# Deep web: the dark side of Internet

It is the encrypted online content that is not indexed by conventional search engine. It is also called dark net. It is the part of deep web. Most deep web contents consists of private files hosted on Dropbox and its competitors or subscriber-only database rather than anything illegal. Specific browsers like Tor-Browser, are required to reach the Dark Web. It provides better privacy. Many dark websites simply provides standard web services with more secrecy, which benefits political dissidents and people trying to keep medical conditions private. Unfortunately, online marketplaces for drugs, exchanges for stolen data, and other illegal online activity get more attention.

## The Dark Web

The Dark Web(also called The Dark Net) is a network within the Internet which is only accessible using certain software and protocols.
The Dark Web has many names, for example *Tor Network* or *Onion Router*.
Anyone can access to the Dark Web by simply downloading software for it. A popular and very much used browser is the Tor Project's Tor Browser
This is just like any other browser such as Google Chrome or Microsoft Edge, except it can also access special website addresses which ends in .onion instead of .com and such.
Any traffic sent through Tor Browser is automatically anonymized and encrypted via many different hosts. The browser also has built-in protection for many kinds of tracking and de-anonymization features.

Accessing The Dark Web
You can access many fun and interesting websites through this browser, also many which co-exist on the regular Internet. For example if you access the following URL's in Tor Browser, your communications will be fully encrypted and anonymized inside the Dark Web:

- Facebook - http://www.facebookcorewwwi.onion/
- DuckDuckGo Search Engine - http://3g2upl4pq6kufc4m.onion/
- The American CIA ("Central Intelligence Agency") - http://ciadotgov4sjwlzihbbgxnqg3xiyrg7so2r2o3lt5wz5ypk4sxyjstad.onion
- The Hidden Wiki, a collection of links and places to explore - http://zqktlwiuavvvqqt4ybvgvi7tyo4hjl5xgfuvpdf6otjiycgwqbym2qad.onion/wiki/index.php/Main_Page

Because of the built-in anonymizing features and encryption, the Dark Net is also host of many criminal websites, marketplaces and networks.

## Benefits of using the dark web

The dark web has a bad rap, but there are benefits to using it. For example, dissidents who fear political prosecution from their governments might use the dark web to communicate with each other. As many as **70.79% of users** claim to use the Tor browser for anonymity, 62.28% said they use it

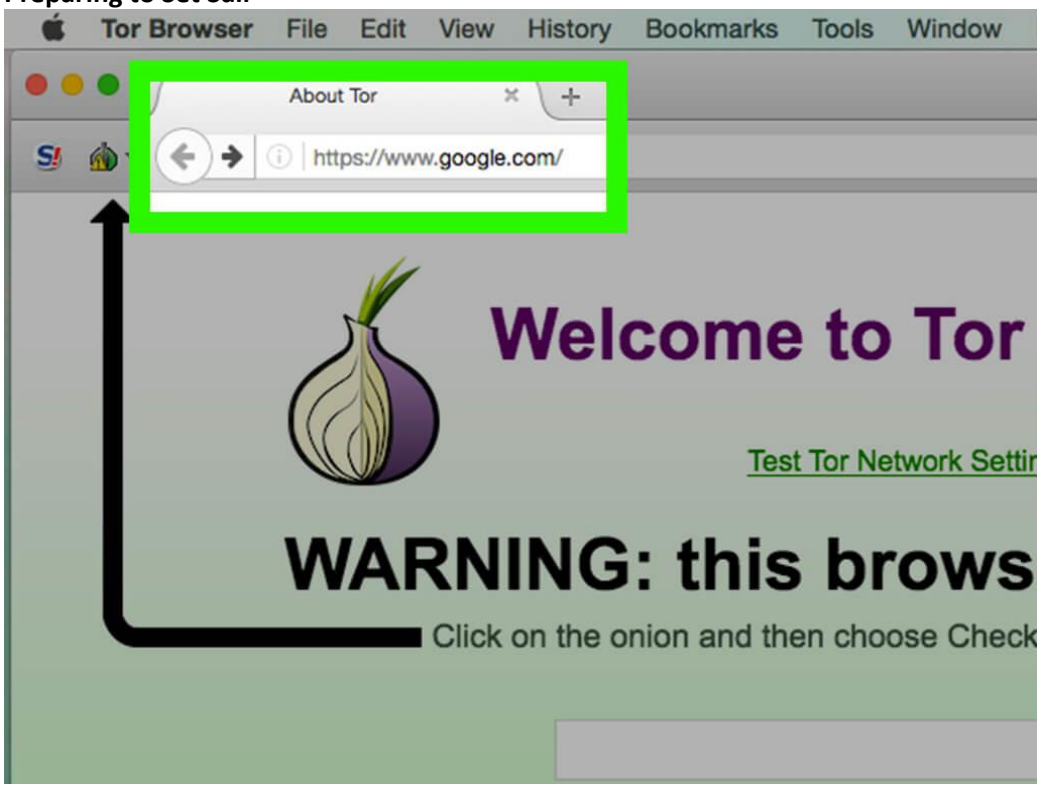
for additional security, and 27.07% used it out of curiosity about the dark web.
Because there's no way to track users, communicating over the dark web ensures the utmost security and privacy. This is integral for people like:

