Censorship circumvention and encrypting your traffic with a VPN (beginning)

“Do I need a VPN?” and “Which VPN should I use?” are questions that often come up during digital security workshops. Learners might hear of Virtual Private Networks, or VPNs, when they’re looking for ways to protect their Internet connection on public WiFi, such as at a coffee shop or in an airport. Others, like journalists, may want to use a VPN as a way of seeming like they are using a different network than the one that they are working from. Learners may also be interested in circumventing Internet censorship in their country. The question of how to know which VPN to use, however, is packed with additional considerations and nuances, and it may be difficult to address these in a clear way. This lesson plan helps learners think through what tools are right for them, and what factors they should consider in their search for a VPN.

Recommended Reading

- Choosing a VPN That's Right for You
- Recommending Tools
- An Introduction to Web Browsing Security
- What Should I Know About Encryption?
- This 2019 consumer-facing report from Wirecutter evalutes VPNs and provides a thorough assessment of how the VPNs were compared for security, privacy and additional consumer considerations.
- This lesson plan from Level Up covers how censorship and Internet circumvention work.
- This blogpost from Localization Lab explores how VPN usage has been popularized in Zimbabwe through memes.
- This post from Freedom of the Press Foundation provides in-depth information on what to look for when choosing a VPN.
- This explainer from CDT covers what a VPN is and how it works.

- This list of questions from CDT for assessing VPNs can help with understanding evaluation criteria.
- It may be useful to have your learners review this NPR article about why VPNs shouldn't automatically be trusted before the lesson.
- For learners who are curious about VPNs as they relate to travel, Great Fire's website might be a useful resource.
- This story from CyberScoop includes a useful example of when someone (like a journalist) may want to use a VPN.

Gotchas and Problems You Might Hit

Learners are often confused about the role of VPNs. It's common for people to confuse VPNs with Tor. Additionally, learners may not understand what data and metadata VPNs can see.

One common misconception is that VPNs are just for one type of device (for example, "I thought a VPN is just for your computer"). An important takeaway to share is that you can have a VPN on your phone, just like you can have one on you computer, to encrypt all traffic between your device and your VPN provider.

Some trainers use metaphors to describe how a VPN works, ranging from a "tube" to a "tunnel" to describe safely transporting something, to a "condom" to describe protection from public wi-fi networks. As with anything else, please evaluate cultural relevance, gender sensitivity, and your level of trust with your audience. For example, consider using the condom/safe sex metaphor sparingly, as it may be an uncomfortable framing for many audiences.

Anticipated Questions and Answers

* You will likely find yourself saying "It depends" for many questions.

Question: "I'm overwhelmed by information! Can't you just recommend one VPN that you like?"

Answer: If there's a VPN that you—the facilitator—like and have spent time assessing for your own uses, it may be okay to recommend it. However, we strongly encourage you to carefully consider how you recommend such a tool. Be sure to share the caveat that it is hard to assess the security and claims of VPNs, and that the security and privacy

considerations for each VPN can change quickly. Encourage learners to stay informed by periodically searching for news involving their VPN.

Question: **“Why is it so hard to get my VPN to work?”**

Answer: A learner may ask this question out of frustration with usability or slow speeds. One possible response is: “The range and quality of VPNs varies a lot from one service to another. Just like email, who you choose as your VPN provider will impact the quality of service a lot.”

Consider returning to this question when discussing the advantages and disadvantages of dedicated VPN software.

Question: “My workplace provides a VPN. Should I just use that?”

Answer: Explain that whatever VPN you choose, you’re entrusting it to provide the Internet for you. You can give the following examples to illustrate the advantages and drawbacks of using a workplace VPN.

“Connecting to a work VPN is a lot like connecting to your WiFi at work. While a workplace-provided VPN will protect against someone snooping on your connection in a coffee shop, it won’t be the best option if you, for example, choose to look at job listings for other companies, or if you want to reach out to a reporter about workplace misconduct. Just as your systems administrator at your workplace will see activity when you are on the network while physically at the office, they can also see your activity when you are connecting to the work VPN from anywhere outside of the office. The most important thing to keep in mind is that you’re shifting the trust from your ISP or WiFi point to the VPN itself.

