PRIVACYSAFE™ FOUNDATION

INSTRUCTOR GUIDE AND NOTES

Navigating the “Dark Web”

A Take Back Your Bytes lesson for adults on private networks: what the “dark web” is, why onion routing matters, and how Tor, I2P and VPNs differ. 50 minutes with a hands-on lab and discussion.

Series	Take Back Your Bytes, PrivacySafe Foundation's cybersecurity education campaign[17]
Audience	Adults, 18 years of age or older. This lesson is not written for use with minors.
Length	50 minutes, with a 30-minute cut
Format	4 slides, an interactive lab, 4 slides, discussion
You will need	Slides (light for print, dark for projecting), the lab on the lesson page, flash cards. Tor Browser is optional and only where policy allows.
Facts checked	October 27, 2026. Tools and guidance change. Re-check before you teach.

PrivacySafe Foundation, Inc. | Take Back Your Bytes | 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. Names of other tools and organizations belong to their owners and are used as examples.

READ THIS FIRST: ADULTS ONLY, AND THE LAW

This lesson is written for readers **18 years of age or older**. The lesson page asks readers to say whether they are, and it does not store the answer. It asks, and it does not check. Do not use these materials with minors, and follow your institution's rules about what you may teach and which networks you may use. Laws about anonymity tools differ by country, and some networks block or log Tor and VPN traffic. This guide does not give legal advice.

The lesson in five sentences

1. “Dark web” is a loose label for sites you can reach only with special software, such as Tor onion services and I2P sites. The technology is neutral. The label mostly carries a reputation[1][5].
2. Without protection, your internet provider can see which sites you visit and each site sees your address. HTTPS hides the content of a page from the network, but not the site you chose.
3. A VPN moves that trust to one company that sees both your address and your destination. Choose a paid service from a company you have researched, because a free service has to pay for itself somehow, and this lesson recommends no provider[8][9].
4. Tor sends traffic through three volunteer relays with a layer of encryption for each, so no single relay knows both who you are and where you are going, and the exit relay can read what is not protected by HTTPS. Onion services protect both ends and need no exit relay[1][3].
5. I2P is a separate network in which every participant routes traffic through one-way tunnels, and its sites, called eepsites, live inside the network[5]. Anonymity supports freedom of opinion and expression, and it works best with sound habits and lawful use[10][11].

LEARNING OUTCOMES

By the end, students can:

1. Explain what people mean by the surface, deep and dark web, and why the term is loaded.
2. Describe how onion routing hides who is talking to whom, and what an exit relay can still see[1][3].
3. Compare a VPN, Tor and I2P by who you must trust and what each is good for[5][8].
4. Explain why anonymity matters for free expression, with real examples[6][7][10].
5. Describe the legal, safety and reporting responsibilities that come with exploring private networks[12].
6. Write a short, realistic safe-browsing plan.

Session plan

SEGMENT	MINUTES	NOTES
Before the lab, slides 1 to 4	12	Includes the prediction: which Tor relay knows both who you are and the site?

Interactive lab	18	Sections 1 and 2 as a class, section 3 in pairs, section 4 alone.
After the lab, slides 1 to 4	12	Onion routing step by step, comparison, why it matters, plan.
Discussion	8	Two questions.

30-MINUTE CUT

Do lab sections 1 and 2 as a demonstration with no pair work. Cover after-lab slides 1, 2 and 4. Use one discussion question.

Before class

- ☐ Optional: the lesson page has a walkthrough video of under five minutes, in a light version for the page and a dark version for projecting, each with a subtitles file. Play it as a recap, or share it with learners who missed the session. Check that it plays on the room computer first.
- ☐ **Confirm the audience.** Everyone should be 18 years of age or older. The lesson page asks, and you should check your institution's own rules.
- ☐ **Check policy and the network.** Some school and work networks block or log Tor and VPN traffic, and some institutions restrict them. Do not ask learners to install software on devices they do not control.
- ☐ **Do not browse random onion sites live.** Everything in the lab is made up. If you demonstrate Tor Browser, use only a mainstream site from a curated list[6] and a throwaway session, and never click through unknown links.
- ☐ Open the lab (demo page) and try all four sections, including every travel mode and the HTTPS and login boxes.
- ☐ **Plan for screens and chat.** Learners may type personal examples. Remind them not to share anything they would not want the class to see.
- ☐ Print the flash cards, double-sided, flipped on the long edge.

