

FLASH CARDS

Navigating the “Dark Web”

Terminology and quiz cards for the Take Back Your Bytes lesson on Tor, I2P, VPNs and private networks, for readers 18 years of age or older.

What is in this set

40 cards: **24 term cards** (term on the front, definition on the back) and **16 quiz cards** (question on the front, answer on the back). Bracketed numbers on the backs, like [1], match the reference list on the last page and in the instructor guide.

How to print

1. Print double-sided on US Letter at 100% scale (no “fit to page”).
2. Choose **flip on the long edge**. The backs are arranged so each answer lands behind its card.
3. Cut along the dashed lines. Each card is 3.75 by 2.5 inches.

How to use them

- **Self-test:** read the front, answer aloud, flip to check.
- **Pairs:** one reads the front, the other answers. Swap every five cards.
- **Boxes:** keep a “missed” pile and a “got it” pile. Re-test the missed pile after a break, then again the next day.
- **Warm-up:** deal a few quiz cards at the start of the next session.

Facts checked October 27, 2026. Tools and models change quickly, so confirm details against the current documentation. These materials are dedicated to the public domain under CC0 1.0 and shared for the public good. The PrivacySafe and PrivacySafe Foundation names and logos are trademarks and are not included in that dedication.

TERM

1 / 40

Surface web

Say it in your own words, then flip.

Navigating the "Dark Web"

PrivacySafe Foundation | CC0 1.0

TERM

2 / 40

Deep web

Say it in your own words, then flip.

Navigating the "Dark Web"

PrivacySafe Foundation | CC0 1.0

TERM

3 / 40

Dark web

Say it in your own words, then flip.

Navigating the "Dark Web"

PrivacySafe Foundation | CC0 1.0

TERM

4 / 40

Cleartnet

Say it in your own words, then flip.

Navigating the "Dark Web"

PrivacySafe Foundation | CC0 1.0

TERM

5 / 40

Onion routing

Say it in your own words, then flip.

Navigating the "Dark Web"

PrivacySafe Foundation | CC0 1.0

TERM

6 / 40

Tor

Say it in your own words, then flip.

Navigating the "Dark Web"

PrivacySafe Foundation | CC0 1.0

TERM

7 / 40

Tor Browser

Say it in your own words, then flip.

Navigating the "Dark Web"

PrivacySafe Foundation | CC0 1.0

TERM

8 / 40

Relay

Say it in your own words, then flip.

Navigating the "Dark Web"

PrivacySafe Foundation | CC0 1.0

TERM

2 / 40

Pages behind a login or not indexed, such as email, banking and cloud files. Most of the web.

[General](#)

Navigating the "Dark Web"

PrivacySafe Foundation | CC0 1.0

TERM

1 / 40

Web pages that search engines index and anyone can open.

[General](#)

Navigating the "Dark Web"

PrivacySafe Foundation | CC0 1.0

TERM

4 / 40

The ordinary internet you reach without special software.

[General](#)

Navigating the "Dark Web"

PrivacySafe Foundation | CC0 1.0

TERM

3 / 40

A loose label for sites reachable only with special software, such as Tor and I2P. The name sounds sinister but the technology is neutral.

[\[1\]](#) [\[5\]](#)

Navigating the "Dark Web"

PrivacySafe Foundation | CC0 1.0

TERM

6 / 40

A network of volunteer relays that uses onion routing. Maintained by the Tor Project, a nonprofit.

[\[2\]](#)

Navigating the "Dark Web"

PrivacySafe Foundation | CC0 1.0

TERM

5 / 40

Wrapping data in layers of encryption, one per relay, so each relay learns only its neighbors.

[\[1\]](#) [\[3\]](#)

Navigating the "Dark Web"

PrivacySafe Foundation | CC0 1.0

TERM

8 / 40

A computer run by a volunteer that passes Tor traffic along.

