Edition: Sections 1–3

PREMIUM



GO INCOGNITO V2

Key Terms

Every term the course leans on, in plain English. Keep it open while you watch, and come back whenever a word slips.

SECTIONS

1 **Foundations** — 22 terms

2 **Your digital identity** — 37 terms

3 **Accounts & authentication** — 48 terms

4 **Browsing & online safety** — Coming soon

5 **Devices & files** — Coming soon

6 **Advanced digital protection** — Coming soon

7 **Networking & hardware** — Coming soon

8 **Lifestyle & advocacy** — Coming soon

9 **Conclusion** — Coming soon

SECTION 1 · INDEX

Foundations

22 terms across 5 lessons · click any entry to jump to it

BY LESSON

1.2	Why should you care?	p. 2
1.3	Privacy vs. security vs. anonymity	p. 3
1.4	Understanding FOSS	p. 3
1.5	Metadata: the invisible trail	p. 5
1.6	Building a threat model	p. 5

A–Z

A	Adversary	1.6	5
	Anonymity	1.3	3
	App store	1.4	3
	Audit	1.4	3
B	Backdoor	1.4	4
D	Data broker	1.2	2
	Digital sovereignty	1.2	2
E	Encryption	1.3	3
	End-to-end encryption (E2EE)	1.3	3
	EXIF data	1.5	5
F	F-Droid	1.4	4
	FOSS	1.4	4
	Fork	1.4	4
M	Metadata	1.5	5
O	Open source	1.4	4
P	Privacy	1.3	3
	Proprietary software	1.4	4
S	Security	1.3	3
	Sideloading	1.4	4
	Surveillance capitalism	1.2	2
T	Threat model	1.6	5
	Turnkey totalitarianism	1.2	2

SECTION 1

Foundations

22 terms · 5 lessons · alphabetical within each lesson

1.2 Why should you care? 4 terms

Data broker

Data brokers compile your name, address, relatives, income estimate, and more into a file, then sell it. A company you've probably never interacted with that may know more about you than the apps you use every day.

Digital sovereignty

The idea that people, communities, and nations should have real control over their own data, instead of a handful of companies.

Surveillance capitalism

When a service is free, you're usually the product. Every search, video, and place your phone records builds a profile that gets sold, rented, and used to influence your decisions. Your behavior is the raw material. The term was coined by Shoshana Zuboff.

Turnkey totalitarianism

Surveillance built in one political moment doesn't disappear when governments change, but gets inherited. Data collected about you today could be used in a future political climate nobody can predict.

1.3 Privacy vs. security vs. anonymity — 5 terms

Anonymity
Unlinking your identity from your actions. It answers the question, "Can this be traced back to me?" The action is real, but the connection to you isn't.

Encryption
Converting readable information into scrambled data that can only be turned back with the right key. Without that key, it's unreadable.

End-to-end encryption
E2EE
Encryption where only you and the person you're talking to can read your messages. Not even the app carrying them can see what you said.

Privacy
Control over your own information. It answers the question, "Who knows what about me, and did I choose that?" Privacy is sharing your medical history with your doctor but not your employer.

Security
Protecting data from unauthorized access. It answers the question, "Can the wrong people get to this?" The vault can be locked, but the people with the keys can still see everything inside.

1.4 Understanding FOSS — 9 terms

App store
The official storefront for installing apps on your device, like Apple's App Store or Google Play. It's convenient, but it's also a gatekeeper. Controlled stores can decide which apps you can get, and governments can pressure companies to remove them.

Audit
An independent review of software by outside security experts. They look for vulnerabilities and check that the software actually does what it says.

1.4 Understanding FOSS (continued)

Backdoor	A weakness deliberately built into software that lets someone bypass its security entirely. In closed software, a backdoor can be hidden without you ever knowing.
F-Droid	An independent Android app store that only carries free and open source apps and runs outside of Google's control. It's smaller than the Play Store, but much harder to pressure, and it lets you add other app repositories
FOSS Free and open source software	Free as in freedom, not just price. It's the freedom to use software for any purpose, study how it works, change it, and share it. There's even paid FOSS.
Fork	Taking a copy of an open source project and carrying it forward under a new name. It's how communities keep a project alive when the original gets abandoned or acquired by someone they don't trust.
Open source	When the source code, the human-readable instructions behind an app, is public. Anyone with the know-how can read it and check that the app does what it claims.
Proprietary software	Software where the code is hidden. You can use it, but you can't see exactly what it's doing, so you're mostly taking the company's word for it.
Sideloading	Installing an app directly from its source instead of from an official app store. The term often gets used to make it sound risky, but it just typically means getting software without going through a big tech company.

