The Myths Hackers Love

Pick up any newspaper, on any day, and you are likely to find a headline about some new computer security threat, hacker attack, or virus. In fact, thousands of computers and networks are hacked every day, and big corporations are not the only victims. Every business, from the one-man-show to the Fortune 1000 enterprise, is a target for these attacks. All it takes is one hacker to spell immediate disaster for your business.

Guess what? This means that some day your business, too, will be a target.

However, your business does not have to become a victim. Protecting your computers, networks, reputation, and private information (like bank records, customer databases, confidential business plans, passwords, trade secrets, and more) is probably much easier and more affordable than you think.

To the delight of hackers, many businesses unknowingly leave their private information exposed to the world because they subscribe to some common myths about computer and network security. All it takes to prevent most common attacks is some education provided in this article and a little bit of your time. Is protecting your business' reputation worth skipping one lunch hour? Below are five common myths and the facts to dispel them.

MYTH - I have virus protection software so I am already secure.
FACT - Viruses and hacker attacks both endanger your business, but are two completely different things. A thief can wreck havoc on your life by breaking in though an open window or an unlocked door. It is important to secure both the doors *and* the windows. Anti-virus software is important to protect against viruses, but it does not do anything to secure your business against hackers or attacks.

MYTH - I have a firewall so I don't need to worry about security threats.
FACT - Firewalls are great and typically provide a good "front line defense" layer of security. However, firewalls commonly perform services such as port forwarding or network address translation (NAT), which could allow a hacker to bypass the firewall completely. It is also surprisingly common for firewalls to be accidentally misconfigured (after all, to err is human).

MYTH - There are too many computers on the Internet for anyone to target my business.
FACT - People understand the need to lock their homes, roll up their car windows, and guard their purses and wallets. Why? Because if you don't, then sooner or later, you will be a victim. However, people are just starting to be aware that the same is true with their computers and networks. A single hacker can scan thousands of computers looking for ways to access your private information in the time it takes you to eat lunch.

MYTH - I know information security is important, but it is too expensive, confusing, or technical.
FACT – It is true that some network security products and services are very expensive and geek-oriented. Nonetheless, simply ignoring your business' information security risks is a disaster waiting to happen. Nothing is ever 100% secure, but taking a few simple and affordable proactive steps can make your business *much* less "attractive" to hackers and attacks.

MYTH - Network and computer security is only important for large businesses.
FACT - Whether you are a casual home user or a global enterprise, your computer contains valuable and sensitive information. This could be financial records, passwords, business plans, confidential files, trade secrets, or any other sensitive data. Hackers will generally follow the path of least resistance and attack a business that is not defended. This is why a few simple steps go a long way to stop your business from becoming a victim.

So, now you understand the necessity to not ignore your business' information security risks. Of course, the big lingering question is still "how to address these risks…" Here are a few simple steps to help keep your business from becoming a victim:

1. Get a remote security analysis of your network. This will tell you exactly where your current vulnerabilities are, how to fix them, and let you know the current quality of security of your network. It is important to fix any outstanding security risks, otherwise any other steps could be useless.

Price Estimate: $25 per computer

2. Install high-quality anti-virus software. Although this won't protect you against hackers or security break-ins, it will protect you from virus infected emails or files. Viruses could also install a Trojan on your network, potentially exposing your sensitive information.

Price Estimate: $45 per computer

3. Install a hardware network firewall device. This will act as a good "front line defense" for your business. There are also software-based firewalls that might provide a layer of protection. However, for business purposes, a hardware-based firewall is much more practical.

Price Estimate: $200 for a small office network

There is no silver bullet to information security. However, taking a few simple, proactive, and affordable steps can go a long way to protect your private data and keep your business from becoming a victim.

This article was written by Jay Jacobson, President of Edgeos, Inc.
<jay@edgeos.com> 480.961.5996
Please visit http://www.edgeos.com for more information.
*** Edgeos - Security is Critical ***
