

AUTHENTIC8

THE PROFESSIONAL ANALYST'S
COMPLETE GUIDE TO

INVESTIGATING THE DARK WEB





Investigating on the dark web: the complete guide for cyberthreat research

*What is the dark web and how does it vary from the internet most of us use everyday?
Which darknet should I use for my investigation? And how can I access it safely?*

The dark web is an area of the internet only available via software clients. It is most notoriously known for the illegal activity it sometimes facilitates. Despite the nefarious associations, there are practical uses for its existence as well, and industry professionals can benefit from becoming familiar with the crucial information that may be lurking there.

In this guide, we will tackle essential questions for analysts seeking to begin a dark web investigation. In the next pages you will find:

- An introduction to the dark web and how it works
- The various darknet types and how they're commonly used
- Plus which ones will be most relevant to your investigation
- How to know if you need dark web access for your investigation and the three questions to ask yourself
- What NOT to do on the dark web
- Step-by-step on how to create a dark web access policy
- The essential tools needed for a successful investigation

What is the dark web?

The dark web grants users encrypted, private access to information, websites and marketplaces. It cannot be found by search engines and requires specific software installation to access. The peer-to-peer sharing model allows for decentralization and anonymity amongst visitors and contributors.

Perhaps best known for its association with criminal activity, the dark web has become infamous for its role in the illegal drug trade. But there are less nefarious reasons to access the encrypted dark web. In many countries it allows demonstrators to subvert authoritarian regimes and provides a free and open internet model that can evade censorship and provide privacy.

Dark web sites are similar in content and style to the surface web, or the internet most people are familiar with, but the traffic is routed and shared differently, making it more difficult to shut down or find the original sources of content.

For investigators, it can hold crucial information that would be otherwise inaccessible. To acquire these datasets, it is important to understand each area of the web, the different clients available to use them and what precautions should be taken before diving in.

Free speech on the dark web

The dark web's role as an anonymous and reliable source of information to dissidents in foreign countries, alongside privacy enthusiasts, is important and legitimate. Many reputable websites have mirrored dark web versions of their website, including news organizations like the BBC, The New York Times and ProPublica. Just because you can't get there by popular search engine, doesn't automatically make it nefarious. But it's important to know the legal, security and privacy implications that come with before attempting to log on to the dark web for research or any other reason.

Is the dark web illegal?

The dark web is infamous for illicit underground dark web marketplaces selling contraband across international borders. [The Silk Road](#) rose to notoriety in 2011 after a longform article was featured on the then popular site, Gawker. The Silk Road was eventually shuttered by law enforcement agents in 2013. But since the bust, several more darknet markets have appeared in its wake, each seeming more competent than the last. Well-known dark web marketplaces for illicit sales include the recently shuttered Alpha Bay and Hansa, Dream Market and countless others.

The digitized version of the black market means the contraband being offered can reach further distances in larger quantities than any physical predecessor. It also sells more than just physical contraband like narcotics and unregistered firearms. Stolen breach data routinely finds its way to dark web auction, compromising the personal and financial information of customers.

These dark web commerce sites are often powered by cryptocurrency, so the users can shroud their purchases in [purported anonymity](#). The encrypted transactions make tracing the real personas behind them difficult, but not as impossible as previously believed.

So with all this illegal activity taking place on to the dark web — is it really okay to log on? Believe it or not, it's not illegal to access the dark web. While the nature of the dark web has led to abuses and exploitations by bad actors, this underside of the internet is not illicit by nature. The dark web can be a beacon of free speech and is celebrated by the privacy-conscious for its unmonitored information access.

It may not be illegal to access the dark web, but doing so comes with considerable risks. The dark web is a place where stumbling into the wrong place (including illegal places) is easy to do. Be sure to read the risks and implications section to learn more.

Surface web vs. deep web vs. dark web

If there is a dark web, is there a light web? Isn't the internet just the internet? There are many more layers to the world wide web than we realize. Many people, including researchers, are surprised to learn that what they consider the internet is actually just the tip of the iceberg and only accounts for a percentage of all the data online. Many also conflate the deep and dark web, which are entirely different in structure. The internet's searchable and unsearchable areas can be divided into three main buckets.