TEACH IT FAIRLY

- **Disclose the affiliations.** PrivacySafe Search and PrivacySafe Bot are run by the PrivacySafe Foundation that publishes this lesson[13][14]. The PrivacySafe.app apps are published by Ivy Cyber, the Foundation's commercial partner[16]. Present them as examples, not the only choice.
- **Do not sensationalize.** Avoid shock stories. Explain that private networks serve many lawful purposes, and that crime also happens on them, as it does on the regular web.
- **Name no VPN provider.** The lesson teaches how to judge one: who owns it, who audits it, how it makes money, and what its policy says[8].
- **Be honest about limits.** No tool makes anyone anonymous by itself. What you tell a site, malware on your device, and mistakes can reveal you.

Slide notes: before the lab

Slide 1: Title

about 2 min

SAY

What is the “dark web”, and why does private networking matter? The promise: you will see how onion routing hides who is talking to whom. Our job: learn the tools, the risks and the habits. State clearly that the lesson is for readers 18 years of age or older. The bar names the four ideas: surface, deep, dark and your tools.

DO

Introduce Take Back Your Bytes[17].

CHECK FOR UNDERSTANDING

Ask: "What do you think of when you hear 'dark web'?" Write a few words on the board and return to them at the end.

Slide 2: What people mean by “dark web”

about 4 min

SAY

- **Surface web:** pages that search engines index.
- **Deep web:** pages behind a login or not indexed, such as email, banking and cloud files. This is most of the web.
- **Dark web:** sites reachable only with special software, such as Tor onion services and I2P sites[1][5].

The name sounds sinister and the technology is neutral. Then read the fair warning: like the rest of the web, you can stumble across things that may not be legal and may be upsetting. The Foundation does not host, run or endorse other sites.

DO

Have learners place familiar sites on the three layers.

CHECK FOR UNDERSTANDING

Ask: "Is your email part of the deep web?" Yes. Most people use the deep web every day.

WATCH FOR

Do not let the label carry the whole lesson. The word is a reputation, not a technical category.

Slide 3: Who can see what you do online?

about 4 min

SAY

- **Directly:** your provider sees which site you visit and the site sees your address. HTTPS hides the page itself from the network.
- **Through a VPN:** your provider sees only the VPN. The site sees the VPN's address. The VPN company sees both[8].

- **Through Tor:** your provider sees only that you use Tor. The entry relay knows you, the exit relay knows the site, and no single relay knows both[1][3].

DO

Point at each column and ask who the observer is.

CHECK FOR UNDERSTANDING

Ask: "Where does the trust go in each case?"

WATCH FOR

The closing line matters: anything you tell a site yourself, such as a login, is not hidden.

Slide 4: What to watch for, and the prediction

about 2 min

SAY

In the lab you will pick a travel mode, select each stop on the path, toggle HTTPS and logging in, wrap a message in three layers and pass it from relay to relay. Read the prediction: in a Tor circuit, which single relay knows both who you are and which site you asked for? Take written guesses.

DO

Collect answers by show of hands after they write them down.

WATCH FOR

Many learners guess the exit relay. The answer is none. The entry relay knows you, the exit relay knows the site, and the middle relay knows neither.

The interactive lab (about 18 minutes)

SECTION	WHAT TO DO	WHAT TO POINT OUT
1. Who can see what?	Choose each travel mode. Select every stop. Untick HTTPS, tick logging in.	With Tor, no stop answers Yes to both your address and the site. With a VPN, one stop does. Logging in tells the site who you are in every mode.
2. Peel the onion	Type a short message, wrap it, then pass it relay by relay.	Each relay removes one layer and learns only its neighbors. The exit relay sees the message, so use HTTPS. The lab does not encrypt anything.
3. Choose the right tool	Pick a tool for five situations, then check.	Several situations have more than one good answer. The ad-tracking question needs no anonymity network.
4. Make your plan	Tick the habits you will adopt and copy the list.	Choose realistic steps, and check local rules first.

