RISK INSIGHTS

DIXONS
COMMERCIAL INSURANCE BROKERS

Protect Your Computer Systems from Malware

Your company might not be a target of global hacker organisations, but don't think that means your computer systems are safe and secure from threats. Malware, short for malicious software, is prevalent and can affect any size company, big or small. A study conducted by leading computer security software company, Sophos, revealed that a new unique malware threat emerges nearly every half second on average.

Arming your company to fight malware threats means using technology to protect your internal computer systems and educating employees on the best practices to stay safe.

What is Malware?

Malware is a general term that describes viruses, worms, Trojan horses, spyware, adware, rootkits and other unwanted software or programs. Once a malware program has gained access to a device it can disrupt normal computing operations, collect info and control system resources. Malware programs are being produced at an alarming rate and are always changing form and purpose, making detection and prevention harder for business owners.

Secure Your Systems and Educate Employees

Computer security industry experts recommend using layered web protection, implementing different tools together, to reduce the surface available to attack.

Some of the top sources of malware programs are the most popular and widely used features of the Internet, including email, social networking, search engines and especially pornography sites. To avoid your employees visiting these sites and potentially exposing their computers and your networks to malware programs, you can implement organisation-wide computer protections such as blocking certain websites.

Other protections that businesses can use include not allowing employees to have administrator rights to install programs, depending on the need for those rights as it relates to the functions of their job. This would prevent employees from falling for fake anti-virus scams, which often display a pop-up window claiming that they must install a program or run a virus scan, which installs a virus program on their computer.

> 'Malware' describes many different kinds of unwanted software. Once a malware program has gained access to a device, it can disrupt normal operations, collect information and control system resources.

Employee communications should be used to inform workers of the potential dangers of malware. Make sure your information security workers are keeping informed on the latest trends and developments in malware hazards. Let employees know about new threats and at-risk websites so they can avoid exposing their computers to them.

It is also important to have trusted anti-virus and anti-spyware programs installed on company devices. These programs should be set to perform scans on a regular basis for unwanted and harmful programs. Often it is best to perform virus scans overnight, when the computer is not needed for work use.

Protect Your Computer Systems from Malware

Emerging Hazards

Computers are not the only technology assets companies possess that are at risk from malware. Company issued tablets, netbooks and smartphones are all susceptible, as well. Anything that has access to the Internet is potentially at risk.

Smartphones are one device that employers should especially keep an eye on. Because phones are often used for a mixture of personal and business use, most employees will browse online and access personal email more frequently on these devices than others. This extra exposure increases the likeliness that the employee could expose the device to malware through a website or email attachment.

Something else to keep in mind is that all computers, no matter their operating system, are at risk for viruses and malware. A common misconception is that Apple® computers can't get viruses. The truth is that Apple computers are susceptible to viruses, worms, adware and spyware, just like all other computers.

However, since the majority of computer users utilise PCs, more malware programs exist to target them. As the market share of Apple computers continues to grow, companies utilising Apple products should be on alert as it is thought that more malware programs are being created to target them.

Contact Dixons Commercial Insurance Brokers for more information on protecting your business's interests from cyber threats.

RISK INSIGHTS