



From The Desk of:

Joseph Stoll
President
Technical Action Group Inc.

Security Alert: Hackers And Cyber Criminals Are Now Concentrating Their Attacks on Small Business

BUSINESS OWNERS BEWARE: For the last two years hackers and cyber criminals have been increasingly turning their efforts to small businesses instead of large enterprise corporations. Why? Because small business networks offer a much easier “lock” to pick, unlike large enterprises who invest far more man power and money into high security for their network.

"As the security becomes better at large companies, the small business begins to look more and more enticing to computer criminals," said Charles Matthews, President of the International Council for Small Business, "It's the path of least resistance."

Think your network is secure? Take a look at these surprising statistics:

- One-fifth of small businesses don't have up-to-date antivirus software installed.
- Sixty percent don't encrypt their wireless links.
- Two-thirds of small businesses don't have a security plan in place.
- Eighty-five percent of the fraud occurs in small and medium-sized businesses.

Why is security so poor for small business? Primarily for two reasons:

Naiveté: Most small businesses believe that nothing could ever happen to them, and therefore don't take the necessary precautions to secure their network, monitor their systems, and train their staff.

They are also ignorant on HOW to get this done (which makes a strong argument for getting all of our clients on one of our managed services plans!) The second reason is that they are being frugal in the wrong places. Some simply refuse to spend money on securing their network. That's akin to having a beautiful home full of expensive furnishings and valuables, but refusing to buy a good lock for the door because it “costs too much.”



So what should you do at a minimum to protect your company? Here are 7 fundamentals:

1. Educate your users on security basics such as using strong passwords, shutting down PCs at night, and not downloading “cute” screen savers and illegal music. Some companies make computer security rules part of their standard HR policies and make each employee sign that they understand the rules.
2. Install a web filtering software to police users and prevent accidental (or intentional) slip-ups on the above- mentioned usage policies.
3. Install a good virus protection system on all computers on your network and maintain it.
4. Install a firewall and check the logs periodically (again, we manage that for our fully managed clients).
5. Remove all unessential services and applications installed on your servers. After e-mail, this is probably the biggest security vulnerability. If a hacker gets in, this will reduce their ability to use a forgotten service or application to exploit your network.
6. Keep all your servers updated with all the latest security patches.
7. Review and adjust the default settings on any of the appliances or software you install. Hackers know what these settings are and will use them to gain easy access to your network. This item nails more systems administrators than we care to admit.

For those clients enrolled in our Essential Care, Professional Care or Total Care Plans, they can rest assured we are taking good care of issues 3 through 7; however, if you would like to conduct a training class and develop an AUP (acceptable use policy) for your staff and then install a content filtering software (issues 1 & 2) to help enforce the policies, give us a call.

This training and software is a small price to pay for the peace of mind you'll have over your network's security. And since better than 80% of all security breaches happen because of an end-user mistake, you'll also be taking a big step towards protecting your assets.

For more insider tips on how to use technology to make your business run faster, easier and more profitably:

<http://www.technicalactiongroup.com/category/blog/>





Newsletter Article – Security Alert

56 The Esplanade, Suite 212
Toronto, ON M5E 1A7
T. 416.489.6312 F. 416-778-1714
Toll-free: 877.287.7701
www.TechnicalActionGroup.com

Provided as an educational service by:

Joseph Stoll, President
Technical Action Group Inc.
56 The Esplanade, Suite 212
Toronto, ON M5E 1A7
T: 416.489.6312
F: 416.778-1714
www.TechnicalActionGroup.com

About Technical Action Group

The Technical Action Group are profit and productivity specialists who simplify technology and operations making them a power tool that increases profitability, productivity, and operations.

The Technical Action Group provides network and infrastructure support to those small to medium-sized businesses that rely on technology to conduct their business and business-focused solutions tailored to each client's unique requirements helping them to:

- maximize their technology investment
- remove the burden of managing their day to day technology environment
- focus their attention on their core business