1.5 Metadata: the invisible trail

2 terms

EXIF data

Metadata hidden inside your photos. It can include where the photo was taken, what device took it, and exactly when.

Metadata

Data about data. It isn't what you said. It's who you talked to, when, for how long, and from where. Context can reveal as much as content.

1.6 Building a threat model

2 terms

Adversary

Whoever might want what you're protecting. That could be a data broker, a scammer, an abusive ex, or in rare cases a government. Knowing your adversary tells you how much protection actually makes sense.

Threat model

Your personal game plan for privacy. Instead of asking "How private can I be?", it asks "What do I need to protect, from whom, and how much does it matter if I fail?"

SECTION 2 · INDEX

Your digital identity

37 terms across 5 lessons · click any entry to jump to it

BY LESSON

2.1	Section 2 introduction	p. 8
2.2	Digital minimalism	p. 8
2.3	Cleaning up your local identity	p. 9
2.4	Cleaning up your online identity	p. 11
2.5	Data brokers & people-search removal	p. 12

A–Z

A	App Privacy Report	2.3	9
	App store privacy labels	2.3	9
	Attack surface	2.2	8
	Automated removal service	2.5	12
B	Background check	2.5	12
	BitLocker	2.3	9
	Browser cache	2.3	9
C	California DROP	2.5	12
	CCPA	2.4	11
	Cookies	2.3	9
	Credential stuffing	2.4	11
	Credit freeze	2.4	11
D	Data breach	2.2	8
	Data deletion request	2.4	11
	Data relationship	2.2	8
	DBAN	2.3	10
	Digital footprint	2.1	8
	Digital minimalism	2.2	9
F	Factory reset	2.3	10
	FileVault	2.3	10
	Full-disk encryption	2.3	10
G	GDPR	2.4	11
H	Hard disk drive (HDD)	2.3	10
	Have I Been Pwned	2.4	11

A–Z (CONTINUED)

J	JustDeleteMe	2.4	12
L	LUKS	2.3	10
O	Opt-out	2.5	13
P	Password hash	2.4	12
	Password reuse	2.2	9
	People-search site	2.5	13
	Public records	2.5	13
S	Solid-state drive (SSD)	2.3	10
	Suppression	2.5	13
T	ToS;DR	2.3	10
V	VeraCrypt	2.3	11
W	Warrantless data purchase	2.5	13
Z	Zombie account	2.4	12

SECTION 2

Your digital identity

37 terms · 5 lessons · alphabetical within each lesson

2.1 Section 2 introduction — 1 term

Digital footprint
Everything you've left behind online and on your devices over the years: accounts, files, app data, and the profiles other companies built from it. Some of it you created on purpose, a lot of it you've forgotten about.

2.2 Digital minimalism — 5 terms

Attack surface
Every point where your data could be exposed. Each app, account, and service adds to it. The smaller your attack surface, the fewer places things can go wrong.

Data breach
When data a company holds gets accessed or stolen by someone who shouldn't have it. Once it's out, it usually gets copied, shared, and sold, and it can't be pulled back.

Data relationship
The exchange that starts the moment you create an account or install an app. You hand over your email, name, and usage patterns, and you get access to something in return. If you stop using the service, the relationship doesn't automatically end on their side.

2.2 Digital minimalism (continued)

Digital minimalism	Being intentional about which apps, accounts, and services earn a place in your life. The goal isn't owning as little as possible; it's choosing the relationships that work for you instead of collecting them by default.
Password reuse	Using the same password on more than one account. It means one breach can unlock every other account that shares that password.

2.3 Cleaning up your local identity 14 terms

App Privacy Report	A built-in iOS feature that shows which apps accessed your camera, microphone, location, and contacts, and which domains they contacted in the background.
App store privacy labels	The summaries in the App Store and Google Play showing what data an app collects and whether it's linked to you. They're a useful first filter, but generally self-reported by developers.
BitLocker	Windows' built-in full-disk encryption tool.
Browser cache	Copies of pages, images, and files your browser saves so sites load faster next time. It also quietly records where you've been.
Cookies	Small files websites store in your browser. Some keep you logged in or remember your settings. Others are tracking identifiers that follow you across sites.