[\[1\]](#) [\[3\]](#)

Navigating the "Dark Web"

PrivacySafe Foundation | CC0 1.0

TERM

7 / 40

The Tor Project's browser, built to use Tor and to limit tracking.

[\[3\]](#)

Navigating the "Dark Web"

PrivacySafe Foundation | CC0 1.0

TERM

9 / 40

Circuit

Say it in your own words, then flip.

Navigating the "Dark Web"

PrivacySafe Foundation | CC0 1.0

TERM

10 / 40

Entry relay

Say it in your own words, then flip.

Navigating the "Dark Web"

PrivacySafe Foundation | CC0 1.0

TERM

11 / 40

Exit relay

Say it in your own words, then flip.

Navigating the "Dark Web"

PrivacySafe Foundation | CC0 1.0

TERM

12 / 40

Onion service

Say it in your own words, then flip.

Navigating the "Dark Web"

PrivacySafe Foundation | CC0 1.0

TERM

13 / 40

Rendezvous point

Say it in your own words, then flip.

Navigating the "Dark Web"

PrivacySafe Foundation | CC0 1.0

TERM

14 / 40

I2P

Say it in your own words, then flip.

Navigating the "Dark Web"

PrivacySafe Foundation | CC0 1.0

TERM

15 / 40

Eepsite

Say it in your own words, then flip.

Navigating the "Dark Web"

PrivacySafe Foundation | CC0 1.0

TERM

16 / 40

Garlic routing

Say it in your own words, then flip.

Navigating the "Dark Web"

PrivacySafe Foundation | CC0 1.0

TERM

10 / 40

The first relay in a circuit. It knows your address but not your destination.

[\[3\]](#)

Navigating the "Dark Web"

PrivacySafe Foundation | CC0 1.0

TERM

9 / 40

The path of relays your Tor connection uses.

[\[3\]](#)

Navigating the "Dark Web"

PrivacySafe Foundation | CC0 1.0

TERM

12 / 40

A service reachable only over Tor, at a .onion address. Both ends stay hidden.

[\[1\]](#)

Navigating the "Dark Web"

PrivacySafe Foundation | CC0 1.0

TERM

11 / 40

The last relay in a circuit. It knows the site but not who you are, and can read traffic that lacks HTTPS.

[\[3\]](#)

Navigating the "Dark Web"

PrivacySafe Foundation | CC0 1.0

TERM

14 / 40

The Invisible Internet Project: a separate network where each user's router relays traffic through one-way tunnels.

[\[5\]](#)

Navigating the "Dark Web"

PrivacySafe Foundation | CC0 1.0

TERM

13 / 40

A relay where you and an onion service meet. It joins two circuits and cannot read the traffic.

[\[1\]](#)

Navigating the "Dark Web"

PrivacySafe Foundation | CC0 1.0

TERM

16 / 40

I2P's layered encryption, which also bundles several messages together.

[\[5\]](#)

Navigating the "Dark Web"

PrivacySafe Foundation | CC0 1.0

TERM

15 / 40

A website hosted inside I2P, with a .i2p address.

[\[5\]](#)

Navigating the "Dark Web"

PrivacySafe Foundation | CC0 1.0

TERM

17 / 40

Tunnel

Say it in your own words, then flip.

Navigating the "Dark Web"

PrivacySafe Foundation | CC0 1.0

TERM

19 / 40

Anonymity

Say it in your own words, then flip.

Navigating the "Dark Web"

PrivacySafe Foundation | CC0 1.0

TERM

21 / 40

End-to-end encryption

Say it in your own words, then flip.

Navigating the "Dark Web"

PrivacySafe Foundation | CC0 1.0

TERM

23 / 40

SecureDrop

Say it in your own words, then flip.

Navigating the "Dark Web"

PrivacySafe Foundation | CC0 1.0

TERM

18 / 40

VPN

Say it in your own words, then flip.