- Journalists and whistle-blowers working together to expose corruption at corporations and government agencies
- Citizens of oppressive or authoritarian governments needing to access news sources critical of their governments that have been blocked by traditional web browsers
- Political protestors wanting to remain anonymous while protesting the actions of their government
- Users seeking medical advice without revealing their identity
- Journalists interviewing sources who must **remain anonymous**

**More on Tor Onions**

The Tor Onion Browser is essential for accessing the dark web, designed for user anonymity. Unlike the regular internet, the dark web doesn't use standard URLs or search engines. Instead, sites have complex .onion addresses, making them difficult to find without the exact URL.
This part of the internet is notorious for illegal activities, facilitated by the anonymity it offers. Crimes range from data theft and selling illegal goods for cryptocurrencies to human trafficking and more severe offenses.
Understanding the dark web, including safe navigation with the Tor Browser, is crucial for anyone interested in internet privacy and security issues, highlighting the balance between anonymity and the potential for misuse.

**Preparing to Set Sail**



Cyber Crime and its Classifications

Classification of Cyber Crimes

(1) Cybercrime against Individual
(2) Cybercrime against Property
(3) Cybercrime against Organization
(4) Cybercrime against Society

**(1) Against Individuals**

(i) Email spoofing : A spoofed email is one in which the e-mail header is forged so that the mail appears to originate from one source but actually has been sent from another source.

(ii) Spamming : Spamming means sending multiple copies of unsolicited mails or mass e-mails such as chain letters.

(iii) Cyber Defamation : This occurs when defamation takes place with the help of computers and/or the Internet. E.g. someone publishes defamatory matter about someone on a website or sends e-mails containing defamatory information.

(iv) Harassment & Cyber stalking : Cyber Stalking Means following an individual's activity over internet. It can be done with the help of many protocols available such as e- mail, chat rooms, user net groups.

**(2) Against Property**

(i) Credit Card Fraud : As the name suggests, this is a fraud that happens by the use of a credit card. This generally happens if someone gets to know the card number or the card gets stolen.

(ii) Intellectual Property crimes : These include Software piracy: Illegal copying of programs, distribution of copies of software. Copyright infringement: Using copyrighted material without proper permission. Trademarks violations: Using trademarks and associated rights without permission of the actual holder. Theft of computer source code: Stealing, destroying or misusing the source code of a computer.

(iii) Internet time theft : This happens by the usage of the Internet hours by an unauthorized person which is actually paid by another person.

**(3) Against Organisations**

i) Unauthorized Accessing of Computer: Accessing the computer/network without permission from the

owner. It can be of 2 forms: a) Changing/deleting data: Unauthorized changing of data. b) Computer voyeur: The criminal reads or copies confidential or proprietary information, but the data is neither deleted nor changed.

(ii) Denial Of Service : When Internet server is flooded with continuous bogus requests so as to denying legitimate users to use the server or to crash the server.

(iii) Computer contamination / Virus attack : A computer virus is a computer program that can infect other computer programs by modifying them in such a way as to include a (possibly evolved) copy of it. Viruses can be file infecting or affecting boot sector of the computer. Worms, unlike viruses do not need the host to attach themselves to.