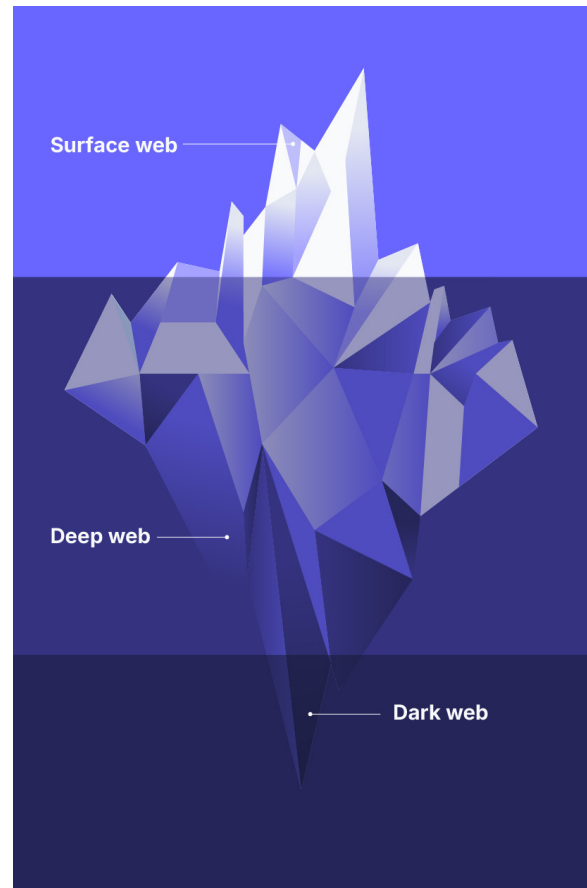
Surface web

The internet most of us use daily — and probably assumed until now is the entirety of the internet — is actually what's known as the open web or surface web. It is the format of the web we're all used to, composed of open pages easily accessed by traditional search engines on any browser. Despite being where so many users default to, the surface web only accounts for a portion of the entire internet.

Deep web

The deep web is the next layer of internet information. These are sites that require login or subscription services. Everything from academic journals, to court record databases, to private company intranets, or even services like Netflix, all make up the deep web.

The deep web has some barriers to accessibility, while being adjacent to the surface web and is typically accessed via the same browsers.



Dark web

The dark web is the area of the internet that can only be accessed by using specific software. There are different versions available, from the most well-known, such as The Onion Router (most commonly known as Tor), to the lesser used, such as Freenet. Each dark web requires its own browser or software to access it. Many users of the dark web access it to remain anonymous, but there may be some fallacy in that assumption of anonymity.

Of all internet traffic, the dark web only composes a very small amount. But limiting your search to the surface web and leaving everything below untouched could be a mistake in your research. Information on the dark web's hidden sites could prove to be essential to shoring up your network's cybersecurity practices and taking a preventative approach to breaches and phishing attempts.

The different dark web networks and how they're used

To access the dark web, a special software or client is needed. Each version of the dark web provides its own dataset, encryption services and risks associated with logging on.



The Tor browser

The most commonly used darknet service is the Tor browser. It stands for The Onion Router. Tor is the largest and most well-known darknet provider.

It was created to provide layers of encryption (hence the reference to onions) in order to anonymize communication between intelligence professionals. Tor operates almost like a traditional web browser. You can download it to your machine and use it to access different sites.

By diverting traffic through multiple nodes on its way to the client, the originator of files and sites can be hidden, making them more difficult to trace. The multi-layered encryption gives anonymity to its users and service providers alike. Many sites are given a random URL that ends in .onion. Anyone can download the Tor browser onto their machine, but like any other browser, there are still ways to track activity and hacking risks.

In the Tor browser, the largest security weakness is the point information travels between the exit node and the destination site. This unencrypted area presents a severe vulnerability to users.



Hyphernet

Hyphernet, formerly known as Freenet, is a decentralized, censorship-resistant peer-to-peer (P2P) network designed for anonymous communication and file sharing. It is used in two forms — the "opennet" allows connection to any user, while the "darknet" connects only to friends. The ability to access only known contacts provides a higher degree of trust than other software.

Access is created through a backend web application and requires a key to gain entry. While it was originally used by dissidents to circumvent censorship laws, it is now popularly used by cyber criminals to offload stolen and malicious content.

The traffic is routed via the closest nodes in the open net to create efficient routing. In the darknet, routes are set up manually and only trusted parties know your node's IP address. The inconvenience of the darknet infrastructure is outweighed by the security it provides. In this system, the information stays available after the publisher has disconnected.

It is often purported that Tor was developed by the U.S. Naval Research Laboratory in 2002. This is partially true. Researchers developed the concept of onion routing.



