TechTip Postcard

Insider Tips and Secrets to Get The MOST Out of Your Computer

Oct. 2015 — VOL 12 — ISSUE 10

Your Computer Network Is Being Haunted!
(And It's Worse Than Ghosts And Goblins)

Your small business is under attack. Right now, extremely dangerous and well-funded cybercrime rings are using sophisticated techniques to hack into thousands of small businesses to steal credit cards, blackmail you to recover data and swindle money directly out of your bank account.

82,000 NEW malware threats are being released every single day and HALF of the cyber-attacks occurring are aimed at small businesses just like yours. You just don't hear about it because it's kept quiet for fear of bad PR, lawsuits and sheer embarrassment.

The National Cyber Security Alliance reports that 1 in 5 small businesses have been victims of cybercrime in the last year and this number is growing rapidly as businesses continue to move to cloud computing and mobile device, and to store more information online.

Here are 7 critical security measures your business must have in place to have any chance of fending off these criminals:

1. Train Employees On Security Best Practices. The #1 vulnerability for business networks is the employees using them. If they don't know how to spot infected e-mails or online scams, they could infect your entire network.

2. Create An Acceptable Use Policy (AUP) And Enforce It! An AUP outlines how employees are permitted to use company-owned PCs, devices, software, Internet access and e-mail. Having this type of policy is critical if your employees are using their own devices to access company e-mail and data.

3. Require STRONG passwords throughout your company. Passwords should be at least 8 characters and contain lowercase and uppercase letters, symbols and at least one number.

4. Keep Your Network Up-To-Date. New vulnerabilities are found almost daily on common software programs you use all the time; therefore it's critical you patch and update systems frequently.

5. Have An Excellent Backup. A quality backup can foil even the most aggressive ransomware attacks, where a hacker locks up your files and holds them ransom until you pay up. If your files are backed up, you don't have to pay to get your data back.

6. Don't Allow Employees To Download Unauthorized Software. One of the fastest ways to access your network is by embedding malicious code in seemingly harmless apps.

7. Don't Scrimp On A Good Firewall. Your firewall is the frontline defense against hackers, so you need a really good one, with monitoring and maintenance done regularly.

Network Concepts

Corporate Office
326 N. Main Street
Souderton, PA 18964
Phone 215-723-3495

Network Concepts

Service & Training Center
1250 Bethlehem Pike Ste E
Hatfield PA, 19440
Phone 215-997-2740

Want Help In Implementing These 7 Essentials?
During the month of October, sign up is **FREE**

Check out the Video & Sign up!
http://www.NCIWD.com/Haunted

Cybersecurity Audit (a $497 value). *Offer is only valid during the month of October 2015.*

Give us a call at 215-723-3495

www.NetworkConceptsInc.com

NCIBackup.com - NCIHosting.com - NCISupport.com - NCIWD.com

NETWORK CONCEPTS