RESOURCE 09 | DON'T CLICK YET COMPANION RESOURCE

Updated Resources and Companion Materials

Companion resource for Don’t Click Yet. Referenced on page 216.

Purpose: Find the current companion materials and updated references connected to the book.
Storage reminder: If you complete this worksheet with sensitive information, store the finished copy somewhere safe.

This appendix is a practical starting point. It is not a complete directory of every useful website, product, service, or organization. Digital safety changes over time, and specific tools may improve, decline, merge, change prices, change privacy policies, or stop being supported.

Use this appendix as a guide for what kinds of resources and tools to look for, not as a substitute for current research or professional advice.

When using any official resource, type the name directly into your browser, use a trusted bookmark, or reach it through a known official source. Be careful with search ads, look-alike websites, fake support numbers, and messages that claim to link to official agencies.

How to Use This Appendix

Begin with official resources when you need to report fraud, identity theft, tax-related identity issues, credit problems, phone scams, or internet crime.

Use tools to support the habits in this book:

- A password manager to reduce password reuse.
- MFA methods to protect important accounts.
- Backup tools to protect important files.
- Built-in device protections to keep phones and computers safer.
- Router and Wi-Fi settings to protect the home network.
- Credit and identity tools when identity theft risk is present.

Do not buy or install a tool simply because you are frightened. A product should solve a real problem, fit your skill level, and be something you can maintain.

Official Fraud and Scam Reporting Resources

Use official reporting resources when you experience fraud, identity theft, cyber-enabled crime, suspicious phone activity, or tax-related identity issues.

Federal Trade Commission ReportFraud

Use this resource to report scams, fraud, and bad business practices. Reports can help consumer protection agencies identify patterns and warn the public.

Use it for situations such as:

- Scam calls, texts, or emails
- Fake business offers
- Online shopping scams
- Impostor scams
- Fake technical support

- Fraudulent payment requests
- Suspicious business practices

Reporting does not guarantee that money will be recovered or that you will receive a personal investigation update. Its value is in creating a record and helping broader enforcement and education efforts.

IdentityTheft.gov

Use this resource when someone may have used your personal information without permission.

It is especially relevant when:

- Someone opened an account in your name.
- A tax return may have been filed using your identity.
- You see credit activity you do not recognize.
- You receive bills or collection notices for accounts that are not yours.
- Your Social Security number or identity documents may have been misused.
- You need a structured recovery plan.

Identity theft is more than a password problem. Treat it as a documentation and recovery process.

FBI Internet Crime Complaint Center

Use this resource to report internet-enabled crimes and cyber-related fraud.

It may be relevant for:

- Online financial fraud
- Business email compromise
- Romance or investment scams
- Cryptocurrency-related scams
- Ransomware
- Cyber extortion
- Online account abuse
- Internet-based impersonation or fraud

If money is actively moving or has just moved, contact your bank, card issuer, or payment service first through a trusted channel. Broader reporting can follow.

Local Police or Law Enforcement

Local law enforcement may be appropriate when:

- Money has been stolen.
- Identity theft occurred.
- Threats or harassment are involved.
- A bank, credit bureau, insurer, or agency requests a police report.
- Physical safety is involved.
- Local victims or local suspects are involved.

A police report may not always lead to a visible investigation, especially if the scammer is distant or overseas. It can still create an official record that may help with recovery.

State Attorney General or Consumer Protection Office

Many states have consumer protection offices or attorney general complaint processes.

These may be useful for:

- Local business fraud
- Contractor scams
- Consumer complaints
- Scam trends affecting residents
- Elder fraud concerns
- State-level identity theft support

Search for your state name plus “attorney general consumer complaint” or “consumer protection office,” and make sure you are on an official state website.

Identity, Credit, and Tax Resources

Annual Credit Reports

Credit reports can help you detect unfamiliar accounts, incorrect information, or possible identity theft.

Use the authorized credit report resource to request reports from the major credit bureaus. Be careful with look-alike sites or services that use the phrase “free credit report” but are not the authorized source.

Review reports for:

- Accounts you do not recognize
- Addresses you do not recognize
- Credit inquiries you did not initiate
- Incorrect balances
- Collection accounts
- Misspelled names or mixed identity information

Checking your credit report is not the same as freezing your credit, but it can help you understand whether something suspicious has already appeared.

