RIVALSHOT ACADEMY · COURSE BOOK

Digital Footprint: Privacy, Posting and Exposure

A companion book to the RivalShot Academy course

ORIGINAL COURSE · ACADEMY.RIVALSHOT.IO

Contents

Foreword: How to use this book

Chapter 1. Read a post the way a stranger would

Chapter 2. Lock the accounts that unlock the rest

Chapter 3. Slow down the message that rushes you

Chapter 4. Find where your details are for sale

Chapter 5. Stand with someone who is targeted online

Chapter 6. Share range days and travel on your terms

Glossary

Where to go next

Sources

Foreword: How to use this book

This book goes with the six lessons of the RivalShot Academy course Digital Footprint: Privacy, Posting and Exposure. The lessons are short on purpose. This book gives each idea more room: more examples, more of the reasoning behind each habit, and more space to think about your own situation.

You can read it straight through, or open the chapter that matches the lesson you just finished. Each chapter has the same parts:

- **The main ideas**, developed further than the lesson could.
- **In practice**: two short fictional stories that show the ideas in everyday places. The people and places are invented.
- **Checklist**: a few actions you can take this week.
- **Key terms**: plain definitions of the words that matter.
- **Talk it through**: three questions for a friend, a family member or a club discussion.
- **Journal prompt**: one question to answer privately, in the course journal or on paper.

A few promises about how this book is written. It will not try to scare you. Many people who see your posts wish you well, and many of the messages you receive are honest. It will not blame anyone who has been harmed: responsibility for misusing information belongs to the person who misuses it. It will not ask you to give up posting, quit the communities you enjoy or become a security expert. And it will never ask you to write down a password, a sign-in code, an account number, your home address or private details about another person. Keep those out of your notes.

Some parts of this book touch on harassment and on people who misuse personal information. If a section brings up something hard, it is fine to stop, step away and come back later, or to skip it. If you are dealing with a frightening situation right now, the “Where to go next” section lists people who can help today.

Finally, this book is educational. It is not legal advice, and finishing it is not a certification of any kind. Laws and services differ from place to place, so check the official source for your jurisdiction when a question turns on the rules where you live.

Chapter 1. Read a post the way a stranger would

Windows and maps

A single post is a small window into your life. Someone looking through it sees a slice: a meal, a view, a grin with a friend. That is usually all anyone wants to see, and it is usually all anyone notices.

The trouble, when there is trouble, comes from the set. A public profile is a row of windows. Look through enough of them, side by side, and they start to work like a map. One photo of a café is a nice morning. Thirty photos of the same café, taken at the same time on the same weekday, tell someone where you will be next Thursday at 7:40. No single post gave that away. The pattern did.

This is the most important idea in the course, and it is a hopeful one. Because much of the risk lives in patterns and in small details, it can often be lowered with small changes: cropping a sign, posting a little later, choosing a smaller audience. You do not have to stop sharing your life. You only have to notice what the set is saying.

The four answers

When you read a post the way a stranger would, you are checking whether it answers four questions that a stranger should have to work hard to answer.

Where are you? Place tags and check-ins answer this out loud. So do street signs, storefront names, distinctive views, building entrances, school logos on clothing and the reflection in a shop window. Some answers are invisible. The FTC points out that a photo taken on your phone may carry information about your location attached to the file, and it suggests turning off location for your camera if you do not want to broadcast where you were. Live location features answer the question in real time. DHS guidance on doxing suggests restricting location tracking and switching off location services, app by app, for anything that does not truly need it.

When will you be there again? This is the routine question. "My usual Saturday," a workout logged at the same hour every day, a weekly "same table, same latte" post: each tells a reader when you will be away from home and where to find you. An older CISA tip on social networking puts it simply: keep your address and details about your schedule or routine off your profile.

Where do you live? House numbers, the view from your porch, the outside of your building, a delivery label on the kitchen counter, a car and its plate in the driveway. Posts that say you are away for a week can lead a viewer to assume your home is empty, even though they do not establish who else is there.

What do you own? A photo of a new television, jewelry, power tools, bikes, sports equipment, a storage cabinet or a shelf full of collectibles tells viewers what is inside your home and sometimes where in the home it is kept. Many viewers will just say "nice." Your post does not get to choose its viewers, though.

DHS lists social media posts, alongside public records, wedding announcements, obituaries and newsletters, among the common places where personal details are gathered. Your posts are one source among many. They are also the one you control most directly.

The stranger's read

The lesson's technique is called the stranger's read. Before you post, look at the photo and caption for about ten seconds as if you were someone who does not know you and does not wish you well. Ask the four questions. Then pick one of five ordinary choices:

1. Post it as it is.
2. Crop or blur a detail.
3. Post it later.
4. Share it with a smaller audience.
5. Keep it for yourself.

Many photos pass in a few seconds and get posted as they are. That is fine. The value is in the habit, not in rejecting things.

Once a month, do the same read on your whole public profile. Scroll it as a stranger would, from the top down. Look at your bio too: a town, a workplace, a gym, a child's team name and a running route together can say a great deal. Old posts count as much as new ones. Many platforms let you archive or limit the audience of older posts in bulk; check your settings.

Audiences you cannot fully control

Privacy settings are worth using. Set your profile so that only people you choose can see most of what you share, limit who can contact you, and review the settings now and then, because platforms change their options. But treat settings as a curtain, not a wall. The FTC notes that even with privacy settings it is impossible to have complete control over who sees your pictures, videos and comments, and that once something is posted you cannot take it back. Friends can screenshot. Posts can be shared beyond the group you picked. Copies can live on other people's devices long after you delete the original.

That is not a reason to panic. It is a reason to make the stranger's read before you post, rather than relying on deletion afterward.

Other people in your posts

Your posts carry other people: grandchildren at a birthday, co-workers at a lunch, friends at a club social. Not all of them chose to be public, and some may have good reasons not to be. The FTC's advice is simple: get someone's OK before you share photos or videos they are in. For children, ask a parent or guardian. Watch for details that point to someone else's routine or location, like a school name on a jersey or a friend's house number in the background.

The same goes in reverse. You can ask friends and family not to tag you or post your location without checking with you first. Many people are glad to be asked.

It helps to say why in a sentence, without drama: "I'm trying to keep where I live and when I'm out a bit more private, so could you check with me before tagging me?" Framed that way, the re-

quest is about your preferences, not about anyone's judgment. Teenagers and older relatives often appreciate a simple, shared family habit more than a long list of rules: "We post trips after we're home" is easy to remember and easy to follow.

What this does not mean

It does not mean you should stop posting, cut yourself off from the communities you enjoy or treat every follower as a threat. Sharing is part of how people find each other, and many viewers are friends, family and fellow hobbyists. It does not mean anyone harmed after posting brought it on themselves. The person who misuses information is responsible for that choice. The goal is narrower and kinder: you decide which of the four answers to give, and to whom.

