The coronavirus pandemic (COVID-19) has sent shockwaves throughout the world bringing with it a sense of fear and unease. There is also desire amongst the population to understand the virus and gain knowledge on how to protect against it. Unfortunately, but not unexpectedly, cyber criminals have used this to their advantage and are seeking to exploit those fears and uncertainty for financial gain. This coupled with the change in working practices with the number of individuals working remotely being at its highest ever levels, provide the perfect feeding ground for cyber criminals.

The World Health Organisation (WHO) has recently reported a fivefold increase in cyber-attacks against the organisation compared to the previous year¹. Scammers have also been impersonating the organisation in emails targeting members of the public and trying to encourage them to make donations to a fake WHO account in a fight against the pandemic and this is just the tip of the iceberg. The National Crime Agency has also warned there have been instances of COVID-19 themed malicious websites and apps, in addition to email phishing attacks all aimed at stealing personal and financial information².

With this in mind, in this article, we summarise the main cyber security issues we have encountered in recent weeks and where possible steps can be taken to minimise the risks of people falling victim to the cyber criminals.

Use of personal devices and Wi-Fi
Whilst organisations moved quickly to get staff connected at home by following the Government guidance during March 2020, many were unable to provide work computers. In some cases, employees began using personal devices. Those devices in many cases were often years, if not decades old, and lacking the tools required to ensure good cyber security such as customised firewalls, antivirus software and backup protection. This has significantly increased the ease with which cyber criminals can access an organisation and facilitate the theft or holding ransom of information, allowing them to intercept emails and re-route money transfers.

Likewise, in an office environment, IT managers generally control the security of all Wi-Fi networks. Unfortunately, home networks are likely to have weaker protocols, allowing cyber criminals to gain easier access to personal and financial information.

---

To minimise these cyber security risks businesses should make every possible effort to provide secure devices to employees and use a virtual private network (VPN). Where this is not possible, remote workers using personal devices should ensure that their operating system is up-to-date, and that firewalls and protective software are activated with the latest security patches as soon as they become available. Businesses should also ensure they are using secure wi-fi with strong password protection.

**Phishing, Smishing and Fraudulent Websites**

Phishing and smishing are emails and SMS messages used by cyber criminals to obtain personal information or gain access to an organisations computer system seeking out valuable personal and financial information. The emails and/or SMS messages appear to be from a genuine source but are in fact fraudsters impersonating a genuine organisation. UK PC magazine reported in March 2020 a 350% increase in phishing emails since January 2020. Generally, remote users are much more likely to fall prey to these phishing emails. The reason for this is unclear - it may be that users feel more secure at home or perhaps are distracted trying to multi-task with home schooling and work and fail to think before clicking on the link.

In addition, fraudulent websites with COVID-19 related domains are also on the increase. Those websites appear genuine but usually contain a link which when clicked attaches malware to the user’s device. Alternatively, the websites seek to obtain personal information from the user which they then exploit.

To prevent a successful phishing or smishing attack and stop fraudulent links being clicked, training of staff is key as well as the use of technology to block suspicious emails and prevent penetration in the event of a fraudulent link being clicked.

**Video conferencing technology**

As businesses have adapted to the new ways of working and have implemented innovative methods to host meetings and keep in touch with colleagues and clients, the use of video conferencing applications has surged. Those applications can collect a wealth of information, including location and IP address. To lessen the risk of privacy and data breaches, remote workers should only use applications which offer long standing IT support and have effective security in place and ensure staff receive training. Both the Information Commissioner’s Office (ICO) and the National Cyber Security Centre (NCSC) have issued guidance on how to use video conferencing technology securely and what risks to look out for.

**Email payment fraud**

This type of fraud occurs when a hacker intercepts the email communications between a business and its clients, compromising online transfers. To minimise the risk of email payment fraud, bank account details and invoices should never be sent in an open email.

If bank details are sent by email, it should be sent as a password protected attachment and the password should never be provided in the same, or a subsequent, email. The sender should instead exchange the password directly by telephone.

