TREND MICRO™ | Securing Your Web World

Top 10 Tips

to Keep Your Small Business Safe

Protecting your business against the latest Web threats has become an incredibly complicated task. The consequences of external attacks, internal security breaches, and Internet abuse have placed security high on the small business agenda—so what do you need to know about security and what are the key elements to address? Trend Micro sheds some light on this tricky subject.

WORRY FREE SECURITY

1 CLOSE YOUR DOORS TO MALWARE

In the same way that you wouldn't dream of leaving your back door unlocked at night, you wouldn't invite cyber criminals into your business. But, by not securing your computers, such as not having adequate firewalls and antivirus software, that could be exactly what you're doing.

In fact, an alert about increases in small business attacks was sent from NACHA, the Electronics Payments Association. *ComputerWorld* reported, "NACHA's alert said that the cyber crooks are apparently targeting small businesses because of their relative lack of strong authentication procedures, transaction controls and 'red flag' reporting capabilities. In some cases, the alert said, attackers are tricking small business workers into visiting phishing sites with the same look and feel as their company's financial institution, where they would log on using their credentials."

Malware is malicious software designed to infiltrate or damage a PC or network without your knowledge or consent.

- **Apply the firewall.** A good Internet router will have an on-board firewall (so don't forget to turn it on), but this is not enough nowadays with the complexity of malware.
- **Protect the PC.** The best security software will go beyond standard protection and will reside on the PC without hindering the performance of your PC, laptop or network. The best protection will encompass identity theft, risky websites and hacker attacks within a single solution.
- **See it to defend it.** Select a solution that helps you keep tabs on mobile users, and all your PCs and servers with a single console.
- **Be easy on mobile users.** Good security will have location awareness. This capability changes the security settings on laptops automatically to the best level of protection for employees as they move inside or outside the office.
- **Clean up email.** Antispam reduces unwanted email, blocks risks and distractions for employees. Stop processing spam by stopping it before it reaches your business.

2 WRITE YOUR POLICY

Think your business is too small for hackers to worry about? Think again. Size is really irrelevant when it comes to online crime and fraud and smaller businesses are easier targets because of stretched IT resources. So it's important that your business takes security seriously: teach employees and re-teach them about your security requirements. Write it. Communicate it. Enforce it.

Your policy should include, but not be limited to:

- **Share turn-ons and turn-offs.** Which applications can be loaded on a company computers and which are prohibited?
- **Require strong passwords.** Refer to Tip 4 on passwords.
- **Enforce consequences.** What happens if the policy is not followed? Be prepared to back up your words.
- **Use it. Don't abuse it.** What is the proper usage of a company-issued computer? This includes use of the Internet.
- **Educate about email.** Include internal and external communications as well as what should and should not be opened or forwarded.
- **Encrypt or be clear.** Decide if an email encryption solution to protect your sensitive information is required and when.
- **Appoint a "Go To."** Who is the person who employees can ask if they have questions about the policy or computer security in general?

3 TACKLE SOCIAL MEDIA BEFORE IT TRIPS YOU UP

Social Media is here to stay, so empower your employees with best practices and guidelines. The following are ways to minimize risks in social networks:

- **Look who's talking.** Decide who can speak on behalf of the company and only allow those employees to write about the internal and external events.
- **Define what's confidential.** In your security policy, cover social media sites like Facebook, Twitter, LinkedIn and more in your non-disclosure agreement for confidential business information.

