Courtesy of
Crendon Insurance Brokers Ltd

CYBERRISKS&LIABILITIES_

Spam, Phishing and Spyware Defined

A computer intrusion could cripple your company, costing you thousands or millions of pounds in lost sales and/or damages. Hackers can obtain access to personal information in many ways, including spam, phishing and spyware. Below are definitions and examples of these three types of scams.

Spam
Spam is any unsolicited electronic content, often known as junk mail. It can take the form of a text message, direct mailer, phone call or email message. Spam emailing in particular is quite common, and spam emails often contain some form of scam, virus and/or invasive or inappropriate content.

Prevent your company from falling victim to scams and viruses in spam messages by teaching employees to ask the following questions while using company email:

- *Do you know the sender?* If employees don't recognise the sender's name, they should not open the email.
- *Is the grammar and spelling poor?* Sometimes spammers intentionally misspell words or use words incorrectly to sneak emails past your company's spam filter. Encourage employees to be on the lookout for this trick.
- *Have you received something from this sender before, but now the email looks drastically different?* It could be a fraudster. Encourage employees to look at all emails with a discerning eye, even those coming from known senders.
- *Does it sound too good to be true?* If it sounds too good to be true, it probably is.
- *Is it in your spam folder?* Make sure employees know the danger of opening messages that go straight to their spam folders. Many people consider spam to be annoying but harmless. However, the majority of computer viruses are 'caught' via email. Employees should never open messages that your system has designated as spam.

Additionally, company policies regarding computer use are an effective way to reduce the impact that spam has on your system. Minimally, your policy should require employees to:

- Turn off computers before leaving the office each day. Spam and viruses can strike a computer at any time when it is sitting idle and still connected to the Internet.
- Keep work email communications separate from personal communications. Employees should use a personal email that is not connected to the company email for personal communications.
- Limit the amount of time employees can spend on social media sites (for example, only allow them to use the sites during breaks), or prohibit their access entirely during the working day.

Phishing
A phishing scam is a phony email or pop-up message used to lure unsuspecting Internet users into divulging personal information, such as credit card numbers and account passwords, which will later be used by hackers for identity theft. A phisher's email can be very persuasive and believable if he or she is impersonating a well-known organisation or individual.

Keep employees safe from phishing scams by teaching them to:

- Be extremely wary of urgent email requests for any personal or financial information (their information or a client's).
- Call the company or individual in question with the number listed on the corporate website or in the phone book. Avoid using phone numbers within the email, as they could be phony too.

Crendon
Insurance
Brokers

This Cyber Risks & Liabilities document is not intended to be exhaustive nor should any discussion or opinions be construed as legal advice. Readers should contact a legal or insurance professional for appropriate advice.

- Do not use the links included in the email unless you are certain that the email is legitimate.
- Do not divulge personal or financial information via the Internet unless the site is secure (sites that start with ‘https’).
- Never disable anti-virus software.

Spyware
Spyware is software that can be installed on a computer without the user’s permission, usually as a result of the user opening an attachment and/or downloading an infected file from an untrusted source. Spyware can be used by hackers to ‘spy’ on Internet users, track browsing habits and collect personal information such as credit card numbers.

Signs that spyware may be installed on a computer:

- The computer starts to suddenly run more slowly.
- Pop-ups appear when the user is offline.
- Internet browser settings are modified. New shortcuts, icons or toolbars may appear.

As most spyware is installed when users download free files from the Internet, it’s important to ensure that your employee Internet usage policy has a clause banning employees from opening or downloading personal files on work machines.

Many Internet Service Providers (ISPs) will offer security software to businesses at no charge, so be sure to ask. It is important to be vigilant and cautious about the content your employees open while using the Internet. Risky employee Internet use can have serious consequences for your company. For more information about safe Internet use and developing an employee Internet use policy, contact Crendon Insurance Brokers Ltd today.