Another consideration is what type of encryption your work VPN provides. Some encryption protocols (or methods) are outdated and in some cases provide very little protection at all. You may suggest that learners pick a public VPN they have investigated themselves for sensitive browsing, or consult with the IT department at their workplace to determine just how safe their work VPN is.”

Question: “I can’t afford a monthly/yearly fee. What should I do? Should I download a free VPN?”

Answer: To consolidate cost, you might suggest using a VPN that is packaged with other security software. Some VPN services require you have an account with them first,

but offer a VPN service for free when you are referenced by another user. There are other free VPN services available, too.

You can say something along the lines of: “The most important thing when investigating a free VPN service is determining how they are able to operate for free. Are they selling your data? If so, are you comfortable with this trade-off? In some instances, free VPNs may have malicious advertising (sometimes called “malvertising”) incorporated in their software.”

Question: “Someone told me I can create my own VPN. Should I do that?”

Answer: Even if your learners are comfortable with systems administration and the command line, setting up a VPN can be very challenging. Some router software (such as OpenWRT or LEDE) will run OpenVPN and allow you to configure it via a web interface, but this should only be suggested for the most advanced users. It may be best not to distract the rest of the learners with details about how to set this up and instead encourage the more advanced learner to contact you after the session.

Question: “I’m traveling to a country that has a reputation for censoring content. What should I do?”

Answer: This is an advanced question often requiring more assistance and context.

Circumstances change, and it’s important to keep up to date on security news for specific countries’ policies on VPNs. For example, it may be illegal to run certain VPNs (or a VPN at all) in certain countries, and it may be risky to have a VPN installed on your computer when entering such counties, especially since the most likely point of search may be when you are entering the country. You can encourage the learner to reach out to you after the workshop.

Question: “If I’m using a VPN, do I need to use HTTPS too?”

Answer: You can mention that HTTPS and VPNs are both forms of transport-layer encryption, providing ways to protect the learner’s traffic from unwanted eavesdroppers. However, the way that HTTPS and VPNs protect that information differs significantly. The main point that learners should come away with is to use HTTPS whenever possible to take full advantage of the additional security protections, including using HTTPS when they are using a VPN or when they are using Tor.

You can point learners to An Overview on Web Browsing Security for a breakdown.

Question: “What’s the difference between a VPN and Tor?”

Answer: While the Tor network uses encryption just like many VPNs do, there is a key difference: with the Tor network, you don’t place your trust in any one company or service.

The Tor network is run by a system of volunteers, and routes through three separate computers that run the Tor software dispersed across the globe before being passed on to the service you’re using. Each Tor software-operating computer server (called a “hop” or “node” or “relay”) along the way unwraps a layer of encryption to reveal the next destination. This is to keep the message contents as well as the route of the message secret. With all three hops working together to obscure your identity, it is extremely difficult—if not impossible—to tell which message is sent from where and by who.

(Note: Some learners might be confused that computers using Tor Browser are not the same as Tor relays. You might need to clarify that Tor relays are explicitly volunteer computers for running Tor software to provide this network.)

The Tor network differs from a VPN, which operates just as a single hop. This is important because it means that a government subpoena or court order could demand data from the VPN company, so you have to trust the VPN company to be diligent in protecting your data (or, even better, not collecting it at all).

Another way to frame the difference between a VPN and Tor is in terms of censorship versus privacy concerns: if you want censorship circumvention but aren’t as concerned about privacy issues, use a VPN. If you want censorship circumvention *and* privacy, you may want to look into using Tor. Give learners the caveat that the Tor network and Tor Browser have their own constraints and recommended practices for use, so interested parties should look at the Tor Project website: torproject.org.

Question: “Can my ISP or government see that I’m using a VPN?"

Answer: Yes, you should expect that your ISP or government will know that you’re using a VPN. Depending on where you are, the government may be able to make this determination in real-time or after contacting the ISP.

Some pieces of software, such as Tor, can mask the fact that the software is in use; however, *in the case of Tor, you must choose this as an option when you start Tor Browser*. You should also be aware that this is not perfect masking: a government may still be able to detect use of Tor using sophisticated methods.