In practice

The running route. Ezra, a graduate student, logs his morning runs in a fitness app that shares each route publicly. He enjoys the encouragement from strangers. One evening he tries the stranger's read on his own activity page and sees that every route starts and ends at the same corner, at the same time, five days a week. The corner is outside his apartment building. He opens the app's privacy settings and finds options to limit who can see his activities and to hide the start and end of routes. He keeps posting runs, now to followers he approves, with the first and last stretch hidden. The encouragement keeps coming. The map is gone.

The park photo. Rosa takes her two grandchildren to the park on Saturday and snaps a wonderful photo of them on the swings. Before she posts, she does the read. The older child's soccer jersey

shows the name of his school, and the park sign is readable behind them. She crops the sign, picks a different shot where the jersey is turned away, and texts her daughter: “Okay if I post this one of the kids?” Her daughter says yes, but asks her to share it with family only. Rosa changes the audience and posts it. Total time: about two minutes.

Checklist

- Try the stranger’s read on your next three posts: where, when, home, what you own.
- Turn off location for your camera app if you do not need it, and remove location tags you did not mean to add.
- Review which apps can use your location, and switch off any that do not need it.
- Scroll your public profile once this month as a stranger would, including your bio and old posts.
- Check your privacy settings and limit who can see and comment on your posts.
- Ask before posting photos of other people, and ask a parent or guardian for children.
- Tell close friends and family how you prefer to be tagged.

Key terms

- **Digital footprint**: the trail of information about you online, including what you post, what others post about you and what is gathered from records.
- **Location data**: information about where a device or photo was, sometimes attached invisibly to a photo file.
- **Routine**: a predictable pattern of where you go and when.

- **Privacy settings**: the controls that decide who can see, share and comment on what you post.
- **The stranger's read**: a ten-second check of a post for the four answers before sharing.

Talk it through

1. Which of the four answers do you think people give away most often without noticing? Why?
2. How do you decide whether to ask permission before posting a photo of someone else? Has anyone ever posted something of yours that you wished they had asked about?
3. What would make the stranger's read feel like a quick habit rather than a chore?

Journal prompt

Scroll your own public posts from the last month. In a few sentences, describe the pattern a stranger might notice, and one small change you will make that still lets you share what you love.

Chapter 2. Lock the accounts that unlock the rest

Hooks and keys

Many people have dozens of online accounts. They are not equally important. A few accounts work like keys that open the others, and protecting those few first does a lot of the work.

Your main email account is the biggest key. When you click "forgot password" almost anywhere, the reset link goes to your email. Whoever controls that inbox can often take over your shopping, social, club and streaming accounts one at a time. Your phone is the next key, because it receives text codes and holds your apps. After that come your password manager, if you use one, your bank and your main social account, which people trust as "you."

So the plan is simple to state: protect the keys first, in order, before worrying about anything else. CISA's Secure Our World campaign describes everyday protection as four habits: use strong passwords and a password manager, turn on multifactor authentication, update software, and recognize and report phishing. This chapter covers the first three. Chapter 3 covers the fourth.

A second step: multifactor authentication

Multifactor authentication, often called MFA, two-factor or two-step verification, means proving it is you with more than a password. NIST explains it with three kinds of evidence:

- **Something you know**, like a password or PIN.

- **Something you have**, like your phone, a security key or a bank card.
- **Something you are**, like a fingerprint or face.

Real MFA combines two different kinds. Two passwords do not count, because both are "something you know." NIST's advice is to use MFA wherever it is offered, especially for your primary email, financial accounts and health records. When MFA is optional, you have to switch it on yourself; many services put it under account settings, then security, with a name like "two-step verification."

Options vary. A code can come by text message or from an authenticator app that makes a fresh code every few seconds. A physical security key plugs in or taps your phone. A fingerprint or face check can confirm it is you. CISA's older MFA page makes a point worth remembering: some methods are stronger than others, but any MFA is better than no MFA. If a text code is all a service offers, use it.

It also helps to know what MFA prompts mean. If your phone suddenly asks you to approve a sign-in you did not start, someone probably has your password. Do not approve it. Deny it, change that account's password from the official app or website, and check the account's recent activity.

Passkeys: nothing to type, nothing to steal

Many services now offer passkeys. A passkey lets you sign in using the same fingerprint, face scan or PIN you use to unlock your phone or computer. Behind the scenes, your device proves who you are without sending a password. The FIDO Alliance, the stan-

dards group behind passkeys, explains that your fingerprint or face data stays on your device rather than being sent to the service.

Because there is no password to type, there is nothing for a fake website to capture. The UK's National Cyber Security Centre recommends choosing passkeys over passwords wherever they are available, because passkeys cannot be intercepted, reused or stolen the way passwords can. NIST's current digital identity guidelines draw the same line in more technical language: codes you type in, whether from a text or an app, are not considered phishing-resistant, while cryptographic methods like the ones passkeys use can be.

What happens if you lose your phone? Some passkeys sync through your device's credential manager, the built-in tool that stores passkeys and passwords, to your other trusted devices; others stay on one device or security key. Find out which kind you have before relying on another device, and take two minutes to check each important account's recovery options: a backup email and phone number you still control, and any recovery codes the service offers, kept somewhere private. A passkey resists a fake sign-in page, but it does not make every account-recovery route or a compromised device safe.

Where a service does not offer passkeys yet, the NCSC's fallback is a strong, unique password, ideally generated by a password manager, plus two-step verification.

Passwords you still need

For accounts without passkeys, three words matter: long, random and unique. CISA's password guidance suggests at least 16 characters, either a random mix or a passphrase of several unrelated

words, and a different password for every account. Reuse is the real danger. When one website suffers a breach, criminals try the stolen email and password combination on other sites. A unique password keeps one breach from becoming many.

Nobody can remember dozens of long, unique passwords. That is the job of a password manager. It creates strong passwords, remembers them, fills them in, and can warn you about weak or reused ones. Many phones and browsers include one, and there are standalone options too. You only need to remember one long passphrase, the one that opens the manager, so make that one good and protect the manager with MFA.

Two pieces of good news from NIST's guidelines for services: well-run websites should let you use password managers and autofill, and they should not force you to change a strong password on a schedule. Change a password when there is a reason, such as a breach notice or a sign that someone else used it.

Devices: updates, locks and backups

Your accounts are only as safe as the devices you use to reach them. CISA's advice on updates is blunt: do not delay them. Updates close the security flaws that criminals look for, and they protect you only after they are installed. CISA's update page names a habit many of us share, tapping "remind me later" over and over. Turn on automatic updates for your phone, computer, browser and apps, and let them run overnight.