ANSWER TO THE PREDICTION

No single relay in a Tor circuit knows both who you are and which site you asked for: the entry relay knows you, the exit relay knows the site, and the middle relay knows neither[1][3].

Troubleshooting

SYMPTOM	LIKELY CAUSE AND FIX
The lab shows a blank page	It needs JavaScript. Check that scripts are allowed for the site.
Clipboard copy fails	Some browsers block copying outside a secure page. Learners can select the steps and copy them by hand.
Animation is too quick or slow	The lab follows your system's reduced-motion setting and jumps straight to the result when it is on.
Learners ask about specific onion sites	Direct them to the curated list[6] and to each organization's own announcement. Do not browse unknown sites in class.

Slide notes: after the lab

Slide 1: Onion routing, step by step

about 3 min

SAY

1. Your Tor software picks three relays run by volunteers: an entry, a middle and an exit.
2. It wraps your request in three layers of encryption, one for each relay.
3. Each relay peels one layer and learns only the relay before it and the relay after it.
4. The exit relay reaches the site. The reply returns the same way.

Onion services work differently: the site hides too. You and the service meet at a rendezvous relay, six relays carry the connection, no exit relay is involved, and the traffic is encrypted end to end[1].

DO

Tie each step to the lab's peel-the-onion section.

CHECK FOR UNDERSTANDING

Ask: "Why is the middle relay there?" So the entry and exit relays cannot easily link a user to a destination.

WATCH FOR

Tor does not encrypt the last leg from the exit relay to a site that does not use HTTPS[3].

Slide 2: Tor, I2P and VPNs

about 4 min

SAY

	VPN	TOR	I2P
How it works	One company relays your traffic	Three volunteer relays, three layers	Every user's router relays through one-way tunnels[5]
Who you trust	The VPN company, completely	No single relay sees both ends	No central directory[5]
Good for	Public Wi-Fi and hiding sites from your network	Anonymous browsing and onion services	Services inside I2P, called eepsites[5]
Watch out	Pay for one you researched	Slower. Use HTTPS. Do not log in as yourself	More setup and mostly an inside network

DO

Say plainly: you put ultimate trust in a VPN. Running servers costs money, so when a service is free it is worth asking how it pays for itself. Some free services earn money from advertising or user data. One 2016 study of 283 free-to-download Android VPN apps found that about three quarters used third-party tracking libraries[9]. That does not describe every free service, and paid does not guarantee safe. Look at who owns it, whether independent audits exist, and what its policy says[8]. We recommend no provider.

CHECK FOR UNDERSTANDING

Ask: "If a VPN company can see everything, how would you judge whether to trust it?"

WATCH FOR

Keep the tone diplomatic. The point is to ask how a service earns its income, not to accuse any company.

Slide 3: Why it matters, and where to look

about 4 min

SAY

- **Private by right:** freedom of opinion and expression includes the freedom to seek and share information[10], and anonymity and encryption help people exercise it[11]. Think of reporters, sources, activists, researchers and survivors.
- **Real-world onion sites:** mainstream sites that also offer onion services, such as BBC News, Deutsche Welle, ProPublica, The Guardian, DuckDuckGo, Proton Mail and Debian, plus SecureDrop tip lines at news organizations[6][7]. Send learners to the list for current addresses, and teach them to check an address against the site's own page[4][6].
- **PrivacySafe:** PrivacySafe Search and PrivacySafe Bot, both run by the Foundation, each have a .onion address[13][14]. The PrivacySafe.app Chat, Inbox, Storage and Contacts apps are end-to-end encrypted and can be used over Tor and I2P[15][16].

DO

Show the list repository on screen if policy allows. Do not click through to onion addresses in class.

CHECK FOR UNDERSTANDING

Ask: "Who is helped when a news organization offers an onion address?"

WATCH FOR

Say that onion addresses can be impersonated. Copy an address only from the site's own page.

Slide 4: Your safe-browsing plan

about 4 min

SAY

1. Get Tor Browser from the official Tor Project site.
2. Keep it updated and leave its settings alone[3].
3. Prefer HTTPS and onion addresses taken from a site's own page.
4. Do not log in as yourself if you need to stay anonymous.
5. If you use a VPN, pay for one you have researched.
6. Never download or share material that may not be legal. Leave, and report it[12].
7. Know the laws and rules where you live, work or study.
8. Use end-to-end encrypted apps for what must stay private.

