DURHAM IT SERVICES

Is Your Business's Cybersecurity Healthy? A Simple Self-Check Guide

Why Cybersecurity Matters for Your Business

As a business owner, you handle sensitive client and company data—financial records, employee information, and proprietary documents. But did you know businesses are prime targets for scams, ransomware, and data breaches? A single weak spot can lead to financial loss, legal trouble, and a damaged reputation.

The good news? A quick security checkup can help you spot risks before they become disasters. This guide walks you through key areas to review. If you're unsure where to start, an IT professional can give you a clear, actionable security assessment.

Your Cybersecurity Self-Check: 6 Key Areas to Review

Take a few minutes to evaluate your business's cybersecurity with this checklist:

01 ✅ Device Protection & Secure Access: Are Your Systems Properly Managed?

Why it's important: Businesses rely on computers, laptops, and cloud applications to operate efficiently. If devices are unprotected, sensitive information could be at risk.

How to check:

- Ensure all office computers, laptops, and mobile devices are set up with secure access controls.
- Confirm that software updates and security patches are applied regularly.
- Check whether staff use strong passwords and multi-factor authentication (MFA) for logins.

💡 **Tip:** If you work remotely or store files in the cloud, secure access management is critical to prevent unauthorized entry into your systems.

02 ✅ Data Backup & Recovery: Can You Restore Important Files If Needed?

Why it's important: Unexpected data loss—due to accidental deletion, hardware failure, or technical issues—can disrupt your business. Regular backups ensure you never lose critical data.

How to check:

- Verify that your business files are backed up daily.
- Ensure backups are stored in a secure, separate location (cloud or offsite storage).
- Perform a test recovery to confirm that files can be restored quickly if needed.

💡 **Tip:** Backups should be automated and regularly checked—it's not enough to assume they're working.

03 ✅ Microsoft 365 Backup: Are Your Emails & Documents Secure?

Why it's important: Many business's use Microsoft 365 for emails, OneDrive, and SharePoint, but Microsoft does not provide built-in long-term backups.

How to check:

- Ask your IT team whether you have a separate backup for Microsoft 365 data.
- Ensure backups retain deleted emails and files in case they need to be restored.

💡 **Tip:** Cloud-based collaboration is convenient, but having an independent backup solution adds an extra layer of security.

4. ✅ Data Encryption: Is Confidential Client Information Properly Secured?

Why it's important: If a laptop or USB drive is lost, unencrypted data could be accessed by unauthorized individuals. Encryption ensures that only authorized users can access sensitive files.

How to check:

- **On Windows devices:** Ensure BitLocker encryption is turned on.
- **On Mac devices:** Confirm that FileVault encryption is enabled.
- If staff use external storage (USB drives, external hard drives), check whether encryption is enabled for those devices as well.

💡 **Tip:** Encryption is a key compliance measure in protecting client data and meeting regulatory standards.

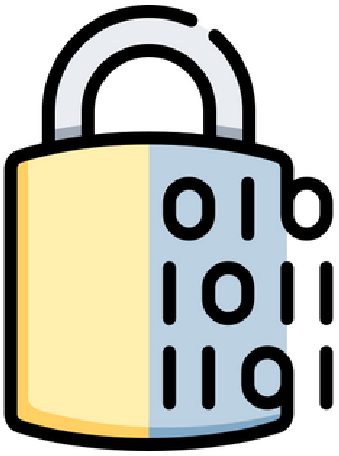
5. ✅ Email Security: Are Your Communications Protected?

Why it's important: Businesses regularly send and receive sensitive information via email. Ensuring secure email communications helps protect data from being accessed or intercepted.

How to check:

- Use email encryption for sending confidential documents.
- Enable Multi-Factor Authentication (MFA) for email accounts.
- Ensure your email provider has security filtering to detect and block suspicious messages.

💡 **Tip:** Clients expect secure handling of their information. Email security measures protect both you and them.



06 ✅ Ransomware Protection & File Security: Is Your Data Safe from Unauthorized Changes?

Why it’s important: Business’s rely on accurate and unaltered records. If files are accidentally or maliciously changed, your ability to operate efficiently is impacted.

How to check:

- Ensure your system monitors for unusual activity in company records and shared files.
- Check if your business has file versioning enabled, so you can revert to previous versions of documents if needed.
- Confirm that you have automated security alerts if unauthorized changes or file encryptions occur.
- 💡 **Tip:** Protecting business data isn't just about keeping it safe—it’s also about ensuring that records remain accurate and trustworthy.

Your Cybersecurity Self-Check: 6 Key Areas to Review

Without a Security Checkup	**With Strong IT Security**
Risk of data breaches	Client data stays protected
Loss of files due to ransomware	Backups ensure quick recovery
Financial loss from downtime	Proactive monitoring prevents disruptions
Increased stress & legal liability	Peace of mind knowing systems are secure

Need Help? Get a Professional Cybersecurity Review

Even with this checklist, it's not always easy to know if your business is truly secure. A professional IT security audit can:

✓ **Identify risks you may have missed**
✓ **Provide a clear security scorecard**
✓ **Offer actionable steps to strengthen your cybersecurity**

If this feels overwhelming or you're unsure where your business stands, consider booking a one-time security checkup with an IT expert. A proactive approach now can save you from costly security failures later.
🔹 **Have questions? Let's chat.**

Final Thoughts: Take Control of Your IT Security

Cybersecurity isn't just for big corporations—it's crucial for any business handling client data. Taking a few minutes to check these key areas can make a huge difference in protecting your business's reputation and financial stability.
If you'd like a deeper security review, talk to an IT professional to ensure your business is fully protected. **A little proactive effort today can prevent major problems tomorrow.**

📢 Need guidance? Want a security checkup? **Let's talk!**

Phone: (905) 231-1303
Email: info@durham-it.ca

Contact us today to get expert help securing your business!

Office :

190 Harwood Ave. S
Ajax, ON
L1S 2H6

Phone Number :

(905) 231-1303

Email :

info@durham-it.ca