CyberGuardian Security Checklist

The CyberGuardian Security Checklist table has 5 columns:

1. **Order** - Importance Order
2. **CyberGuardian Security Checklist Item**.
3. **CyberGuardian Book Section**
4. **Priority Group** of importance – VH for very high, H for high, M for medium, L for low but still important.
5. **When To Do** - when to do it.

Order	CyberGuardian Security Checklist Item	Book Section	Priority Group	When To Do
1	Freeze your credit at the 4 credit bureaus (and check it periodically).	R. Financial Security	VH	Once, then Frequently
2	Set up two-factor authentication (2FA; MFA) at all your important online accounts (government, banks, investments, credit cards)	G.2. Two Factor Authentication (2FA)	VH	Once at beginning and then every time you get a new device or register at an important website
3	Be suspicious when receiving unexpected emails, texts, or phone calls, especially when accompanied by requests for personal information or money. Don't click on links or attachments.	J. Email K. Texting P.4. Vishing (Spam Calls)	VH	Always
4	Keep software (operating system, web browser, apps, …) up to date on all PCs and smartphones using only the native auto-update feature.	O. Personal Computers P. Smartphones and Tablets	VH	Weekly
5	Encrypt your devices and cloud storage.	O.3. Disk (Storage) Encryption	VH	Continuously; monthly monitor
6	Maintain a remote, multi-version backup of your files.	S.3. Backup Strategy	VH	Continuously; monthly monitor

Order	CyberGuardian Security Checklist Item	Book Section	Priority Group	When To Do
7	Protect all devices with cybersecurity software, including antivirus and firewall. Keep it updated.	D.8. Antivirus Software to the Rescue F.7. Firewalls	VH	Weekly
8	Use long, unique, memorable passwords for all online accounts and use a password manager to manage them.	G. Passwords G.1. Password Managers	VH	Once when you get new device, register at a new web site, etc
9	Use Public Wi-Fi only with a secure VPN. Avoid online financial transactions on public Wi-Fi.	F.3. Public Networks	VH	Always
10	Set up non-Administrator accounts for yourself and other users on your PC.	O.1. Separate Accounts for Multiple Users on PCs	VH	Once
11	Minimize sharing of your personal information on the internet to protect your privacy.	D.2. Online Privacy	VH	Always
12	Set up your home router securely.	F.2. A Secure Home Router is a Must	VH	Once, then annually
13	Set your devices to lock after a short time of inactivity.	O.2. Physical Access Control	VH	Once when you get a new device
14	Change all potentially compromised passwords when a major breach occurs.	D.9. Major Data Breach?	H	Always
15	If virus-infected, run antivirus and/or consult a professional (see W.1. Consulting a Professional)..	D.8. Antivirus Software to the Rescue	H	Always
16	When web browsing to a new site, examine the address bar details to ensure security.	H. Web Browsing	H	As needed
17	If scam victim, change passwords, run antivirus, call police, contact credit bureaus & financial companies. Consult a	D.10. Are You a Victim?	H	Always

Ord-er	CyberGuardian Security Checklist Item	Book Section	Priority Group	When To Do
	professional, if necessary (see W.1. Consulting a Professional)..			
18	Don't send important personal information in email.	J. Email	H	Always
19	Frequently monitor financial accounts and set up automatic alerts.	R. Financial Security	H	Daily
20	Avoid sending important personal information in text messages.	K. Texting	H	Always
21	Avoid entering online contests/surveys, mailing in warranty cards and excessive posting on Social Media.	D.7. Scams	H	Always
22	Turn off unnecessary "local" communications features (e.g. Bluetooth, AirDrop, network sharing) when in public places.	E.6. The Outside World	H	Whenever
23	Use touch/facial recognition (if available) and a non-obvious pass code for all devices.	P.1. Physical Device Security	H	Once
24	After migrating to a new computer, carefully erase all files. Consult a professional, if necessary (see W.1. Consulting a Professional)**..**	O.4. How do I securely dispose of my old personal computer?	H	Always
25	After migrating to a new smartphone, carefully erase all files. Consult a professional, if necessary (see W.1. Consulting a Professional).	P.7. Migrate from Old to New Smartphone (Securely)	H	Always
26	Set up a pin access code with your phone service provider.	P.3.3 Minimize Telephone Account Access	H	Once
27	Set up a guest network in your home WI-FI router for visitors who might request access.	F.2. A Secure Home Router is a Must	H	Once