I2P, Invisible Internet Project

Another darknet network is I2P, or the “Invisible Internet Project,” released in 2003. Unlike the previous two sources for websites and file sharing, I2P focuses most heavily on encrypting communication between users. Instead of using a single thread in the style of Tor, I2P is built on peer-to-peer encryption.

Access to I2P uses a browser and an application in the background. It provides untraceable communication by establishing one-way tunnels through peers. Each client becomes a node in the tunnel, and tunnels then expire after 10 minutes. The system is referred to as “garlic routing.” The one-way messages are encrypted for recipients, as well as their delivery instructions.

I2P is popular for criminal enterprises to spread untraceable messages to associates.



ZeroNET

Lesser known darknets include ZeroNet, a peer-to-peer-based web hosting model developed in 2015, that doesn’t use IP addresses or domains for websites. Sites are not hosted via a typical service and can only be accessed by public key. Sites are free to create and share, and nearly impossible to shut down.

To access ZeroNet, you can use a regular browser with the application running in the background. Information from it can also be downloaded and made available offline. The content is made available via BitTorrent, which shares bits of information across many peers, each one hosting a piece of the information needed. By distributing the information through many hosts, it becomes nearly impossible to track down or scrub all of the pieces of content from the web. Each peer can then reshare and distribute it themselves once downloaded. Unlike Tor, ZeroNet is not anonymous.

Learn how Silo provides [secure, anonymous, one-click access](#) to the dark web

One-click Tor access within Silo provides secure, authorized access for investigators. Comprehensive audit oversight ensures compliance and legal protections for practitioners and their employers alike.

Where to look when searching the dark web

So which darknet is the right choice for your investigation? That depends on what you're looking for. Each dark web service has different advantages and may be utilized for different reasons. To recap:

- Typical uses for Tor include being used by bad actors to host websites and forums, as well as dark marketplaces to sell malware and contraband; non-malicious actors also use it to spread information in censored countries or to avoid data tracking
- Less popular though still noteworthy, Zeronet is most often used to host websites that cannot be taken down and are viewable offline; it is most infamous for being utilized by terrorists like ISIS
- I2P, on the other hand, is mostly used for encrypted communication; it is gaining popularity as an alternative to Tor because it is less monitored
- Freenet is often used as a delivery mechanism for selling breached data and malware

Should you access the dark web for your investigation?

Each of these darknet services can benefit analysts who work in cybersecurity, financial services or threat hunting. The dark web can be a resource to track data leaks, understand the latest phishing methods and even uncover breaches before your system is alerted. The dark web can also provide the context of how stolen data is tracked and transmitted.

Many hackers discuss trade secrets in dark web forums. This information can help mitigate cyberthreats before they are committed or be used to recover leaked data from a breach. They may also post leaked passwords and accounts or sales of hacked devices. Stolen online bank account information and credit cards routinely make their way to darknet marketplaces and forums.

The discussion of tactics can even allow red teams the ability to try out methods and test systems before criminals get the chance. The dark web is a treasure trove of information for creating proactive network security.

Intelligence analysts typically leave no stone unturned. Yet when it comes to exploring the dark web, there are inherent risks that come along with looking below. To determine whether or not you should pursue dark web investigations, start by asking yourself these questions:

1. Can you find the information anywhere else?
2. Do you understand all the possible risks?
3. Will you be able to access it safely?

And if the answer to these considerations leads you to pursue a dark web investigation, there are additional resources to consider in order to protect yourself and your company.

Is a dark web investigation necessary for your investigation?

The first way to determine if accessing the dark web is for you is simple — is it the only place that offers the information you need? The dark web itself only accounts for a small amount of all internet data, just 0.01% according to Britannica. That means, when determining where you need to look, statistics are on the side of what you already have available. Most of the data you seek is likely on the surface web most people are familiar with or the deep web.

With so much of the internet freely available, you may not even need to take on the risks of trying to access a darknet. The simple answer is always the best answer — if you don't need to access it, you shouldn't. However, if the leads you chase are constantly dipping below the surface, there are ways to protect yourself and your company while following your investigation in every direction it may take you.

Don't be afraid of the dark

Figuratively waltzing into a hotbed of criminal activity is reasonably intimidating and there are legitimate risks associated that we'll outline below.

But when it comes to threats, efficiency means going to the source. If you need to learn more about a specific suspect or a leak, taking your investigation to where the bad actors commonly reside simply makes sense. With the right understanding of risks and precautions, you can access the dark web without compromising your security.



Do you fully understand the risks of dark web investigations?

