Cyber Security Checklist

Protect Your Business From Unauthorized Access and Attacks

ADVANCED SECURITY SOLUTIONS

According to IT Governance, the number of records breached in 2010 and in 2016 jumped from 3.8 million to 3.1 BILLION. Protection is no longer a luxury but a necessity.

Infinity, Inc. understands the risks facing SMBs today. We believe that the better educated people are about the variety of threats we face, the better our chances of stopping those attacks from spreading.

Use the following checklist to start building up your business's cyber security. Consult with your IT services provider to ensure these steps are being taken to your satisfaction, and feel free to contact the team at Infinity, Inc. if you have questions or want help along the way.

Keep your network and data safe so you can keep serving your customers.

INFINITY CALL 912.629.2426 TO DISCUSS YOUR CYBER SECURITY NEEDS

CYBER SECURITY CHECKLIST

Cyber criminals aren't going away anytime soon. But you can take steps to guard your business against them. Use the following list to protect your business.

- ☐ **Conduct a security risk assessment.** Understand potential security threats (e.g., downtime from ransomware) and the impact they may have on your business (lost revenue). Use this information to shape a security strategy that meets your specific needs.
- ☐ **Train your employees.** Because cyber security threats are constantly evolving, an ongoing semi-annual training plan should be implemented for all employees. This should include examples of threats, as well as instruction on security best practices (e.g., lock laptops when away from your desk). Hold employees accountable.
- ☐ **Protect your network and devices.** Implement a password policy that requires strong passwords that expire every 90 days. Deploy firewall, VPN, and antivirus technologies to ensure your network and endpoints are not vulnerable to attacks. Consider implementing multifactor authentication. Ongoing network monitoring should also be considered essential. Encrypt hard drives.
- ☐ **Keep software up to date.** Using up-to-date software products and being vigilant about patch management is critical. Cyber criminals exploit software vulnerabilities using a variety of tactics to gain access to computers and data.
- ☐ **Create straightforward cyber security policies.** Write and distribute a clear set of rules and instructions on cyber security practices for employees. This will vary from business to business but may include policies on social media use, bring your own device, authentication requirements, etc.
- ☐ **Back up your data.** Daily backups are essential for recovering from data corruption or loss resulting from security breaches. Consider using a modern data protection tool that takes incremental backups of data periodically throughout the day to prevent data loss.
- ☐ **Enable uptime.** Choose a modern data protection solution that enables "instant recovery" of data and applications. Application downtime can significantly impact your business's ability to generate revenue.