2.3 Cleaning up your local identity (continued)

DBAN Darik's Boot and Nuke	A free tool that overwrites an entire traditional hard drive so old data can't be recovered.
Factory reset	Restoring a device to its original settings. On its own, it may only remove the pointers to your data. Combined with full-disk encryption, it typically makes the data unreadable.
FileVault	macOS's built-in full-disk encryption.
Full-disk encryption	Encrypting everything on a device's storage so it's unreadable without your password or key. It also makes selling or disposing of a device far simpler since a reset destroys the key.
Hard disk drive HDD	A traditional storage drive with spinning platters. Data stays put until it's physically overwritten, which is why overwriting the whole drive works well here.
LUKS	The standard full-disk encryption on Linux, usually set up when you install the operating system.
Solid-state drive SSD	The faster storage in many modern computers and phones. It manages data in ways that make overwriting individual files unreliable, so encryption followed by a reset is the way to wipe it.
ToS;DR Terms of Service; Didn't Read	A free site that grades popular services from A to E and summarizes the key clauses of their terms in plain English. It's a fast way to spot red flags before reading the full policy.

2.3 Cleaning up your local identity (continued)

VeraCrypt
A free, open source encryption tool, commonly used on Windows or Linux as an alternative to BitLocker and LUKS respectively.

2.4 Cleaning up your online identity 9 terms

CCPA
The California Consumer Privacy Act. Among other things, it gives California residents the right to request that companies delete their personal data.

Credential stuffing
An automated attack that takes email and password pairs from a breach and tries them on hundreds of other sites. It's the main reason reusing passwords is so risky.

Credit freeze
Locking your credit file so nobody can open new credit in your name, even with your stolen details. In regions that offer it, it's one of the best protections against fallout from data breaches.

Data deletion request
A formal request asking a company to delete what it holds about you. Under laws like GDPR and CCPA, many companies have to respond within a set time, even if they don't offer a delete button.

GDPR
The General Data Protection Regulation, the EU and UK data protection law. It gives you the right to ask companies what they hold about you and to have it deleted.

Have I Been Pwned
A free service run by security researcher Troy Hunt. It checks whether your email address appeared in known public breaches, and it can notify you about future ones.

2.4 Cleaning up your online identity (continued)

JustDeleteMe
A free, open source directory of direct links to account deletion pages for hundreds of services. Each one is color-coded by how hard deletion is, from easy to impossible.

Password hash
A scrambled version of a password that sites store instead of the password itself. Weak or poorly protected hashes can often be cracked back into the real password.

Zombie account
An account you created, stopped using, and forgot about, but which still exists and still holds your data.

2.5 Data brokers & people-search removal 8 terms

Automated removal service
A company that submits opt-out requests to data brokers on your behalf, usually for a fee. Results vary between services, so it's worth looking into which one you pick.

Background check
A report on someone's history, often pulled from data broker profiles. Employers, landlords, and tenant screening services use them, and they sometimes include information that shouldn't legally factor into a decision.

California DROP
California's free Delete Request and Opt-out Platform, run by the state's privacy agency, CalPrivacy. It lets California residents send one deletion request to every registered data broker at once.

2.5 Data brokers & people-search removal (continued)

Opt-out	Asking a data broker or people-search site to remove or hide your listing. Opt-outs often need repeating, because brokers keep pulling in fresh data.
People-search site	A website where anyone can type in a name and city and find someone's address, phone number, relatives, and more, often with no account or verification. Spokeo, Whitepages, and BeenVerified are common examples.
Public records	Government records anyone can access, like property records, court filings, and voter registrations. Data brokers index them, and opt-outs don't remove anything from the records themselves.
Suppression	A request that stops a people-search site from showing your record in search results. On some sites, like those owned by PeopleConnect, it's a separate option from deletion and the one that actually hides your listing.
Warrantless data purchase	When government agencies buy data, such as location history, from data brokers instead of getting a warrant. It's legal in many cases precisely because the data is sold commercially.

SECTION 3 · INDEX

Accounts & authentication

48 terms across 6 lessons · click any entry to jump to it

BY LESSON

3.1	Section 3 introduction	p. 16
3.2	Passwords	p. 16
3.3	Two-factor authentication	p. 18
3.4	Passkeys & passwordless authentication	p. 19
3.5	Safe communication	p. 21
3.6	Aliasing	p. 22

A–Z

A	Advanced Data Protection	3.5	21
	Aliasing	3.6	22
	Authentication	3.1	16
B	Backup codes	3.3	18
	Breach aggregation	3.6	23
	Brute-force attack	3.2	16
C	Ciphertext	3.5	21
	Credentials	3.1	16
	Custom domain	3.6	23
E	Email alias	3.6	23
	Emergency access	3.2	16
F	Federation	3.5	21
	FIDO2	3.4	19
H	Hardware security key	3.3	18
	Hide My Email	3.6	23
K	KeePass	3.2	17
	Keylogger	3.2	17
L	Local password manager	3.2	17
M	Master password	3.2	17
O	One-time password (OTP)	3.3	18
	Onion routing	3.5	21
P	Passkey	3.4	20