- **Provide guidelines and a forum to develop them.** Social media blogging and posting for the company should have guidelines about what information is okay and who can post. Guidelines need to go beyond security:
  - Blogger should identify themselves as employed/paid by your company. You'll get backlash otherwise.
  - Define the tone of the blog.
  - Protect customer information and egos. Remind customers not to share personal information in a post and where to go for help with questions involving confidential information.
  - Decide when support information should be released in social media.
  - Get executive/owner sponsorship so guidelines can be adapted quickly with business needs in mind.
  - Use resources like BlogWell (www.blogwell.com) to develop your guidelines and learn about social media.
- **Be social, but be smart.**
  - You should only publish information that you are perfectly comfortable with being disseminated widely, depending on what you want to accomplish.
  - Assume the worst to get the best results. Encourage employees to limit the amount of personal information they share online for their safety and your company's safety.
  - Add only people you trust to your contact list.
  - Avoid clicking unexpected links coming from people you do not know.
  - Never trust anyone fully that you do not know that well.

4 PROTECT WITH PASSWORDS

Like it or not, passwords are the key to most small business networks, so they are important to protecting access to your networks. You don't have to be a statistics whiz to know that the more keystrokes and characters you add the stronger your password will be.

- **Start out strong.** Require strong passwords with a length of at least 8 characters with embedded numbers, so you can stop simple attacks that guess passwords.
- **Time to change.** Time out old passwords and require password changes frequently.
- **Keep them safe.** Educate employees about why writing down passwords, storing passwords on cell phones, or using guessable choices puts company security at risk.
- **Get the combination.** For the strongest passwords, don't use words at all. Use random letters, numbers and special characters. Make a pattern on your keyboard if you have to qWe4%6yUi is much stronger than goIrish#3.

5 GET CRITICAL ABOUT INTERNET SECURITY

The Internet is a fantastic business enabler. But, it can also increase malware exposure if your security does not provide proactive content scanning to track malware and alert you to the potential problems. Select security solutions that can help you conquer the latest threats with fewer distractions for your employees:

- **Stop the mad links.** Don't rely on employees to think about security or restrict where and when they can access the network or Internet. Automate updates and make security transparent for employees.
- **Keep the web productive.** Along with guidelines for acceptable web use, select solutions that stop unacceptable use. URL filtering can limit access to unproductive sites completely or during business hours and defends against risky links will keep your business, your employees and your data in your hands, not in the hands of identity or data thieves.

6 ASK EMPLOYEES FOR HELP

We've all seen the headlines that high profile data loss cases cause, but did you know that up to 80% of all data loss is caused by human error—either sending out confidential or sensitive information to the wrong people or in an unsecured way?

- **Comply or die.** Well, maybe not die, but the implications for data loss and accidental leaks are becoming even greater with increasing regulations. So, educate employees about regulatory requirements and best practices to protect information. Explain the risks not following the rules can present. Let them know it's their job to reduce the risks with their vigilance.
- **Explain to employees why they are important.** If individuals don't let scans run, or send inappropriate materials, the business can be a risk from malware, lawsuits, and a damaged reputation.
- **Get confidential.** Let all employees know what type of information is confidential and what potential problems can arise if these kinds of documents or files get out.

7 MAKE YOUR RESELLER/CONSULTANT RELATIONSHIP WORK FOR YOU

Having a good relationship with your IT reseller/consultant will mean that you always have a trusted advisor to turn to when it comes to IT issues.

- **Ask for more.** Rather than just giving you the best price or selling you on a promotion, the reseller or consultant you work with should be able to give you unbiased advice on your IT infrastructure. They can and should help you select the right solution for your business that will grow with your needs and protect your IT investment if they aren't, change resellers.
- **Outsource management.** Your reseller or consultant might even offer to remotely manage your security solution for you—meaning less hassle and even greater protection for you and your business, make it known that security is an important task for every employee.

8 LEAD BY EXAMPLE

If you don't walk the walk no one will walk with you. Whether you have a leadership position or not people look around to see what everyone else is doing. It only takes one person to make a difference.

- **Don't be the one.** It only takes one person to spread a nasty virus across the company.
- **Be an advocate.** If you have found a way to have better protection or hear about a new threat on the horizon let people know. Share best practices across departments.

9 BE CURRENT

Be sure your mobile users, PCs and servers are using the best available threat intelligence. Manual or infrequent updates for your security software open the door to threats. The cliché holds true; you are only as safe as your last update.