(iv) Email Bombing : Sending large numbers of mails to the individual or company or mail servers thereby ultimately resulting into crashing.

(v) Salami Attack : When negligible amounts are removed & accumulated in to something larger. These attacks are used for the commission of financial crimes.

(vi) Logic Bomb : It is an event dependent program. As soon as the designated event occurs, it crashes the computer, release a virus or any other harmful possibilities.

(vii) Trojan Horse : This is an unauthorized program which functions from inside what seems to be an authorized program, thereby concealing what it is actually doing.

(viii) Data diddling : This kind of an attack involves altering raw data just before it is processed by a computer and then changing it back after the processing is completed.

**(4) Against Society**

(i) Forgery : Currency notes, revenue stamps, mark sheets etc. can be forged using computers and high quality scanners and printers.

(ii) Cyber Terrorism : Use of computer resources to intimidate or coerce people and carry out the activities of terrorism.

(iii) Web Jacking : Hackers gain access and control over the website of another, even they change the content of website for fulfilling political objective or for money.

## Phishing

Cybercrime is defined in simple words as a crime that is done online. Here, the medium used to commit crime digitally is the computer, network, internet, or any electronic device. The main targets of cybercrime are users of the system, websites, company defamation, gaining money, etc.

Some of the activities of cyber-criminals are listed below:

- Spread viruses and malware to cause harm to computers and sensitive data.
- Attacks a computer to reach the target or victim's computer via network.
- Hack the victim's system and steals confidential information from the user's data.
- Gaining unauthorized access to user accounts.
- Paving ways for online scams and frauds.
- Generate profit by selling or locking crucial data.

As newer technologies are rolling out, cybercrimes are also increasing. Cybercrime covers attacks like illegal downloading, credit card fraud, cyberbullying, **phishing**, creation, and distribution of viruses, spam, etc.

**Phishing**

Phishing is one type of cyber attack. Phishing got its name from "**phish**" meaning fish. It's a common phenomenon to put bait for the fish to get trapped. Similarly, phishing works. It is an unethical way to dupe the user or victim to click on harmful sites. The attacker crafts the harmful site in such a way that the victim feels it to be an authentic site, thus falling prey to it. The most common mode of phishing is by sending spam emails that appear to be authentic and thus, taking away all credentials from the victim. The main motive of the attacker behind phishing is to gain confidential information like

- Password
- Credit card details
- Social security numbers
- Date of birth

The attacker uses this information to further target the user and impersonate the user and cause data theft. The most common type of phishing attack happens through email. Phishing victims are tricked into revealing information that they think should be kept private. The original logo of the email is used to make the user believe that it is indeed the original email. But if we carefully look into the details, we will find that the URL or web address is not authentic. Let's understand this concept with the help of an example:

***Phishing***

In this example, most people believe it's YouTube just by looking at the red icon. So, thinking of YouTube as a secure platform, the users click on the extension without being suspicious about it. But if we look carefully, we can see the URL is supertube.com and not youtube.com. Secondly, YouTube never asks to add extensions for watching any video. The third thing is the extension name itself is

weird enough to raise doubt about its credibility.

**How Does Phishing Occur?**

Below mentioned are the ways through which Phishing generally occurs. Upon using any of the techniques mentioned below, the user can lead to Phishing Attacks.

- **Clicking on an unknown file or attachment:** Here, the attacker deliberately sends a mysterious file to the victim, as the victim opens the file, either malware is injected into his system or it prompts the user to enter confidential data.
- **Using an open or free wifi hotspot:** This is a very simple way to get confidential information from the user by luring him by giving him free **wifi**. The wifi owner can control the user's data without the user knowing it.
- **Responding to social media requests:** This commonly includes social engineering. Accepting unknown friend requests and then, by mistake, leaking secret data are the most common mistake made by naive users.
- **Clicking on unauthenticated links or ads:** Unauthenticated links have been deliberately crafted that lead to a phished website that tricks the user into typing confidential data.

**Types of Phishing Attacks**

There are several types of Phishing Attacks, some of them are mentioned below. Below mentioned attacks are very common and mostly used by the attackers.