Credit Freezes

A credit freeze restricts access to your credit report, making it harder for someone to open new credit in your name.

A freeze may be appropriate if:

- Your identity documents were stolen.
- Your Social Security number was exposed.
- You are dealing with identity theft.
- You want stronger prevention against new-account fraud.
- You do not plan to apply for new credit soon.

A credit freeze can usually be lifted when you need to apply for credit. Keep records of how to manage freezes at each credit bureau.

Fraud Alerts

A fraud alert tells potential creditors to take extra steps to verify your identity before opening new credit.

A fraud alert may be useful if:

- You suspect identity theft.
- Your personal information may have been exposed.
- You want lenders to take extra care before opening accounts.

A fraud alert and a credit freeze are not the same thing. In some situations, you may use one or both.

IRS Tax-Related Identity Theft Resources

Use official tax identity theft guidance if:

- You receive a tax notice about a return you did not file.
- More than one tax return appears to have been filed using your information.
- Your refund is delayed because of possible identity verification issues.
- Someone may have used your Social Security number for tax purposes.
- You receive IRS correspondence that does not match your activity.

Tax-related identity theft can take time to resolve. Keep copies of letters, notices, forms, dates, and case numbers.

Phone, Text, and Caller ID Resources

FCC Consumer Resources

Phone scams often use spoofing, which means the caller ID may display a number or name that is not truly the caller. Do not trust a call simply because the number looks familiar, local, or official.

Use official phone and communications resources to learn about:

- Caller ID spoofing
- Robocalls
- Unwanted texts
- Phone-number porting issues
- Mobile carrier problems
- Complaints related to phone service

If a caller claims to be from a bank, government agency, utility, or technology company, hang up and contact the organization through a known official route.

Mobile Carrier Support

Your mobile carrier can help with account security settings such as:

- Account PIN
- Number lock
- Port-out protection
- SIM swap protection
- Transfer protection
- Device loss or theft

- Suspicious account changes

Different carriers use different names for these protections. Ask specifically how to prevent unauthorized transfer of your phone number.

General Cybersecurity Education Resources

CISA Public Guidance

CISA provides public cybersecurity awareness guidance for individuals and families. Its core themes align with the habits in this book:

- Recognize and report phishing.
- Use strong passwords.
- Turn on MFA.
- Update software.

This kind of resource is useful for simple reminders, family conversations, workplace awareness, and community education.

Public Library, Community Center, or Senior Center Classes

Many people learn digital safety better in person than from a website.

Look for classes or workshops offered by:

- Public libraries
- Community centers
- Senior centers
- Adult education programs
- Local colleges
- Nonprofit organizations
- Consumer protection offices
- Banks or credit unions
- Local cybersecurity groups

When attending a class, be careful about anyone who pressures you to buy a product immediately, share account access, or provide passwords.

Password Managers

A password manager helps you create and store strong unique passwords.

A good password manager should:

- Work on the devices you actually use.
- Work with your main browser.
- Generate strong passwords.
- Store passwords securely.
- Support MFA for the vault.
- Provide understandable recovery or emergency access options.
- Allow safe family sharing if needed.
- Be easy enough for you to use consistently.

Do not choose a password manager only because someone says it is the “best.” The best choice for you is one that is secure, reputable, understandable, and usable in your daily life.

Before choosing one, compare:

- Cost
- Device compatibility
- Browser compatibility
- Family plan options
- Emergency access
- Recovery process
- Export options
- Customer support
- MFA support
- Secure note storage
- Ease of use

Use Appendix D to compare options.

MFA Tools

MFA tools provide a second layer beyond passwords.

Common MFA options include:

- Authenticator apps
- Passkeys
- Security keys
- Device prompts
- Text-message codes
- Email codes
- Backup codes

For many everyday users, text-message codes are better than no MFA, but authenticator apps, passkeys, or security keys may offer stronger protection when available and manageable.

When choosing MFA methods, consider:

- Can I use this reliably?
- What happens if I lose my phone?
- Are backup codes available?
- Where will I store recovery information?
- Does this account support more than one method?
- Is this account important enough for a stronger method?

Use Appendix E to track MFA setup.

Backup Tools

Backup tools protect important files, photos, contacts, and documents.