A–Z (CONTINUED)

P	Passphrase	3.2	17
	Password manager	3.2	17
	Perfect forward secrecy	3.5	21
	PGP	3.5	21
	Phishing	3.3	18
	Phishing-resistant	3.4	20
	Post-quantum encryption	3.5	21
	Private key	3.4	20
	Private mailbox (PMB)	3.6	23
	Public key	3.4	20
	Public-key cryptography	3.4	20
R	RCS	3.5	22
	Real-time phishing (relay) attack	3.3	18
S	Seed phrase	3.5	22
	Shared secret	3.4	20
	Signal Protocol	3.5	22
	SIM swap	3.3	18
	SS7	3.3	19
T	TOTP	3.3	19
	TOTP seed	3.3	19
	Two-factor authentication (2FA)	3.3	19
V	Vault	3.2	17
	Virtual card	3.6	23
	VoIP number	3.3	19
W	Warrant	3.5	22
	WebAuthn	3.4	20

SECTION 3

Accounts & authentication

48 terms · 6 lessons · alphabetical within each lesson

1 2 3 4 5 6 7 8 9

3.1 Section 3 introduction — 2 terms

Authentication
Proving who are when you log in. Passwords, 2FA codes, security keys, and passkeys are all ways to authenticate.

Credentials
The information you use to prove your identity to a service, like a username and password. Whoever holds your credentials can usually get into your account.

3.2 Passwords — 9 terms

Brute-force attack
When an attacker guesses your password by trying countless combinations until one works. Long, random passwords make this impractical, while short or common ones can fall in hours.

Emergency access
A password manager feature that lets a trusted person request access to your vault if something happens to you. You set a waiting period so you can deny the request if you're still around.

3.2 Passwords (continued)

KeePass	An open source password manager format that stores your vault as an encrypted file on your own device instead of a company's server. There are many compatible apps across platforms, but you handle syncing and backups yourself.
Keylogger	Malware that secretly records what you type, including passwords. A keylogger is how attackers captured a LastPass engineer's master password in 2022.
Local password manager	A password manager that keeps your vault only on your own devices, with no company holding a copy. You get more control and a smaller attack surface, but you become the sync, backup, and recovery system.
Master password	The one password that unlocks your password manager. It should be long, unique, and used nowhere else since it protects everything inside your vault.
Passphrase	A password made of several words strung together like a short sentence. Passphrases are long and strong but much easier to remember than random characters, which makes them great for master passwords. For example: *copper-violin-harbor-tulip-sunrise*.
Password manager	An app that generates strong, unique passwords and stores them in an encrypted vault. You remember one master password, and it handles the rest.
Vault	The encrypted storage inside a password manager that holds your passwords and other sensitive information. It's unreadable without your master password or key.

3.3 Two-factor authentication

11 terms

Backup codes	One-time codes a service gives you when you enable 2FA, for getting back in if you lose your authenticator or security key. Store them somewhere safe, like printed or in a separate backup vault.
Hardware security key	A small physical device you plug in or tap to log in like a YubiKey. It's the strongest 2FA option because it won't authenticate on a fake website. Always use more than one.
One-time password (OTP)	A code that works for a single login and then expires. OTPs can arrive by text, by email, or be generated by an app.
Phishing	Tricking someone into handing over their login details or codes, usually with a fake website, email, or text that looks legitimate.
Real-time phishing (relay) attack	A phishing attack where a fake site passes your password and 2FA code to the real site the moment you type them in. TOTP codes can be stolen this way, but hardware keys and passkeys can't.
SIM swap	An attack where someone convinces your mobile carrier to move your phone number to a SIM card they control. They then receive your texts, including SMS login codes.

3.3 Two-factor authentication (continued)

SS7
Signaling System No. 7

The decades-old system phone carriers use to route calls and texts between networks. Weaknesses in SS7 let attackers intercept text messages, which is how SMS codes were stolen in the 2018 Reddit breach.

TOTP
Time-based one-time password

A six-digit code generated by an app on your device that changes every 30 seconds. It's created locally, so there's nothing for your carrier or email to leak.

TOTP seed

The secret you scan as a QR code or type in when setting up TOTP. Your app uses it to generate every future code, so anyone with the seed can generate your codes too. Keep a backup somewhere safe.

Two-factor authentication (2FA)

Requiring a second step after your password, like a code or a security key. Even if someone steals your password, they can't get in without that second factor.

