

## Security Alert:

### Hackers And Cyber Criminals Are Now Concentrating Their Attacks On Small Business

At the recent 2009 Visa Security Summit, a new trend was revealed: hackers and cyber criminals are now turning their efforts to small “mom and pop” 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:

**Lack of knowledge.** 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 unaware of HOW to get this done.

**Being cheap in the wrong places.** Some companies 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.
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. Never keep any of the manufacturer's 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 care to admit.

If you haven't reviewed your network security recently or are concerned about potential vulnerabilities please contact us. We can help you develop an AUP (acceptable use policy) for your staff and then install a content filtering software or hardware solution to help enforce the policies.

This training and software or hardware 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.

Contact:

Ben Bolte, IT Director

800.834.7700

[bbolte@abc-computers.com](mailto:bbolte@abc-computers.com)