

Best Practices for Better Security

Protecting Your Data and Eliminating Vulnerabilities

You wouldn't leave your office door unlocked so anyone could come in and walk off with your company's equipment, read your files or wreak other havoc. That same sense of caution should apply to managing your company's Internet connection. When the Web and e-mail are integral parts of your business, you become vulnerable to viruses, worms, spyware, phishers and other security risks. Without common-sense precautions, they can cost your company through reduced network performance, diminished productivity, and even a damaged reputation.

Committing to security

Like insurance coverage and disaster planning, data security is about reducing risk. The open nature of the Internet makes a business more vulnerable to security issues. Viruses, worms and other malware can bring down a computer system. Spyware programs may let a third party surreptitiously monitor your computer usage to steal information. Phishers may pose as legitimate companies in an effort to get you to reveal confidential information. New hazards seem to arise daily.

Instituting some basic network security practices will help protect you against these threats. In fact, companies that manage their information security needs frequently gain benefits in a number of areas:

Information access. Your client lists, product development programs, employee data, financial records and other confidential information need to remain that way. This is the information that your company runs on, so it must remain available to those that need it, and inaccessible to those that might misuse it.

Productivity. An effective network security program boosts productivity across your organization. Employees spend less time on non-productive tasks such as sifting through spam or dealing with viruses. By keeping your network and Internet connections safe, you can also take advantage of productivity-enhancing tools such as wireless networks, workgroup and collaboration solutions, Internet-based telephony and conferencing, mobile computing or remote access.

Customer service. Keeping your Internet connection safe means that customers can reach you when they need to. A virus that brings down your network can impact your ability to serve your customers. If you can't take orders because your systems are down, you run the risk of losing business. Plus, an admission that you've lost confidential client information can irreparably hurt your company's reputation. But a commitment to security gives customers and business partners the confidence that their information remains safe.

Regulatory compliance. Many industries are now required to take steps to ensure the privacy of their customer records. Anyone conducting credit card transactions must adhere to guidelines of the financial industry, including the Payment Card Industry (PCI) Data Security Standard. Healthcare providers must comply with the guidelines of the Health Insurance Portability and Accountability Act (HIPAA). A strong security program takes these regulations into account and ensures that your company operates in compliance to protect not only company data, but also customer data.



Many industries are now required to take steps to ensure the privacy of their customer records.

Basic steps for security

The best data security practices are often a mix of technologies and policies that ensure that those technologies are used correctly. Below are some of the basic protections that a small/midsize company should take:

Develop a plan: The first step toward ensuring that your network remains secure is to have a clear, comprehensive security policy in place that lets employees know what their responsibilities are when it comes to using your network and the Internet. If this seems too formal, remember that if your security procedures aren't set down in writing, they're easy for employees to dispute or disregard. Your plan should cover:

- The components of your network, including the various hardware and software platforms and outside connectivity.
- Standards to be used for data security, including virus protection, firewalls, encryption, intrusion detection, etc.
- Employee responsibilities regarding acceptable use of the network, including remote access, appropriate Internet use and allowable software.
- The manner in which security breaches will be reported and handled. For instance, are there instances where law enforcement officials will need to be notified?

Assess risk: Review your network and Internet connections to determine where you are most vulnerable to security threats. If this is too daunting a task, take advantage of the services of a security expert—your network solution provider, for instance. Have this person run a security audit and make recommendations.

Protect against viruses, spyware and spam:

Viruses are perhaps the most prevalent security threat, and they are frequently sent via e-mail or through other "sharing" applications. Virus protection software will alert you to viruses, worms, Trojan horses and spyware, and may be able to eliminate them before they cause any harm. Virus protection should occur at two levels. First is at the individual computer level—each station on your network can be equipped with anti-virus software so that all files are scanned and cleaned regularly. Just as important, your service provider should offer anti-virus protection at the "network" level, meaning that data and e-mail that travel to your server are first scanned and inoculated before they reach your inbox.

