

# PLAYING IT **SAFE**

Be **Cyber-Safe** with these helpful tips provided by  
**Crendon Insurance Brokers Ltd**

## Protecting Your Internet Privacy

*Avoid scams, viruses and other internet threats*

Because you work at a computer every day, your personal information, along with company information, is always at risk. asks that you follow our Internet use policies, including taking the following precautions to protect your computer at work.

### **Avoiding Phishing Scams**

Internet phishing scams use phony email or pop-up messages as bait to hook unsuspecting Internet users – like you –into divulging personal information such as credit card numbers and account passwords to be used for identity theft. A phisher's phony email can be very persuasive and believable. To avoid getting reeled in by a phishing scam:

- Be extremely wary of urgent email requests for any personal or financial information (yours or a client's); if you suspect the message is phony, do not use the links included in the email.
- Email personal or financial information only if the site is secure (addresses that start with https://).
- Never disable our anti-virus software.

### **Outsmarting Spyware**

Do not download any unauthorised programmes or files to your computer. Free MP3 files or other programmes often include software (adware) that tracks your Internet

activity. While legitimate adware companies disclose the data collected, some adware can also identify your personal information, which can be sold to a third party without your knowledge. That's considered spying and can put important company or personal information at risk.

### **Understanding Cookies**

When you visit a Web page, a cookie is placed on your computer as a unique identifier. Cookies allow a Web server to store information on your computer and later retrieve it—like a personalised user ID.

Cookies have many useful capabilities. They allow the customisation of website experiences and let e-commerce businesses track visitors, page hits and popular pages. Internet settings can be personalised for higher or lower security levels regarding cookies. We have all company computers defaulted to the appropriate security level, including the cookies function—please leave this setting as is. Contact IT if you have questions.

### **Use Common Sense**

If you ever suspect that an email, website or link is not legitimate, do not click on it! It could have serious consequences if it contains a virus or spyware.



### **Trust Your Spam Folder**

Most people consider spam, or electronic junk mail, to be annoying but harmless. However, most computer viruses are 'caught' via email. Our spam filter is almost always effective in distinguishing spam from legitimate email, so do not open messages that our system has designated as spam.

This flyer is for informational purposes only and is not intended as medical or legal advice.

© 2004-2010, 2012 Zywave, Inc. All rights reserved.



**Crendon  
Insurance  
Brokers**