CyberGuardian: A SecureTheVillage Guide for Residents
Security Checklist

Book Section	Security Checklist Item	Priority [1]	When
D.5. The Dark Web	Check your personal exposure on the Dark Web at https://haveibeenpwned.com .	M	Often
D.7. Scams	Avoid entering online contests/surveys, mailing in warranty cards and excessive posting on Social Media.	M	Always
D.8. Antivirus Software to the Rescue	Install antivirus on personal computer(s) and smartphone(s) and run it weekly.	VH	Weekly
D.8. Antivirus to the Rescue	If virus-infected, run antivirus and/or consult a professional (W.1. Consulting a Professional).	H	Always
D.9. Major Data Breach?	Change all passwords when a major breach occurs.	H	Always
D.10 Are You a Victim?	If scam victim, change passwords, run antivirus, call police, contact credit bureaus & financial companies. Consult a professional, if necessary (see W.1. Consulting a Professional).	VH	Always
E.6. The Outside World	Only use your own cable connected to a traditional (120V) plug if charging device in a public place.	M	Always
E.6. The Outside World	Turn off your “local” communications features (e.g. Bluetooth, AirDrop, network sharing) when in public places.	L	Whenever

[1] VH for very high, H for high, M for medium, L for low but still important.

CyberGuardian: A SecureTheVillage Guide for Residents
Security Checklist

Book Section	Security Checklist Item	Priority [1]	When
F.2. A Secure Home Router is a Must	Set up your home router with a non-personal SSID, memorable and strong password, WPA2 encryption, firewall enabled and remote management turned off. Consult a professional, if necessary (see W.1. Consulting a Professional).	VH	Once
F.2. A Secure Home Router is a Must	Login to your home router to perform needed maintenance (e.g. update firmware) annually. Consult a professional if necessary (W.1. Consulting a Professional).	M	Yearly
F.2. A Secure Home Router is a Must	Set up a guest network in your home WI-FI router if visitors request access.	L	Once
F.3. Public Networks	Use Public Wi-Fi only with a secure VPN. Avoid online financial transactions on public Wi-Fi.	H	Always
F.7. Firewalls	Setup a software firewall on personal devices through operating system or security suite.	H	Once
G. Passwords	Create long, unique, memorable passwords for all online accounts.	VH	Once
G.1. Password Managers	Use a Password Manager, browser-based or add-on, to manage your passwords.	H	Once
G.2. Two Factor Authentication (2FA)	Set up two-factor authentication (2FA) at all your important online accounts (government, banks, investments, credit cards, …..).	VH	Once
G.3. Minimize Sharing Your Phone Number	Minimize sharing of your cell phone number.	M	Always
H. Web Browsing	When web browsing to a new site, examine the address bar details to ensure security.	M	As needed
H.1. Securing Your DNS Interactions	Secure your Web browsing by encrypting your DNS requests.	L	Once

CyberGuardian: A SecureTheVillage Guide for Residents
Security Checklist

Book Section	Security Checklist Item	Priority [1]	When
H.3. Minimizing & Avoiding Personal Tracking	Minimize tracking of your browser activity by going incognito or installing a blocking extension.	L	As needed
H.3. Minimizing & Avoiding Personal Tracking	Avoid clicking on ads when browsing – you may be clickjacked!	L	When-ever
H.4. Shoppers Beware;	Establish accounts at major, official websites before a scammer does it for you.	L	Once
H.5. Clean Up Stale Digital Haunts and Personal Data	Clean up stale website personal data.	L	Yearly
I.1. Social Media	Review sharing and privacy settings for all social media accounts at least annually.	L	Once
I.1.1 Plant Your Flag!	Establish accounts at major social media apps before a scammer does it for you.	L	Once
J. Email	In email, don't click on attachments or links unless SURE of source.	VH	Always
J. Email	Don't send important personal information in email.	M	Always
J. Email	Set up personal email address aliases for your important online accounts.	M	Once
J.1. Consider Paying for Your Email Service	If email is important, upgrade to business service for nominal cost.	M	Once
J.2. Reduce Stored Emails	Reduce stored emails.	L	Yearly
K. Texting	Don't send important personal information in text messages.	M	Always
K.1. Have You Been Smished?	If smished, forward the message to 7726 to report it.	L	When-ever
L. Gaming	Gamers should document suspected hacking and report it to developers.	L	Always
M. Parenting Do's & Don'ts	Get involved if your young children are online.	M	Always
N. Working from Home Securely	Protect your employer's business with secure home computing.	H	Always

