Cyber-Risks and Liabilities

January/February 2021

How to Avoid Electronic Signing Service Scams

Although utilising an electronic signing service can be a convenient way for your organisation to digitally sign and exchange important documents (eg contracts, tax documents and legal materials) with stakeholders, doing so also carries significant cyber-security risks.

Cyber-criminals can utilise a variety of scamming techniques to trick electronic signing service users into sharing sensitive information, such as their signature, financial information and other personal data. From there, the criminals can use that information for a range of destructive purposes—including identity theft and other costly forms of fraud. These scams have become an increasingly prevalent threat in the midst of the ongoing COVID-19 pandemic, as many organisations have transitioned to fully remote operations.

In fact, DocuSign—a popular electronic signing service provider—recently released a statement regarding several new phishing scams that cyber-criminals have implemented to fool victims into thinking they are using DocuSign's services. These scams entail the victim receiving a fraudulent email that appears to be from DocuSign, urging them to either click on a malicious link (which then downloads malware on the individual's device) or provide their personal information (which scammers then access to commit fraud).

Whether your organisation uses DocuSign or a different electronic signing service, it's important to educate yourself and your stakeholders—including employees, investors, customers and suppliers—on how to detect and avoid falling victim to these phishing scams. That being said, consider the following cyber-security tips:

- Be wary of responding to emails that claim to be an electronic signature request—especially if you weren't expecting a request or don't recognise the name of the individual or organisation sending the request. Trusted senders would let you know they are sending a signature request before doing so.
- Never click on links from electronic signature emails that appear suspicious—especially if the URLs for those links redirect to websites that aren't secure or recognisable.
- Review electronic signature emails for generic wording, grammatical errors and misspellings (both in the body of the email and within the sender's email address). These mistakes are often key indicators of a phishing scam.

For additional cyber-security guidance, contact us today.

Dixons Commercial Insurance Brokers
01727 736 970
www.dixonsinsurance.co.uk

DIXONS
COMMERCIAL INSURANCE BROKERS

Smart Device Security Best Practices

As remote work continues to be a popular offering for many organisations, some employees have begun taking advantage of their own smart devices—such as smartphones or tablets—for work-related purposes.

While this practice can certainly help employees expand their remote work capabilities, utilising smart devices within a work setting can lead to elevated cyber-security risks. This is because your employees' smart devices may not be initially equipped with the security measures necessary to defend against cyber-criminals, thus increasing the likelihood of a cyber-attack taking place.

Don't let employees' smart devices lead to a cyber-security disaster within your organisation. Utilise the following guidance to promote smart device security:

- Establish a Bring Your Own Device (BYOD) policy that includes standards employees must uphold when using their smart devices for work-related purposes.
- Have employees create complex passwords for their smart devices. Encourage staff to enable multifactor authentication on their devices, if possible.
- Restrict employees from connecting to public Wi-Fi networks on their smart devices. Be sure to establish a virtual private network for staff to use to ensure a safe, secure connection.
- Have employees conduct routine software updates on their smart devices to prevent potential security gaps.

For more cyber-security best practices, contact us today.

Preparing for 2021 Cyber-security Trends

2020 saw a wide range of changes and advancements in workplace technology utilisation for organisations. But as digital offerings continue to evolve, so do cyber-security threats. That's why it's crucial to remain up-to-date on the latest technology trends and adjust your cyber-risk management strategies accordingly. As your organisation starts to prepare for 2021, keep the following emerging cyber-security concerns in mind:

- **Remote work issues**—While remote working is a valuable method for protecting staff from the ongoing COVID-19 pandemic, this practice can also lead to increased cyber-security vulnerabilities. After all, many employees may not have the same security capabilities in their work-from-home arrangements as they do in the workplace. As such, make sure your organisation provides remote staff with appropriate cyber-security training and resources, as well as implements effective workplace policies and procedures.
- **Cloud hijacking concerns**—With more employees working from home, maintaining cloud security is crucial. Cloud breaches have become more common in the past year, as cyber-criminals have developed a method for hijacking cloud infrastructures via credential-stealing malware. To avoid this concern, utilise trusted anti-malware software and update this software regularly.
- **Elevated ransomware threats**—Cyber-criminals continue to create new and improved ransomware attack methods each year. According to recent research from Cybersecurity Ventures, ransomware attacks are expected to cost organisations more than $20 billion in 2021, with an attack estimated to take place every 11 seconds. To help protect your organisation from ransomware attacks, use a virtual private network, place security filters on your email server and educate staff on ransomware prevention.
- **Data privacy expectations**—As more organisations start storing sensitive information on digital platforms, data privacy is a growing concern. If your organisation stores sensitive information digitally, it's vital to utilise proper security techniques to protect such data (eg encryption) and abide by all relevant data privacy regulations.
- **Skills shortages**—Despite ongoing advancements in workplace technology, cyber-security skills shortages have become a major issue for many organisations—with the demand for cyber-security professionals exceeding the number of individuals who are qualified for such a role. This shortage emphasises the importance of investing in effective cyber-security tools across all workplace devices to help minimise your risks.

With these trends in mind, it's important now more than ever for your organisation to secure adequate cyber insurance. For more information, contact us today.