What is Dark Web? Who uses it? The potential dangers of Dark Web and warnings

What is Dark Web? What content does Dark Web contain? It must be a question that makes many people feel curious. Read this article to learn more about Dark Web, the potential dangers of the ice block's iceberg and the Dark Web approach.

What is Dark Web? What content does Dark Web contain? It must be a question that makes many people feel curious. Read this article to learn more about Dark Web, the potential dangers of the "iceberg" of the Internet block and the notices of the Dark Web approach.

In December 2014, British Prime Minister David Cameron announced a new police and intelligence agency to monitor Dark Web (according to The Independent's report). "The Dark Net is the next aspect of the problem when pedophiles and extremists are sharing images, but not using Internet components as they normally do," Cameron said.

Independent web consultant Mark Stockley agrees with this statement, in a statement with Naked Security, saying that Dark Web attracts people who want to participate in illegal areas such as robbery, prostitution, and trade. weapons, terrorism, distribution of pedophile books, . On the International Business Times, author Charles Paladin and Jeff Stone said electronic goods, murderers under contracts, weapons, passports , Fake IDs and hiring hackers are always available and abundance on Dark Web, in addition to illegal drugs and pornography, pedophile books.

For most of the public, the Ross Ulbright arrest in 2013, known as Dread Pirate Roberts, the founder of the Dark Web called Silk Road - was the first evidence of hidden web, Dark Web. Silk Road is one of many websites beyond the ability to search for common web browsers such as Google Chrome, Firefox, Safari, . Although most products sold on Silk Road are illegal drugs, but The success of the website has led to other Dark Webs such as the Sheep Marketplace and Black Market Reloaded with restrictions on products and services offered for sale.

As a result of the lack of legal regulations, David J. Hickton, an American lawyer in the western district of Pennysylvania, called Dark Web the "Wild West Region of the Internet" in an interview with Rolling Stone. IBM's Managed Security Services Threat Research team calls hidden sites a place for drugs, weapons, stolen data and anything else criminals need to buy and sell, they also advise their customers that Dark Web is not an area to visit, for whatever reason.

So in the end what is Dark Web, Black Web? Why is the government and security agencies so "hostile" to it? To better understand these issues, we first need to understand the structure of the Web.

Web stratum:

The term Internet and World Wide Web are often used interchangeably, but in fact they are not one. The Internet refers to an extensive network of networks, millions of computers connecting around the world, where any computer can communicate with each other, provided they are connected to the Internet. The World Wide Web is an information sharing model, built on the Internet, using HTTP protocols, browsers like Chrome, Firefox and websites to share information. The web is a huge part of the Internet but not the only component. For example, email, messages are not part of the web but are part of the Internet.

Some analyzes have compared the web to the ocean, a large range of unidentified locations and are not accessible by most users. Like the ocean, most of the web is "invisible" to ordinary users, relying on search engines.

Web on the surface:

According to PC Magazine, surface web is a web part available to the public, complete with links indexed by search engines. BrightPlanet, a smart web service, defines web surfaces that contain only indexed web pages and can be searched by popular search engines like Google, Bing, and Yahoo. Sometimes, they are also called tangible web. The surface web usually includes websites with domain names ending in .com, .org, .net, .vn or similar variations. The content of these websites does not require any special configuration to access. This part of the web is most familiar to all users and it is constantly expanding:

1. 4.62 billion pages indexed by Google (as of May 2016, according to WorldWideWebSize)
2. Nearly 148 million unique domains or websites (according to Domain Tools estimates)
3. More than 3.5 billion Google searches include more than 20 billion pages per day (according to Internet Live Stats reports).

Although the numbers may sound big, the surface web contains less than 5% of the entire Internet. According to CNNMoney, users often surf the web "floating on a vast information ocean," which contains tens of trillions of unreachable web pages, un indexed websites, including everything. from boring statistics to the sale of parts of the human body.

Deep Web

If you continue the Internet wallet is an ocean, the durable part under the web surface is Deep Wep.