CyberGuardian: A SecureTheVillage Guide for Residents
Security Checklist

Book Section	Security Checklist Item	Priority [1]	When
O. Personal Computers	Keep software (operating system, web browser, apps, …) up to date on all PCs using only the native auto-update feature.	VH	Always
O.1. Separate Accounts for Multiple Users on PCs	Set up non-Administrator accounts for yourself and other users on your PC.	H	Once
O.2. Shutdown Weekly	Shutdown your Windows PC or Mac weekly to remove any lingering malware in computer memory.	L	Weekly
O.3. Physical Access Control	Set your devices to lock after a short time of inactivity.	L	Once
O.4. Disk (Storage) Encryption	Encrypt your files on all devices. Consult a professional, if necessary (see W.1. Consulting a Professional).	M	Once
O.5. How do I securely dispose of my old personal computer?;	When migrating to a new computer, carefully erase all files. Consult a professional, if necessary (see W.1. Consulting a Professional).	M	Always
P. Smartphones and Tablets	Keep software (operating system, web browser, apps, …) up to date on all smartphones using only the native auto-update feature.	VH	Always
P.1. Physical Device Security	Create a smartphone lock screen with alternate phone number and email.	M	Always
P.1. Physical Device Security	Use touch/facial recognition (if available) and a non-obvious pass code for all devices.	M	Once
P.3. Location Sharing	Minimize use of location sharing.	M	Always
P.4. Contact Sharing	Minimize use of contact sharing.	M	Always
P.5. Telephone Account Access	Set up a pin access code with your phone service provider.	M	Once
P.7. Guidance to Minimize Vishing (Spam Calls)	For excessive robo calls, contact phone service providers for blocking services.	L	Once

CyberGuardian: A SecureTheVillage Guide for Residents
Security Checklist

Book Section	Security Checklist Item	Priority [1]	When
P.8. Migrate from Old to New Smartphone (Securely)	When migrating to a new smartphone, carefully erase all files. Consult a professional, if necessary (see W.1. Consulting a Professional).	M	Always
Q.6. Voice Assistant "Leakage"	Don't use your voice assistant to find numbers for important calls.	L	When-ever
Q.7. Dealing with "Leakage"	If you are investing in a smart home, create a second, separate Wi-Fi network for your IoT devices and check that your devices adhere to cybersecurity standards (e.g. UL 2900).	L	Once
Q.7 Dealing with "Leakage"	Ensure that the firmware in your IoT devices are up-to-date.	L	Annually
R. Financial Security	Freeze your credit at the 4 credit bureaus and check your credit rating annually at each.	VH	Once, then Yearly
R. Financial Security	Frequently monitor financial accounts and set up automatic alerts.	H	Daily
R.1. Protect Your Identity	Get an IP Pin annually from the IRS at irs.gov to protect your tax submissions from fraud.	L	Annually
R.4. Making Payments Securely in the 21st Century	Use smartphone "Pay" apps for more secure payments.	L	When-ever
S.1. What to Keep and How Long to Keep It?	Purge unnecessary files on all devices periodically.	L	Yearly
S.3. Backup Strategy	Maintain a remote, multi-version backup of personal computer and smartphone files.	VH	Continuou sly; monthly monitor
T. Kicking the Bucket	Create a printable record of personal cyber details (Kick the Bucket letter) for your family (heirs).	H	Once; updated as needed