Order	CyberGuardian Security Checklist Item	Book Section	Priority Group	When To Do
28	If you are investing in a smart home, create a second, separate Wi-Fi network for your IoT devices.	Q.8. Dealing with "Leakage"	M	Once
29	Secure your web browsing by encrypting your DNS requests.	H.2. Securing Your DNS Interactions	M	Once
30	Minimize tracking of your browser activity by going incognito or installing a blocking extension.	H.4. Minimizing & Avoiding Personal Tracking	M	Whenever
31	Avoid clicking on ads when browsing – you may be clickjacked!	H.4. Minimizing & Avoiding Personal Tracking	M	Whenever
32	If email security is very important, consider an enhanced email service.	J.1. Consider Paying for Your Email Service	M	Once
33	Get involved if your young children are online.	M. Parenting Do's & Don'ts	M	Always
34	Review sharing and privacy settings for all social media accounts at least annually.	I.1. Social Media	M	Once
35	Ensure that the firmware in your IoT devices is up-to-date.	Q.8. Dealing with "Leakage"	M	Annually
36	Get an IP Pin annually from the IRS at irs.gov to protect your tax submissions from fraud.	R.1. Protect Your Identity	M	Annually
37	Quarterly, check your personal exposure on the Dark Web at https://haveibeenpwned.com . Change passwords as needed.	D.6. The Dark Web	L	Often
38	Protect your employer's business with secure home computing.	N. Working from Home	L	Always
39	Set up personal email address aliases for your important online accounts.	J. Email	L	Once
40	Minimize sharing of your cell phone number.	G.3. Minimize Sharing Your Phone Number	L	Always

Order	CyberGuardian Security Checklist Item	Book Section	Priority Group	When To Do
41	Only use your own cable connected to a traditional (120V) plug if charging device in a public place.	E.6. The Outside World	L	Always
42	Create a smartphone lock screen with alternate phone number and email; enable *Find My Phone*.	P.1. Physical Device Security	L	Always
43	Delete unnecessary, personal files on all devices periodically.	S.1. What to Keep and How Long to Keep It?	L	Yearly
44	Minimize use of contact sharing.	P.3.2 Minimize Contact Sharing	L	Always
45	Minimize use of location sharing.	P.3.1 Minimize Location Sharing	L	Always
46	Create a printable record of personal cyber details (Kick the Bucket letter) for your family (heirs).	T. Kicking the Bucket	L	Once; update as needed
47	Periodically clean up stale personal data on websites.	H.6. Clean Up Stale Digital Haunts and Personal Data	L	Yearly
48	Establish accounts at major, official websites before a scammer does it for you.	H.5. Shoppers Beware	L	Once
49	Establish accounts at major social media apps before a scammer does it for you.	I.1.1 Plant Your Flag!	L	Once
50	Reduce stored emails.	J.2. Reduce Stored Emails	L	Yearly
51	If smished, forward the message to 7726 to report it.	K.1. Have You Been Smished?	L	Whenever
52	Gamers should document suspected hacking and report it to developers.	L. Gaming	L	Always
53	For excessive robo calls, contact phone service providers for blocking services.	P.5. Guidance to Minimize Vishing (Spam Calls)-	L	Once

Order	CyberGuardian Security Checklist Item	Book Section	Priority Group	When To Do
54	Don’t use your voice assistant to find numbers for important calls.	Q.7. Voice Assistant “Leakage”	L	Whenever
55	Use smartphone "Pay" apps for more secure payments.	R.4. Making Payments Securely in the 21st Century	L	Whenever
56	When concerned about misuse, request collected personal data from offending company.	D.2. Online Privacy	L	Whenever