PORT::ZERO CYBERSECURITY QUICK CHECK

24 practical safeguards for stronger cyber readiness

PORT::ZERO CYBER SOLUTIONS

Protect Against Cyber Threats®

Check each item your organization currently practices.
A simple way to strengthen your cyber hygiene and reduce everyday risk.

Date: _____

Your Score: _____ / 24

1. Password & Account Security

- ☐ Use long, unique passwords or passphrases (ideally 16+ characters).
- ☐ Never reuse passwords across accounts.
- ☐ Use a reputable password manager.
- ☐ Enable multi-factor authentication (MFA) on every account that supports it (prefer phishing-resistant methods when available).

2. Phishing & Social Engineering

- ☐ Pause before clicking unexpected links or opening attachments.
- ☐ Verify sender addresses, domains, and unusual requests.
- ☐ Confirm sensitive or financial requests through a trusted second channel (e.g., phone or known contact).
- ☐ Report suspicious messages using your organization's reporting process.

3. Safe Web & Network Use

- ☐ Verify the website and domain before entering credentials or sensitive information.
- ☐ Avoid downloads, extensions, and software from untrusted sources.
- ☐ Avoid sensitive activity on networks you do not trust.
- ☐ Use your organization's approved VPN when required for remote access.

4. Devices & Software

- ☐ Enable automatic operating system and application updates.
- ☐ Lock devices whenever they are unattended.
- ☐ Keep approved endpoint protection and firewall controls enabled.
- ☐ Install software only from trusted or organization-approved sources.

5. Data Protection & Recovery

- ☐ Back up important information regularly and confirm it can be restored.
- ☐ Protect sensitive data with encryption and appropriate access controls.
- ☐ Store business data only in approved locations and services (e.g., company cloud).
- ☐ Securely dispose of sensitive digital and paper information when no longer needed.

6. Cybersecurity Awareness

- ☐ Complete required cybersecurity training and periodic refreshers.
- ☐ Stay informed about current scams and attack techniques.
- ☐ Report mistakes and suspicious activity quickly (no blame).
- ☐ Encourage a security-conscious culture and help coworkers practice good cyber hygiene.

TURN A STRONGER CYBER HYGIENE FOUNDATION INTO A MORE RESILIENT BUSINESS

PORT::ZERO CYBER SOLUTIONS
Protect Against Cyber Threats®

Your Quick-Check Result

Add up the 24 items you checked on page 1.

Your Score: _____ / 24

15 – 24	**Strong foundation** You're on the right track. Keep it up and look for continuous improvements.
10 – 14	**Improvement opportunities** You have key safeguards in place, but there are important gaps to address.
0 – 9	**Priority action recommended** Focus on the core safeguards as soon as possible to reduce your risk.

Five Priority Moves for the Next 30 Days

If your score is below 15, start here.

1. **Enable MFA everywhere possible.**
   Start with email, your cloud services, and any account with sensitive data.
2. **Update all systems and applications.**
   Turn on automatic updates and address any overdue patches.
3. **Strengthen your backup and recovery**
   Confirm that critical data is backed up and can be restored.
4. **Reduce phishing risk.**
   Reinforce training, verify requests through a second channel, and use email security controls.
5. **Protect sensitive data.**
   Use encryption, limit access, and store data only in approved locations and services.

Go Deeper with PORT::ZERO

This checklist is a starting point. Take the next step with tools designed to help small and mid-sized businesses improve their cyber readiness and response capabilities.

Cyber Readiness Score
Take the free assessment to see how your organization stacks up and get personalized recommendations.
readiness.portzerocyber.com

Incident Response Plan Builder
Create a customized incident response plan to be ready when it matters most.
plan.portzerocyber.com

Authoritative Source Map

This checklist is informed by widely recognized cybersecurity and risk management frameworks, including:

NIST Cybersecurity Framework (CSF 2.0)
Risk management framework for identifying, protecting, detecting, responding, and recovering.
nist.gov/cyberframework

NIST SP 800-53 (Rev. 5)
Security and privacy controls for information systems.
csrc.nist.gov/pubs/sp/800/53/r5/upd1/final

NIST SP 800-63B (Digital Identity)
Guidance on authentication and federated identity.
pages.nist.gov/800-63-4/

Center for Internet Security (CIS)
Controls for prioritized, actionable safeguards for organizations.
cisecurity.org/controls

OWASP Top 10
Common web application security risks to be aware of.
owasp.org/projects/top-ten

SANS Security Awareness
Practical guidance for building a security-aware culture across your organization.
sans.org/security-awareness

This Quick Check is intended for general cybersecurity awareness and does not constitute a formal security assessment. Use it as a starting point for stronger cyber hygiene and to identify areas for additional focus.

Version 2.0 | October 2026
© 2026 PORT::ZERO Cyber Solutions