If you have already determined that what you are looking for can only be located on the dark web, you need to understand the risks before diving in. Many dark web services — including the largest, Tor — have risks involved just with signing on, to you personally and for your employer. Before you begin, make sure you fully understand what's at stake.

The dark web, like anywhere on the internet, comes with cyber risks. Just clicking on a link or visiting a site could introduce malicious content to your machine and network. More importantly, you should know even unknowingly viewing child sexual exploitation material is a crime in all U.S. jurisdictions. Haplessly wandering into forums without security measures in place, like [blur features](#), can be traumatizing and have legal consequences.

Due to the dark web's more unscrupulous users looking to ward off any unwanted attention, darknets are particularly rife with cyberthreats. Simply logging on with your main work computer or personal laptop without any additional precautions could pose serious threats. Secure access is needed to avoid revealing company secrets or personal information.

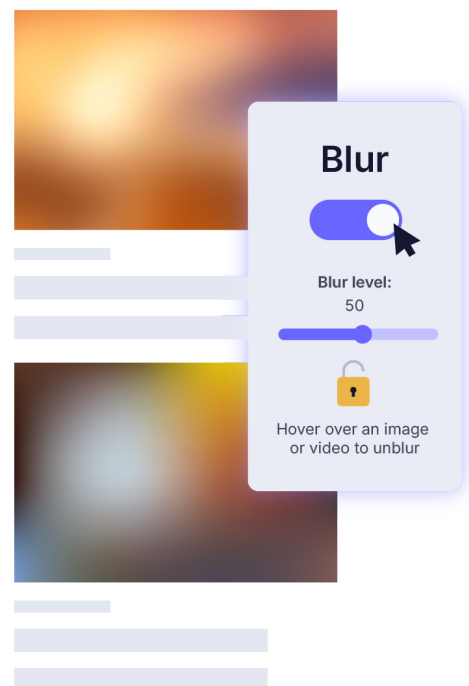
The next thing to consider is your digital fingerprint. Your IP address, browser history and cookies are all giving away information about you that you don't want found. Even the [language](#) your device is set to or what browser you choose may give away important context that could tip off investigative targets as to who you are and where you're visiting from.

This could lead not only to retaliation (cyber or physical), but disrupt the investigation due to a target creating disinformation to throw you off or wiping any trace of involvement.

Beyond malware and hacking risks, there are still other issues to consider. For instance, if accessing blogs or marketplaces known for criminal activity, you yourself might be assumed to be a criminal by law enforcement officials.

You need to be sure dark web investigations are covered in your organization's IT policies and any necessary monitoring and auditing are in place.

Before accessing the darknet, make sure both you and your company are familiar with all risks involved and have created a detailed game plan for how to mitigate them.

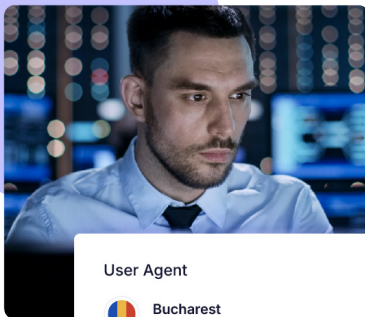


Will you be able to conduct dark web investigations safely?

With all the risks in mind that go along with logging on to the dark web, it's important to ask if you will be able to protect yourself and your employer properly before you begin.

- Do you have an access policy?
- Has legal counsel been consulted?
- Do you have a resource for concealing your identity and protecting your network from malware?
- What is the audit process?

Only once all of these questions have been answered, should you seek out the tools to access the dark web. To mitigate risks, you must consider security, anonymity, legality and compliance.



User Agent

 Bucharest

Chrome (Win 10)

IP: Language:

Device

Google Pixel 2 XL

Save

Learn more:

[Why online investigators need managed attribution](#)

Security through web isolation

Ensuring your browsing is [100% isolated](#) from your corporate device and network is the only way to completely eliminate cyberthreats. By isolating a user's session on cloud infrastructure, clicking on a malicious link from a web search or visiting a malicious website doesn't put their organization at risk — the code from that website is never executed on the computer being used.

Instead, the user is merely seeing and interacting with a benign video display of the web code rendered in the cloud.

Anonymity through managed attribution

If you're under the assumption the dark web is anonymous, think again. There are still plenty of ways darknets track users and relay information to webmasters. To conceal your identity and the purpose of your dark web investigation, researchers need to manipulate the details of their digital fingerprint.

