Quadrillion Tech Solutions Phone: 617-410-3790 Cybersecurity Checklist for Small Businesses

1. Secure Your Network

Use a business grade firewall

Implement enterprise-level firewall protection to safeguard your network perimeter from external threats and unauthorized access attempts.

Change default router passwords

Replace factory-set credentials immediately with strong, unique passwords to prevent easy exploitation of known default settings.

Enable network segmentation for guest Wi-Fi

Create separate network zones to isolate guest access from your core business systems and sensitive data.

2. Protect Devices & Endpoints

Install antivirus/anti malware tools

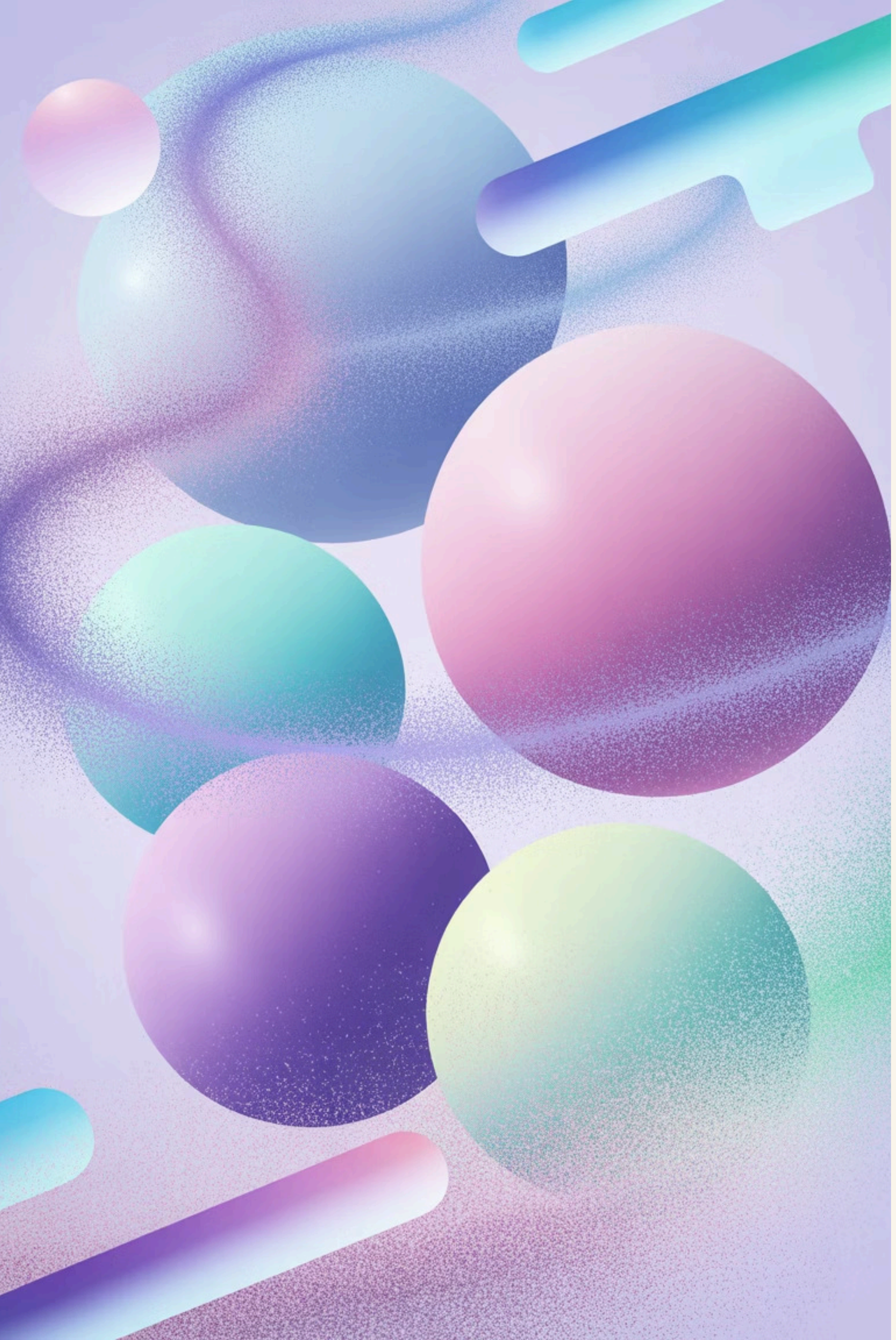
Deploy comprehensive security software across all devices to detect and neutralize threats before they can cause damage.