Learning Objectives

Learners will:

- Be able to name at least one of the benefits of using a VPN (security, privacy on untrustworthy/unfamiliar WiFi networks, censorship circumvention, protecting data from ISPs, protecting data from governments)
- Be able to give an overview of what an Internet Service Provider (ISP) can see when you use a VPN, versus what your VPN provider can see.
- Be aware that VPNs provide additional protection if they don't trust the network, and will be able to give common examples of untrustworthy networks (e.g., WiFi at internet cafe, hotels, or airports —all extremely unsafe networks).
- Know that VPNs are available for phones, not just for desktop computers.
- Have a framework for evaluating the trustworthiness of VPNs and be able to describe at least two considerations they should weigh when picking a VPN (e.g., the VPN's privacy and security claims, business model, reputation, data collection practices, and encryption protocols/methods, as well as the laws applicable in the VPN's jurisdiction).

- Know that if they want to browse anonymously, they should use Tor—and seek training separately on how to use the Tor Browser.

Prerequisites

- What Should I Know About Encryption
- How Do I Protect Myself Against Malware?

Ratio

Instructor: Learners
10:1

Suggested Materials

- paper and pens for the drawing activity
- a projector or a whiteboard to illustrate the portion for how VPN connections work

Lesson Content

Warmup: Blocked Content, Exploring Trustworthiness and Partner Introductions

Ask the following question: “Raise your hands if you have done the following. Have you ever tried to read an article, watch a TV show, or play an online game on a network that wouldn’t let you?” If learners appear stuck, you can give the example of being blocked from a site or service while on a school network, at work, or in another country.

If learners seem comfortable, you can follow up with the question: “What did you do when you found out the content was blocked?”

Some of them may answer with: “try the mobile site,” “try the site with a different country URL at the end,” “go through Google translate,” “google a block of text to find the content hosted somewhere else,” “try the HTTPS version of the site,” “use Tor Browser,” “give up,” or “use a VPN.” Highlight any answers about a VPN—you can ask a volunteer to elaborate on how they used it and what it looked like for them.

Then, have attendees break into small groups of four or five. Give them five to ten minutes to introduce themselves with the following icebreaker questions:

1. What’s your name and pronouns?
2. What brought you here today?
3. Has someone ever asked you to watch over something of theirs? For example, has someone ever asked you to watch their bag?

- How did they know you were trustworthy?
- What did you do with the valuable information or item they gave you?

Now reconvene and have participants share examples of the valuables that they were entrusted to protect. Ask: Has this ever happened with a stranger? Did they ask you to watch their wallet, bag, or computer when you’re at a coffee shop, bus stop, or a train station?

Knowledge Share: Introduce the general idea of what an ISP can see, and what a VPN is.

You can use their answers to the warmup as a transition to explain how participants' Internet Service Providers (ISPs) are also entrusted with valuable information.

Facilitator: "Internet Service Providers, or ISPs, are able to see valuable information when you connect to a WiFi network. What are some examples of what they can see?"

Answers you may get are, "my email" or "my browsing history." Some participants may also bring up Net Neutrality when discussing what ISPs are able to see and control, like blocking or slowing down content.

Then ask whether participants place the same level of trust in their ISP as they would place in their friends or family with sensitive information or belongings.

A Virtual Private Network (VPN) is software that masks your IP address and makes it look like you're coming from somewhere else, by routing your Internet activity through a server. It is often used for censorship circumvention—for example, when you are using a school's censored Internet connection or in a country that blocks content. Using a VPN, you should be able to access blocked websites.

The facilitator should highlight the following point: There is no "one size fits all" VPN. Each person may have different needs for how they hope to use a VPN.

Then, explain that just as you trust some people more or less than others, some VPNs are more or less trustworthy than others as well. It's often difficult to assess a VPN's trustworthiness, but there are a few specific things that you can look for when investigating a VPN's trustworthiness.

Knowledge Share: What makes a trustworthy VPN?

Have participants get back into their groups, and pose the question:

"What might you look for when choosing a VPN? Think of what makes you trust another person, and use that as a guide. In five minutes, we'll share what we discussed."

Have the groups discuss with each other and reconvene. Have participants share what answers they came up with in their groups. Some answers you may get are, “They have a good reputation,” or, “They have a history of others trusting them.” Explain that just like with deciding whether to trusting another person, a VPN’s reputation matters. Other answers that may come up are, “They keep their data safe,” and explain how a VPN’s use of encryption technologies can help with keeping data safe.

