



SMALL BUSINESS CYBERSECURITY CHECKLIST

Simple steps for a stronger, safer business.



A few smart habits today can help protect your business, your customers and your peace of mind tomorrow.

1 PASSWORDS & ACCOUNTS



☐ Use a unique password for every important account.



☐ Store passwords securely in a password manager.



☐ Enable multi-factor authentication (MFA/2FA) wherever possible.



☐ Keep recovery email address and phone number up to date.

2 DEVICES & SOFTWARE



☐ Keep your operating system, apps and browsers up to date.



☐ Use reputable security protection on your devices.



☐ Lock your computer and mobile devices when unattended.



☐ Remove unused software, apps and user accounts.

3 WEB & EMAIL



☐ Verify unexpected login or account requests before entering credentials.



☐ Check web addresses carefully. Look for misspellings, extra words and strange subdomains.



☐ Remember: HTTPS (padlock) means the connection is encrypted, not that the site is legitimate.



☐ Pause before opening unexpected attachments or clicking urgent links.

4 BUSINESS & RECOVERY



☐ Back up important files and your website regularly.



☐ Test your backups to make sure they can be restored.



☐ Give employees, contractors and vendors only the access they need.



☐ Have a plan for what you will do if an account is compromised.

STOP • LOOK • VERIFY



If something doesn't look right:

- ✓ Don't enter your password.
- ✓ Close the page.
- ✓ Go directly to the official website.
- ✓ When in doubt, ask someone you trust.

Small steps today. Stronger security tomorrow.



Run Your Business From Anywhere

🌐 Domains | ✉ Email | 🌐 Websites

SMALL BUSINESS CYBERSECURITY CHECKLIST

Simple steps for a stronger, safer business.

A few smart habits today can help protect your business, your customers, and your peace of mind tomorrow.

1 PASSWORDS & ACCOUNTS

- ☐ Use a unique password for every important account.
- ☐ Store passwords securely in a reputable password manager.
- ☐ Enable multi-factor authentication (MFA/2FA) wherever possible.
- ☐ Keep your recovery email address and phone number up to date.

2 DEVICES & SOFTWARE

- ☐ Keep your operating system, apps, and browsers up to date.
- ☐ Use reputable security protection on your devices.
- ☐ Lock your computer and mobile devices when unattended.
- ☐ Remove unused software, apps, and user accounts.

3 WEB & EMAIL

- ☐ Verify unexpected login or account requests before entering credentials.
- ☐ Check web addresses carefully for misspellings, extra words, and strange subdomains.
- ☐ Remember: HTTPS (the padlock) means the connection is encrypted — not that the site is legitimate.
- ☐ Pause before opening unexpected attachments or clicking urgent links.

4 BUSINESS & RECOVERY

- ☐ Back up important files and your website regularly.
- ☐ Test your backups to make sure they can actually be restored.
- ☐ Give employees, contractors, and vendors only the access they need.
- ☐ Have a plan for what you will do if an account is compromised.

STOP • LOOK • VERIFY

Pause before you click.
Check the URL and details.
Make sure it is really legitimate.

If something doesn't look right:

- ✓ Don't enter your password.
- ✓ Close the page.
- ✓ Go directly to the official website.
- ✓ When in doubt, ask someone you trust.

A simple habit worth adopting: If an email asks you to log in and you aren't sure it's authentic, don't click first. Verify it — or ask someone you trust to check it.

Small steps today. Stronger security tomorrow.

Barefoot Domains • Run Your Business From Anywhere