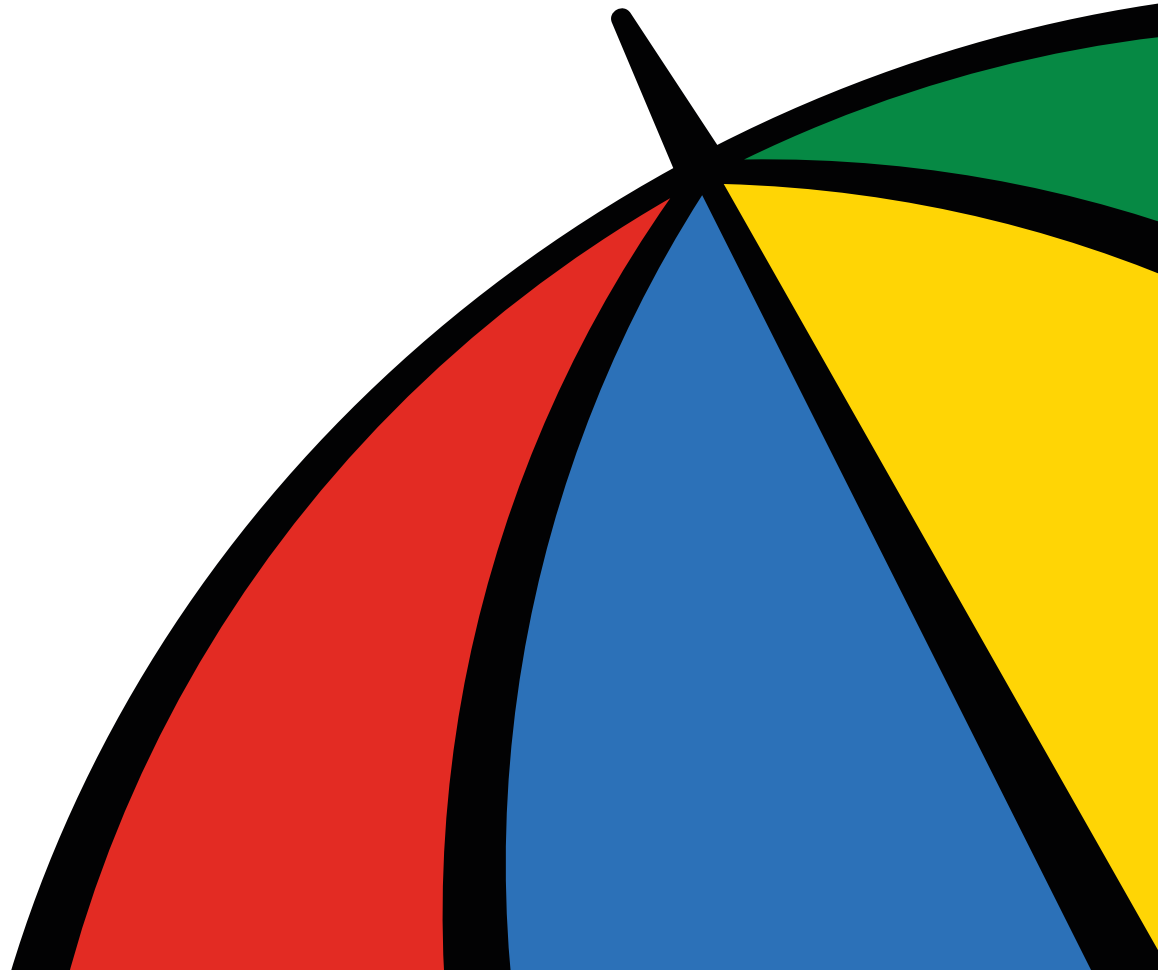
Intermediary Cyber Security Good Practice Guide

Legal & General Information Security Supplier Assurance

June 2022



Introduction

Legal & General use a large number of external suppliers. The number of these external suppliers continues to increase, as does the importance of:

- Maintaining controls over their processes & systems and any personal data or business sensitive information they may have access to; and
- Ensuring availability of service(s) they provide to the business

In regards to the **intermediary business** that is provided to **Legal & General,** this is not a traditional supplier relationship, in this context the **intermediary brokers,** including **Independent Financial Advisors (IFA)** are Data Controllers within their own right, and therefore, they retain the accountability for meeting regulatory requirements and ensuring adequate data and security governance controls are in place.