There are ways to achieve managed attribution without needing to create a fake persona or using a burner device. [Managed attribution](#) allows you to control what can be learned about you as you conduct your dark web investigation, providing anonymity without making you appear suspicious to algorithms or your subject.

Implications and risks of dark web research

Despite the benefits, many analysts may have reasonable doubts and concerns about accessing the dark web. While accessing it is not illegal per se, it is important to take steps to mitigate any risks or potential legal threats, especially when entering areas of the dark web where illegal activity is being conducted. Dark web research requires careful policies, auditing abilities and security measures before logging on.

Since darknet marketplaces and forums are often monitored by law enforcement, it can be difficult to distinguish between criminal actors and good-faith investigators. Avoid implications or attributions by having a plan. Be sure to document your plan of operation before gathering information or accessing a criminal forum. Maintain a complete record of activities while on the dark web and [have a policy](#) in place for “rules of engagement” when on sites where criminal activity may occur.

For more resources on the legality of dark web access, consult “[Legal Considerations](#) when Gathering Online Cyber Threat Intelligence and Purchasing Data from Illicit Sources” by the United States Department of Justice.

Other risks include the security of investigators and their machines. While the dark web's purpose is to provide some anonymity, there are still risks of malicious content or attribution when accessing. The safest way to gain access is by using a secure cyber-service product.

Legal and compliance considerations for dark web investigations

Work with your company's legal counsel to create a protocol for when and how to access the dark web. Create a detailed process to work as a guide for investigators. Be sure to document each step of your investigation and keep notes about how your activity is in line with the company policy. Purpose-built investigation platforms like [Silo](#) come with policy and audit features — as well as the needed security, managed attribution and workflow capabilities — baked in.

First, develop processes and procedures for your company and any employees who may be utilizing the dark web for their research, as seen below. Be sure to consult your company's legal counsel in this step, as they will have the best guidance for your circumstances and organization.

What may be seem obvious is still worth stating — even when communicating in forums where

criminal activity may be taking place, be sure to stay on the right side of the law. Again, documentation can go a long way in protecting you should any questions of legality arise. Luckily the same programs that protect your digital security can also help assist in this area.

Combining dark web and OSINT

Any good investigator may already find themselves among a sea of information. It's important to remember that the dark web is part of OSINT — there is plenty of information to be found on sites open to anyone looking; however, the webmaster may be looking back.

Investigators need to ensure security and control the details they disclose to sites in the course of their search. Without proper management of their digital fingerprint, adversaries and investigative targets could use disclosed details to uncover an analyst's identity and intent, spoil the investigation or seek retribution.

Creating a policy step-by-step

A formal, dark web access policy not only sets expectations and guidance on safe practices for end users, but also helps inform and alleviate concerns from other stakeholders in an organization who may only be familiar with the dangers of the darknet — and not its value to strategic cyber intel.

Of course, policy must be implemented to be effective. In this case, that means not only having the right technical tools for the job, but also the training, techniques and procedures to execute safely and effectively.

In 2020, the Department of Justice's Cybersecurity Unit issued guidance to the private sector on gathering cyberthreat intelligence in dark marketplaces. You can read the complete memo [here](#). The DOJ's recommendations are helpful for organizations to consider when crafting a dark web access policy and forming best practices laid out below.

(The memo and following discussion does not constitute legal advice. Authentic8 is prohibited from offering you legal advice. Please consult your attorney or your organization's attorney for legal advice before undertaking the activities considered here.)



Create "rules of engagement"

What are the reasons and situations that call for accessing the dark web? Is this a one-time access admittance or a daily visit? Knowing when, why, and under what circumstances dark web access is permitted can protect analysts and their direct supervisors from pushback and legal scrutiny.



Get approval from legal counsel

If you haven't talked to your lawyer, you're not ready to access the dark web. Getting counsel shores protection for the individual analyst and the company.



Engage with law enforcement

The problem with entering darknet forums where stolen credit card information is being shared, is you may look like someone trying to steal credit card information. In order to avoid potential implications, it can be beneficial to inform law enforcement of your security research.



Document plans and activity

Being able to audit every step to ensure legal compliance is crucial for a dark web initiative. Built-in audit assurance with monitoring and evidentiary chain-of-command is the best way for both companies and individual analysts to protect themselves from suspicion. Learn more about how audit-ready investigation platforms can bring reassurance to a cyberthreat workflow.

Keep these recommendations in mind when developing a dark web access policy to mitigate risk and protect your organization.