Common backup options include:

- Built-in phone backup
- Cloud photo backup
- Cloud storage folders
- Dedicated cloud backup services
- External hard drives
- External solid-state drives
- Network storage
- Manual copies of critical files
- Secure document vaults

A good backup plan should include:

- The files that matter most
- More than one copy
- At least one copy separate from the everyday device
- Protection for sensitive documents
- A tested recovery process
- A simple routine you can maintain

Cloud sync can be useful, but it is not always the same as backup. Understand what happens if a file is deleted, changed, or corrupted.

Use Appendix G to create your backup plan.

Antivirus and Device Protection

Modern devices include built-in protections, and those protections are often useful when the device is kept updated. Some users may still choose additional antivirus or device security software, especially if they want more features, broader family coverage, identity monitoring, parental controls, or technical support.

Before buying security software, ask:

- What problem am I trying to solve?
- Does my device already include built-in protection?
- Will this product slow down or confuse the device?
- Does it duplicate tools I already use?
- Does it include support I will actually use?
- Is the company reputable?
- Is the price clear?
- Is it easy to cancel?
- Does it pressure me with fear-based warnings?

Avoid products that rely on frightening pop-ups, fake infection warnings, aggressive sales tactics, or unclear renewal terms.

A security product can help, but it cannot replace updates, unique passwords, MFA, backups, and cautious behavior.

Identity Monitoring Services

Identity monitoring services may alert you if certain personal information appears in suspicious places or if new credit activity is detected. Some services also provide recovery assistance.

These services may be useful for some people, especially after identity theft or data exposure. They are not a guarantee that identity theft will be prevented.

Before paying for identity monitoring, ask:

- What exactly is monitored?
- Does it include credit monitoring?
- Does it include dark web monitoring?
- Does it include recovery support?
- Does it include insurance or reimbursement, and what are the limits?
- What do I need to do if I receive an alert?
- Can I get similar protection through a bank, employer, credit card, insurance provider, or breach notification?
- How easy is it to cancel?
- What personal information must I provide to use it?

Identity monitoring is most useful when you understand what action to take after an alert.

Credit Freezes and Monitoring

For many people concerned about identity theft, credit freezes may be more directly protective against new-account fraud than monitoring alone. Monitoring may tell you something happened. A freeze may help prevent some new accounts from being opened in the first place.

A sensible identity protection plan may include:

- Reviewing credit reports
- Freezing credit when appropriate
- Using fraud alerts when appropriate
- Watching bank and card accounts
- Protecting email and phone accounts
- Securing tax and government accounts
- Keeping identity documents private
- Responding quickly to suspicious notices

No single tool solves identity theft by itself.

VPNs

A VPN can create an encrypted connection between your device and a VPN provider. It may be useful in some privacy or travel situations, especially when using networks you do not trust.

A VPN does not:

- Make fake websites safe
- Stop phishing
- Protect you from sharing codes
- Fix weak passwords
- Replace MFA
- Stop you from sending money to a scammer
- Make an infected device safe
- Replace updates or backups

Before paying for a VPN, ask what problem you are trying to solve. Many everyday users need stronger passwords, MFA, updates, and backups before they need a VPN.

Secure DNS and Content Filtering

Some DNS or filtering services can block known malicious websites, adult content, or other categories of sites. These tools may be useful for families, schools, small offices, or households that want an additional layer of protection.

Before using DNS filtering or parental controls, ask:

- What will it block?
- Who controls the settings?
- Can it be bypassed?
- Will it interfere with legitimate sites?
- Is it appropriate for the people in the household?
- Does it create privacy concerns?
- Can the household maintain it?

Filtering can help, but it should not be treated as a substitute for conversation, supervision, verification, or account security.

Parental Controls and Family Safety Tools

Parental controls can help manage children's device use, app downloads, screen time, web access, purchases, location sharing, and content restrictions.

These tools can be useful, but they work best when combined with conversation.

Before choosing parental controls, consider:

- Child's age and maturity
- Devices used
- App store settings
- Screen time needs
- Purchase restrictions
- Location sharing comfort
- Privacy expectations
- School device policies
- Emergency contact needs
- How rules will change as the child grows

The goal should be safety and guidance, not secret surveillance.

Router and Home Network Tools

Many households can improve safety through basic router settings rather than advanced tools.