Navigating the "Dark Web"

PrivacySafe Foundation | CC0 1.0

TERM

20 / 40

HTTPS

Say it in your own words, then flip.

Navigating the "Dark Web"

PrivacySafe Foundation | CC0 1.0

TERM

22 / 40

Metadata

Say it in your own words, then flip.

Navigating the "Dark Web"

PrivacySafe Foundation | CC0 1.0

TERM

24 / 40

Censorship

Say it in your own words, then flip.

Navigating the "Dark Web"

PrivacySafe Foundation | CC0 1.0

TERM

18 / 40

A service that sends your traffic through one company's servers. That company sees your address and destinations.

[\[8\]](#)

Navigating the "Dark Web"

PrivacySafe Foundation | CC0 1.0

TERM

17 / 40

A one-way path through I2P routers. Messages leave through outbound tunnels and arrive through inbound ones.

[\[5\]](#)

Navigating the "Dark Web"

PrivacySafe Foundation | CC0 1.0

TERM

20 / 40

Encrypted web traffic. It hides content from the network, but not which site you visit.

[\[3\]](#)

Navigating the "Dark Web"

PrivacySafe Foundation | CC0 1.0

TERM

19 / 40

Not being identifiable. Tools help, but what you tell a site can still reveal you.

[\[3\]](#)

Navigating the "Dark Web"

PrivacySafe Foundation | CC0 1.0

TERM

22 / 40

Data about your traffic, such as who talks to whom and when, rather than what is said.

[General](#)

Navigating the "Dark Web"

PrivacySafe Foundation | CC0 1.0

TERM

21 / 40

Encryption so only the two ends can read the message. Onion services use it.

[\[1\]](#)

Navigating the "Dark Web"

PrivacySafe Foundation | CC0 1.0

TERM

24 / 40

Blocking people from information or expression. Private networks can help people get around it.

[\[10\]](#) [\[11\]](#)

Navigating the "Dark Web"

PrivacySafe Foundation | CC0 1.0

TERM

23 / 40

An open-source system that lets sources send tips to journalists, often through an onion service.

[\[7\]](#)

Navigating the "Dark Web"

PrivacySafe Foundation | CC0 1.0

QUIZ

25 / 40

What is the difference between the deep web and the dark web?

Navigating the "Dark Web"

PrivacySafe Foundation | CC0 1.0

QUIZ

26 / 40

Which relay in a Tor circuit knows both who you are and the site?

Navigating the "Dark Web"

PrivacySafe Foundation | CC0 1.0

QUIZ

27 / 40

Why does Tor use three relays?

Navigating the "Dark Web"

PrivacySafe Foundation | CC0 1.0

QUIZ

28 / 40

Why do you still want HTTPS with Tor?

Navigating the "Dark Web"

PrivacySafe Foundation | CC0 1.0

QUIZ

29 / 40

How is an onion service different from visiting a site over Tor?

Navigating the "Dark Web"

PrivacySafe Foundation | CC0 1.0

QUIZ

30 / 40

What does a rendezvous point do?

Navigating the "Dark Web"

PrivacySafe Foundation | CC0 1.0

QUIZ

31 / 40

Who sees what in a VPN connection?

Navigating the "Dark Web"

PrivacySafe Foundation | CC0 1.0

QUIZ

32 / 40

Why ask extra questions about a free VPN?

Navigating the "Dark Web"

PrivacySafe Foundation | CC0 1.0

QUIZ

26 / 40

None. The entry relay knows you, the exit relay knows the site, and the middle relay knows neither.

[\[1\]](#) [\[3\]](#)

Navigating the "Dark Web"

PrivacySafe Foundation | CC0 1.0

QUIZ

25 / 40

The deep web is anything not indexed or behind a login. The dark web needs special software such as Tor or I2P.

[\[1\]](#) [\[5\]](#)

Navigating the "Dark Web"

PrivacySafe Foundation | CC0 1.0

QUIZ

28 / 40

The exit relay can read traffic that the site does not protect.

