howden
specialist insurance brokers

RICS PARTNER

Cyber protection – The essentials

Regardless of the size of your business, you are an attractive target for hackers. Don't ever say "It won't happen to me" and don't underestimate how clever cyber criminals can be.

We know the topic of cyber security can be baffling and the terminology is like an alien language however it is important to be aware of the risks and what they mean to you personally and to your business. If you work from home and your family share the computer you use for work, they may also need to read these essential tips (which apply to the use of computers for personal purposes just as they do for business purposes).

1. Practice good password management

Change your passwords every thirty days. Use a mix of characters e.g. numbers, letters, lower case, upper case and punctuation marks. Don't use the same password for multiple sites. Don't share your passwords with others. Don't write them down, and definitely don't write them on a note attached to your monitor or even hidden in your desk drawer. Use a password manager to help you to manage multiple, complex passwords.

2. 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 so no one can use it while you're gone. If you keep sensitive information on a flash drive or external hard drive, lock them up as well.

3. Don't think that your mobile device is safe from threats

Mobile malware is the fastest growing segment of malware. When downloading apps, download from trusted sources and choose apps from trusted developers. Install a trusted security app on your mobile device.

4. Always be careful when clicking on attachments or links in an email

If it's unexpected or suspicious for any reason, don't click on it. Double check the URL of the website because bad actors will often take advantage of spelling mistakes and direct you to a harmful domain. Also, be aware that just because you're at work and protected by security solutions, it doesn't mean malicious spam can't slip through.

5. Sensitive browsing should only be done on a device that belongs to you, on a network that you trust

This includes any form of browsing that includes accessing or divulging your banking details for example online shopping or online banking. If you do it on a friend's phone, a public computer, or a cafe's free WiFi – your data could be copied or stolen.

What does it all mean?

Botnet: computers that, without their owner being aware of it, have been set up to forward transmissions to other computers on the internet.

Phishing: an online method used by fraudsters to access valuable personal details, such as usernames and passwords.

Vishing: a telephone call to someone, by a fraudster, in an attempt to get the user to surrender private information that will be used for identity theft.

Password attacks: a third party trying to gain access to your systems by working out your password.

Denial of Service attacks (DOS): attackers send high volumes of data or traffic through the network to disrupt the service to a network. Eventually, the network becomes overloaded and can no longer function.

Malware: software that is specifically designed to gain access to or damage a computer without the knowledge of the owner. Malware often masquerades as legitimate and necessary security software that will keep your system safe (known as rogue software).

Malvertising: you click on an affected advert which then compromises your computer with malicious code that is downloaded to your system.

Man in the Middle (MITM): by impersonating the endpoints in an online information exchange (i.e. the connection from your smartphone to a website), the MITM can obtain information from the end user and the entity they are communicating with.

Drive-by downloads: through malware on a legitimate website, a program is downloaded to a user's system just by visiting the site. It doesn't require any type of action by the user to download.

Spyware: programs that secretly record what you do on your computer.

6. Be cautious about what you share on social networks

Criminals can befriend you and easily gain access to a shocking amount of information – where your children go to school, where you work, when you are on holiday. Information like this could help them gain access to more valuable data.

7. Browse with Care

Another favourite of cybercriminal's is poisoned search results or black hat SEO. Malware writers use our curiosity against us by exploiting high-profile events. This could include a celebrity scandal, new tech gadget or major events like the Olympics, an election or sporting event. While search engines like Google are very good at protecting us from these threats, cybercriminals can successfully launch entire websites within hours of sensational news breaking. No matter how enticing these sites may appear, rest assured, they are designed with the sole purpose of delivering malware. It may take Google a few hours to identify and remove these sites from its search results, but in that time plenty of users can already be infected. Always be careful what you're searching for and what sites you visit. Again, don't assume you're protected because you believe your work has good security. Threats – especially newly created threats – can always slip through.

8. Back up your data regularly and keep your anti-virus software up to date

The best defence against malware is to always update software programs when prompted. If a message appears on your screen to update a trusted software application, do it as the update will often be designed to correct an issue that may have serious security implications. If your organisation uses an automated patching solution, these updates should be deployed automatically. However, be mindful of Zero-day alerts from your IT team as these may instruct you to avoid using certain programs when a threat is identified.

