RESOURCE 10 | DON'T CLICK YET COMPANION RESOURCE

Companion Workbook with Monthly and Annual Review Checklists

Digital Safety Master Checklist

Companion resource for Don’t Click Yet. Referenced on page 245.

Purpose: Use a longer workbook to review your digital safety habits monthly and annually.
Storage reminder: If you complete this worksheet with sensitive information, store the finished copy somewhere safe.

This checklist is not meant to be completed in one sitting. Treat it as a map. Some items can be done in a few minutes. Others may require help, more time, or a second visit. The goal is not perfection. The goal is to reduce the most common risks in a practical order.

Begin with the accounts and devices that matter most: your main email account, phone, financial accounts, password manager, cloud storage, and any account used for recovery. Once those are stronger, the rest of your digital life becomes easier to protect.

1. Main Email Account

Your main email account is often the account behind the accounts. Protect it first.

- ☐ I know which email account is my main account.
- ☐ My main email has a strong, unique password.
- ☐ That password is not used anywhere else.
- ☐ Multi-factor authentication is turned on.
- ☐ My recovery phone number is current.
- ☐ My recovery email address is current and secure.
- ☐ I have reviewed recent sign-in activity.
- ☐ I have signed out of old or unknown devices.
- ☐ I have checked for forwarding rules or filters I did not create.
- ☐ I know how to reach my email provider’s account recovery page from a trusted route.

2. Passwords

The goal is not to remember every password. The goal is to stop one stolen password from opening several accounts.

- ☐ I use a password manager or have chosen one to begin using.
- ☐ My password manager has a strong master password.
- ☐ My password manager has MFA turned on.

- ☐ I have saved recovery information for the password manager in a safe place.
- ☐ My email password is unique.
- ☐ My bank and credit card passwords are unique.
- ☐ My phone provider password is unique.
- ☐ My Apple, Google, or Microsoft account password is unique.
- ☐ My cloud storage password is unique.
- ☐ My payment app passwords are unique.
- ☐ I have started replacing reused passwords, beginning with the most important accounts.
- ☐ I do not send passwords by text, email, or chat.
- ☐ I have a safe method for sharing passwords with trusted family members if truly necessary.

3. Multi-Factor Authentication

MFA adds a second lock. It works best when you understand when and why codes appear.

- ☐ MFA is turned on for my main email account.
- ☐ MFA is turned on for financial accounts where available.
- ☐ MFA is turned on for my password manager.
- ☐ MFA is turned on for my Apple, Google, or Microsoft account.
- ☐ MFA is turned on for cloud storage.
- ☐ MFA is turned on for payment apps where available.
- ☐ MFA is turned on for important social media accounts.
- ☐ I understand that I should not share codes with unexpected callers or messages.
- ☐ I know that a real code can still be used in a scam.
- ☐ I have saved backup codes for important accounts in a safe place.
- ☐ I know what to do if I lose the phone or device used for MFA.

4. Phone Security

Your phone is part of your security system. It may receive codes, hold banking apps, store photos, and control account recovery.

- [ ] My phone has a strong screen lock.
- [ ] I do not use an obvious PIN such as a birth year, repeated number, or address.
- [ ] Lost-device features are turned on.
- [ ] I know how to locate, lock, or erase my phone from another device.
- [ ] My phone operating system is up to date.
- [ ] Important apps are updated.
- [ ] I have removed apps I no longer use.
- [ ] I have reviewed app permissions, especially location, camera, microphone, contacts, and photos.
- [ ] Sensitive message previews are hidden from the lock screen.
- [ ] My phone photos are backed up.
- [ ] My contacts are backed up.
- [ ] My mobile carrier account has a strong, unique password.
- [ ] My mobile carrier account has an account PIN, number lock, or port-out protection if available.
- [ ] I avoid installing apps from random links or unfamiliar websites.

5. Computer Security

A home computer does not need to be complicated, but it does need maintenance.

- [ ] My computer operating system is updated.
- [ ] My browser is updated.
- [ ] I have removed programs I no longer use.
- [ ] I have reviewed browser extensions and removed unnecessary ones.
- [ ] Built-in security protection is active.
- [ ] I do not call support numbers from pop-ups.
- [ ] I do not allow remote access unless I initiated support through a trusted channel.
- [ ] I download software only from official or trusted sources.
- [ ] I know which files on my computer are important.

☐ Important files are backed up.

☐ I know when to seek professional help, especially after remote access, malware warnings, financial exposure, or business-data exposure.

6. Home Wi-Fi and Router

Your router is the front gate of the home network.

☐ I know where my router is located.

☐ I know whether the router belongs to me or my internet provider.

☐ The router administrator password has been changed from the default.

☐ The router administrator password is stored securely.

☐ My Wi-Fi network name does not reveal personal information.

☐ My Wi-Fi password is strong.

☐ My home Wi-Fi uses WPA2 or WPA3 security.

☐ I do not use outdated Wi-Fi security such as WEP.

☐Router firmware updates are enabled or checked when possible.

☐ I have a guest network for visitors if my router supports it.

☐ Guests use the guest network instead of the main household network.

☐ Smart devices are connected thoughtfully.

☐ Old or unsupported routers are replaced when needed.

☐ I do not make router changes I do not understand without trusted help.

7. Banking, Shopping, and Payment Apps

Money should move slowly when something feels urgent.

☐ My banking passwords are unique.

☐ MFA is enabled on financial accounts where available.

☐ Transaction alerts are turned on.

☐ I know how to reach my bank through the official app, website, or number on the card.