Useful router features may include:

- Strong administrator password
- WPA2 or WPA3 Wi-Fi security
- Guest network
- Firmware updates
- Device list
- Basic parental controls
- DNS settings

- Separate network for smart devices, when supported
- Provider app for monitoring and support

Before buying a new router, consider:

- Whether your internet provider can replace old equipment
- Whether your current router still receives updates
- Whether it supports a guest network
- Whether it supports modern Wi-Fi security
- Whether coverage is adequate
- Whether you can manage the settings
- Whether trusted help is available for setup

A powerful router is not helpful if nobody in the household understands or maintains it.

Smart-Home Device Tools

Smart-home devices may include cameras, doorbells, speakers, thermostats, locks, appliances, lights, and security systems.

Before adding a smart device, ask:

- Does this device need internet access?
- What account controls it?
- Is the account protected with a unique password and MFA?
- Does the device receive updates?
- What data does it collect?
- Who can access it?
- Are privacy settings understandable?
- Does it need to be on the main network?
- What happens if the company stops supporting it?

Convenience is valuable, but connected devices should enter the home intentionally.

Browser and Email Safety Tools

Many browsers and email providers include safety features such as:

- Phishing warnings
- Unsafe site warnings
- Spam filtering
- Suspicious attachment warnings
- Password breach alerts
- Pop-up blocking
- Extension review
- Privacy settings

These features are helpful, but they are not perfect. A suspicious message may still arrive. A fake website may still look convincing. A warning may be missed.

Use built-in warnings as signals, not as your only defense.

Choosing Paid Tools Carefully

Before buying any digital safety product, ask:

- What specific problem does this solve?
- Do I already have a tool that does this?
- Is this product recommended by a trusted source?
- Does the company explain pricing clearly?
- Does the product use fear to pressure me?
- Can I cancel easily?
- Does it work on my devices?
- Will I actually use it?
- Does it create new passwords or accounts I must protect?
- Does it require personal information I am comfortable providing?

Avoid buying under pressure. A real product will still be available tomorrow.

When to Get Professional Help

A trusted professional may be appropriate when:

- A stranger had remote access to your device.
- Money was stolen or transferred.
- Business, client, patient, student, donor, or legal data may be involved.
- Identity theft is suspected.
- Ransomware appears.
- A device continues behaving strangely after basic cleanup.
- You are locked out of critical accounts.
- You are helping an older adult and the situation affects finances, health, or legal documents.
- You are unsure whether continuing to use a device is safe.

Professional help should be clear about cost, scope, and what will be done. Be cautious of anyone who appears through a pop-up, unexpected call, frightening warning, or search ad and immediately asks for remote access or payment.

Questions to Ask a Professional

Before allowing a technician, consultant, or service provider to help, ask:

- Who are you and what company do you represent?
- How did I reach you?
- What exactly will you do?
- What will it cost?
- Do you need remote access?
- Why do you need that access?
- Will you see passwords, files, or financial information?
- Should I change passwords from another device first?
- Will you provide a written summary of the work?
- What should I do after the service?

A legitimate professional should be willing to explain the process.

Product Recommendation Policy for This Book

This book focuses on habits, systems, and decision-making. Tools can help, but they are not the foundation.

When considering a tool mentioned by this book, Click Giraffe, a consultant, a family member, or any online source, remember:

- Use tools that solve a real problem.
- Prefer reputable providers.
- Read current pricing and terms.
- Protect the account connected to the tool.
- Avoid panic buying.
- Avoid tools that use fake warnings or pressure.
- Understand cancellation and renewal.
- Keep recovery information safe.
- Review tools periodically.

If a product recommendation includes an affiliate relationship, referral commission, sponsorship, or other financial benefit, that relationship should be clearly disclosed.

Resource Notes

Use this space to record resources, tools, or providers you decide to use.

Password manager chosen:

Backup service or method chosen:

Identity protection or credit monitoring service, if any:

Antivirus or security software, if any:

Trusted professional support contact:

Official reporting resources bookmarked or saved:

Other useful resources:

Final Reminder

The best resource is the one you can find, understand, and use when you are under pressure.

The best tool is the one that supports safer habits without creating confusion.

Do not measure your safety by how many products you buy.

Measure it by whether you can pause, verify, recover, and ask for help when it matters.