9. Think before you plug a new device into your computer

Malware can be spread through infected flash drives, external hard drives, and even smartphones.

10. Think before your download

Cybercriminals know that users are concerned about security and often employ messages and pop-up screens that appear to be legitimate programs on your PC requesting updates. Clicking on these links can lead to downloading malware and installing rogue applications. These rogues may claim to be antivirus products or system cleaning programs. They look authentic, but they are designed to infect your PC to extort money from you, or to install additional malware on your computer. If you see a warning claiming your PC is infected, don't click anything. Contact your IT team or provider. It is important to never take the chance.

11. Be wary offline as well as online

If someone calls or emails you asking for sensitive information, it's normal to be wary. You can always call the company directly to verify credentials before giving out any information.

12. Regular monitoring

Check your financial accounts for suspicious activity. If you see something unfamiliar, no matter how small the amount, it could be a sign that your accounts have been compromised.

13. Employee awareness

Make sure that everyone is aware of the need to be careful and that they follow this guidance.

Our expertise

Cyber risks are multi-dimensional and will impact different firms in different ways. To ensure that surveying businesses are equipped to respond rapidly and effectively in the event of a data breach and are covered for any losses arising, we have developed an exclusive cyber liability insurance product for RICS regulated firms. Underwritten by leading Cyber Liability insurers, CFC, the product provides breadth of cover, access to specialist incident response services and discounted premiums for RICS regulated firms. For larger, more complex businesses requiring a tailored approach, our cyber liability experts will use their knowledge of the surveying industry and cyber exposures to develop bespoke solutions.

Howden expertise in the Professional Services industry

Howden is the Royal Institution of Chartered Surveyor's preferred Professional Indemnity Insurance broker and preferred Cyber Liability Insurance Broker. With over 20 years' experience in the surveying sector, we place over £25m of premium a year on behalf of the industry, looking after several of the UK's largest property services firms. Our specialist property and construction team has over 200 year's combined industry experience and we look after the full range of surveying firms from sole trader building surveyors through to estate agents and quantity surveyors and valuation surveyors and panel managers.

We recognise the importance of developing strong relationships with both your business and your insurers. We believe in building relationships based on trust and respect. We work with businesses that take their insurance seriously and recognise the value that working with a specialist broker can add.

Our first priority is always to ensure that you and your business benefit from breadth of coverage and that the person you deal with understands the cover you require and can clearly articulate the product you are buying. Where coverage requires tailoring to meet a specific business need we have the knowledge to identify the requirement, the expertise to design the solution and the negotiating strength with insurers to deliver it. Our experience and relationships with insurers combine to enable us to find and develop insurance solutions at a time when insurers don't or can't underwrite the business due to rising claims volumes. This is why we dominate some of the most challenging professional sectors

Established in 1994, Howden UK Group employs over 2,200 people around the world. Whilst our size gives us a significant advantage when it comes to negotiating coverage, premiums and claims with insurers, we remain absolutely committed to ensuring our customers continue benefitting from the personal relationships, quality of service and specialist knowledge they have received over the last 20 years.

Greg Harrison
Account Executive
020 7133 1505
greg.harrison@howdengroup.com

Andrew Broome
Accountants Executive
020 7133 1425
andrew.broome@howdengroup.com

Rob Skingley
Director
020 7133 1439
robert.skingley@howdengroup.com

Matt Farman
Director
020 7133 1565
matt.farman@howdengroup.com

Natalie Deacon
Account Executive
020 7133 1437
natalie.deacon@howdengroup.com

Matt Baker
Associate Director
020 7133 1567
matt.baker@howdengroup.com

Please call the Howden Professional Indemnity Team

T 020 7133 1300
E pii@howdengroup.com
@howdenpii

Howden UK Group Limited
16 Eastcheap
London
EC3M 1BD
United Kingdom

www.howdengroup.com

Part of the Hyperion Insurance Group

Broker at LLOYD'S