SEIB INSURANCE BROKERS
Over 50 years of excellent service

PREPARING FOR THE INCREASED RISK OF CYBER ATTACKS DURING THE COVID-19 PANDEMIC

By SEIB Insurance Brokers, NAFD preferred insurance provider

Cyber attacks are far from just being the concern of big business, we are all targets. With that in mind, there are things we can all do to keep ourselves a lot safer online – ensuring the convenience of having connected devices isn't overshadowed by cyber threats.

Cyber criminals are using the disruption and challenges caused by the COVID-19 virus outbreak to increase attacks on businesses and individuals. For example, in January a number of phishing emails emerged that referenced COVID-19 but, by early March, they represented a significant percentage of all malicious email traffic. Likewise, an increasing number of malicious websites are being created using COVID-19, or related terms, with over 42,000 sites of this nature being registered since early February.

In addition, following the imposition of a Government lockdown to counter the spread of COVID-19, there has been a substantial increase in the number of people now working from home - many for the first time in their career - and this is another development that can provide hackers with more opportunities to breach IT security.

Extra vigilance is needed to defeat these attacks. We must not let ourselves become complacent in these unprecedented and challenging times when, perhaps, our focus is naturally drawn elsewhere.

A particular concern for funeral directors is that, during the past year, personal data has been the most targeted by cyber criminals. Under recent GDPR legislation, whilst a personal data breach may only apply to living individuals, the personal data for relatives of the deceased person still needs to be handled carefully and securely.

Care is also needed to avoid personal data breaches that could provide cyber criminals with information they can use to hold your business to ransom, damage your reputation, gain money from the press or even be sold on through other mediums, such as the dark web.

To help NAFD members, we set out below guidance on the most common types of cyber attacks, followed by advice on ways in which you can protect your business from cyber criminals.

Common methods of attack

Phishing emails:

- emails that appear genuine are sent, asking you to install software onto a device;

> FOLLOWING THE IMPOSITION OF A GOVERNMENT LOCKDOWN TO COUNTER THE SPREAD OF COVID-19, THERE HAS BEEN A SUBSTANTIAL INCREASE IN THE NUMBER OF PEOPLE NOW WORKING FROM HOME.

- special offers from commercial organisations offering free medical products or trials;
- a coronavirus cure;
- tax refund support or the offer of financial aid from the UK Government;
- safety advice from the World Health Organisation;
- home working and contacts from bogus HR Departments; or
- extortion requests demanding payment otherwise confidential information will be released.

You can find examples of phishing emails and what to look out for on the HMRC official website.

Malicious websites:

- creation of malicious websites, eg a bogus John Hopkins University website map that provides COVID-19 updates.

Smartphones:

- COVID-19 tracker applications (downloaded from third-party App stores).

Accessing these websites, or downloading the software to your computer, smartphone or tablet, is very dangerous. There's a very strong chance that you are downloading malware (malicious software) that could lock you out of your device or lock all of your files. There will then be a demand for money within a set time, otherwise all information on the device will be deleted. Other types of malware can monitor your activity without your knowledge, or take control of your device and use it to attack others.

Defeat the cyber criminals

Many cyber attacks can be defeated by following good practice and implementing basic security controls. These include the following:-

- continually raise awareness and remind individuals of the importance of computer security;

- encourage and support individuals with training so they can identify threats and how to respond;
- back up your data regularly, and in more than one place, if you are using an external hard drive, do not leave your backup connected to your device when not in use;
- although the cloud computing market is reasonably mature and most providers have good security practices built-in, we recommend you read the National Cyber Security Centre (NCSC's) Cloud Security Guidance before selecting a cloud service provider;
- keep portable devices safe, eg use PIN/password protection/ fingerprint/face recognition, keep device software updated, do not connect to public hot spots, use 3G/4G or VPNs and replace any devices no longer supported by manufacturers;
- prevent malware damage, eg regularly update anti-virus software and update your devices with the latest software patches. Only use approved software, control access to removable media, eg memory sticks, and ensure your firewall is always enabled;
- avoid phishing attacks, eg scan for malware, change passwords if a successful attack is detected and look out for poor spelling, grammar or images that may be indicative of a rogue email;
- protect data using strong passwords and encryption. Avoid using predictable passwords, and provide secure storage for passwords;
- have a tried and tested response plan in the event you do fall victim to an attack;
- continually assess and test the robustness of your cyber defences; and
- learn from any incidents and update your defences.

The NCSC also provides expert advice on how to enhance your cyber security on its website - at www.ncsc.gov.uk - where you can also find out about seeking certification under the Government's Cyber Essentials scheme, which demonstrates to others that you take the protection of data seriously.

Cyber Insurance

Having specific cyber insurance in place to mitigate the risk of a cyber attack can make a big difference in reducing the financial impact. Conventional business insurance policies may not cover many of the losses associated with cyber risks, such as having access to expert IT, legal, forensic and media relations advice and support when an incident occurs. This alone can help to greatly reduce the financial impact of a cyber event and any subsequent reputational damage.

To find out more about cyber insurance, cyber threats and what you can do to reduce the risk, please contact Liam Casserley, our Schemes Manager, on 07388 379203 or by email to lcasserley@seib.co.uk

A 'thank you' from SEIB

The past month or so has seen a dramatic change to everyone's lives. For some of us, it`ll be our first time witnessing such a rapid change within our communities. Drastic measures have been put in place to prevent the spread of COVID-19 and key workers, like you, have been working hard to support our communities and keep essential services running. Whether you're a funeral director, embalmer, celebrant or, indeed, work in any part of the funeral trade, we would like to say a sincere and heartfelt **thank you!**

About SEIB

SEIB has been supplying insurance to the funeral industry, including NAFD members, for over 40 years, giving us expert insight and understanding of such a unique industry. To find out more about tailored insurance protection please call us on 0345 450 0648 for a review of your cover requirements, or visit www.seib.co.uk.

SEIB
INSURANCE BROKERS.
Over 50 years of excellent service