Here are the 4 things NOT to do on the dark web

So you're in? That's it, right? Wrong.

01

Don't access forums in an unauthorized manner

If you come across a forum on the dark web that requires a credential for access, do not attempt to evade the authorization requirements.

02

Don't assume someone else's identity

If you need a persona to access or interact on the dark web, don't use someone else's identity (name, photo, phone number, email, etc.) to do so without their consent. Posing as someone else can not only create legal trouble for you, it also puts the other person at risk of receiving targeted malicious activity from criminal actors whom you've interacted with.

The best approach for the dark web is to create an entirely fake persona that cannot be connected to you or your organization.

Learn how to control your digital fingerprint to match browser and device details to your online identity and [avoid tipping off investigative targets](#).

03

Don't research without a plan

This is important for two reasons. First, having a set of written guidelines will help keep your research efforts focused and within the bounds of your organization's risk appetite. Secondly, documented plans, policies and procedures are helpful in the event you or your organization comes under investigation from law enforcement.

04

Don't put your corporate network at risk

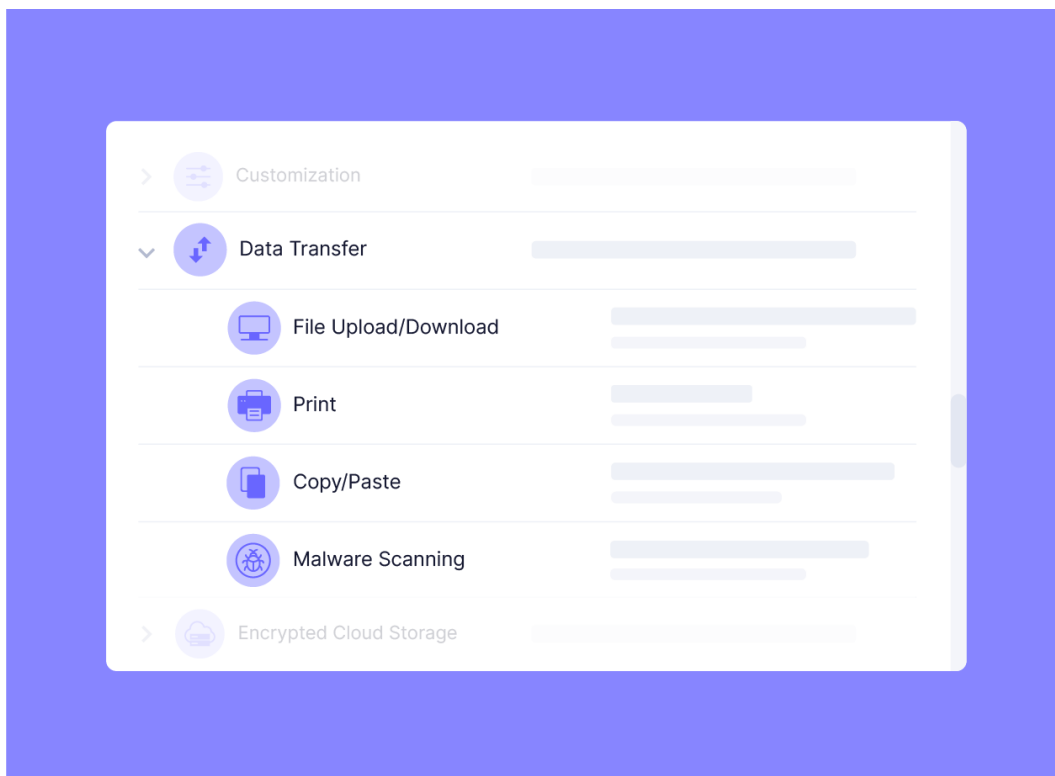
This one is up there with the "goes without saying" category of what not to do on the dark web. But you can never be too careful, especially when it comes to activities that pose both technical and operational risks like dark web investigations.

Learn more about isolated, cloud-based browsing that provides [100-percent separation between the web and your device](#)

Play it smart

When conducting a dark web investigation where criminal activity is taking place, there are [several risks to consider](#). Make sure legal challenges for your team aren't among them by creating a [best practices protocol](#). These simple pieces of advice can go a long way toward avoiding legal pushback, but as always, consult your legal and security departments to create an official policy.

To protect yourself, use a program to document your activity on the dark web, such as [Silo](#). In addition to managed attribution for safe browsing, Silo protects investigators and their employers in an audit.



Learn how Silo protects, masks and
accelerates cyberthreat insights.

[Book a demo today](#)