Give your phone a screen lock with a PIN or passcode, plus a fingerprint or face unlock if you like. Back up your photos and files to an external drive or a cloud service, as the FTC recommends, so that a lost, broken or locked device is an inconvenience rather

than a disaster. While you are in your settings, remove apps and browser extensions you no longer use. DHS notes that unneeded apps and extensions can collect personal data.

Your phone number is a key too. Ask your mobile carrier what account protections it offers, such as an account PIN, so that nobody can move your number to another phone without your say.

The key-account hour

The lesson's technique is a key-account hour. Before changing settings, consider whether a partner or another person may be monitoring your device or accounts. If so, changes could be noticed; use a device they cannot monitor to speak with a domestic violence advocate about a safety plan first. The FTC's stalkerware guidance explains this concern, and Chapter 5 covers support. For ordinary account upkeep when that concern does not apply, work through these steps in one sitting:

1. Open your main email's security settings. Turn on a passkey or two-step verification.
2. Check that the recovery phone number and backup email are current and yours.
3. Look at signed-in devices and sign out of any you do not recognize.
4. Set up a password manager if you do not have one, with a long passphrase.
5. Turn on automatic updates on your phone and computer.
6. Write down, by name only, the next three accounts to fix, and schedule ten minutes for each next week.

Done in order, a little at a time, this beats a perfect plan you never start.

What this does not mean

It does not mean you need to become an expert, buy special products or reach perfection. No setting makes an account unbreakable. The aim is to stop being the easy target that a reused password makes you. And if an account is taken over anyway, it is not a personal failing. Contact the provider through its official website or app, not through any message about the problem, and if personal or financial information was exposed, IdentityTheft.gov from the FTC walks you through recovery steps.

In practice

The lost phone on the bus. Kofi, a night-shift nurse, leaves his phone on a bus seat after a long shift. A year ago this would have meant a week of locked accounts. Since then he has moved his email and bank to passkeys, checked that they sync to his other devices, and kept his password manager synced. At home, he signs in to his email from his laptop and uses the device's "find my phone" feature to lock and erase the lost phone remotely. When his new phone arrives, he signs in to his credential manager, and his passkeys appear. The only thing he could not get back was the little keychain clipped to the case.

The 2 a.m. prompt. Alma, the treasurer of a small hiking club, is woken by her phone asking her to approve a sign-in to the club's shared email. She did not start one. She taps "deny," then opens the email provider's app herself, changes the password to a new one from her password manager, and checks recent activity. In the morning she tells the club's board what happened, and they agree to move the account to a passkey. The prompt was not the problem. It was the warning that worked.

Checklist

- If someone may be monitoring your device or accounts, talk with a domestic violence advocate from a device they cannot monitor before changing settings.
- Turn on a passkey or two-step verification for your main email first.
- Confirm your email's recovery phone and backup email are current.
- Set up a password manager and protect it with a long passphrase and MFA.
- Replace reused passwords on your most important accounts, starting with money and health.
- Turn on automatic updates for your phone, computer, browser and apps.
- Set a screen lock and turn on backups for photos and files.
- Never approve a sign-in prompt you did not start.
- Ask your mobile carrier about account protection for your phone number.

Key terms

- **Multifactor authentication (MFA)**: signing in with two or more different kinds of evidence, such as a password plus a code or fingerprint. Also called two-step verification.
- **Passkey**: a sign-in method that uses your device's unlock (fingerprint, face or PIN) instead of a typed password.
- **Password manager**: a tool that creates, stores and fills in strong, unique passwords.

- **Credential manager**: the built-in tool on a phone or computer that stores passkeys and passwords and can sync them across your devices.
- **Phishing-resistant**: a sign-in method that a fake website cannot trick you into handing over.
- **Automatic updates**: a setting that installs security fixes without waiting for you.

Talk it through

1. Which of your accounts would cause the most trouble if someone else controlled it? Why that one?
2. What has stopped you, or people you know, from turning on two-step verification or passkeys? What would make it easier?
3. How could a club or family help members with these settings without anyone sharing passwords?

Journal prompt

List, by name only, your three most important accounts. For each, write what protects it now and the next step you will take, with a date.

Chapter 3. Slow down the message that rushes you

The business of hurry

Many scams do not break into computers. They break into moments. Phishing is a message designed to make you act before you think: click a link, pay a bill, share a detail, read back a code. It arrives as an email, a text, a direct message, a voicemail or a live call. Social engineering is the broader craft: getting what someone wants by working on people's trust, helpfulness, fear or hurry instead of on technology.

The FTC describes how these messages tell a story. There is suspicious activity on your account. A payment did not go through. Here is an invoice you do not recognize. You are owed a refund. You have won a free gift. Each story ends with the same request: tap here, now.

Pressure, not polish

For years people were taught to spot scams by bad spelling. That clue is fading. CISA's phishing guidance notes that tools like AI now help scammers write polished messages, so careful grammar proves nothing. Logos, signatures and friendly tone are just as easy to copy.

Look instead at what the message asks for and how it pushes:

- **A deadline or threat**: "Your account will be locked in one hour."

- **An unusual payment method**: gift cards, wire transfers, cryptocurrency or payment apps to a stranger.
- **A request for secrets**: your password, a sign-in code, your full card number or Social Security number.
- **Something you did not expect**: an attachment, an invoice, a delivery problem for a package you never ordered.
- **A relationship that does not exist**: a company you have no account with.
- **Secrecy or a channel switch**: "Keep this between us" or "Text me on this other app."

The FTC states one rule plainly: legitimate companies won't email or text you a link to update your payment information.

When the message knows things about you

Social engineering gets more convincing when it borrows details from your life. A caller who knows your club's name, your dog's name or where you were on Saturday sounds like someone you should trust. But knowing a detail is not proof of identity. As Chapter 1 showed, many details are sitting in public posts. CISA's older social engineering tip describes how attackers piece together small bits of information, gathered from different places, until they sound like insiders. It also describes pretexting: posing as a new employee, a repair person or a researcher with a believable reason to ask questions.

Phone calls deserve a special mention. CISA notes that caller ID can be faked, so a call that shows your bank's name may not be from your bank. Treat any request on an unexpected call the same way you would treat it in an email.

Watch for familiar patterns:

- The friend or relative with a “new number” who needs money quickly and asks you not to tell anyone.
- The text saying your reservation, delivery or membership has a problem and you must pay to fix it.
- The “fraud department” that asks you to read back a code it just texted you.

That last one deserves a stop sign. A code sent to your phone is a key to your account. Real companies do not call to ask you for it. The person asking is usually the one trying to get in.

Pause, leave, look up

The lesson’s technique has three steps.