DO

Ask learners to pick the first step they will take this week.

Discussion (about 8 minutes)

QUESTION 1: WHO NEEDS ANONYMITY MOST?

"Who needs anonymity most, and what would they lose without it?"

- Journalists and their sources, human rights workers, people living under censorship or surveillance, domestic abuse survivors, and researchers[7][10][11].
- Everyday privacy is also a value: people may not want every search or visit recorded and sold.

QUESTION 2: HANDLING THE HARMS

"How should a society handle the harms that private networks can also enable?"

- Crime exists on every network, including the regular web. Targeted investigation and enforcement are the response, and weakening privacy for everyone is a trade-off worth debating.
- Encourage multiple views and evidence. There is no single right answer.

Answer key and assessment

QUESTION	ANSWER
What is the difference between the deep web and the dark web?	The deep web is anything not indexed or behind a login. The dark web is sites reachable only with special software such as Tor or I2P[1][5].
Which Tor relay knows both who you are and the site?	None[1][3].
Why is HTTPS still needed with Tor?	The exit relay can read traffic that the site does not protect[3].
How do onion services differ?	Both ends are hidden, six relays carry the connection, there is no exit relay, and traffic is encrypted end to end[1].
What is the main risk of a VPN?	You trust one company with your address and destinations[8].
Name one difference between Tor and I2P.	I2P users each route traffic over one-way tunnels, and its sites live inside the network[5].

EXIT TICKET (3 MINUTES)

1. In your own words, explain why the “dark web” is a loaded term.
2. Why would a free VPN deserve extra questions?
3. Name one step you will take this week, or one rule you will check first.

HOMEWORK

- Read the Tor Browser manual's safety section[3] and the EFF guide on choosing a VPN[8].
- Only where policy and law allow, install Tor Browser from the official site and open one mainstream news site's onion address taken from its own announcement. Do not follow links to unknown sites.
- Stretch: read the human rights framing[11] and write a paragraph on one case where anonymity protected expression.

Common questions and misconceptions

QUESTION OR BELIEF	RESPONSE
"The dark web is all crime."	Activity that may not be legal exists there, as it does on the regular web. Many onion services belong to news organizations, universities, software projects and privacy tools[6].
"Using Tor is against the law."	In many countries Tor is legal, and some restrict it. Check the law and the rules where you are. This guide is not legal advice.
"Tor makes me anonymous automatically."	No. What you log in to, what you type, malware and mistakes can reveal you. Follow the Tor Browser advice[3].
"A VPN makes me anonymous."	It changes who can see your traffic, and the VPN company sees everything[8].
"Free VPNs are fine."	Some are. Ask how the service pays for itself, and look at ownership, audits and policy[8][9].
"I2P is just another Tor."	They share goals, but I2P uses one-way tunnels, has no central directory, and focuses on services inside its own network[5].
"Everything on an onion address is safe."	No. An onion address proves only that you reached that service. Impersonation exists, so copy addresses from the site's own page[4].

IF YOU COME ACROSS HARMFUL CONTENT

Leave right away. Do not download, save or share it. If it is child sexual abuse material, report it to the National Center for Missing and Exploited Children's CyberTipline if you are in the United States[12], or to your national hotline or law enforcement elsewhere. Anyone who feels upset afterward should talk to a trusted adult or a counselor.

References and further reading

Citations in this guide use bracketed numbers. Links were checked on October 27, 2026. Tools and guidance change, so confirm details before you teach.

#	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.

ABOUT THESE MATERIALS

The slides, lab, flash cards and this guide were written for the PrivacySafe Foundation's Take Back Your Bytes campaign. They are dedicated to the public domain under CC0 1.0[18]. The Foundation names and logos are trademarks and are not included in that dedication. PrivacySafe Search and PrivacySafe Bot are run by the Foundation. The PrivacySafe.app apps are published by Ivy Cyber. This lesson is independent of the other organizations and tools named in the references. The lesson is for adults and is not legal advice.