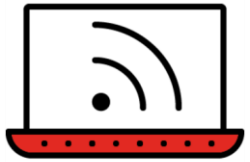
Recently there have been several security incidents at intermediary firms and this guidance document is a response to these, it's aim is to help support those smaller intermediaries of **Legal & General** who may need extra support, to provide advice and guidance as to some best practices that can be adopted by an intermediary or IFA in order to reduce their risk exposure.

You can reach out to the **Legal & General Supplier Assurance Team** if you require any support or guidance based on this document.

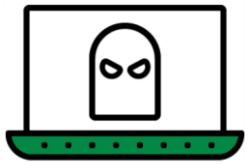
Guidance Contents

Password Security

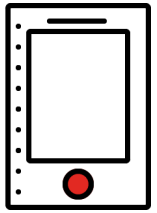
Firewall & Anti-Virus Protection



Public Wi-Fi



Ransomware



Secure Mobile Devices

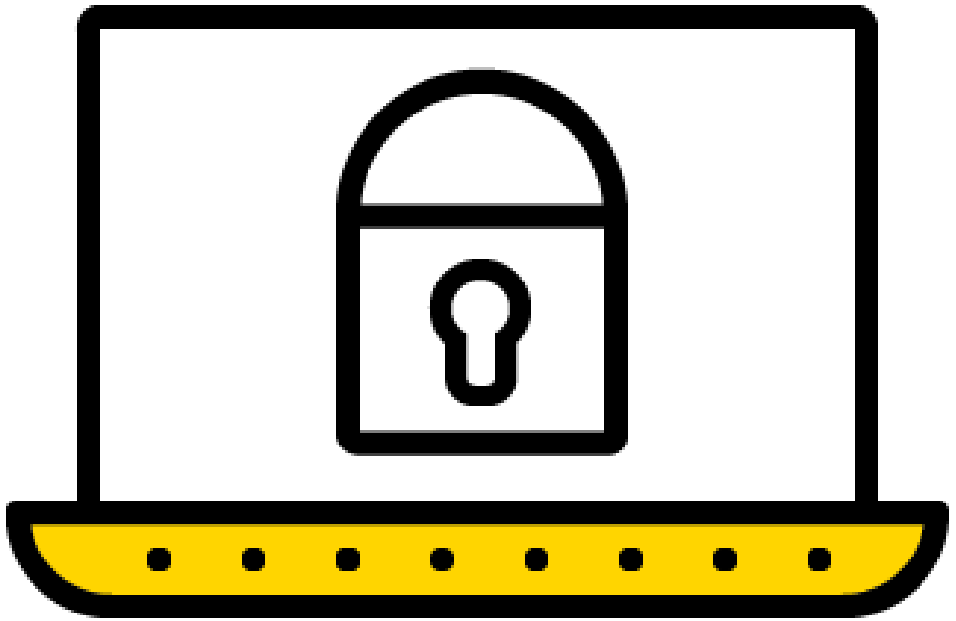
Keeping Your Software Up to Date (Patching)

Multifactor Authentication

Password Security

Weak passwords are one of the greatest entry points for hackers and many recent attacks were successful due to weak passwords and ineffective password management practices. It is therefore recommended that you:

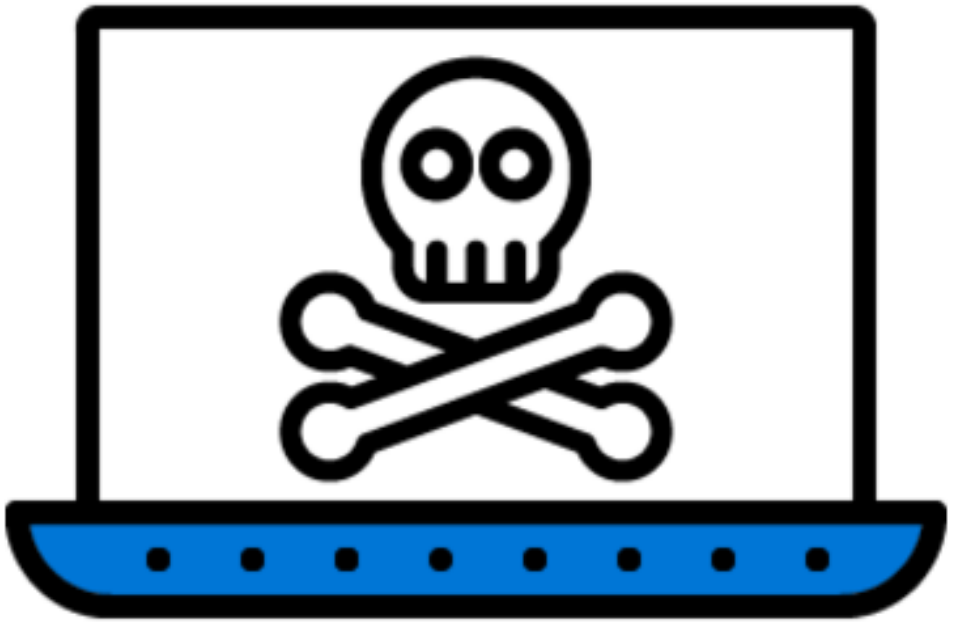
- Enforce strong passwords that are 15 characters or longer with no expiry (or 12 characters if password expiry is implemented)
- Use complex passwords i.e. contain a combination of upper case, lower case, numbers and special characters (£%$^)
- Use unique passwords for each and every one of your logins
- Use a password manager that stores your passwords in an encrypted database, so that you can easily manage each individual login and password
- Avoid changing your password on a regular basis so you do not use the same password with slightly changed characters or using the same password across multiple platforms e.g. LinkedIn, Facebook etc
- Avoid using familiar or dictionary words, instead use joined phrases



Firewall & Anti-Virus Protection

Anti-virus (AV) protection software has been one of the most prevalent solutions to fight malicious attacks. AV software blocks malware and other malicious viruses from entering your device and compromising your data.

- Use anti-virus software from trusted vendors
- Only run one AV tool on your device
- Ensure that this is setup to run and update virus signatures automatically

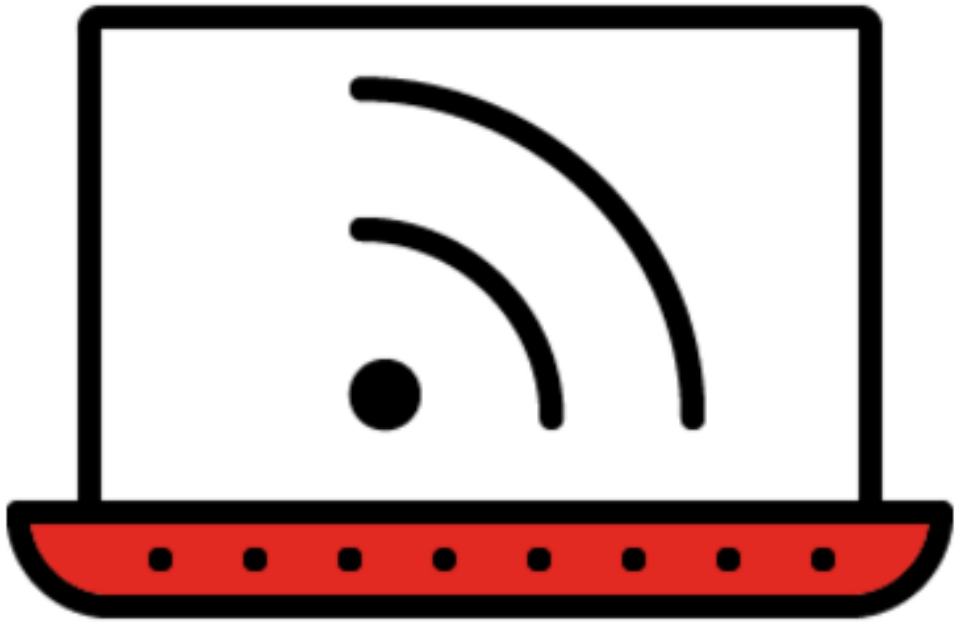


Using a firewall is also important when defending your data against malicious attacks. A firewall helps screen out hackers, viruses, and other malicious activity that occurs over the Internet and determines what traffic is allowed to enter your device. Windows and Mac OS X comes with their respective firewalls, aptly named Windows Firewall and Mac Firewall. Your router should also have a firewall built in to prevent attacks on your network.