Pause. When a message makes you feel rushed, scared, guilty or flattered, notice the feeling and name it: “This is pressure.” The feeling is information, not an instruction.

Leave. Do not use the message’s links, attachments, phone numbers or reply button. CISA also advises against using “unsubscribe” links in suspicious messages, since they can lead to the same places.

Look up. Contact the company or person through a channel you choose: its app, a web address you type yourself, the number on your card or statement, or the number already saved in your phone for a friend. The FTC recommends exactly this: if you have an account with the company, contact it using a phone number or website you know is real. CISA gives the same advice for odd messages from friends: confirm with them by a call or text to a number you already have.

If an alert was genuine, you will see the same issue when you sign in the normal way. Nothing is lost by checking. A lot can be lost by hurrying.

Report it and recover

Reporting helps protect others, and it takes a minute. The FTC suggests:

- Forward phishing emails to the Anti-Phishing Working Group at reportphishing@apwg.org.
- Forward phishing texts to 7726 (which spells SPAM).
- Report scams at ReportFraud.ftc.gov.

Many email and messaging apps also have a built-in “report” or “report junk” option.

If you already responded, act quickly rather than waiting to be sure. If you shared information such as a Social Security, card or bank account number, IdentityTheft.gov gives steps based on what was exposed. If you clicked a link or opened an attachment that may have installed something harmful, the FTC suggests updating your security software, running a scan and removing anything it flags. Change the password on any account you revealed, add the protections from Chapter 2, and call your bank using the number on your card.

Shame-free by design

Being fooled is not a sign of foolishness. Scams are professional work, tested and tuned to catch smart, busy and kind people at the wrong moment: tired after a shift, worried about a relative,

distracted at the front desk. Many people who are tricked never say so because they feel embarrassed, and that silence helps the scammer.

So make it easy, in your family, club or workplace, to say "I think I clicked something." Thank the person. Help them through the recovery steps. Never scold.

It also helps to agree on a few house rules in advance, while everyone is calm. For example: anyone in the family who gets an urgent request for money from "a relative" calls that relative back on a saved number before doing anything, no exceptions and no hurt feelings. A club treasurer never pays an invoice or changes bank details based on an email alone; a second person confirms by phone. A front desk never reads out a member's details to a caller, however official they sound. Rules decided ahead of time take the pressure off the person on the spot. They can simply say, "Our rule is that I call back," and the scammer's clock stops working.

What this does not mean

It does not mean you should distrust every message or ignore real alerts. Banks, doctors' offices and clubs do contact people. The answer is to verify through your own channel, not to stop listening. And you never need to argue with, test, trick or confront a scammer. Just leave and report.

In practice

The call from the bank. Malik's phone shows his bank's name. The caller is calm and professional: there has been a suspicious charge, and to block it, they just need him to read back the code they are texting now. The code arrives. Malik notices the pressure

and remembers the stop sign. “I’ll call you back,” he says, and hangs up. He turns over his debit card and calls the number printed on the back. The bank’s real fraud team finds no suspicious charge and notes that someone tried to reset his online banking password a few minutes earlier. The code was the key to that reset. Malik changes his password and switches his banking app to a passkey.

The new number. Delia gets a text from an unknown number: “Hi Aunt Dee, it’s Marco, I got a new phone. Can you send $300 for rent? Pay you back Friday. Please don’t tell Mom.” The message sounds like her nephew. The secrecy is what makes her pause. She does not reply to the new number. She calls Marco’s saved number, and he picks up at work, puzzled. He never changed phones. Delia forwards the text to 7726, deletes it, and sends a quick note to the family group chat so her sister knows to watch for the same trick.

Checklist

- Learn the pressure signs: deadlines, threats, odd payment methods, requests for codes, secrecy.
- Never read a sign-in code to anyone who contacts you.
- Leave suspicious messages: no links, attachments, numbers, replies or unsubscribe links.
- Verify through your own channel: the app, a typed web address, the number on your card, a saved contact.
- Forward phishing emails to reportphishing@apwg.org and phishing texts to 7726.
- Report scams at ReportFraud.ftc.gov.
- If you shared sensitive information, go to IdentityTheft.gov and contact your bank quickly.

- Make it easy for others to tell you they were fooled.

Key terms

- **Phishing**: a message that pretends to be from someone trusted to get you to click, pay or share information.
- **Smishing**: phishing by text message.
- **Vishing**: phishing by voice call.
- **Social engineering**: manipulating people, rather than technology, to get access or information.
- **Pretexting**: inventing a believable reason or role to get information.
- **Spoofing**: faking a sender's name, email address or caller ID.

Talk it through

1. Which kind of pressure works best on you: urgency, fear, guilt or flattery? Why do you think that is?
2. What are the trusted channels you already have for your bank, your club and your family?
3. How could a group you belong to make it easier for members to report being fooled?

Journal prompt

Describe a message, real or imagined, that would be most likely to rush you. Then write the exact words you will say to yourself, and the channel you will use to check it.

Chapter 4. Find where your details are for sale

The footprint you did not post

Most of this course is about what you share. This chapter is about what is shared about you. The FTC explains that data brokers are companies that collect information about people and sell or share it with others. People-search sites, sometimes called people-finder sites, are one kind of data broker. They assemble reports about individuals and sell them to anyone who pays.

Where does the information come from? The FTC lists three main sources: other data brokers, public social media profiles, and government public records. Public records cover a lot: property records, voter registration, court and bankruptcy records, professional licenses, and birth, marriage, divorce and death records. Starting from just a name or a phone number, a report can show someone's age, past names, current and past addresses, property transactions, education and work history, and the names and addresses of relatives.

Why this matters, calmly

Many lookups are ordinary. People search for old friends, check out a contractor or confirm a landlord's name. The FTC notes these everyday uses. It also notes the other side: survivors of domestic violence or stalking may not want their location or their family's details exposed.

DHS's guidance on doxing lists the common sources of personal information that get gathered and released: social media posts, property and court records, wedding announcements and obituaries, newsletters, public conferences and voter registration lists. Those are ordinary documents, and most of them do good work in the world. The point is not to fear them. The point is that if you have a visible hobby, a public role, a recent online disagreement or simply a preference for privacy, making your home address harder to find is a reasonable, quiet step.

Turning off the tap: what you feed the system

Before opting out, think about what flows in. DHS suggests removing personal details like your address, date of birth and phone number from your social media profiles, reviewing your followers and turning on privacy settings. Other ideas:

- **Bios and "about" pages**: a city, an employer and a family member's name together can do a lot of work.
- **Announcements**: wedding, birth and graduation announcements can be lovely without a street name or full date.
- **Club newsletters and member directories**: ask whether they need full names, towns or photos, and whether members can opt in rather than out.
- **Event sign-ups and contests**: share the minimum, and read what the organizer does with the list.

