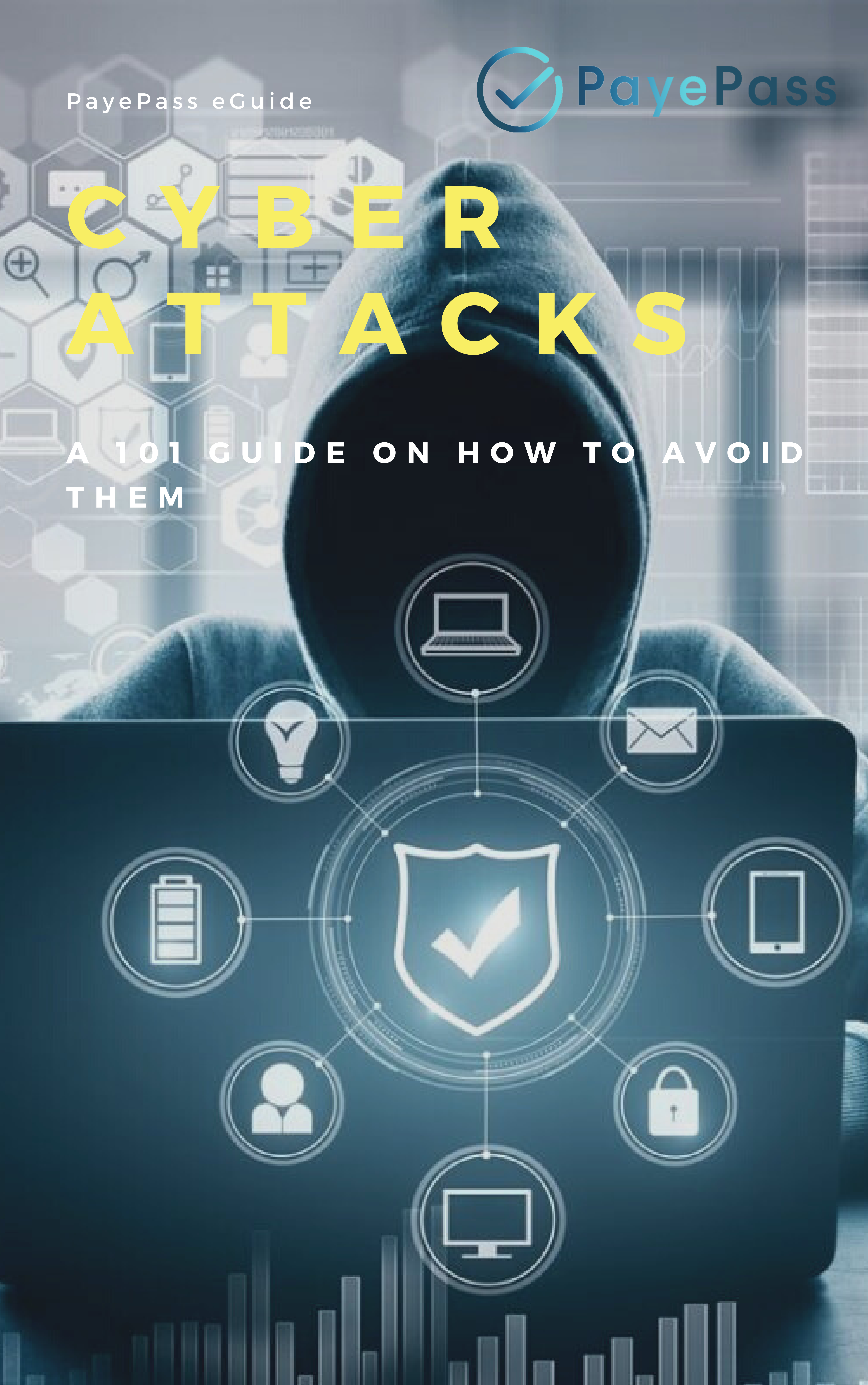
PayePass eGuide

PayePass

CYBER ATTACKS

A 101 GUIDE ON HOW TO AVOID THEM



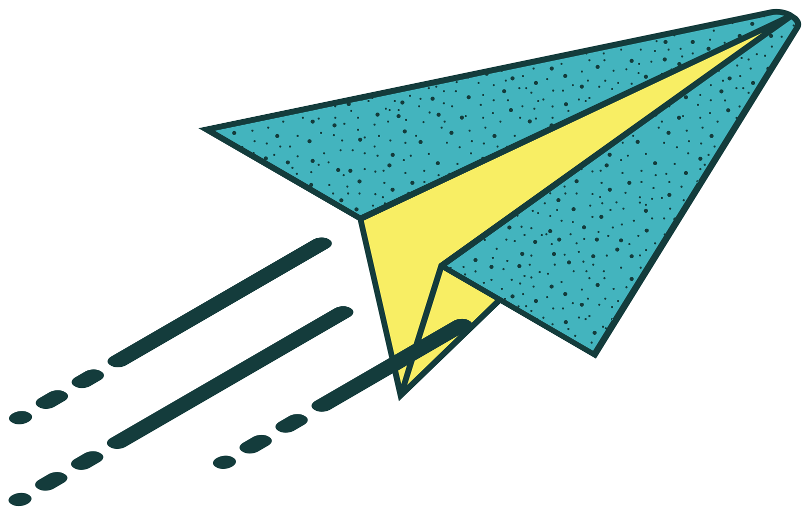
Cyber attacks in the UK have reached an all time high. Whether it be global corporations, privately owned SMEs or public organisations, all can fall victim to a cyber attack. Cyber Attacks are a potential risk for every organisation, no matter how big or small and it's everyone's responsibility to minimise that risk as much as possible.