Public Wi-Fi

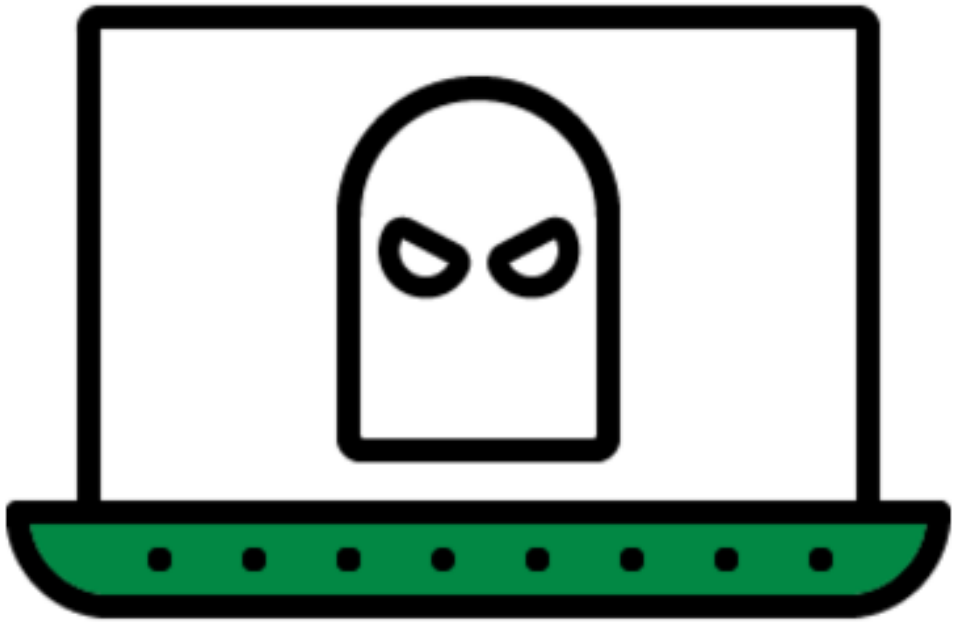
Public Wi-Fi could be at places like the airports, trains, cafes etc. These are usually free and only require a agreement to terms before you can start using the internet

- Don’t use a public Wi-Fi without using a **Virtual Private Network (VPN).** By using a VPN, the traffic between your device and the VPN server is encrypted. This means it’s much more difficult for a cybercriminal to obtain access to your data on your device
- Use your mobile providers network if you don’t have a VPN when security is important



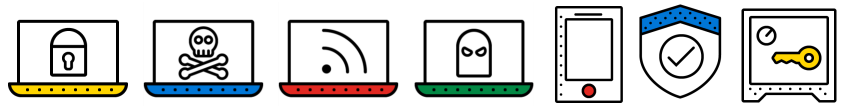
Ransomware

Ransomware is one of the most common types of attacks cyber criminals enact on people and organisations, leaving people unable to retrieve their data, or even being locked out of their network. In a **phishing scam**, the attacker poses as someone or something the sender is not, this is to trick the recipient into divulging credentials, clicking a malicious link, or opening an attachment that infects the user's system with malware, trojan, or **zero-day** vulnerability exploit. This often leads to a ransomware attack. In fact, **90%** of ransomware attacks originate from phishing attempts.



A few important cyber security tips to remember about phishing scams include:

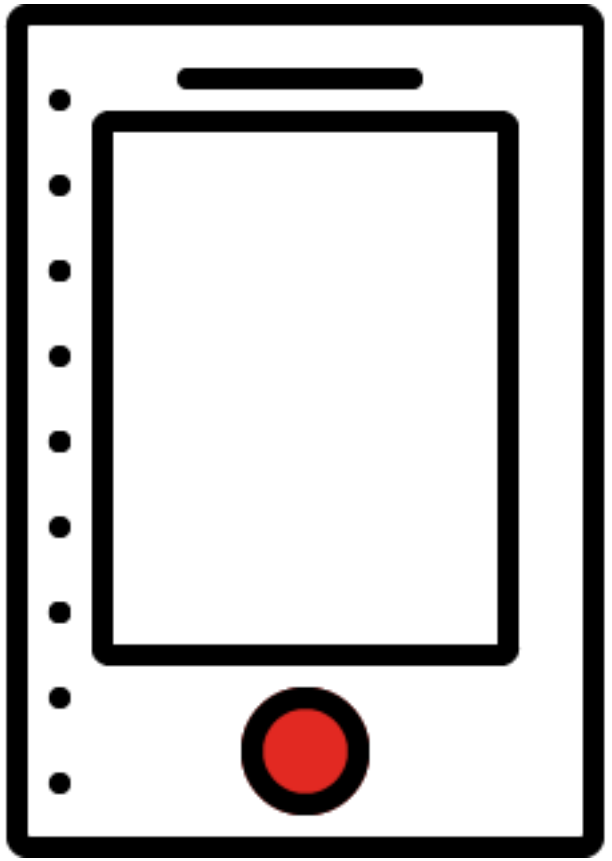
- Don't open email from people you don't know
- Know which links are safe and which are not – hover over a link to discover where it directs to
- Be suspicious of the emails sent to you in general – look and see where it came from and if there are grammatical errors
- Malicious links can come from friends who have been infected too. So, be extra careful!
- Be vigilant when you receive any phones calls or text messages from unsolicited sources, calls and texts you are not expecting, generally include the application of pressure or a sense of urgency. End the call/delete the message and report it, you can always call back the organisation to confirm it was them calling or not, most of the time it is not them.
- Back up your data - Attackers encrypt your data and demand ransom. You need to back up all your data. When a ransomware attack happens, the perpetrator will encrypt your data and demand a ransom (£) to unencrypt and gain access to your information again. It is therefore recommended that you conduct regular backups - Remember data held locally on your machines as well as data in the cloud/SaaS applications such as Office 365 – This will ensure that hopefully should the worse occur, you can retrieve data from a backup and not pay the ransom.

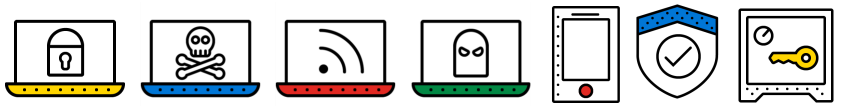


Secure Mobile Devices

Your mobile device is now a target to more than **1.5 million** new incidents of mobile malware. Here are some quick tips for mobile device security:

- Create a difficult mobile passcode – Not your birthdate or bank PIN
- Only install apps from trusted sources
- Keep your device updated – Hackers use vulnerabilities in unpatched older operating systems
- Avoid sending Personally Identifiable Information (PII) or sensitive information over text message or email
- Leverage **Find my iPhone** or the **Android Device Manager** to prevent loss or theft



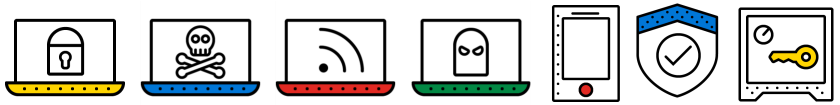


Keeping Your Software Up to Date (Patching)

Make sure software is patched and up to date. Attackers look for known vulnerabilities first, so don't make it easy for them, so you should ensure you update apps and systems regularly.

One of the first steps that should be taken to **lower the risk of** a cyber-attack is to update all of the applications and systems that you actively use (like Adobe or Windows). Software providers make it easy to check which version of their product you are currently using and any new updates that are available (you've probably seen their notifications pop up before). Once up to date, make sure you continue to update each system as soon as possible when new versions and software are released. Don't ignore those notifications! Using older software or computer applications can leave you vulnerable to security breaches.

- Turn on automatic system updates for your devices
- Make sure your desktop web browser uses automatic security updates
- Keep your web browser plugins like Flash, Java, etc. updated



Multifactor Authentication

Many applications now offer **multi-factor identity authentication** (when you get a code via text or email to complete sign-in). This is a great way to enhance your security. Make sure it is always enabled if an option. It is therefore recommended that you:

- Consider requiring a phone app or text based second factor authentication for all applications and resources. As this is very useful in preventing **brute-force login attempt**