None of this is about hiding. It is about not refilling the well while you are trying to empty it.

The opt-out routine

The lesson's technique follows the FTC's outline.

1. **Search for yourself** on a people-search site, starting with your phone number or address.
2. **Find the opt-out.** If a report includes your information, look for the site's opt-out link and follow it. If you cannot find one, search the site's name with words like "opt out" or "remove my information."
3. **Repeat** on other people-search sites. The FTC points to lists maintained by others, such as a guide from the National Network to End Domestic Violence, to help identify sites.
4. **Check back** periodically and submit new requests when information reappears.

Keep a simple log with four columns: the site, the date you asked, whether you got a confirmation, and a date to check again. Keep the log private, and keep it general; you do not need to copy your personal details into it.

Some people use a separate email address only for opt-out requests, so confirmations do not clutter their main inbox and the main address does not end up on yet another list. Sites may ask for information to confirm your identity; the FTC notes this. Give only what the form actually needs. If a request feels excessive, stop and look up the site's reputation before continuing.

Paying for help

Removal services will do the searching and requesting for a fee. That is a choice, not a requirement, and it can be worth it for people with less time or more exposure. Before signing up, the FTC suggests asking three questions:

- How many websites does the service cover?
- Will it give you a report of the sites it opted you out of?
- How often does it rescan for information that reappears or is newly listed?

Compare the answers with what you could do yourself in an hour each season.

The limits, honestly

Opting out stops a site from selling the report it had. It does not delete your information from public records, which the FTC is careful to point out. If records change, after a move, a refinance or a new voter registration, your details can reappear. They may also show up inside a relative's, neighbor's or associate's report. That is why this is maintenance, not a one-time cleanse. A check every few months, using your log, keeps the effort small.

Reading a report without panic

The first time you see your own report, it can be unsettling. A few things are worth knowing. Reports are often partly wrong. They may mix you up with someone with a similar name, list an address you left years ago, or guess at relatives. You do not need to correct these errors, and supplying corrections can simply give the site better data. Your goal is removal, not accuracy.

A listing also says nothing about who, if anyone, has looked at it. Treat what you find as a to-do list, not as evidence that something is wrong.

Helping the people you live with

Opt-outs are personal. Each adult in a household usually has a separate listing, and each listing has to be removed on its own. If an older parent, a partner or an adult child would like help, offer to sit with them while they search for themselves and submit their own requests, rather than searching for them without asking. For children, a parent or guardian can decide what to do. Doing it together is often more pleasant than doing it alone, and it makes a reasonable seasonal habit for a household: a cup of coffee, a shared checklist and twenty minutes each.

When there is a specific safety concern

If someone has threatened or stalked you, your situation calls for more than a general routine. A local victim advocate can explain what additional options exist where you live; some places have programs for people with specific safety needs. Laws and programs vary, so check the official source for your jurisdiction. This book does not give legal advice. The National Domestic Violence Hotline, listed in “Where to go next,” can help you find local support.

What this does not mean

You cannot vanish, and you do not need to. The aim is to make yourself harder to find, not to erase yourself from public life. Finding your own listing does not mean anyone is targeting you; a

listing alone says nothing about who has looked. And opting out is not an admission that something is wrong. It is just housekeeping.

In practice

A year of upkeep. After the open house that started it all, Priya opted out of three people-search sites and set a reminder for every three months. At the first recheck, two listings were still gone and one had quietly returned with the same details. She submitted a new request and noted it in her log. After she refinanced her home later that year, a fourth site appeared with her updated address. That one took five minutes. By the end of the year, her log showed eleven requests and about two hours of total effort, spread across four quiet evenings.

The club newsletter. Wen volunteers as secretary for her community garden club. Reading the stranger's read in this course, she looks at the club's monthly newsletter, which is posted publicly as a PDF. Each issue lists new members by full name and neighborhood, with a photo. Wen brings it to the next meeting, not as an alarm, just a suggestion: first names only, no neighborhoods, and photos only for members who opt in. The group agrees in five minutes. Two older members say they had been uneasy about it for years but did not want to complain.

Checklist

- Search for yourself on a people-search site, starting with your phone number or address.
- Follow each site's opt-out process and repeat on other sites.
- Keep a private log: site, date asked, confirmation, recheck date.

- Give only the information each opt-out form needs.
- Remove your address, birth date and phone number from social profiles.
- Ask clubs and groups to limit what they publish about members.
- Set a recurring reminder to recheck every few months.

Key terms

- **Data broker**: a company that collects information about people and sells or shares it.
- **People-search site**: a data broker that sells reports about individuals to anyone who pays.
- **Public record**: information held by government that is generally open to the public, such as property or court records.
- **Opt-out**: a request asking a site to stop showing or selling your information.
- **Doxing**: gathering someone's personal information and releasing it publicly to harm them.

Talk it through

1. What surprised you most about where people-search sites get their information?
2. Which of the groups you belong to publish information about members? Is all of it needed?
3. How would you explain opt-outs to a friend without making them anxious?

Journal prompt

Before you search, write down what you expect to find. After you search, write in general terms what surprised you, and set your first recheck date.

Chapter 5. Stand with someone who is targeted online

What targeting looks like

Online targeting takes many forms. A pile-on of hostile comments under an ordinary photo. An account pretending to be someone. A stream of threatening messages. Private photos shared without permission. An account taken over and used to embarrass its owner. And doxing, which DHS describes as gathering someone's personal information and releasing it publicly for malicious purposes, such as public humiliation, stalking, identity theft or targeting for harassment.

For the person on the receiving end, it can feel as if the walls of home have gone thin. People who are targeted often describe feeling watched, exposed and unsure whom to trust. They may also feel embarrassed, even though they did nothing wrong.

When it happens to someone you know, you do not need special skills to help. You need to be steady, follow their lead and avoid making it bigger. This chapter shows how.

Start with belief and two questions

Your first words matter most. Say that you believe them. Then ask two questions:

- "Are you safe right now?"
- "What would help most?"

Let them lead. Someone being targeted has already lost some control over their own story. Taking over their accounts, reporting on their behalf without asking, or telling others without permission can make that loss worse, even with the best intentions.

Leave out questions that sound like blame, such as “Why did you post that publicly?” or “Why did you have that photo at all?” There may be a time for the privacy steps in this course, but not in the first conversation, and never as a judgment. Sharing a photo never earns harassment.

Practical help, offered not imposed

Once you know what they want, offer specific help they can accept or decline.