VoIP number

A phone number that runs over the internet instead of through a traditional carrier SIM, like Google Voice or MySudo. Useful for keeping your real number private, though some banks and services reject them. Also bypasses some cellular infrastructure.

3.4 Passkeys & passwordless authentication 8 terms

FIDO2

The open standard behind hardware security keys and passkeys developed by the FIDO Alliance. It uses public-key cryptography and ties each login to the real website, which makes it phishing-resistant.

3.4 Passkeys & passwordless authentication (continued)

Passkey	A login method that replaces your password with a cryptographic key stored on your device or in your password manager, unlocked with your face, fingerprint, or PIN. Passkeys can't be phished or leaked from a server.
Phishing-resistant	Authentication that can't be used on a fake website even if you're tricked into trying. Hardware keys and passkeys are phishing-resistant because each login is tied to the real site's address.
Private key	The secret half of a cryptographic key pair, which never leaves your device. It signs your logins, so keeping it private is what keeps you secure.
Public key	The shareable half of a cryptographic key pair. A service stores your public key to check your logins, and it's useless to an attacker on its own.
Public-key cryptography Also called asymmetric cryptography	Encryption that uses a matching pair of keys: a public key you can share and a private key you keep. It's the foundation of passkeys, hardware keys, and end-to-end encrypted messaging.
Shared secret	Information that both you and a service know, like a password or the seed behind a TOTP code. Because the service also holds it, a shared secret can be stolen, guessed, or phished.
WebAuthn Web Authentication	The part of the FIDO2 standard that lets websites and browsers use passkeys and hardware security keys.

3.5 Safe communication

11 terms

Advanced Data Protection

An optional Apple setting that end-to-end encrypts most of your iCloud data, including iMessage backups. Without it, Apple can access those backups.

Ciphertext

Encrypted data that looks like scrambled nonsense without the key. With end-to-end encryption, ciphertext is all the messaging company ever sees.

Federation

A setup where independently run servers can talk to each other, the way email works across different providers. Matrix uses federation so no single company controls the network.

Onion routing

Sending data through several relays, each wrapped in its own layer of encryption, so no single relay knows both who sent it and where it's going. Tor and Session use onion routing.

Perfect forward secrecy

A design where each conversation uses fresh, temporary encryption keys. Even if a key is stolen later, past messages can't be decrypted with it.

PGP

Pretty Good Privacy

A standard for encrypting email between any providers using public and private keys. Powerful, but managing keys yourself makes it for many people an advanced workflow.

Post-quantum encryption

Encryption designed to hold up against future quantum computers, which could break some of today's methods. Messaging apps are adding it now to protect messages that are being collected today.

3.5 Safe communication (continued)

RCS
Rich Communication Services

The modern replacement for SMS, with typing indicators, read receipts, and better media. Google Messages encrypts RCS chats between Android users, and at the time of this writing RCS with E2EE is in beta on iOS.

Seed phrase

A list of words that acts as the master key to an account, used by apps like Session to restore your identity. Anyone with your seed phrase can take over the account, so store it safely.

Signal Protocol

The end-to-end encryption protocol created for the Signal app. It's widely considered the strongest available for messaging and calls, and other apps use it too.

Warrant

A court order that lets law enforcement search or seize something, including data held by a company. If a platform can read your messages, a warrant can compel it to hand them over.

3.6 Aliasing 7 terms

Aliasing

Giving each service a unique, disposable identifier, like an email address, phone number, or card number instead of your real one. If one leaks, you disable it and nothing else is affected.

3.6 Aliasing (continued)

Breach aggregation	Combining data from many separate breaches into one dataset, cross-referenced by things like your email address. Aggregation can reveal far more about you than any single breach, as we saw with the 26-billion-record Mother of All Breaches.
Custom domain	A domain you own, like yourname.com, that can be used for email and aliases. It's portable and under your control, but every alias shares it, which can tie your accounts together.
Email alias	A forwarding address you give a service instead of your real email. Messages forward to your inbox, replies come from the alias, and your real address stays private.
Hide My Email	Apple's built-in email aliasing feature, included with iCloud+. Its aliases use the same domain as regular iCloud addresses, so services rarely reject them.
Private mailbox (PMB)	A real street address that receives your mail and packages without revealing where you live. Use it anywhere a service asks for an address.
Virtual card	A unique card number linked to your real account that you can lock to one merchant, cap, or delete anytime. If a merchant is breached, only that virtual number is exposed.

SECTION 4 **Browsing & online safety** Added with the next section