Hopefully the tips in this guide will help mitigate your cybersecurity attack risk.

1. Keep software up-to-date
Installing software updates and patches for your operating system and programs is critical. Cyber criminals use weaknesses in software and applications to attack your devices and steal information. Software and application updates are designed to fix these weaknesses and installing them as soon as possible will help keep your devices secure.

2. Keep hardware up-to-date
Outdated computer hardware may not support the most recent software security upgrades. Additionally, old hardware makes it slower to respond to cyber-attacks if they happen. .

3. Use anti-virus and anti-malware
When connected to the internet in any way, it’s impossible to have complete and total protection from malware. However, the risks can significantly be reduced by ensuring you have an antivirus program from a reputable provider installed. Keep virus definitions, search engine and software up-to-date to ensure your programs remains effective.



4. Use a secure file sharing solution
The documents, data and files you share are only as secure as the tools you use to share them with. Always use a secure file sharing solution to encrypt your files when sharing and at rest to prevent unauthorised access and keep your files safe.

5. Store important information in secure locations

When storing information online, you will want to keep it in a location that cannot be accessed by unauthorised users. This tip can be combined with a safe file sharing solution.

6. Use a VPN

For a more secure and disguised network, use a VPN to encrypt your connection and protect your private information.

7. Avoid opening suspicious emails

If an email looks the slightest bit suspicious, resist the temptation to open it and click on any link or attachment. It could potentially be a phishing scam.

In a phishing attempt, the attacker poses as someone by tricking the recipient into divulging credentials or by means of clicking a malicious link or opening an attachment that can infect the user's system with malware, trojan or a zero-day vulnerability exploit. This can often lead to a ransomware attack. Approx 90% of ransomware attacks originate from phishing attempts.

Phishing scams can be carried out by phone, text or through social networking sites - but most commonly they are done via email.
Be suspicious of any “official-looking” email message or phone call that asks for personal or financial information.

8. Check links before you click

Links can easily be disguised as something they’re not, so it is best to double check before you click on a hyperlink. On most browsers, you can see the target URL by hovering over the link. Do this to check links before you click on them.

Avoid visiting unknown websites or downloading software from untrusted sources. These types of websites can often host malware that will automatically install and could potentially compromise your computer and then give access to your data.

If attachments or links in an email are unexpected or suspicious for any reason, don’t click on them.

9. Have strong passwords and keep them secure

It might seem obvious, but many people still do use their names, date of birth or those of their partner and children for passwords and keep them on their desktops or worse on a notepad on their desk. It is important to use a combination of letters, numbers and special characters for each required password . If you are likely to forget your new style passwords, store them in an encrypted format or adopt a password management tool.

10. Avoid Bluetooth if you can, or disable when not needed

Hacking via Bluetooth is commonplace and one of the easiest ways to gain access to your data. If you do not need it, turn it off.

11. Enable 2-factor authentication

2-factor authentication is now commonplace with many of our personal online accounts, so add it to your business ones to keep them more secure. It's another layer of protection that helps verify that it's actually you who is accessing your account and not someone who's unauthorised.

2. Always check for HTTPS on websites

When browsing a website that isn't using HTTPS, there's no guarantee that the transfer of information between you and the site's server is secure. Double-check that a site is using HTTPS before you give away personal or private information.

