



Small Business Guide to Protecting Critical Data

www.crusolutions.com

The Changing Data Security Landscape

The global Web links businesses like never before and it helps us deliver better products and services to our clients. However, our dependency on computing devices from smartphones to laptops increases our exposure to security risks like identity theft, malware and viruses. The use of social media opens new threat paths, and more small businesses are moving sensitive data like customer or financial information to the cloud.

What would happen if all your data disappeared? Security threats are evolving, small business security practices are not keeping pace, and the risk of loss, cost and exposure is increasing. In short, security disruptions can mean lost business.

Consider these statistics from Intel:

- 75% of small businesses experience two or more cyber attacks a year.
- Employee mobility increases the risk of PC and data loss. 15,000 laptops go missing EVERY WEEK in airports throughout North America and Western Europe.
- 50% of small businesses lack a plan to deal with IT disruptions.
- Only 23% of businesses back up data daily.
- On average, small businesses experience three IT disruptions a year.
- 50% of small businesses have lost critical data in the last year.

Clearly, protecting and preserving critical data and systems are key components of proper network management.

No business is too small to neglect proper network security. In fact, certain security measures are now required by compliance organizations like PCI DSS (Payment Card Industry Data Security Standard) and HIPAA (Health Information Portability and Accountability Act).

Use this guide to help you make informed decisions along with your IT provider.

Understanding External Network Threats

One of the most dangerous aspects of online threats is their ability to cloak their existence. Hackers and authors of malicious spyware and malware programs go to great lengths to create programs that are difficult to identify and remove. They are also highly experienced at finding tiny, overlooked loopholes in your security to access and infect your network undetected.

That means a malicious program can be downloaded and doing its dirty work on your network long before you are aware of it. Spyware, malware and hackers are among the three most common threats you'll need to guard against:

Spyware

Spyware is Internet jargon for hidden programs advertisers install on your PC. Often you unwittingly give permission for this software to be installed—it is in the fine print that most users skip during installation. But sometimes, out-of-mainstream vendors install this software without your permission. Either way the purpose is the same: to spy on you, gather information, and report this information about you and your online activities to some outside person.

Spyware is NOT harmless; it can be responsible for delivering a boatload of spam, altering your web browser, slowing down your PC, and serving up a bounty of pop-up ads. In some of the more extreme cases, spyware can also steal your identity, passwords, e-mail address book, and even use your PC for illegal activities.

Most spyware finds its way onto your computer network via file downloads including free programs, music files, and screen savers. While you “think” you are only downloading a legitimate program to add emoticons to your e-mails, you are unknowingly also downloading a heaping spoonful of spyware programs. **All it takes is one employee downloading a questionable file to infect your entire network.**

Spyware piggybacks the download and runs undetected in the background collecting information about you and sending it back to its originator until it is removed. Although spyware has malicious components, it is not illegal, and it is not considered a virus because it doesn't replicate itself or destroy data.

To protect yourself against spyware, consider drafting a company policy for acceptable downloads. Also, keep in mind that anti-virus software does not remove spyware.

Malware

Malware is short for **malicious software** and represents all programs, viruses, Trojans, and worms that have malicious intent to damage or disrupt a system. Malware is harder to remove and will fight back when you try to clean it from your system. In some extreme cases, we have had to completely wipe out all of the information on the computer's hard disk and start with a complete re-install of the operating system.

Among other things, a malware infection can corrupt your files, alter or delete data, distribute confidential information such as bank accounts, credit card numbers, and other personal data; it can also disable hardware, prevent you from using your computer, and cause an entire network to crash. Malware is designed to replicate itself from one computer to the next, either through a network connection or via your e-mail account without your knowledge or consent.

Hackers

Hackers are computer programmers turned evil. They are the people who design the spyware and malware programs that attack your computer.

Some of them have criminal intent and use these programs to steal money from individuals and companies. Some have a grudge against the big software vendors (like Microsoft) and seek to harm them by attacking their customers (you). Others do it purely for fun. Whatever the reason, hackers are getting more intelligent and sophisticated in their ability to access computer systems and networks.

