+44 345 094 0945
www.waterstons.com

Article

Jan 2022

12 Cyber questions to ask you and your business…

At the end of 2021 we launched the 12 days of Cybermas on our LinkedIn channel, with the aim of sharing cyber security information, and top tips and tricks to keep you safe. But cyber tips aren't just for Christmas! These are relevant all year round. We've compiled our posts together here, so grab a brew and a biscuit (unless you've also joined in on the new year, new me…) and consider the following questions to see how your organisation's security measures up.

Have you got a contingency plan in place?

A 2020 report by FireEye found that only 24% of cyber-attacks occur during normal work hours. Attacks are often launched during out of office hours or in the middle of the night when the response is likely to be slowest. Therefore, unsupervised IT networks and systems over any holiday or bank holiday period provide an easy opportunity for attackers to exploit. A contingency plan is essential to avoid a scramble to contact key individuals when everyone is off. We recommend that all organisations develop a comprehensive cyber incident response plan for vulnerable periods and have a full incident response plan in place all year-round.

Does your business have a positive Cyber Security Culture?

As most cyber attacks on rely on human intervention although technology systems will reduce risk, it's important that your colleagues know how to defend against cybercrime.

At Waterstons, we make sure all new starters undertake a cyber safety course as part of their induction, no matter what part of the business they are in. This enables them to develop their understanding of security risks, helping to better protect them and the company.

Some top tips for creating a positive culture around cyber security.

1. Raise awareness: ensure your people know who and how to report an incident to
2. Knowledge: ensure your people have a good understanding of cyber security and how it can impact them at work
3. Culture: ensure your people feel comfortable reporting this, without feeling at fault
4. Share cyber success: praise those who have prevented an attack

Have you considered social media phishing?

With over 1.3 billion users a day, social media is becoming a favourite target for many hackers.

A study by Google found that email phishing is on average 13.7% effective. In contrast, a later study by Blackhat found that social media phishing attacks were up to 66% effective.

Whilst there is any number of spam-filtering tools and technologies in the market, the best way to prevent attacks is to educate your people about the potential threats, as they are the first line of defence.

For more information, read the full article here: What is social media phishing and how can it affect you and your business? | Waterstons

How strong are your passwords?

Research shows that using a **passphrase** is a better defence against hackers. This is typically created with three random words, you can also include symbols and numbers e.g ChocolateSnowmanHedgehog! Using a passphrase instead of a simple password can increase the time it takes a hacker to crack using a supercomputer from around 1 second to potentially thousands of years. We recommend this as it's both memorable and secure!

Have you switched on your VPN?

When out shopping or in a public space, remember to switch on a VPN (virtual private network). This is an encrypted network that allows secure connections for remote users. Joining a public Wi-Fi without a VPN makes it easier for cyber criminals to access your private information.

Have you set MFA up?

Multi-Factor Authentication (MFA) is an effective way of preventing hackers accessing your accounts even if they managed to crack your password (or better yet, passphrase).

MFA is a security measure, requiring two or more proofs of identity to access accounts. We recommend that businesses implement MFA as soon as possible.

There are multiple forms of a secondary authentication, such as an Authentication App.

When was the last time you updated?

All IT equipment that is not up to date usually contains weaknesses, making it easier to hack. Ensuring that operating systems and applications are up to date (also known as patching) is a simple, yet essential part of improving and maintaining your IT security.

Therefore, we recommend turning on automatic updates wherever possible, or ensuring systems are checked regularly.

Have you considered the remote working security risks?

Many organisations are still largely working from home, but with this comes added risk to cyber security. This is due to most work locations having more protection through firewalls and IT management.

The first step to increasing security, is identifying the vulnerabilities. Check with your IT team about implementing a company VPN, antivirus software, and multi-factor authentication. Also, educating employees on cyber security is a great defence.

Have you considered your cloud vulnerability?

The cloud is a vast platform of hundreds of tools that has changed the way businesses do IT. However, as cloud adoption increases, so do the cloud cyber security threats.

Misconfigurations of cloud settings are a leading cause of cloud data breaches. It is important to have suitable security management strategies in place for protecting this infrastructure.

A fully managed cloud solution, can protect and enhance the long- term security and effectiveness of your environment.

Are you aware of your *organisation's* digital footprint?

A digital footprint is a record of all your interactions online and it is important to be aware of this, as it can have a huge impact. All organisations and staff members will have one. Two key areas to consider:

Security: your digital footprint can contain sensitive information that cyber criminals can use to their advantage. Open-source intelligence (OSINT) is intelligence gathered from publicly available sources, like social media. To protect your business, it is best to check what is already out there. Get information about a company - GOV.UK (www.gov.uk)

Reputation: If you are a business, how is your organisation perceived online? Look into reviews, comments, posts by employees, and the news.

Are you aware of your *personal* digital footprint?

Two key areas to consider:

Employment: One thing to consider is future employment opportunities, as employers may search for you online. You want to ensure that your footprint is a positive one.

Personal privacy: Protect your personal information by limiting what you share and avoid answering social media posts which can allude to passwords, such as 'favourite pets name' and 'mother's maiden name'.

Are you aware of the changes to Cyber Essentials and Cyber Essentials Plus?

Cyber Essentials and Cyber Essentials Plus are UK certification schemes that help you protect your organisation against security threats. The NCSC and IASME have released a significant update to the Cyber Essentials and Cyber Essentials Plus standards, which will take effect as of January 24th 2022.

To provide a grace period of implementation, Cyber Essentials submissions started before January 24th will be honoured for **6 months**, allowing you time to comply with the new standard.

Additionally, organisations awarded with the previous Cyber Essentials standard will be audited against the previous Cyber Essentials Plus standard version, as long as this is done within 3 months of achieving Cyber Essentials.

More information can be found here.

We hope some of these tips have been useful. If you have any questions or concerns, then please get in touch with our dedicated cyber resilience team. They can work with you to design, implement, and optimise pragmatic security controls aligned with best practice such as Cyber Essentials and ISO 27001 to ensure your critical data and systems are always protected whether on premise or in the cloud– helping you sleep easier at night.

To find out more and how to protect yourself and your business online, take a look at our cyber security course on our online academy.