Enable automatic security updates

Configure systems to automatically download and install critical security patches to maintain protection against emerging vulnerabilities.

Encrypt laptops and mobile devices

Apply full-disk encryption to protect sensitive business data in case of device loss or theft.



3. Strengthen Password Security

Require strong, unique passwords

Enforce password policies that mandate complex combinations of characters, numbers, and symbols, with different passwords for each account.

Use Multi-Factor Authentication (MFA) on all accounts

Add an extra layer of security by requiring a second form of verification beyond just passwords for account access.

Implement a password manager

Provide employees with secure password management tools to generate, store, and autofill complex credentials safely.

4. Secure Business Emails

01

Enable spam/phishing filters

Activate advanced email filtering systems to automatically identify and quarantine malicious messages before they reach employee inboxes.

02

Use DMARC, SPF, and DKIM email authentication

Implement email authentication protocols to verify sender identity and prevent domain spoofing attacks targeting your organization.

03

Train staff to recognize phishing attempts

Educate employees on identifying suspicious emails, malicious links, and social engineering tactics used by cybercriminals.

5. Backup Critical Data

Automate daily backups

Schedule automatic backup processes to run daily, ensuring consistent protection of your business-critical information.

Store backups in two separate locations (cloud + offline)

Maintain redundant backup copies in both cloud storage and physical offline media to protect against various disaster scenarios.

Test data restoration quarterly

Regularly verify that your backup systems work correctly by performing test restorations every three months.

6. Control Access to Information

Assign role-based permissions

Grant employees access only to the systems and data necessary for their specific job functions, following the principle of least privilege.

Remove access for former employees immediately

Disable all accounts and revoke system access for departing staff members on their last day to prevent unauthorized entry.

Limit admin rights to essential staff only

Restrict administrative privileges to a small number of trusted personnel who require elevated access to perform their duties.

7. Train Employees Regularly

Conduct quarterly cybersecurity awareness training

Hold mandatory training sessions every three months to keep staff informed about the latest security threats and best practices.

Simulate phishing attacks to test readiness

Run controlled phishing simulations to assess employee vigilance and identify areas where additional training is needed.

Provide clear reporting procedures for suspicious activity

Establish straightforward channels for employees to report potential security incidents without fear of repercussions.