You can defend yourself from hackers with company policies about approved software, approved installation processes, and strong edge device (firewall) security. The strength of the firewall is usually directly proportional to the cost of the device.

Signs Your Computer May be Infected

Since most malicious programs are designed to hide themselves, detecting their existence is not always easy. However, there are a few surefire signs that you have been infected:

- You start getting swamped with pop-up ads that seem to come from nowhere and constantly interrupt your use of the computer.
- Your computer is unstable, sluggish, locks up, or crashes frequently.
- Your web browser's home page changes on its own and you cannot modify the settings. You may also see toolbars on your web browser that you did not set up.
- You get a second or third web browser popping up behind your main browser that you didn't open or request.
- Mysterious files suddenly start appearing.
- Your CD drawer starts opening and closing by itself.
- You get constant runtime errors in MS Outlook/Outlook Express.
- You find emails in your "Sent Items" folder that you didn't send.
- Some of your files are moved or deleted or the icons on your desktop or toolbars are blank or missing.

Widespread Misconceptions about Spyware, Malware, and other Computer Threats

#1: Spyware and Malware are easy to remove.

Some spyware and malware CAN be easily removed using a program such as Spybot's Search & Destroy (you can download it for free at: www.safer-networking.org) or Ad-Aware (you can download it at www.lavasoftusa.com/support/download). Please read the end user license agreement carefully and be sure to stay in compliance.

However, not all malicious programs can be removed – or even detected – using the above software. Many programs integrate so deeply into the operating system that it takes a skilled technician several hours to fully diagnose and remove the malicious program. In some extreme cases, we have had no alternative but to wipe the hard disk clean by deleting all of the files on it and re-installing the operating system.

Obviously this is NOT an ideal situation and we do everything within our power to avoid it. Unfortunately there are some malicious programs that are so intelligent that there is simply no other way of removing them.

Of course you can use Spybot or Ad-Aware as a first attempt at cleaning your machine; however, if you continue to notice that your computer runs slow, if you continue to get crippling pop-ups, or any other of the tell-tale signs discussed earlier, you will need to seek the help of an experienced IT provider.

#2: It is my computer's fault that I continue to get attacked by spyware, malware, and viruses.

In all cases, malware, spyware, and viruses are a result of some action taken by the user (you or an employee). Remember, cyber criminals are *incredibly clever* and gain access to your computer via some of the most innocent and common activities you are performing; that is why it SEEMS as though it is your computer's fault.

For example, one of your employees could innocently download an emoticon software program. Emoticons are the smiley faces and action characters that you see at the bottom of many people's e-mails. It could also be a seemingly productivity-improving toolbar. In doing so he/she also (unknowingly) downloaded a payload of spyware and malware to your network.

Other deadly programs to avoid are free "enhanced" web browsers, screen savers, and just about any "cute" programs you come across that are free to download. Always read the terms and conditions before downloading ANY program to look for clauses that allow them (the software vendor) to install spyware programs on your computer. Employees should be restricted from downloading any of these programs from the web and educated to the dangers of these programs.

Installing programs is not the only way a hacker or malware program can access your computer. If you do not have the most up-to-date security patches and virus definitions installed on your

computer, hackers can access your PC through a banner ad on the web that you accidentally clicked on or through an e-mail attachment that you opened.

Just recently, hackers have even been able to figure out ways to install malicious programs on your computer via your Internet Explorer web browser EVEN IF YOU DIDN'T CLICK ON ANYTHING OR DOWNLOAD A PROGRAM. Microsoft is constantly providing patches to their operating system software and all it takes is one missed update to leave you completely vulnerable.

Finally, you should COMPLETELY AVOID any and all peer to peer file sharing networks such as KaZaa and Limewire. These sites are the absolute WORST online activities you can participate in for your computer's health because they are pure breeding grounds for hackers, spyware, malware, and other malicious attacks. Again, most of the infections we see come from employees accessing these websites for personal use on company machines.

#3: If my computer network is working fine right now, I don't need to perform maintenance on it.

This is probably one of the biggest and most deadly misconceptions for most business owners. Computer networks are just like cars. If you don't change the oil, change the filter, rotate the tires, flush the transmission, and perform other regular maintenance on your car, it will eventually break down and cost you FAR MORE to repair than the cost of the basic maintenance.