Keep the evidence. DHS suggests preserving evidence: save emails, voicemails and text messages, and take screenshots or photos of comments. Evidence may matter later for platform reports, police reports or other steps. You can be the evidence keeper. Capture each post or message with the date, the time, the username and the web address visible if possible. Save the files to a folder your friend controls, and do not forward them around. This way your friend does not have to read every cruel message to protect their options.

Report to the platform. DHS suggests asking platforms or websites to take down false, abusive or threatening content under their rules. Many platforms have report buttons on posts and profiles, and some have specific forms for impersonation and for posted personal information. Sitting with your friend while they file reports can make a draining task feel lighter.

Report threats. If there is a threat to physical safety or your friend feels criminally harassed, DHS suggests reporting to local law enforcement as well as to the platform. Online crime can also be reported to the FBI's Internet Crime Complaint Center at ic3.gov. If anyone is in immediate danger, call 911.

Close the doors, later. Once the first wave passes, the steps from Chapters 2 and 4 help: tighter privacy settings, two-step verification or passkeys on key accounts, fresh passwords where anything may have been exposed, and people-search opt-outs to make an address harder to find. Offer to help with these when your friend is ready, not in the first hour.

What not to do

Some of the most natural reactions make things worse.

- **Do not repost the attack**, even to condemn it. Every share sends the content, and often the personal details, to new people.
- **Never repost leaked details**, even in a screenshot that says "look what they did."
- **Do not reply in anger** in the comments. Harassers often want attention; a public fight gives it to them.
- **Do not try to unmask the harasser or dig up their information.** Counter-doxing can spread harm, put you at risk and complicate any later report.

The FTC's advice for online harassment is to keep a cool head and not respond, block the person, report the abuse to the site, save the evidence and ask someone you trust for help. Quiet,

steady action avoids feeding a loud public fight. The same instinct, helping without making things worse, applies in everyday, offline situations too.

When the problem may be someone close

Sometimes the person causing harm is not a stranger. If your friend suspects that a current or former partner or a family member is tracking their phone or reading their accounts, take extra care. The FTC describes stalkerware, software installed on a device without the owner's knowledge that can reveal location, messages, photos and activity. Possible signs include the other person knowing where your friend has been or what they said in private, or a phone that suddenly drains its battery, uses more data or behaves strangely.

Here is the hard part. Sudden changes can be noticed. The FTC warns that an abuser who suspects their access is being cut off may escalate, and it suggests reaching a domestic violence advocate first, ideally from a device that may not be monitored, such as a friend's phone. Advocates can help with a safety plan, preserving evidence and talking with law enforcement. The FTC also advises documenting evidence before resetting or replacing a phone, and not restoring apps from an old backup, which could reinstall the software.

The National Domestic Violence Hotline is 1-800-799-7233 (1-800-799-SAFE). You can also chat at thehotline.org or text START to 88788. Your role is to help your friend reach an advocate, not to search, wipe or reset their phone yourself.

The three-offer message

The lesson's technique is a message with belief and a short menu: "I believe you, and I'm here. I can save screenshots for you, sit with you while you report it, or just check in tomorrow. What would help?"

Specific offers are easier to accept than "let me know if you need anything," which leaves all the work with the person who is already overwhelmed. After they choose, do what you said, and check in when you said you would. Steadiness over days matters more than intensity in the first hour.

Your limits matter too

You are not their investigator, lawyer, therapist or bodyguard. You never need to confront the harasser, visit anyone, or put yourself at risk. Decisions about reporting belong to the person targeted, except when someone is in immediate danger. Supporting someone through harassment can be heavy. It is fine to step back a little, share the load with others they trust, and point them toward advocates and hotlines who do this every day.

In practice

The lounge photo. Leila posts a cheerful photo from her club's lounge after her first members' social night. A stranger reposts it with mocking comments, and by morning someone has added her employer and neighborhood. She messages her friend Sam at 7 a.m.: "I don't know what to do. Everyone can see it." Sam's thumbs are already moving toward the comment box. Instead, Sam calls. "I believe you. Are you safe right now? What would help most?" Leila says she cannot stand to look at it. Sam offers to take the screenshots. Over the next hour, Sam captures each

post with the date and username, saves them to a folder Leila shares, and sits on the phone while Leila reports the reposts and the comment naming her employer. Two are removed by afternoon. Sam texts the next evening, and the evening after that. Nobody fights in the comments.

The group chat. In a club's group chat, a member shares a screenshot of a stranger's post that lists another member's home street: "Can you believe someone did this?" The chat's moderator, Teresa, deletes the screenshot within minutes, then posts a short note: "Please don't share this, even to help. Every copy spreads it. If you want to support, message them privately." She messages the targeted member separately with a three-offer message. The member chooses help with reporting and asks that the group not discuss it. Teresa respects that.

Checklist

- Start with belief: "I believe you."
- Ask: "Are you safe right now?" and "What would help most?"
- Offer specific help: saving evidence, reporting together, checking in.
- Capture evidence with dates, usernames and web addresses, stored where they control it.
- Never repost the attack or the leaked details, and do not reply in anger.
- If there is a threat to safety, support reporting to local police and the platform; call 911 in an emergency.
- If someone close may be monitoring them, help them reach an advocate first.
- Look after your own limits and share the load.

Key terms

- **Doxing**: gathering someone's personal information and releasing it publicly to harm them.
- **Pile-on**: many people targeting one person with hostile messages at once.
- **Impersonation**: an account or message pretending to be someone else.
- **Stalkerware**: software secretly installed on a device to monitor its owner.
- **Evidence keeper**: a supporter who saves records of harassment so the targeted person does not have to.
- **Takedown request**: a request to a platform or website to remove content under its rules.

Talk it through

1. Why do you think reposting an attack to condemn it can still cause harm?
2. What makes a message of support feel helpful rather than overwhelming?
3. How could a group chat, club or team agree in advance on how to respond if a member is targeted?

Journal prompt

Write the first message you would send to a friend who tells you they are being targeted online. Then note one thing you would hold back from doing, and why.

Chapter 6. Share range days and travel on your terms

Good moments, worth sharing

A first range visit, a safety class finished with friends, a weekend competition, a road trip to a new club: these are good moments, and sharing them is part of how people find their community. This chapter is not about sharing less. It is about sharing on your terms.

Range days and travel posts tend to bring all four answers from Chapter 1 together in one frame: where you are, when you go, where you live and what you own. A few seconds of checking keeps the joy and drops the map.

What a range-day photo can say

Collection. A series of posts showing equipment tells viewers what is in your home and roughly what it is worth. That is useful information to a thief, and it is information you do not need to give. Secure storage at home is a related topic of its own. The posting side is simply not advertising what you keep, where you keep it, or how much of it there is.

Routine. “Every Saturday at eight” tells readers when you are away from home and where to find you. So does a weekly post from the same club at the same time.

