10 SIMPLE SECURITY STEPS TO PROTECT YOUR BUSINESS FROM THE RISKS OF DOWNLOADING OR INSTALLING ILLEGAL SOFTWARE FROM THE INTERNET

Downloading software from the Internet can be a “risky business” unless it’s from a reputable source. With many sites offering what appear to be terrific deals, it can be easy to find yourself in an unsuspecting customer base. Why gamble with Internet piracy if you don’t have to?

The BSA is providing a check list of “10 simple steps,” which can protect you and your business against the risks of using illegal software from the Internet. The majority of these can be implemented easily and without expense. Protect your business with these 10 simple steps:

1. Create and Enforce an Internet Usage Policy for Employees.
Include a policy on Internet usage as part of an employee’s employment contract. Have all employees agree to a policy, which prohibits them from downloading software or other applications from the Internet. An example of a policy document is available on the BSA’s website at http://w3.bsa.org/singapore/events/besamready/upload/codeofethics.pdf.

2. Engage and Train Your People.
Solicit your employees’ support to protect their work and your business’ assets by having them take personal responsibility for the contents of their work computer or laptop.

Regular, short training sessions would help those who are not IT experts and may not realize the impact of downloading content from the wrong Internet source. The threat to your business also threatens their jobs and livelihoods.

3. Install Firewalls and Virus Protection.
As the first-line barrier for the protection of your computers, ensure that you install and maintain the latest firewalls, spam filters, anti-spyware and anti-virus software.

4. Limit the Use of ‘Foreign Devices.’
Require that employees use only approved accessories such as company issued CD-ROMs, USB memory sticks and other devices. Home PCs rarely have the same level of security protection, making them more likely to be infected by viruses and other threats, which can be transmitted from home to work by such devices.

5. Check Before You Buy.
Before purchasing new software, check the dealers’ credentials. Be wary of buying from spam e-mail offers or online auction sites where software appears remarkably cheap. If in doubt, don’t buy. When purchases arrive, check the authenticity of the packaging and the license agreements. If you have any questions, contact the manufacturer.

6. Appoint a ‘Software Officer.’
Assign one of your employees to take responsibility for software use in your organization. That way, have your own company expert who can focus on what software employees require to perform their job and ensure these products are available from reputable sources so employees are less tempted to acquire software themselves.

7. Secure Software Master Disks and Paperwork.
Archive all the documents relating to your official software purchases, such as license agreements and print off license agreements if you download your software from a website. When you buy or download, a reputable site should require that you click a box confirming you have read and understood the license agreement and, at this stage, you can print your own copy for future reference. Whether you download software from a website or purchase a boxed item, any reputable dealer will require that you agree to the terms of the license. Store the master disks in a safe place that is only accessible by authorized personnel.

8. Conduct Software Audits.
Conduct an inventory of your hardware and software assets using tools available at: http://www.bsa.org/country/Tools%20and%20Resources/Free%20Software%20Audit%20Tools.aspx?sc_lang=en-US-SG

or by enlisting an independent specialist to check the software on each computer in your company. This audit will ensure that your employees are complying with your corporate policy while identifying rogue software and as part of your general business continuity strategy.

9. Stay Informed.
Visit the websites of the companies whose software or applications you use for up-to-the minute information and news about Internet security. Check with your security software provider on their update process and ensure you know whether updates to tackle new threats will be conducted automatically or if they will need action from you. You can find many of these links at BSA’s website at http://www.bsa.org.

10. Get Expert Help and Advice.
Visit the websites of local government agencies and business organizations—such as Intellectual Property Office of Singapore —for guidance on copyright protection and advice on protecting your business. This information is usually available free or at low cost.