8. Protect Your Website & Applications

Enable HTTPS with SSL certificates

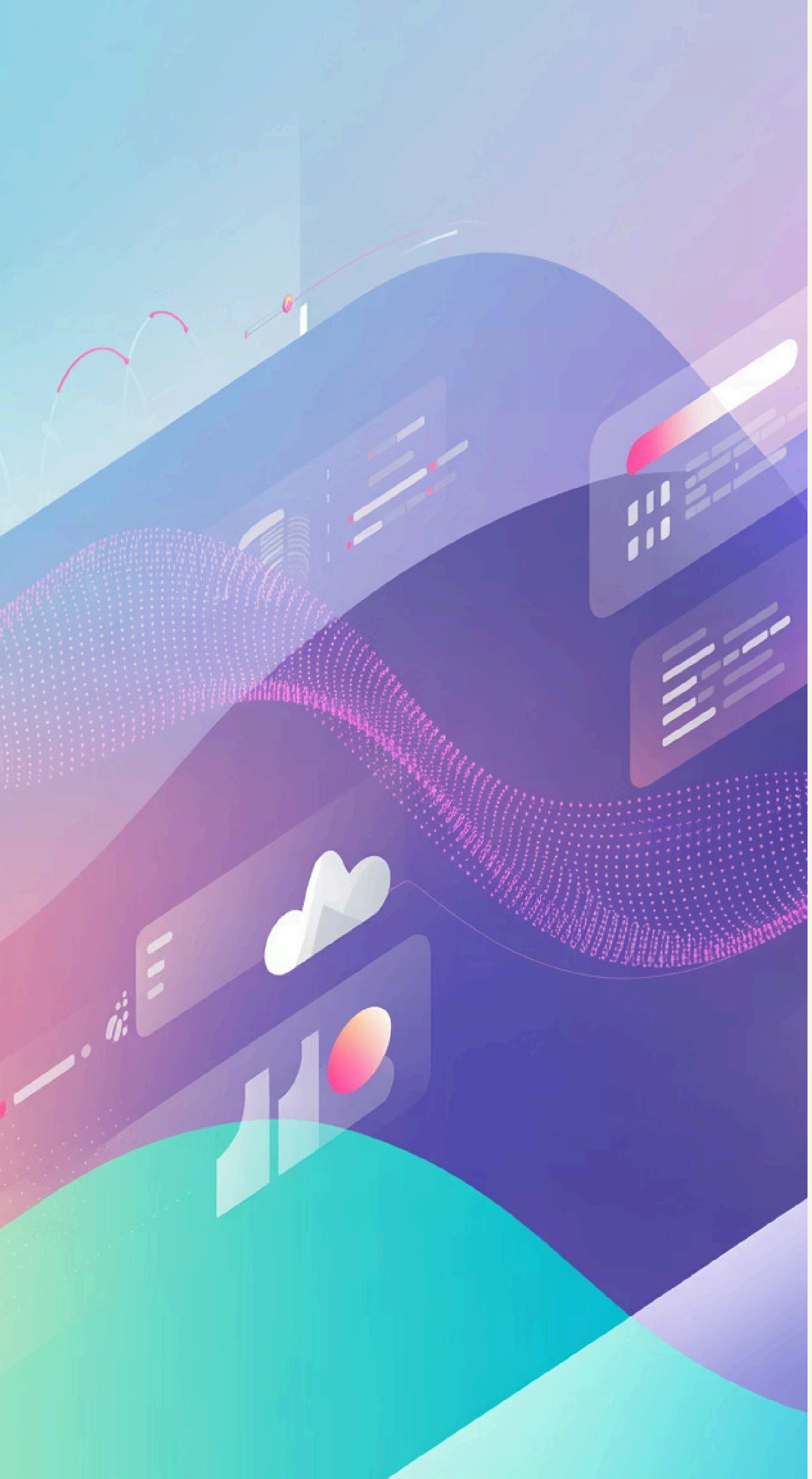
Secure all web traffic with SSL/TLS encryption to protect data transmitted between users and your website from interception.

Patch CMS plugins and software regularly

Keep your content management system, plugins, and all web applications up to date with the latest security patches.

Use Web Application Firewalls (WAF)

Deploy WAF solutions to filter and monitor HTTP traffic, blocking malicious requests before they reach your web applications.



9. Monitor Systems & Logs

1

Enable real-time threat monitoring

Implement continuous monitoring solutions that detect and alert you to security threats as they occur across your infrastructure.

2

Review security logs weekly

Conduct regular reviews of system logs every week to identify patterns, anomalies, or indicators of compromise.

3

Activate alerts for suspicious login attempts

Configure automated notifications for failed login attempts, unusual access patterns, or other suspicious authentication activities.

10. Prepare an Incident Response Plan

Define roles and responsibilities

Clearly assign specific tasks and decision-making authority to team members for various types of security incidents.

Create a step-by-step breach response checklist

Document detailed procedures for containing, investigating, and recovering from security breaches to ensure swift and effective response.

Maintain emergency contact list (IT, legal, insurance)

Keep an updated list of critical contacts including IT support, legal counsel, insurance providers, and law enforcement for immediate access during incidents.

11. Secure Vendor & Third-Party Access

Review vendor security policies

Evaluate the cybersecurity practices and policies of all third-party vendors before granting them access to your systems or data.

Require MFA for any third-party access

Mandate multi-factor authentication for all external vendors and partners who need to access your business systems or networks.

Revoke access when no longer needed

Promptly disable third-party access credentials when projects are completed or vendor relationships end to minimize security exposure.

12. Maintain Regulatory Compliance

1

Ensure compliance with state and federal data laws

Stay current with all applicable data protection regulations including GDPR, CCPA, HIPAA, and other industry-specific requirements that govern your business operations.

2

Document all security policies

Maintain comprehensive written documentation of your cybersecurity policies, procedures, and controls for audit purposes and employee reference.

3

Conduct annual security audits

Perform thorough security assessments at least once per year to identify vulnerabilities, verify compliance, and improve your overall security posture.