Most websites known as Deep Web, sometimes called hidden web, invisible web, refer to all digital content that cannot be found with a search engine. It includes email in Gmail accounts, online bank statements, intranets, direct messages via Twitter, images marked privately when uploaded to Facebook. Government, researchers and raw data storage companies cannot reach the public. This content is stored on dynamic web pages (built on query information) and locked pages, individual pages that are not linked to the outside. According to Trend Micro, an important part of the Deep Web is dedicated to personal or political blogs, news sites, discussion forums, religious websites and even radio stations.

An article in Electronic Publishing estimates that, in 2001, the Deep Web contained nearly 550 billion personal documents, 550 times more than the surface web document. Although hidden from regular search engines, 95% of the content on the Deep Web can be accessed by users, although custom tools such as "Direct query engine" must be used by BrightPlanet.

People often use the Deep Web content without realizing it. Much of the information users find on the Deep Web will be generated automatically through a website they visit on the surface web and is a unique page that is seen only when the user requests it.

For example: Travel sites such as Hotwire and Expedia provide software that allows searchers to directly access aviation databases and hotels, through the search box, such as the name of the destination. The content of most government databases is also achieved in the same way through specialized search engines.

Thus, the Deep Web is not really all bad, horrible things like we still imagine. But there is still one floor below the Deep Web, which is Dark Web.

Read more: Deep Web: The sink of the Internet iceberg

Dark Web

Each device connected to the Internet has a unique IP (Internet protocol) address. A person's name and physical address can be obtained through an Internet service provider with legal permission, while IP allows anyone to determine the location of the connected computer. Therefore, stakeholders will easily find a specific Internet user.

With an aim to remain anonymous - especially when the government seeks to protect sensitive information and intelligence networks - has led to the development and development of The Onion Router (Tor) by laboratory staff. US Navy research experience created. The name Onion (onion) comes from the fact that you have to peel off many "shells" to find the true identity of the user.
Tor, released free to users in 2004, provides privacy by encrypting and navigating traffic through a "virtual tunnel" series, delivering traffic. translate through multiple random computers on the Internet, so no computer connects users to their premises or destinations. Unlike surface web pages (ending in .com, .org, .net or similar variants), Tor pages end in .onion and can only be opened with Tor software.

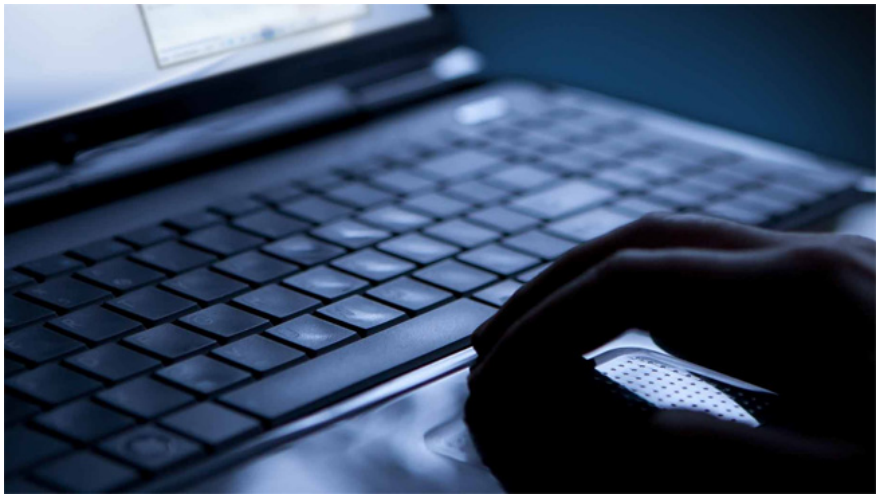
Tor also uses hidden servers that can only be accessed with another Tor address to make identification even more complicated. According to Tor's website, the network is an effective deception tool, allowing users to access content, blocked destinations.

According to Cryptorials, other free anonymous peer-to-peer networks will be layer-coded including I2P (Invisible Internet Project), Freenet, GNUNet, FAI (Free Anonymous Internet), and ZeroNet. Using such networks to access the Internet has created Dark Web, part of the site is not indexed and has content protected by firewalls, hidden IP addresses and encryption layers.