[\[3\]](#)

Navigating the "Dark Web"

PrivacySafe Foundation | CC0 1.0

QUIZ

27 / 40

So no single relay can link a user to a destination.

[\[3\]](#)

Navigating the "Dark Web"

PrivacySafe Foundation | CC0 1.0

QUIZ

30 / 40

It joins your circuit to the service's circuit. It cannot read the traffic.

[\[1\]](#)

Navigating the "Dark Web"

PrivacySafe Foundation | CC0 1.0

QUIZ

29 / 40

Both ends stay hidden, six relays carry the connection, there is no exit relay, and traffic is encrypted end to end.

[\[1\]](#)

Navigating the "Dark Web"

PrivacySafe Foundation | CC0 1.0

QUIZ

32 / 40

Running servers costs money, so a free service has to pay for itself somehow, and some use advertising or user data.

[\[8\]](#) [\[9\]](#)

Navigating the "Dark Web"

PrivacySafe Foundation | CC0 1.0

QUIZ

31 / 40

Your provider sees only the VPN. The site sees the VPN's address. The VPN company sees both.

[\[8\]](#)

Navigating the "Dark Web"

PrivacySafe Foundation | CC0 1.0

QUIZ

33 / 40

Does a VPN make you anonymous?

Navigating the "Dark Web"

PrivacySafe Foundation | CC0 1.0

QUIZ

34 / 40

Name one difference between Tor and I2P.

Navigating the "Dark Web"

PrivacySafe Foundation | CC0 1.0

QUIZ

35 / 40

What is an eepsite?

Navigating the "Dark Web"

PrivacySafe Foundation | CC0 1.0

QUIZ

36 / 40

Why can logging in defeat anonymity?

Navigating the "Dark Web"

PrivacySafe Foundation | CC0 1.0

QUIZ

37 / 40

Where should you copy an onion address from?

Navigating the "Dark Web"

PrivacySafe Foundation | CC0 1.0

QUIZ

38 / 40

Why does anonymity matter for free expression?

Navigating the "Dark Web"

PrivacySafe Foundation | CC0 1.0

QUIZ

39 / 40

What should you do if you meet content that may not be legal and may be upsetting?

Navigating the "Dark Web"

PrivacySafe Foundation | CC0 1.0

QUIZ

40 / 40

Name one step from your safe-browsing plan.

Navigating the "Dark Web"

PrivacySafe Foundation | CC0 1.0

QUIZ

34 / 40

I2P routers each relay through one-way tunnels, there is no central directory, and its sites live inside the network.

[\[5\]](#)

Navigating the "Dark Web"

PrivacySafe Foundation | CC0 1.0

QUIZ

33 / 40

No. It moves trust to the VPN company, which sees your address and destinations.

[\[8\]](#)

Navigating the "Dark Web"

PrivacySafe Foundation | CC0 1.0

QUIZ

36 / 40

You tell the site who you are. No network can hide what you tell the site yourself.

[\[3\]](#)

Navigating the "Dark Web"

PrivacySafe Foundation | CC0 1.0

QUIZ

35 / 40

A website hosted inside I2P, with a .i2p address.

[\[5\]](#)

Navigating the "Dark Web"

PrivacySafe Foundation | CC0 1.0

QUIZ

38 / 40

It lets people seek and share information without fear, such as reporters, sources and activists.

[\[10\]](#) [\[11\]](#)

Navigating the "Dark Web"

PrivacySafe Foundation | CC0 1.0

QUIZ

37 / 40

The organization's own page, because look-alike addresses exist.

[\[4\]](#) [\[6\]](#)

Navigating the "Dark Web"

PrivacySafe Foundation | CC0 1.0

QUIZ

40 / 40

For example: get Tor Browser from the official site, keep it updated, use HTTPS, pay for a VPN you researched, know the local rules.