Location. The club’s name on the wall, a lobby sign, the building’s front door, a distinctive view from the parking lot.

Identity. A membership card on the counter, a name tag on a bag, a sign-in sheet in the background, a lanyard badge.

Vehicles. Your car or truck with its plate visible in the parking lot, and any parking permits or stickers that point to your neighborhood or workplace.

Other people. Lane neighbors, instructors, staff and children who did not agree to appear in your post. The FTC's advice applies: get someone's OK before you share photos or videos they are in.

Ask the range first

Before you take a photo at all, ask the staff about the range's photography rules. Many ranges and clubs set their own policies, including areas where photos are not allowed and rules about photographing other members. They are the right people to ask, and following their rules is part of being a considerate member and a good lane neighbor.

Frame, delay, audience

The lesson's technique has three parts.

Frame. Check the four corners and the background before you post. Look for signs, plates, badges, cards, documents, screens, reflections and other people's faces. Crop or blur what does not need to be there. Many phones have a simple markup or blur tool built into the photo editor.

Delay. Post trips and range days after you are home. A photo shared on Sunday night tells the same story as one shared on Saturday morning, without a live map of where you are or a hint

that your home may be unattended. Turn off location for your camera, as the FTC suggests, and skip the location tag. If you want to name the club, consider doing it after you have left.

Audience. Share with a close-friends list or a private group when that fits the moment. Remember the FTC's caution that privacy settings never give complete control, so the frame and delay checks still matter.

Travel adds a few details

- **"Away" posts** can invite assumptions about an unattended home, though they do not prove it is empty. Save "back next week" for after you are back.
- **Boarding passes and booking screens** carry codes and personal details. Keep them out of the frame entirely.
- **Hotel room numbers**, on key sleeves or doors, and **event badges** with your full name are worth a second look.
- **The name of the event you are heading to**, plus dates, tells readers where you will be. Share it after.
- **Temporary stories** feel safe, but DHS's guidance on doxing reminds people to be careful even with photos and videos meant to disappear. Anyone can screenshot a story before it vanishes.
- **Live streaming** is the most "right now" form of sharing. If you stream, avoid showing your arrival, your vehicle or your lodging.

Purchases, packages and gear posts

Unboxing and "new gear" posts deserve their own frame check. Shipping boxes and receipts often show your full name and address, and order screens can reveal what you bought and when it is arriving. If you want to share something new, photograph it away from the packaging, after the boxes are recycled, and leave out prices and quantities. A post about learning something new, such as a class you finished or a skill you are building, tells your story better than an inventory does, and it gives a stranger far less to work with.

When friends post you

Range days are often group outings, and your friends may post before you do. A quick word before the photos start saves awkward requests later: "Happy to be in photos, but could we post after we've all left, and skip the location?" Many people say yes without a second thought. If someone has already posted something that shows more than you would like, a private message asking them to crop, delay or remove it is reasonable and usually welcomed. Return the courtesy by asking before you post them.

Comments and attention

Range photos sometimes attract strangers, and not all of them are friendly. Use your platform's comment controls: limit who can comment, filter words, and hide or restrict accounts. You never owe a provocation a reply. Stepping away is a skill, not a defeat.

The earlier chapters pay off here. Strong account protection makes your account harder to hijack. People-search opt-outs make your home harder to find. Thoughtful framing keeps routine, vehicle and lodging out of view. Together, they reduce what a

hostile viewer can stitch together. If a post does attract harassment, Chapter 5's steps apply to you too: save evidence, report it and ask someone you trust for help.

What this does not mean

It does not mean hiding your hobby, feeling ashamed of it or giving up on posting. It does not mean every viewer is a threat; many are friends and fellow members cheering you on. It is not legal advice about photography or privacy rules; ask the range about its policies and check official sources where you live. And if someone misuses what you share, the fault is theirs.

In practice

The parking-garage selfie, take two. Andre and his teenage daughter spend a Saturday at a club three hours from home. In the parking garage he takes a selfie of the two of them by his truck, with the club's sign behind them, the plate in view and the hotel key sleeve on the dashboard. He starts typing "Weekend away! Back Monday" and stops. He has done the stranger's read enough times now that it is automatic. He saves the photo instead of posting it. Sunday night, at home, he crops out the plate and the dashboard, removes the location, and shares it with his close-friends list: "Best Saturday in months with this one." His daughter approves the photo before he posts. The comments are all about her smile.

The newcomers' class photo. Bea teaches a newcomers' safety class at a community range. At the end, the group wants a photo in the classroom. Before she takes it, she asks everyone: "I'd like to post this on the club page. Anyone prefer not to be in it?" Two people say they would rather not. Bea takes one photo with ev-

eryone for the group to keep privately and a second, for the club page, with only the people who agreed. She posts it the next day, with no last names, no class schedule in the caption and no sign-in sheet in the background. One of the two who opted out thanks her privately for asking.

Checklist

- Ask staff about the range's photography rules before taking photos.
- Ask before including anyone else in your post.
- Check the four corners and background for signs, plates, badges, cards, documents and screens.
- Post range days and trips after you are home.
- Turn off camera location and skip location tags.
- Keep boarding passes, hotel room numbers and full-name badges out of frame.
- Choose your audience; use close-friends lists when they fit.
- Use comment controls, and do not argue with provocations.

Key terms

- **Frame check**: scanning a photo's corners and background for details that do not need to be shared.
- **Delayed posting**: sharing an outing after you are home rather than in real time.
- **Close-friends list**: a smaller audience for posts, offered by many platforms.
- **Comment controls**: settings that limit who can comment and filter or hide unwanted comments.

- **Live location**: real-time sharing of where you are, through check-ins, stories, streams or location features.

Talk it through

1. What do you most enjoy about sharing range days or trips, and what would you lose if you stopped? What would you lose by waiting until you are home?
2. How do you think a club should handle photos of members, guests and children?
3. What is one detail in your own photos you had never noticed until this course?

Journal prompt

Write your personal delay rule for range-day and travel posts in one sentence. Then list what your frame check will look for before you share.

Glossary

- **Automatic updates**: a setting that installs software fixes without waiting for you to approve each one.
- **Close-friends list**: a smaller audience for posts, available on many platforms.
- **Credential manager**: the built-in tool on a phone or computer that stores passwords and passkeys and can sync them across your devices.
- **Data broker**: a company that collects information about people and sells or shares it.
- **Delayed posting**: sharing an outing after you are home rather than while you are there.
- **Digital footprint**: the trail of information about you online, from your own posts, other people's posts and records.
- **Doxing**: gathering someone's personal information and releasing it publicly to harm them.
- **Evidence keeper**: a supporter who saves records of harassment for someone who is targeted.
- **Frame check**: scanning a photo's corners and background before sharing.
- **Impersonation**: an account or message pretending to be someone else.
- **Location data**: information about where a device or photo was, sometimes attached invisibly to a photo file.
- **Multifactor authentication (MFA)**: signing in with two or more different kinds of evidence. Also called two-step verification or two-factor authentication.