Your learners may have questions instead of answers—such as “How do I know if a VPN does what it says it does?” Encourage these questions, as they show critical thinking around hard issues that security professionals also grapple with when evaluating software. You can revisit their questions after explaining how VPNs work.

Activity: Drawing “You,” “ISP,” and “VPN.”

Participants will now be asked to draw, either individually or in groups, what they think the relationship is between themselves, their ISP, and their VPN. Before they start to draw, explain some of the helpful imagery that they might use in their illustration:

- “Tubes,” “pipes” or “tunnels” can be used to illustrate paths through which information flows.
    - Tubes can be *nested* inside other tubes.
- “Scrolls” or “postcards” can be used to illustrate bits of valuable information. Some examples of valuable information include: messages between friends, websites you visit, articles you read.
- “Robots” or “computers” can be used to illustrate ISPs and VPNs, who can either:
    - Hold up a tube (keeping the infrastructure running by supporting it), or
    - Be a point where a tube begins or ends (e.g., where the connection goes).

Give participants 5 or 10 minutes to draw. Ask them to label each of the components. If learners are stuck, you can give them the following guidelines for their drawings:

- The drawing must show the initiating computer or phone attempting to connect with a website.
- The drawing must show a connection with a VPN.
- The drawing must show a connection with an Internet Service Provider.
- The drawing must show the intended destination (the website) of the initial computer.

Once the drawings are done, learners can post up their drawings on a wall.

Some things to ask when going over their illustrations:

- What is happening in this diagram?
- What information is being shared?

Review some of the drawings, giving positive feedback when you see something that hints at the way VPNs really work. Be careful to take note of any places of misunderstanding in their explanations, and go over these misconceptions with the group as a whole.

More nuanced questions you can ask to check for their understanding are:

- Is the [connection metaphor, e.g., tube or tunnel] transparent? Or is it hiding contents inside?
- What can the Internet Service Provider see if you're *not* using a VPN?
- What changes when you connect to a VPN?
- What can the VPN see?
- Where does the Internet Service Provider think you are connecting from?
- Where does the VPN think you are connecting from?

After going over the participants drawings, you can illustrate your own version of a diagram, which describes this relationship.

Knowledge Share: VPN constraints

Now that your learners have a general sense of the role of a VPN, you can go in more detail on VPN characteristics.

Privacy and Security Claims

Some VPNs claim to not share or sell data. You should encourage learners to think about: how can you verify these claims? Encourage learners to look closely at all claims that a VPN makes, and emphasize that marketing claims are not guarantees. For example, reviewing the the privacy policy for a VPN will often uncover details about how the VPN monetizes your data, even if the VPN doesn't sell it directly to third parties.

Business Model

Even if a VPN isn't selling your data, it must be able to stay in operation *somehow*. If the VPN provider doesn't sell its service (i.e., if its a free VPN service), teach your learners to ask: How is it keeping its business afloat? Does it solicit donations? What is the VPN's business model? Some VPNs run on a "freemium" model, meaning they are free to join but will charge you after you transfer a certain amount of data over their service. Others are completely free, but they might come at a privacy cost (e.g., they may sell or otherwise monetize data). Particularly if your users' budgets are constrained, these are important considerations for your learners to be aware of. These are all important considerations that your learners should think about *before* settling on the VPN that is right for them.

Reputation

Another consideration is reputation. This can be a difficult judgement to make. It is worthwhile to do some research on the people and organizations associated with the VPN. Is it endorsed by security professionals? If a VPN is established by people that are known in the information security community, it is more likely to be trustworthy. Does the VPN have news articles written about it? Be skeptical of a VPN offering a service that no one wants to stake their personal reputation on, or one that is run by a company that no one knows about.

Data Collection Practices

A service that does not collect data in the first place will not be able to sell that data. When looking through the privacy policy, see whether the VPN actually collects user data. If it doesn't explicitly state that no user connection data is being logged, chances are that it is. And, depending on jurisdiction, a government can demand that data or issue a subpoena for it.

Even if a company claims not to log connection data, this may not always be a guarantee of good behavior. Encourage your learners to investigate instances where a VPN has been mentioned in the media. They may have been caught misleading or lying to their customers. A simple search can go a long way.