☐ I do not click banking links in texts or emails.

- ☐ I check suspicious bank messages through the official app or known phone number.
- ☐ My payment apps are protected with strong sign-in settings.
- ☐ I verify recipients before sending money.
- ☐ I do not send money to unfamiliar third parties under pressure.
- ☐ I treat gift cards, wire transfers, cryptocurrency, and fast payment apps as high-risk when requested urgently.
- ☐ I have reviewed saved payment cards in shopping accounts.
- ☐ Important shopping accounts use unique passwords.
- ☐ I use official apps or websites to check delivery and order problems.

8. Backups and Important Files

A file is not safe if it exists in only one fragile place.

- ☐ I know which files would hurt most to lose.
- ☐ Important photos are backed up.
- ☐ Important contacts are backed up.
- ☐ Tax records are backed up.
- ☐ Legal documents are backed up.
- ☐ Medical or insurance documents are backed up.
- ☐ Business or freelance records are backed up if applicable.
- ☐ Important files exist in more than one place.
- ☐ I understand which folders are actually syncing to the cloud.
- ☐ I know the difference between cloud sync and backup.
- ☐ I have tested recovery by opening or restoring at least one file.
- ☐ Sensitive documents are stored securely.
- ☐ At least one important copy is separate from my everyday device.
- ☐ I have a simple backup routine I can maintain.

9. Family Digital Safety Plan

A family plan should exist before fear, secrecy, or urgency takes over.

- My family has chosen one or two trusted contacts for suspicious messages or account problems.
- We have a family verification phrase.
- The phrase is not based on public information.
- Family members know when to use the phrase.
- We have agreed that urgent money requests must be verified.
- We have agreed that secrecy is a warning sign in money or emergency requests.
- We have agreed not to share verification codes with unexpected callers.
- We have agreed not to allow unexpected remote access.
- We have discussed what to do if someone clicks, pays, shares, or feels unsure.
- We have a no-shame agreement: help first, blame never.
- Trusted family members know where emergency digital instructions are stored.

10. Account Recovery and Digital Paperwork

Recovery should be planned before the account is locked, the phone is lost, or the person who knows the password is unavailable.

- I have a critical accounts list.
- The list includes main email, phone provider, bank, credit card, cloud storage, password manager, health portal, insurance, tax or government accounts, and major device accounts where applicable.
- The list does not expose passwords unnecessarily.
- It explains where passwords or recovery information are stored.
- Recovery emails and phone numbers are current.
- Backup codes are stored securely.
- Trusted contacts know how to help in an emergency.
- I have considered emergency access for my password manager or critical records.
- Sensitive documents are organized and findable.
- I know where identity documents, tax records, legal papers, and insurance records are stored.
- I review recovery information at least once a year.

11. Scam Warning Signs

You do not need to memorize every scam. Learn the pattern.

- The message creates urgency.
- The message asks for secrecy.
- The message asks for money in an unusual way.
- The caller or message asks for a verification code.
- The message asks me to click a link to fix a problem.
- The caller asks for remote access.
- The sender claims to be a bank, government agency, tech company, delivery service, or family member but wants me to act immediately.
- The request makes verification feel disloyal, rude, or dangerous.
- The payment method involves gift cards, cryptocurrency, wire transfer, payment apps, or an unfamiliar recipient.
- The message tells me not to call anyone else.
- The situation feels emotionally intense, confusing, or rushed.

When several of these signs appear together, stop and verify through another route.

12. If Something Goes Wrong

The goal is containment, not panic.

- I stop interacting with the message, caller, website, or remote session.
- I do not provide more information while uncertain.
- I use a trusted device to secure important accounts.
- I change exposed passwords and any reused versions.
- I review email, financial accounts, password manager, phone provider, and cloud storage.
- I contact the bank, card issuer, or payment service immediately if money is involved.
- I disconnect a computer from the internet if remote access or malware is suspected.
- I preserve evidence before deleting anything.
- I save screenshots, emails, texts, receipts, phone numbers, usernames, websites, and case numbers.
- I tell a trusted person.
- I report the incident through appropriate official channels.
- I watch for follow-up scams pretending to offer refunds, recovery, or technical help.

13. Monthly Maintenance

A short routine can prevent long periods of neglect.

- Review bank and credit card activity.
- Check for pending computer and phone updates.
- Confirm important photos and files are backing up.
- Add new important passwords to the password manager.
- Remove apps or programs you no longer use.
- Review suspicious messages before deleting them.
- Check that no urgent digital problem is being ignored.

14. Annual Review

Choose a predictable time each year, such as tax season, New Year's, or your birthday.

- Review main email recovery settings.
- Review phone provider account security.
- Review password manager emergency access or recovery information.
- Review MFA methods and backup codes.
- Review critical accounts list.
- Review trusted contacts.
- Review family verification phrase.
- Review cloud storage and backups.
- Review old devices and remove devices no longer used.
- Review important documents and update records.
- Replace unsupported devices when necessary.

Minimum Safety Baseline

If the full checklist feels overwhelming, start here:

- Secure your main email account with a unique password and MFA.
- Use unique passwords for email, banking, phone provider, cloud storage, and payment apps.
- Protect your phone with a strong screen lock and lost-device features.
- Turn on banking alerts.
- Do not click financial links in texts or emails.

- Back up important photos and documents.
- Create a family verification phrase.
- Never share verification codes with unexpected callers.
- Never allow unexpected remote access.
- Ask for help early if something feels wrong.

You do not need to finish everything today. Start with the first item that would cause the most damage if it failed. Then move to the next one.