There is concern about the significant increase of COVID-19 related cyber scams and with more businesses operating remotely, the NCSC has recently issued guidance urging businesses to consider six key cyber security questions.

The NCSC guidance is recommending that businesses evaluate their cyber security measures and assess whether there are any deficiencies. For those businesses that have taken out a cyber insurance policy they will need to consider whether the current working practices impacts the policy.

---


In light of the heightened risk for cyber security breaches during these unprecedented times, the ICO has launched an information hub dealing with data protection issues and COVID-19 in order to support both individuals and organisations, which includes information about how data is being used during the pandemic to ensure that it remains safe in accordance with the requisite data protection legislation, as well as an update on the latest scams.

What we have learned from the pandemic is that working environments and how businesses operate have changed or will have to change. With these changes comes challenges, especially as we are moving out of the lockdown phase and businesses are preparing for employees to return to their workplace, with many operating by way of a hybrid system with a combination of employees working either in their businesses’ offices or continuing to work remotely from home. However, the key message in relation to minimising the risk of a cyber attack in these unprecedented times is to remain vigilant and remember to follow recommended guidance.

Other factors to be considered are:-

- Who has access to your IT systems and data and whether it is adequately protected
- Ensure all patches and updates are applied as soon as they become available
- Ensure backups are run frequently and are tested and the key people know who has access to the backup and where it is stored
- Only open emails or download software/applications from trusted sources
- Secure email systems to protect from spam emails
- To not click on links or open attachments in emails which you were not expecting to receive, or come from an unknown sender
- Use strong and unique passwords which should be changed regularly
- If you are uncertain about anything discuss the issue with your Data Protection Officer

For further information:

**Shauna McAuley**
Senior Associate Solicitor
Professional Negligence, Carson McDowell
+44 28 9034 8814
Shauna.McAuley@Carson-Mcdowell.com

**Joanne Cracknell**
Associate Director
Willis Towers Watson
+44 117 976 9376
Joanne.Cracknell@WillisTowersWatson.com

Each applicable policy of insurance must be reviewed to determine the extent, if any, of coverage for COVID-19. Coverage may vary depending on the jurisdiction and circumstances. For global client programs it is critical to consider all local operations and how policies may or may not include COVID-19 coverage.

The information contained herein is not intended to constitute legal or other professional advice and should not be relied upon in lieu of consultation with your own legal and/or other professional advisors. Some of the information in this publication may be compiled by third party sources we consider to be reliable, however we do not guarantee and are not responsible for the accuracy of such information. We assume no duty in contract, tort, or otherwise in connection with this publication and expressly disclaim, to the fullest extent permitted by law, any liability in connection with this publication. Willis Towers Watson offers insurance-related services through its appropriately licensed entities in each jurisdiction in which it operates.

COVID-19 is a rapidly evolving situation and changes are occurring frequently. The information given in this publication is believed to be accurate at the date of publication shown at the top of this document. This information may have subsequently changed or have been superseded, and should not be relied upon to be accurate or suitable after this date.

Willis Towers Watson is a trading name of Willis Limited, Registered number: 181116 England and Wales. Registered address: 51 Lime Street, London EC3M 7DQ. A Lloyd's Broker. Authorised and regulated by the Financial Conduct Authority for its general insurance mediation activities only.

About Willis Towers Watson
Willis Towers Watson (NASDAQ: WLTW) is a leading global advisory, broking and solutions company that helps clients around the world turn risk into a path for growth. With roots dating to 1828, Willis Towers Watson has 45,000 employees serving more than 140 countries and markets. We design and deliver solutions that manage risk, optimise benefits, cultivate talent, and expand the power of capital to protect and strengthen institutions and individuals. Our unique perspective allows us to see the critical intersections between talent, assets and ideas — the dynamic formula that drives business performance. Together, we unlock potential. Learn more at willistowerswatson.com.