13. Use HTTPS on your website

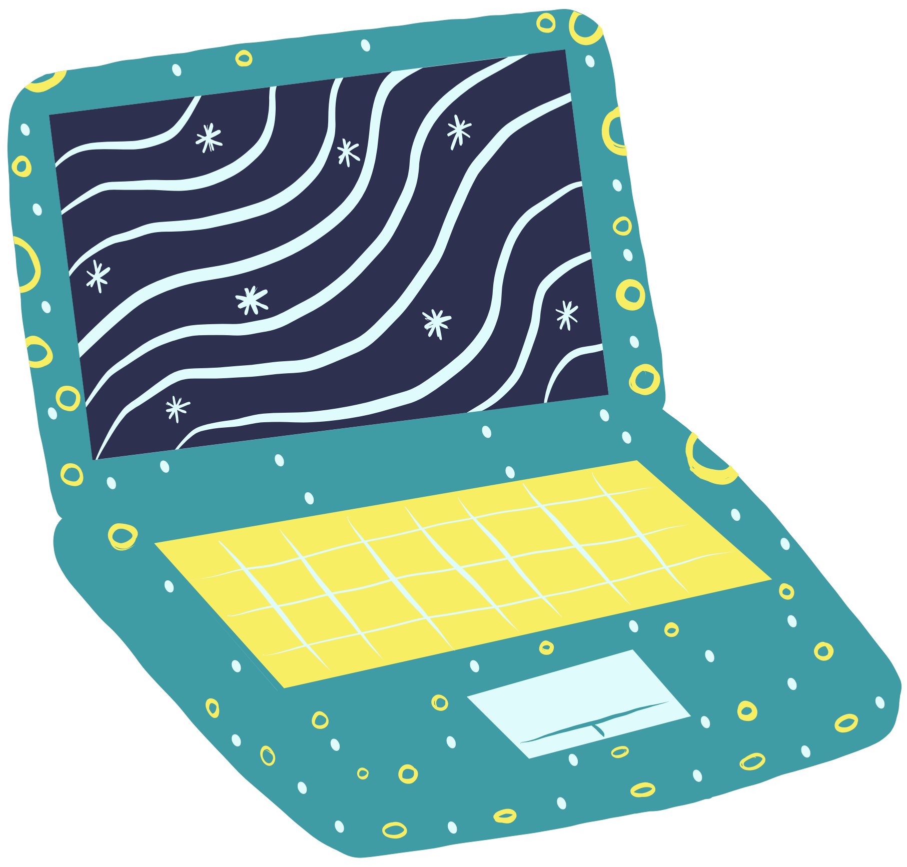
Having an SSL certificate installed, and HTTPS enabled on your website will help encrypt all information that travels between a visitor's browser and your web server.

14. Disable USB ability

Staff bring in their own devices and connecting them to your computers and systems can be very dangerous and also expose businesses to malicious use of them. An option to avoid this could be to disable USB ports.

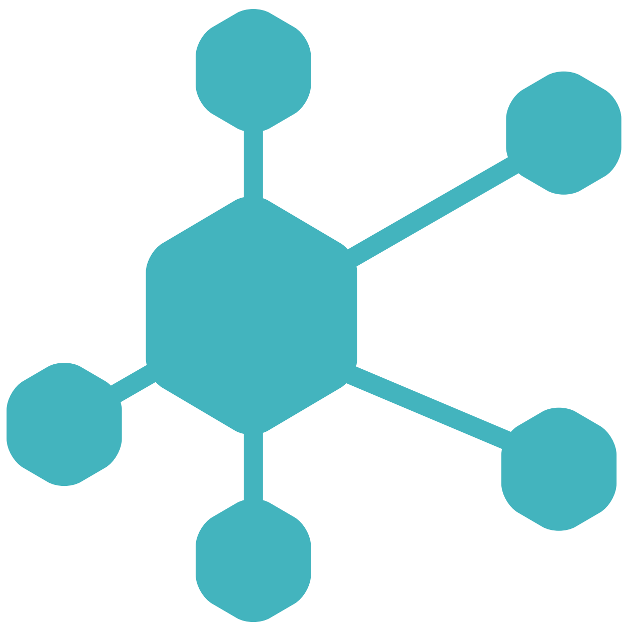
15. Scan external storage devices for viruses

External storage devices are just as prone to malware as internal storage devices. If you connect an infected external device to your computer, the malware can spread. Always scan external devices for malware before accessing them.



16. Avoid using public networks

When you connect to a public network, you're sharing the network with everyone who is also connected. Any information you send or retrieve on the network is vulnerable. Stay away from public networks or use a VPN when you are connected to one. By using VPN software, the traffic between your devices and the VPN server is encrypted.



17. Back up your data regularly

Business critical as well as personal data can be lost as a result of a security breach. To make sure you are prepared to restore data once it's lost, you should ensure your data is backed up frequently in a cloud solution, a local storage device or both. Anything sensitive should be encrypted. Adopt the 3-2-1 backup rule. You keep three copies of your data on two different types of media (local and external hard drive) and one copy in an off-site location (i.e cloud storage).

18. Invest in training your staff

The key to making cybersecurity work is to make sure your staff are well trained, understand the risks, and are consistently exercising security practices. Sometimes, one mistake from an improperly trained employee can cause an entire security system to crumble.

19. Develop a full range of policies

There is little point in only the business owners and IT team knowing what security measures are in place, so all measures should be clearly documented in plain English for all staff to be able to easily read and understand them. They can form part of a training plan for your staff.

20. Bring in a "White hat" tracker

Not all hackers are criminals. Some hackers expose security risks for the sake of helping others improve their cybersecurity by keeping them aware of security flaws and patching them. These hackers are known as "white hat" hackers. It might benefit you to hire one to help you find risks you never knew you had.

In conclusion

There is plenty that can be done without delay and with no or limited cost to minimise your risks of a successful cyber attack.

If you do not have in-house cyber security expertise to implement the more technical options, consider bringing in an expert either as a member of staff or a consultant. The additional cost will at least help business owner sleep easier, or could prevent the collapse of the business if the worst happens.

Get in touch...

0151 440 2993
askus@payepass.com
www.payepass.com