6 Basic Steps for Better Security

Businesses of all sizes are vulnerable to security threats, and new hazards seem to arise daily. Small and midsize business may have fewer resources for dealing with security threats, but no less responsibility for them. How do you reduce the risk of data exposure, minimize vulnerabilities in your network, ensure regulatory compliance and still maintain productive access to information?

The best data security practices are often a mix of technologies and policies that ensure that those technologies are used correctly. **Follow these six essential steps to help protect your business and improve productivity.**

1. **Develop a Plan** A clear, comprehensive written security plan should cover:
   - □ The components of your network.
   - □ Standards to be used for data security, including virus protection, firewalls, encryption, intrusion detection, etc.
   - □ Employee responsibilities regarding acceptable use of your network and the Internet.
   - □ How security breaches will be reported and handled.

2. Assess Risk

- □ Review your network and Internet connections to determine where you are most vulnerable to security threats.
- □ If needed, engage a security expert such as your network solution provider to conduct your security audit and make recommendations.

3. Protect Against Viruses, Spyware and Spam

- □ Equip each computer on your network with anti-virus software so that all files are scanned and cleaned regularly.
- □ Your service provider should offer anti-virus protection at the network level to neutralize threats before they reach your inbox.

4. Maintain a Firewall

- □ A firewall is particularly crucial when your Internet connection is always on.
- □ Your firewall establishes a protective layer between the outside world and your network to prevent unauthorized access.
- □ Many network routers include a firewall as part of the solution.

5. Track Your Security Logs

- □ Your network administrator should regularly review network access logs for unusual usage.
- □ Administrators should also set up reports to inform business leaders when viruses, potential hackers or other threats are blocked.

6. Educate Your Team on Security Threats

- □ Urge employees not to download files or e-mail attachments from people they don't know and to be wary of e-mails requesting sensitive information.
- □ Talk to your network administrator about using content controls that monitor Web use.
- □ Educate employees on how to choose strong passwords and remind them not to keep password reminders near their computers.
- □ Have your network administrator set computer log-ins so that the system suspends the log-in after three unsuccessful attempts.

Excerpted from the white paper "Best Practices for Better Security: Protecting Your Data and Eliminating Vulnerabilities." Download the full white paper now.

CenturyLink™
Business