Office: 720-731-3179
Email: support@rmts-colorado.com
Website: www.rmts-colorado.com

Digital Safety Checklist

Purpose
This checklist helps individuals verify that their personal digital environment is reasonably secure against common threats such as account compromise, malware, identity theft, and data loss.

How to Use This Checklist

- Review each item and check the box if completed
- Mark **N/A** if an item does not apply
- Note any gaps for follow-up
- Review this checklist **annually** or after major changes (new device, security incident)

---

1. Devices

Goal: Ensure all devices are secure, supported, and protected if lost or stolen.

Computers (Laptop / Desktop)
☐ Operating system is supported and not end-of-life
☐ Automatic operating system updates are enabled
☐ Antivirus or endpoint protection is installed and updating
☐ Device requires a password, PIN, or biometric login
☐ Screen locks automatically after inactivity
☐ Full-disk encryption is enabled (e.g., BitLocker, FileVault)
☐ Unnecessary or unused software has been removed
☐ Device is backed up regularly (cloud or external backup)

Mobile Devices (Phone / Tablet)
Cell Phone:_____
Tablet:_____
Wearables:_____

☐ Device requires a PIN, password, or biometric unlock
☐ Automatic OS updates are enabled
☐ Device encryption is enabled

Office: 720-731-3179
Email: support@rmts-colorado.com
Website: www.rmts-colorado.com

☐ "Find My Device" or remote wipe is enabled
☐ Apps are installed only from official app stores
☐ Unused or suspicious apps have been removed
☐ Device backup is enabled

Home Network & Other Devices
Wifi Name:_____
Internet Service Provider:_____
☐ Home Wi-Fi uses WPA2 or WPA3 encryption
☐ Router admin password has been changed from default
☐ Router firmware is up to date
☐ Unused smart devices are disconnected or disabled
☐ Shared or public computers are not used for sensitive activities
Smart Things Installed in Home:_____
_____
_____

---

2. Accounts

Goal: Prevent account takeover and limit impact if an account is compromised.

Passwords
☐ Each important account has a unique password
☐ Passwords are long and complex (14+ characters recommended)
☐ Passwords are not reused across personal, work, or financial accounts
☐ A password manager is used (recommended)
Where are passwords currently kept if not in password manager:
_____

Multi-Factor Authentication (MFA)
☐ MFA is enabled on email accounts
☐ MFA is enabled on financial accounts
☐ MFA is enabled on cloud storage accounts
☐ MFA is enabled on social media accounts
☐ MFA uses an authenticator app
If no auth app is used what is the MFA mechanism? (email, cell phone #, etc.)
_____

Office: 720-731-3179
Email: support@rmts-colorado.com
Website: www.rmts-colorado.com

Account Management & Recovery
☐ I know which accounts are tied to my primary email
☐ Account recovery information is current
☐ Backup recovery codes are stored securely
☐ Old or unused accounts have been closed or archived
☐ I review account security or login alerts

---

3. Configurations & Settings

Goal: Reduce exposure by tightening security and privacy settings.

Email & Messaging
☐ Spam and phishing filtering is enabled
☐ Unexpected links or attachments are verified before opening
☐ Email auto-forwarding rules have been reviewed
☐ Work credentials are not reused for personal email

Web Browsing
☐ Browser is up to date
☐ Only trusted browser extensions are installed
☐ Unused or unknown extensions are removed
☐ Browser Guard or Web Browsing protection installed and enabled
☐ Sensitive accounts are not accessed on public Wi-Fi

Privacy & Data Sharing
☐ Social media privacy settings limit public exposure
☐ Location sharing is disabled unless necessary
☐ App permissions are limited to what is required
☐ Cloud sharing links are reviewed and restricted
☐ I understand what personal information is publicly visible

---

4. Safety Awareness & Habits

Goal: Reduce risk through consistent, informed behavior.

Office: 720-731-3179
Email: support@rmts-colorado.com
Website: www.rmts-colorado.com

Phishing & Social Engineering

☐ I am cautious of urgent or threatening messages
☐ Requests for money, passwords, or codes are verified
☐ I do not rely solely on sender name or caller ID
☐ Suspicious messages are reported or deleted

Backups & Recovery

☐ Important data is backed up in more than one location
☐ I know how to restore data from backups
☐ Backup accounts are protected with MFA

Incident Readiness

☐ I know how to reset passwords quickly
☐ I know how to lock or wipe my device if lost device
☐ I know who to contact for help if something seems wrong
☐ I act quickly when I suspect a security issue

Final Review

☐ Checklist completed
☐ Gaps identified
☐ Follow-up actions documented
☐ Next review date: _____

Notes / Follow-Up Actions