Maintenance checks that need to be done on a regular basis:

- Daily (like virus updates and spam filtering)
- Weekly (like system backups and a spyware sweep)
- Monthly or quarterly (like checking for and installing security patches and updates, disk defrag, spyware detection and removal, checking the surge suppressor and the integrity of the hard drive, and others)

Your IT provider should be adamant that you have regular maintenance done on your computer and should offer to set up automatic virus definition updates, spam filtering (to avoid viruses), and automatic system backups that are stored on an OFF SITE location (this protects the backup from fire, flood, or other natural disasters).

#4: The firewall and security tools provided in the Microsoft Operating System are all the maintenance and protection I need.

Again, this is a terrible misconception. Microsoft does NOT include ALL of the security features to protect your data from viruses, hackers, and data loss or prevent your PC from running slowly. As a matter of fact, there is no one single vendor that provides ALL of the system security features you need to keep your computer and files safe from harm.

Network Security Basics

Network security includes any activities that are designed to protect your computer network. Generally, security is required in two places: at the “edge” (where your network meets the Internet), and “inside” (devices in your internal network like desktops and laptops, policies for data security, and users who follow the policies). While no network is 100% secure, the right combination of hardware, software and user awareness can create a strong defense against threats.

Here are 6 tips to help secure your network from malicious attacks and avoid data loss:

#1: Use a Firewall or Unified Threat Management Device and Keep it Updated

Regardless of the size of your business, it is imperative that you do your best to secure your network from the myriad of outside threats on the Internet. At a minimum, make sure you have a firewall and that it is updated regularly. A more robust choice is a Unified Threat Management device that includes the benefits of the firewall with additional services including content filtering.

- A **firewall** is a hardware device with software that attaches to your network and controls traffic between your network and the Internet. The most basic function of the firewall is to conceal your network structure from outside threats, making it harder to break through. It helps block out hackers who can try to reach your computer. It is your first line of defense against threats. Basic firewalls can begin as inexpensively as \$100.
 - To check your firewall’s firmware to make sure it is updated, jot down the model number from the bottom of the unit. Go to the manufacturer’s support page on their website. Locate your model and follow the instructions for checking your firmware version and how to update it.
- We generally recommend a more robust edge security device called a **Unified Threat Management (UTM)** appliance. The UTM not only delivers basic firewall services, but it also includes gateway anti-virus, gateway anti-spyware and intrusion prevention to provide real-time security protection against the latest blended threats, including viruses, spyware, worms, Trojans, software vulnerabilities and other malicious code. In addition, a content filtering service can be locally controlled to block objectionable Web content, both for increased protection and productivity. UTM devices generally begin at around \$875.
 - Typically UTM appliances have annual subscriptions to keep these services up to date. While this is the first line of defense, you must still maintain protection at each computer attached to the network. If some type of worm is released inside your network, UTMs typically prevent it from leaving your network. Containment is the first step to eradication. UTMs often include VPN server services too. This moves VPN encryption for remote users to the edge of the network (rather than performing VPN functions on a server inside your firewall).

#2: Use Anti-Virus and Anti-Malware on Every Desktop or Laptop

In addition to edge security, each desktop or laptop on your network should have its own anti-virus and anti-malware. You might wonder why if you have those services on your firewall/UTM already. Occasionally, a threat may get through your edge security, so a second line of defense is needed. Perhaps more often, a threat can be introduced from inside your network, especially if users transfer files from their work computer to a home computer and back.

If people in your office use any type of removable media such as a flash drive or USB hard drive to copy files from one computer to another (like to a home computer), when that device is returned to the desktop at work it could introduce a virus or other threat. The user has bypassed all edge security, and the virus introduced to the desktop can then spread through the network.

Safe practices for copying files between computers should also be included in your company policies and procedures. Be aware that remote users or “working at home” users expose the company network to potentially unhealthy content of the home network. If someone uses a home computer for work activities, the work files could be exposed to threats from downloaded video games, online games, coupon sites, or other potentially unsafe sites commonly found on home computers.