Dark Web users:

Recognize the benefits of online anonymity, criminals and terrorists as well as free politicians who quickly exploit new software. The number of Dark Web users has increased, adding some new Dark Web users including:

1. **Those who fight freely to oppose oppression:** Many Tor users are an important component in Arab Spring 2010/2011. People in China and Russia use it to cross the Great Wall firewall in their country to reach blocked foreign websites. Dr. Watson, professor of information and communications law at Queen Mary University in London, warned in the Motherboard that visitors to the Dark Web must always remember "terrorists are free fighters. ". It is not surprising that ISIS uses Dark Web to promote their views, as SITE reported.
2. **People denouncing sensitive content can be retaliated:** According to Wired, The New Yorker is running the Strongbox - a Dark Web - so whistleblowers can leave documents and messages safely. Dead Man Zero provides those who denounce a system capable of automatically publishing and publicizing their secrets if they are injured, killed or arrested. If a user does not regularly log in to the site at predefined intervals, the information will be automatically released to a set of email addresses and user-set alerts.
3. **Victims of abuse and discrimination:** Dark Web's anonymity allows individuals to share their private stories and comfort those who share corn scenes without fear of their private information being revealed. . Websites for rape victims, transgender people and other abused groups, regardless of religion, politics or culture.
4. **Corporations and governments:** Dark Web is a safe place to keep and limit access to sensitive information, whether it be a company profile or political information. Law enforcement forces use Dark Web to hide their identity while accessing websites, creating fake pages to trick criminals.



In principle, many Internet users have complained about corporations accessing personal information from their online activities. Moreover, many people object to government agencies, the national security agency collects data from their personal calls, messages and emails. According to Peter Yeung, an author on Motherboard, Dark Weeb brings comfort, ideals and a community together with illegal, immoral and bizarre.

A 2016 Intelliagg report and US Counterpart, DARKSUM, suggested that Dark Web is much smaller than originally expected - about 30,000 sites - and that half of their content is legitimate (according to British law). and the United States). However, illegal content in Dark Web includes full criminal activities, from pornography to retailing of drugs, weapons and violence. Because Dark Web visitors are anonymous, it is not possible to determine the number of users accessing these websites, whether legal or illegal.

Warning when accessing Dark Web:

For ordinary Internet users, Dark Web can be a dangerous place. Browsing hidden websites without precautions is like trying to be safe when traveling through a village infected with Ebola (an extremely dangerous disease). Anonymous access often encourages illegal activities including the sale of illegal drugs, weapons, IDs and fake passports, stolen electronic devices. Web sites in Dark Web advertise services for hackers, map makers and even killers.

At the same time, many Dark Web sites are rogue to attract unsecured victims or enforced by law enforcement agencies to identify and track actual and potential criminal activity. Because anonymity exists on both sides, users can never be 100% sure about the intent of the person they are interacting with.

Malware:

The ability to access Dark Web may suffer from malware infection is very high, unless precautions are taken. According to a Motherboard article, random visitors to Dark Weeb may accidentally let their computer suffer from the following programs:

1. **Vawtrack:** Designed to access the victim's financial account.
2. **Skynet:** Used to steal bitcoins (a virtual currency) or engage in DDos (denial of service) attacks on other websites with the victim's computer.
3. **Nionspy:** Can record keystrokes, steal documents, records, videos, and use infected computers.

Government oversight:

In addition to the dangers of malware, a Dark Web visitor to political websites should pay attention to attracting the attention of government agencies and becoming the main surveillance object. awake, though not desirable. In Rolling Stone, Jeremy Gillula, an Electronic Frontier Foundation technology officer (EFF), said: *"In some countries, access to political websites on democracy can cause you to be abandoned. That is the most powerful reason why Tor must exist "* . Visitors to Tor websites involving illegal goods or expressing opposing political views in the eyes of the government should know that Dark Web is regularly monitored and penetrated by network police, many visitors and Website owners were exposed, including 3 versions of Silk Road.

These software to make Dark Web more transparent are constantly being developed, just as criminals try to develop software to hide their activity. Government agencies and law enforcement forces can now use Memex, a search engine recently developed by DARPA and specifically designed for Dark Web, to find websites in it as well. store data for later analysis. According to Scientific American, law enforcement agencies recognize software by detecting and finding trafficking activities in the United States and other countries.