Encryption

You can encourage your learners to look at how safe their VPN encryption is; that is, if the transport-layer encryption utilized by a VPN is doing its intended job. You can use the analogy of how "transparent" or "fragile" a tube is in the previous drawings. If a VPN is using broken encryption—such as Point-to-Point Tunneling Protocol (PPTP) or weak

encryption ciphers—it is as if your tunnel is see-through. Any data flowing through it can be seen by your ISP, government or bad actors. Evaluating the strength of a VPN's encryption can be difficult to do, so you may want to point the learners to the technical considerations outlined in the Freedom of the Press Foundation's helpful VPN guide or the "technical security" column in this VPN comparison chart. If any of your learners are using (or considering using) a workplace VPN, encourage them to contact their IT department and inquire about the security of the connection.

Location and Laws

Finally, some learners may choose a VPN based on where its headquarters are located. You can mention that for some people, such as activists and high-stakes journalists, choosing a VPN based on the applicable data privacy laws may be an important factor. But also be sure to mention that company policies and laws are subject to change at any time.

Knowledge Share: VPNs and Software

Now that your learners know some of the criteria for evaluating VPNs, you can go into more detail about *how* they might connect to a VPN, and what they should be thinking about when installing software. You can explain:

Facilitator: "Some VPNs have you install a custom application that is specific to that particular VPN. How can this be helpful?"

One answer you might hear is that it is more convenient to connect using an application that is specific to their particular VPN. VPNs with friendly user interfaces are often easier to adopt than generic interfaces that require custom configuration (e.g., entering server names and port numbers in order to connect).

You can explain:

"Yes, having a dedicated, separate program that is provided by your VPN can be really useful. It can make connecting to that VPN a painless process, without the need to enter confusing settings such as the server name and port number."

You can then pose the question:

"But, what might be dangerous about installing VPN software?"

Someone may answer, “Because VPNs can be untrustworthy!” Unlike ISPs, it’s easy for anyone on the Internet to set up a VPN service with minimal effort. You may explain that because any piece of software you install can be malware in disguise, it is important to establish the trustworthiness of any software *before* you install it. It is worth reinforcing this point:

Facilitator: “You must be very confident in any VPN software you choose to install, since any malicious software installed on your machine can do a lot of harm. Very few VPNs have had formal **‘security audits,’** which means allowing external evaluators to comprehensively examine a software’s security and practices.”

Encourage participants to do their research on VPN providers and look for articles from reputable media sources on any VPN software they are considering installing before they install it.

Recap Activity: VPNs - What are they good for? What aren’t they good for?

Now that you’ve covered the benefits of using a VPN and the important considerations your learners should be thinking about when assessing the privacy and security of any particular VPN service , you’ll want to review the material with your learners.

Have the room break into groups. Give them the following prompt and have them write down their answers on sticky notes, with one idea per note:

Facilitator: “You have five minutes to come up with answers to the following question: **‘**How would a VPN would be useful?’”

Meanwhile, in a visible area, you can write the following categories:

Security

Privacy on untrustworthy networks (e.g., unfamiliar WiFi)

Censorship circumvention

Protecting data from ISPs

Protecting data from governments

After learners have written their ideas on the sticky notes, explain the categories you've provided. Then, have the participants come up and place their answers in the appropriate categories. After everyone is done, you can explain how students can see for themselves that VPNs have a wide range of uses, keeping the caveats in mind. Read some of the notes aloud and provide positive reinforcement for the answers that stand out.

Once this is done, ask your learners to discuss in their groups: "What are VPNs *not* good for? In a few minutes, we'll share what we talked about."

After they have chatted in their groups for 2-3 minutes, ask them to share what they talked about. Answers may include: "VPNs aren't good for real anonymity," or "VPNs won't protect a government from accessing your data with a subpoena," or "VPNs don't protect my browser from trackers."

Learners will likely have many questions. Be sure to allocate enough time for questions and answers.

Learners will need refreshers on the topics covered in this lesson. Be sure to point them to follow-up resources, such as:

- Choosing the VPN That's Right For You
- What Should I Know About Encryption?
- An Overview of Web Browsing Security

For learners who are concerned about anonymity (rather than censorship circumvention) or about privacy from ISPs *and* governments, you may want to point them to SSD's Tor Browser guides (MacOS, Linux, Windows), as well as the Tor Project's resources on how to use the Tor Browser. Please note that Tor Browser has unique considerations for maintaining anonymity, so special training is recommended.