

# SecureMe Personal Security Checklist

## Your Digital Life, Secured

**Security is a journey, not a destination.**  
**Start with the basics and keep improving over time.**

### **Device Security**

- **Lock it down**  
Set up strong PIN codes, passwords, or biometric authentication on all devices.
- **Update regularly**  
Schedule monthly "update days" to keep operating systems and apps current.
- **Encrypt your devices**  
Enable full-disk encryption on laptops, phones, and tablets.
- **Install security software**  
Use reputable antivirus/anti-malware protection.
- **Clean up unused apps**  
Delete apps you no longer use (they may be collecting data or have vulnerabilities).
- **Review app permissions**  
Does your flashlight app really need access to your contacts? 🤔
- **Enable remote wipe**  
Set up "Find My Device" or equivalent to locate or erase lost devices.

### **Password Management**

- **Use a password manager**  
Stop using "Summer2023!" for everything. Let a password manager create and store unique passwords.
- **Create strong master password**  
Make it long, memorable, and complex. Consider a passphrase.
- **Enable two-factor authentication (2FA)**  
Protect important accounts with an additional verification step.
- **Avoid SMS-based 2FA when possible**  
Use authentication apps or security keys for better protection.
- **Set up recovery methods**  
Add backup email addresses and recovery phone numbers to important accounts.
- **Password audit**  
Schedule quarterly reviews to update weak or reused passwords.

### **Browsing Safely**

- **Use a secure browser**  
Consider browsers that prioritize privacy.
- **Install privacy extensions**  
Ad blockers, tracker blockers, and HTTPS everywhere enhance security.
- **Clear browsing data regularly**  
Set your browser to clear cookies and history when you close it.
- **Be cautious with downloads**  
Only download files from trusted sources.
- **Check for HTTPS**  
Look for the padlock icon before entering sensitive information on websites.
- **Use private browsing for sensitive activities**  
Banking, health research, etc. benefit from incognito mode.

### **Email Security**

- **Use separate email addresses**  
Consider different emails for important accounts, shopping, and newsletters.
- **Be skeptical of unexpected attachments**  
Even from people you know. When in doubt, verify via another channel.
- **Hover before clicking**  
Check link destinations before clicking by hovering your cursor over them.
- **Watch for phishing red flags, even if AI do it better**  
Unusual urgency, grammar errors, and generic greetings are warning signs.
- **Use email aliases**  
Create disposable addresses for one-time signups.



### Network Protection

- **Secure your home WiFi**  
Use WPA3 encryption if available and a strong, unique password.
- **Change default router credentials**  
Update the default admin username and password on your router.
- **Use a VPN for public WiFi**  
Never conduct sensitive business on unsecured public networks without protection.
- **Enable firewall**  
Make sure your operating system's firewall is active.
- **Create a guest network**  
Keep visitors off your main network.



### Data Backup

- **Follow the 3-2-1 rule**  
Keep 3 copies of important data, on 2 different media types, with 1 copy stored off-site.
- **Automate backups**  
Set up scheduled backups so you don't have to remember.
- **Test your backups**  
Verify quarterly that you can actually restore from your backups.
- **Encrypt sensitive backups**  
Especially those stored in the cloud.



### Security Mindset

- **Think before you share**  
Once information is online, it's potentially there forever.
- **Limit personal information online**  
Review privacy settings on social media regularly.
- **Be aware of physical surroundings**  
Use privacy screens in public and be mindful of shoulder-surfers.
- **Have an identity theft response plan**  
Know what to do if your identity is compromised.
- **Stay informed**  
Follow trusted security sources to keep up with new threats.



### Level Up Your Security

- **Use a security key**  
Hardware authentication keys provide superior protection for critical accounts.
- **Consider a password-protected phone number**  
Services exist to mask your real phone number.
- **Set up a security freeze**  
Prevent credit checks without your explicit permission.
- **Review data broker opt-outs**  
Request removal of your information from people-search sites.
- **Create an emergency plan**  
Prepare instructions for trusted contacts in case you're incapacitated.

## Keep Track of Your Progress

Category	Beginner	Intermediate	Advanced	Your Score
Device Security	2 items	4 items	All 7 items	
Password Management	2 items	4 items	All 6 items	
Browsing Safely	2 items	4 items	All 6 items	
Email Security	2 items	3 items	All 5 items	
Network Protection	2 items	3 items	All 5 items	
Data Backup	1 item	2 items	All 4 items	
Security Mindset	2 items	3 items	All 5 items	
Level Up	0 items	2 items	All 5 items	

Download the latest version of this checklist and get personalized security recommendations at [SecureMe.digital-forge.com](https://SecureMe.digital-forge.com)