Secure access and encryption: A simple way to protect your network is to equip your users with secure access via a Virtual Private Network (VPN). It provides you with the tools to authorize users to the network and provides auditing and reporting so that you can control user access to network resources. The VPN provides built-in encryption via IP Security (IPSec) or Secure Sockets Layer (SSL) technology standards. For additional protection, you may consider encrypting data on laptops in order to prevent data loss if the device is lost or stolen.

Maintain a firewall: A firewall establishes a protective layer between the outside world and your network to prevent access by anyone who does not use the proper log-in information. Firewalls can be composed of software or software-and-hardware combinations, and are particularly crucial when your network has an always-on connection to the Internet. Many network routers include this as part of the solution.

Track your security logs: Your network administrator should regularly review network access logs to see who has been trying to gain access to your servers and when they have been doing so. Keep an eye out for unusual usage. For example, a remote access attempt that is continually denied could point to a hacker trying to breach your firewall. An employee who appears to be trying to sign on during off-hours and weekends could indicate a stolen password. Also, be sure that each



user has a unique password, and never use vendor-supplied default system passwords—they're often the first ones that hackers will try. Treat every concern as a possible threat and always err on the side of caution. Administrators should also set up reports to inform business leaders when viruses, potential hackers or other threats are blocked. This helps keep data security practices top-of-mind and showcases the return on investment.

Exercise common sense

Remember the basics of computer and Internet security.

- Make sure employees know not to download files or e-mail attachments from people they don't know.
- Employees should be wary of e-mail from seemingly reputable sources that request information such as account numbers, credit card numbers, passwords or other personal information.
- Talk to your network administrator about using content controls that monitor Web use. These controls alert

you when employees are engaging in risky online behavior, sharing information or exchanging instant messages outside of the company.

- Educate employees on how to choose passwords that include a mix of uppercase and lowercase letters and numbers; avoid easy-to-guess words such as your child's name, your pet's name or your birthday.
- Encourage employees not to write passwords down on a piece of paper and put them next to their computer.
- Have your network administrator set computer log-ins so that the system locks up after three unsuccessful attempts.

These practices are just the beginning of establishing a culture that protects data and minimizes vulnerabilities. Thinking of security as part of the business process will help you incorporate data protection into the way your employees conduct business every day. That way, your business' data, reputation and productivity can remain safe and secure.



Secure Internet and Network Connectivity from CenturyLink

CenturyLink takes the security of your network seriously and provides a number of solutions that help ensure that network connectivity remains safe and secure. Whether you're connecting using CenturyLink High-Speed Internet or one of our more advanced services such as CenturyLink iQ Integrated Access or CenturyLink iQ Networking, we have options that help you monitor and manage your network security.

Some of the key security features available as part of CenturyLink's connectivity solutions include:

Anti-virus/anti-spam software: Protect your network from malicious content. CenturyLink's anti-virus protection solutions scan email and traffic moving over your connection to help ensure suspicious files don't make it through. Because this protection is maintained centrally, our security professionals respond quickly to add protection for new virus incidents.

Customizable content controls: Keep tabs on online activities. You can set limits on Internet access by time, day of week, type of activity or device. It also is possible to provide access to only the Web sites you identify while choosing content categories to block.

Professional-grade firewall: This solution uses two layers of firewall protection – hardware and software – to constantly monitor threats to your network and to help actively block unauthorized access to your computers and their contents. Reporting features give you details on the sources of threats and let you view security alerts by risk levels to see all inbound and outbound connections.

Managed security services: Protect your vital business data and enjoy greater peace of mind. CenturyLink Managed Security Service provides comprehensive threat protection and options for malware (viruses) mitigation, Web filtering, spam filtering, access control and VPN support. CenturyLink combines around-the-clock monitoring, management and support – along with visibility into service information through an online self-service portal. Leveraging IBM Internet Security Systems X-Force®, CenturyLink can help you improve system uptime and performance, optimize security investments, demonstrate compliance and improve employee productivity.

Why CenturyLink?

CenturyLink delivers reliable, scalable data and voice networking solutions, across one of the largest U.S. fiber footprints, with industry-leading SLAs and world-class customer service.

Learn more about the security features of CenturyLink's solutions at: www.CenturyLink.com/business