[General](#)

Navigating the "Dark Web"

PrivacySafe Foundation | CC0 1.0

QUIZ

39 / 40

Leave, do not download or share it, and report it. For child abuse material in the US, use the NCMEC CyberTipline.

[\[12\]](#)

Navigating the "Dark Web"

PrivacySafe Foundation | CC0 1.0

Reference list

Links were checked on October 27, 2026.

#	SOURCE	WHAT IT SUPPORTS
[1]	Tor Project, Onion Services overview https://community.torproject.org/onion-services/overview/	How onion services work: introduction points, rendezvous points, six relays in all, location hiding and end-to-end encryption.
[2]	Tor Project, About Tor and its history https://www.torproject.org/about/history/	Where onion routing came from and what the Tor Project is.
[3]	Tor Project, Tor Browser User Manual https://tb-manual.torproject.org/	How Tor Browser works, circuits, the advice not to add extensions, and how to stay safer.
[4]	Tor Project, Onion-Location https://community.torproject.org/onion-services/advanced/onion-location/	How a website advertises its onion address so Tor Browser can offer it.
[5]	I2P, Introduction https://geti2p.net/en/docs/how/intro	Routers, one-way tunnels, the internal network database and garlic wrapped messages.
[6]	Real-World Onion Sites, a list kept by Alec Muffett https://github.com/alecmuffett/real-world-onion-sites	A list of mainstream sites that also offer onion services. Licensed CC BY-SA. Entries are checked against each site's own announcement.
[7]	SecureDrop https://securedrop.org/	An open-source whistleblower submission system, and its directory of news organizations that run it.
[8]	EFF Surveillance Self-Defense, Choosing the VPN That's Right for You https://ssd.eff.org/module/choosing-vpn-thats-right-you	Plain-language advice on what a VPN does and does not do, and how to judge a provider.
[9]	Ikram, Vallina-Rodriguez, Seneviratne, Kaafar and Paxson, An Analysis of the Privacy and Security Risks of Android VPN Permission-enabled Apps (2016) https://doi.org/10.1145/2987443.2987471	A study of 283 Android VPN apps. About three quarters used third-party tracking libraries. It is a 2016 study of one platform.
[10]	United Nations, Universal Declaration of Human Rights, Article 19 https://www.un.org/en/about-us/universal-declaration-of-human-rights	The right to freedom of opinion and expression, including the freedom to seek, receive and impart information.
[11]	UN Special Rapporteur on freedom of expression, report on encryption, anonymity and human rights (A/HRC/29/32, 2015) https://www.ohchr.org/en/documents/thematic-reports/ahrc2932-report-encryption-anonymity-and-human-rights-framework	How encryption and anonymity support freedom of opinion and expression.
[12]	National Center for Missing and Exploited Children, CyberTipline https://report.cybertip.org/	Where US readers can report child sexual abuse material. Readers elsewhere should use their own national hotline or law enforcement.
[13]	PrivacySafe Search https://privacysafe.is	A privacy-respecting search service run by PrivacySafe Foundation.
[14]	PrivacySafe Bot https://privacysafe.bot	A password and passphrase generator that runs in your browser, run by PrivacySafe Foundation. Its page declares an onion address.
[15]	PrivacySafe, 3NWeb architecture https://github.com/PrivacySafe/3NWeb-architecture	Notes that hiding IP addresses can be done with VPNs, Tor and mixnets by reusing existing transport layers.
[16]	PrivacySafe.app https://privacysafe.app	End-to-end encrypted Chat, Inbox, Storage and Contacts, published by Ivy Cyber.
[17]	PrivacySafe Foundation https://privacysafe.foundation/	The Take Back Your Bytes education campaign and the Foundation's other work.
[18]	Creative Commons, CC0 1.0 Universal https://creativecommons.org/publicdomain/zero/1.0/	The public-domain dedication that covers these lesson materials.