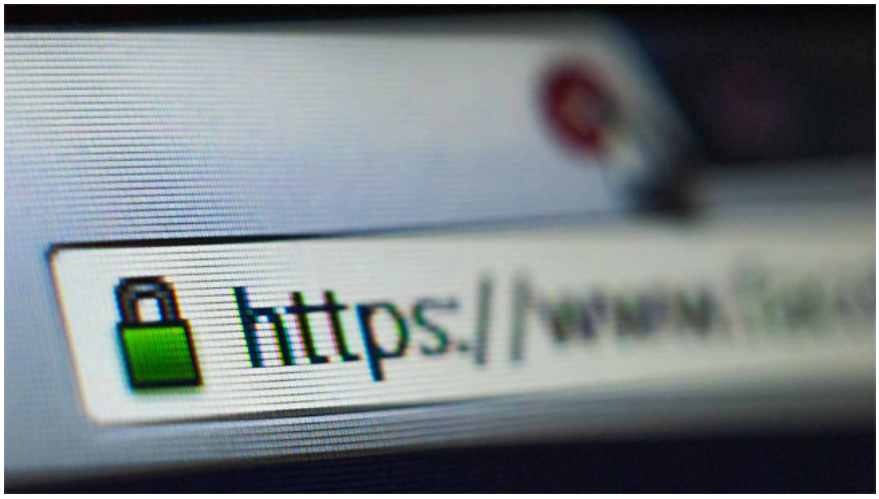
Practice to browse the web:

Many web experts claim that web surfaces - the Internet that most users visit - are no different from Dark Web, meaning that it also has many similar dangers. There are thousands of websites related to violence and racism. Advertisers collect and sell personal data, as well as your browsing history. Malware can arise from a surface web site, no different from Dark Web and the government still monitors Internet traffic as well as messages sent over the network.

Therefore, many Internet experts recommend that when you access the web on all Internet levels, you should do the following:

1. **If someone is unusually friendly to you,** ask yourself why. Try to be aware of the consequences that can occur when interacting on the web and trusting your instincts.
2. **Identity protection:** Create a free email address. Do not use any usernames you have used before with your email. Never use your real name or provide personal data unless you are working on a trusted website that uses encryption. Do not use the same password for online accounts.
3. **Avoid using personal credit cards:** Instead of using a credit card that can be accessed directly to you and displaying financial information, use a prepaid card, a one-time purchase card for direct transactions. online. If you need to use a credit card, make sure the website is secure by checking the website address. The address should start with "https: //" and not "http:///". The "s" stands for SSL and it means that the data sent and received through this site is encrypted.
4. **Keep track of financial accounts with online alerts:** Most banks and credit card companies allow you to set up unusual alerts whenever you receive money, pay or take money from account.
5. **Do not download, open files online especially from Dark Web.** If you have to download something, or scan it with antivirus software (or a free service like VirusTotal) before opening it to detect viruses, worms, trojans and other malicious software. Don't click on suspicious links, especially ads about illegal activities.
6. **Always update your web browser.** Customize browser settings for better security, the default browser configuration is not set to ensure the best security. For example, set your security level to High / High even if this will disable some features such as ActiveX and Java.

More reference: Safe web browsing



Last words:

People often describe Dark Web as a hidden network, only to serve the most vicious, insane and lustful desires of visitors. According to Fortune, things that users can buy on Dark Web are terrible. Law enforcers have to say that the Dark Web makes their work much more difficult because people can buy everything from tigers, grenades to banned substances.

But on the other hand, Internet privacy advocates claim that Dark Web is essential for freedom.

Whether you agree with these points of view or not, if you intend to access the Dark Web, consider carefully the potential risks that those sites may bring.

You finished reading the article "**What is Dark Web? Who uses it? The potential dangers of Dark Web and warnings**" edited by the **TipsMake** team. We hope this article has provided you with many useful tech tips and tricks. You can search for similar articles on tips and guides. Thank you for reading and for following us regularly.