- **Opt-out**: a request asking a site to stop showing or selling your information.
- **Passkey**: a sign-in method that uses your device's unlock (fingerprint, face or PIN) instead of a typed password.
- **Password manager**: a tool that creates, stores and fills in strong, unique passwords.
- **People-search site**: a data broker that sells reports about individuals to anyone who pays.
- **Phishing**: a message pretending to be from someone trusted, designed to get you to click, pay or share information.
- **Phishing-resistant**: a sign-in method that a fake website cannot trick you into handing over.
- **Pretexting**: inventing a believable role or reason to get information.
- **Privacy settings**: controls that decide who can see, share and comment on what you post.
- **Public record**: information held by government that is generally open to the public.
- **Smishing**: phishing by text message.
- **Social engineering**: manipulating people, rather than technology, to get access or information.
- **Spoofing**: faking a sender's name, address or caller ID.
- **Stalkerware**: software secretly installed on a device to monitor its owner.
- **Takedown request**: a request to a platform or website to remove content under its rules.
- **Vishing**: phishing by voice call.

Where to go next

Finding qualified, hands-on help

Reading is a start. Hands-on help makes settings stick.

- **Your device maker and mobile carrier** offer official help pages and in-store or phone support for setting up screen locks, backups, passkeys and account protections. Use the support contacts on their official websites.
- **Public libraries and community centers** often run free digital skills sessions where a person can sit with you while you change settings.
- **CISA's Cyber Volunteer Resource Center**, linked from its High-Risk Communities page, lists volunteer cybersecurity clinics and how to request help.
- **Victim advocates** can help with safety planning when online harassment, stalking or monitoring is involved. Start with the National Domestic Violence Hotline: 1-800-799-7233, chat at thehotline.org, or text START to 88788.
- **For legal questions**, such as protective orders or rules about records where you live, contact a qualified legal professional or your local legal aid organization. Laws vary; check the official source for your jurisdiction.

Official resources

- CISA Secure Our World: https://www.cisa.gov/secure-our-world
- FTC phishing advice: https://consumer.ftc.gov/articles/how-recognize-and-avoid-phishing-scams

- Report scams to the FTC: https://reportfraud.ftc.gov
- Identity theft recovery: https://www.identitytheft.gov
- FTC on people-search sites: https://consumer.ftc.gov/articles/what-know-about-people-search-sites-sell-your-information
- FTC on stalkerware: https://consumer.ftc.gov/articles/stalkerware-what-know
- FBI Internet Crime Complaint Center: https://www.ic3.gov
- NIST on multifactor authentication: https://www.nist.gov/itl/applied-cybersecurity/tig/back-basics-multi-factor-authentication
- UK National Cyber Security Centre on passkeys: https://www.ncsc.gov.uk/passkeys
- Forward phishing emails to reportphishing@apwg.org and phishing texts to 7726.

Related topics

- Joining communities with confidence.
- Secure storage at home: the storage side of what you own.
- Stepping away from provocations, online and off.
- Helping without making things worse: steady, safe choices when someone needs help.
- Range etiquette, including respect for other members.

Sources

All sources below were re-read on 2026-10-15. Statements in this book that rely on a source name it in the text.

Cited in the course lessons

- CISA — Secure Our World. https://www.cisa.gov/secure-our-world (checked 2026-10-15)
- NIST — Back to basics: Multi-factor authentication (MFA). https://www.nist.gov/itl/applied-cybersecurity/tig/back-basics-multi-factor-authentication (checked 2026-10-15)
- UK National Cyber Security Centre — Passkeys: what you need to know. https://www.ncsc.gov.uk/passkeys (checked 2026-10-15)
- FTC Consumer Advice — How To Recognize and Avoid Phishing Scams. https://consumer.ftc.gov/articles/how-recognize-and-avoid-phishing-scams (checked 2026-10-15)
- FTC Consumer Advice — What To Know About People Search Sites That Sell Your Information. https://consumer.ftc.gov/articles/what-know-about-people-search-sites-sell-your-information (checked 2026-10-15)
- DHS Office of Partnership and Engagement — Resources for Individuals on the Threat of Doxing (January 16, 2024). https://www.dhs.gov/sites/default/files/2024-01/24_0117_ope_resources-for-individuals-on-the-threat-of-doxing-508.pdf (checked 2026-10-15)
- FTC Consumer Advice — Stalkerware: What To Know. https://consumer.ftc.gov/articles/stalkerware-what-know (checked 2026-10-15)

- FTC — Living Life Online. https://consumer.ftc.gov/sites/default/files/articles/pdf/pdf-0006-living-life-online_0.pdf (checked 2026-10-15)

Additional background used in this book

- CISA — Secure Our World: Use Strong Passwords. https://www.cisa.gov/secure-our-world/use-strong-passwords (checked 2026-10-15)
- CISA — Secure Our World: Turn On MFA. https://www.cisa.gov/secure-our-world/turn-mfa (checked 2026-10-15)
- CISA — Secure Our World: Update Software. https://www.cisa.gov/secure-our-world/update-software (checked 2026-10-15)
- CISA — Secure Our World: Recognize and Report Phishing. https://www.cisa.gov/secure-our-world/recognize-and-report-phishing (checked 2026-10-15)
- CISA — More than a Password. https://www.cisa.gov/MFA (checked 2026-10-15)
- CISA — Avoiding Social Engineering and Phishing Attacks. https://www.cisa.gov/news-events/news/avoiding-social-engineering-and-phishing-attacks (checked 2026-10-15)
- CISA — Staying Safe on Social Networking Sites. https://www.cisa.gov/news-events/news/staying-safe-social-networking-sites (checked 2026-10-15)
- CISA — High-Risk Communities. https://www.cisa.gov/audiences/high-risk-communities (checked 2026-10-15)
- NIST SP 800-63B-4 — Digital Identity Guidelines: Authentication and Authenticator Management. https://pages.nist.gov/800-63-4/sp800-63b.html (checked 2026-10-15)

• FIDO Alliance — Passkeys. https://fidoalliance.org/passkeys/ (checked 2026-10-15)

RivalShot Academy · Original course book, authored 2026-10-15.

Educational material only. Completing this course is an educational record, not a licence, qualification or certification. Laws and requirements vary by place; check the official source for your jurisdiction. For hands-on skills, find qualified, certified instruction.

Typeset in Space Grotesk and DM Sans (SIL Open Font License 1.1). The RS mark is the original RivalShot identity.