Anti-virus and anti-malware software is generally scanning everything going in and out of your machine in real time. To keep up with evolving threats, it needs to be updated frequently, at least once a week, and keep your annual anti-virus and anti-malware subscriptions current.

#3: Maintain Critical Software Security Patches

In addition to edge security and workstation anti-virus and anti-malware, make sure that security patches from Microsoft or other software providers are installed on your computer. These security patches repair vulnerabilities in the software and protect your network.

User tip: Check for Critical updates from Microsoft at least monthly. Download them and apply to each computer (desktops, laptops, and servers)! To do this open Internet Explorer, Click on “Safety” and “Windows Update”. Let Microsoft scan your computer and recommend updates. Remember that if you already have a spyware or malware problem, this won’t fix it. You still need to remove the infections; the patches will help prevent a reinfection of same ailment.

Talk with your IT provider to make sure the devices in your network are being patched on a regular basis, at least monthly.

#4: Secure Your Wireless Network

Wireless access networks can be another entry point for threats. According to the TrustWave 2011 Global Security Report, 55% of breaches come through remote access.

- A wireless access point broadcasts signals outside your building – almost as though you are running network cables from your office into the parking lot and inviting anyone to plug in.
- At a minimum, make sure that you or your IT provider changes the manufacturer default security settings that come with your access point. If you're using a Unified Threat Management device, you could also consider putting the wireless access point on the "DMZ" (demilitarized zone), which provides a path from the wireless device to the Internet side of the UTM. That way, the only way a wireless user gets to the inside of your network is to open a secured VPN tunnel.
- Take all available steps to insure that if security to the access point is breached, only the Internet would be accessible, NOT your entire network.

#5: Ensure Secure Access for Remote Users

Remote users could be accessing your network from home, from on the road, or from another office.

A Virtual Private Network (VPN) creates secure access over the Internet from the remote user to the office network. Through a VPN, users can access their network directly, remote control one machine (from a laptop to a desktop, for example), or access a Terminal Server. Using VPN software, you create a secure, encrypted connection between the endpoints.

#6: Develop Computer Use Policies and Procedures, Educate Your Users and Keep Them Vigilant

As in most things, network security is only as strong as its weakest link. Often, that comes down to user awareness of basic security measures.

Make sure you have a computer use policy that outlines your expectations for the use of e-mail, confidentiality of company information, Internet use, and prohibited activities (such as computer gaming, illegal file copying, downloading unauthorized files such as video or music, etc.). Help employees understand how their computer use directly impacts the security of the company's data. In the past, some of these restrictions were considered heavy handed management. Today, users must understand that these activities present a genuine threat to the company—not unlike leaving the front door unlocked over a weekend.

A few basics for employees:

- Use passwords and don't share them with other staff people. The more complex the password the more secure it is. Don't use relatives' names, pet names, or hobbies. Here's the balance—make the password as complex as you can, but not so complex that you have to write it down!
- Don't download files like emoticons (☺), or other “cute” files from the Internet – those are often filled with viruses.
- Don't open e-mails from unknown sources or emails from known sources with questionable subject lines. When in doubt, delete.
- Don't open attachments to e-mails from unknown sources.
- Be cautious when using social networking sites. If it looks suspicious, it probably is. Facebook pages can be hacked and you can receive a message that looks like a message from a friend that is really a link to malware.

Security Protocol Checklist

Here's a summary of the six tips for securing your computer network:

- ✓ **Use a Firewall or Unified Threat Management Device and Keep it Updated**
- ✓ **Use Anti-Virus and Anti-Malware on Every Desktop or Laptop**
- ✓ **Maintain Critical Software Security Patches**
- ✓ **Secure Your Wireless Network**
- ✓ **Ensure Secure Access for Remote Users**
- ✓ **Develop Computer Use Policies and Procedures, Educate Your Users and Keep Them Vigilant**

About CRU Solutions

CRU Solutions, based in Cleveland, Ohio, helps small and medium-sized enterprises select and manage the right computer technology. Specializing in Managed IT Services, CRU Solutions has been helping organizations keep their networks secure for 29 years. To learn more, please visit us at www.crusolutions.com.