- **Free the PCs.** If your security solution is slowing your PCs, you are not alone. This is a common complaint with conventional security solutions. Look for solutions that make the vendor's datacenter do the work for you by using hosted capabilities. Save your PCs and servers for processing your business needs, not security.
- **Don't rely on old antivirus.** Traditional antivirus security caught threats by comparing files against their fingerprints or "signature" files on each computer. However, new threats are multiplying exponentially—over 2,000% since 2004—so sending more signature files is simply going to clog your PCs. New methods of detection perform the equivalent of background checks on email senders, files, and websites to protect better and faster without slowing your PCs.
- **Automate OS updates.** Make it as simple as possible for your PCs to have the latest patches. The vulnerabilities in your OS are a key enabler of attacks. Be sure to deploy these patches quickly and automatically.
- **Require and check patch compliance.** Give your users details about versions of software they need and how to check which the version they have. Provide links and directions on how to update to the correct version. If users see you are serious about compliance, they will be more likely to comply.

10 CHOOSE A SECURITY PARTNER, NOT JUST A VENDOR

Select a vendor who understands the unique needs of security in a small business environment.

- Choose a security vendor. Consider if your vendor is focused on security as a core business or as a part of their conglomerate.
- Check their record. Vendors with a proven track record of years of defense against multiple threats, with knowledge of both small business and enterprise experience can best support your protection.

RESOURCES

- TrendWatch offers educational videos, whitepapers and more: http://us.trendmicro.com/us/trendwatch/
- www.worryfree.com offers videos and information on Trend Micro products specifically designed for small business.

TAKE THE NEXT STEPS

Use the checklist below to see where your company is doing well. Then, determine which steps you want to take next.

TIP	**CHECK STEPS FULLY COMPLETED**
1. Close your doors to malware	□ Install and use security with protection from multiple threats (viruses, web threats, spyware, bots, etc.) □ Select a solution that can view and manage remote and local PCs, servers □ Know what's protected by choosing a solution with a single console for remote users, internal PCs, file and mail servers. □ Be easy on mobile users by selecting location aware solutions □ Clean up email with antispam
2. Write your policy	□ Put your policy in writing. (It is that important!) □ Educate employees and treat IT security policy like a contract □ Enforce the consequences of not following policies □ Define what employee can and can't do on companyPCs □ Educate about email best practices to avoid phishing, spam □ Encrypt email if you need to protect the content □ Assign a "Go To" or lead contact for IT security
3. Tackle social media	□ Define who can blog about the company publicly □ Define what's confidential or fair game □ Provide guidelines and a forum to develop them □ Be social, but be smart with what information you, employees make public
4. Begin with passwords	□ Require strong passwords □ Time out passwords for users □ Keep passwords safe, not on a post-it or iPhone □ Combine letters and numbers to stop thieves
5. Get critical about Internet security	□ Location is important, so make it easy to protect remote employees with location aware solutions □ Automate protection to block out risky web links and unproductive websites
6. Get help from employees	□ Comply with regulations, and good security practices □ Explain why employees are important to security □ Implement security policies □ Stress what is confidential, again
7. Make reseller/consultant work	□ Ask for more than order filling; find a business partner who can be a trusted advisor □ Outsource security management to your reseller/consultant, and take back valuable time and energy for your business
8. Lead by example	□ One person is key, so check your actions against the policy □ Find a trusted resource for security information and use it once per week
9. Be current	□ Free your PC by choosing a solution that offers hosted data center processing □ Don't rely on old antivirus; get multiple detection processes □ Automate OS updates □ Require and check patch compliance
10. Choose a security partner	□ Select security-focused vendor □ Check vendor's record by choosing an established company with enterprise and small business expertise

For more information, contact your Trend Micro Account Manager or visit: www.worryfree.com.

TREND MICRO™