- **Email Phishing:** The most common type where users are tricked into clicking unverified spam emails and leaking secret data. Hackers impersonate a legitimate identity and send emails to mass victims. Generally, the goal of the attacker is to get personal details like bank details, credit card numbers, user IDs, and passwords of any online shopping website, installing malware, etc. After getting the personal information, they use this information to steal money from the user's account or harm the target system, etc.
- **Spear Phishing:** In spear phishing of phishing attack, a particular user(organization or individual) is targeted. In this method, the attacker first gets the full information of the target and then sends malicious emails to his/her inbox to trap him into typing confidential data. For example, the attacker targets someone(let's assume an employee from the finance department of some organization). Then the attacker pretends to be like the manager of that employee and then requests personal information or transfers a large sum of money. It is the most successful attack.
- **Whaling:** Whaling is just like spear-phishing but the main target is the head of the company, like the CEO, CFO, etc. a pressurized email is sent to such executives so that they don't have

much time to think, therefore falling prey to phishing.

- **Smishing:** In this type of phishing attack, the medium of phishing attack is SMS. Smishing works similarly to email phishing. SMS texts are sent to victims containing links to phished websites or invite the victims to call a phone number or to contact the sender using the given email. The victim is then invited to enter their personal information like bank details, credit card information, user id/ password, etc. Then using this information the attacker harms the victim.
- **Vishing:** Vishing is also known as voice phishing. In this method, the attacker calls the victim using modern caller id spoofing to convince the victim that the call is from a trusted source. Attackers also use IVR to make it difficult for legal authorities to trace the attacker. It is generally used to steal credit card numbers or confidential data from the victim.
- **Clone Phishing:** Clone Phishing this type of phishing attack, the attacker copies the email messages that were sent from a trusted source and then alters the information by adding a link that redirects the victim to a malicious or fake website. Now the attacker sends this mail to a larger number of users and then waits to watch who clicks on the attachment that was sent in the email. It spreads through the contacts of the user who has clicked on the attachment.

**Impact of Phishing**

These are the impacts on the user upon affecting the Phishing Attacks. Each person has their own impact after getting into Phishing Attacks, but these are some of the common impacts that happen to the majority of people.

- **Financial Loss:** Phishing attacks often target financial information, such as credit card numbers and bank account login credentials. This information can be used to steal money or make unauthorized purchases, leading to significant financial losses.
- **Identity Theft:** Phishing attacks can also steal personal information, such as Social Security numbers and date of birth, which can be used to steal an individual's identity and cause long-term harm.
- **Damage to Reputation:** Organizations that fall victim to phishing attacks can suffer damage to their reputation, as customers and clients may lose trust in the company's ability to protect their information.
- **Disruption to Business Operations:** Phishing attacks can also cause significant disruption to business operations, as employees may have their email accounts or computers compromised, leading to lost productivity and data.

- **Spread of Malware:** Phishing attacks often use attachments or links to deliver malware, which can infect a victim's computer or network and cause further harm.

**Signs of Phishing**

It is very much important to be able to identify the signs of a phishing attack in order to protect against its harmful effects. These signs help the user to protect user data and information from hackers. Here are some signs to look out for include:

- **Suspicious email addresses:** Phishing emails often use fake email addresses that appear to be from a trusted source, but are actually controlled by the attacker. Check the email address carefully and look for slight variations or misspellings that may indicate a fake address.
- **Urgent requests for personal information:** Phishing attacks often try to create a sense of urgency in order to trick victims into providing personal information quickly. Be cautious of emails or messages that ask for personal information and make sure to verify the authenticity of the request before providing any information.
- **Poor grammar and spelling:** Phishing attacks are often created quickly and carelessly, and may contain poor grammar and spelling errors. These mistakes can indicate that the email or message is not legitimate.
- **Requests for sensitive information:** Phishing attacks often try to steal sensitive information, such as login credentials and financial information. Be cautious of emails or messages that ask for sensitive information and verify the authenticity of the re
- quest before providing any information.
- **Unusual links or attachments:** Phishing attacks often use links or attachments to deliver malware or redirect victims to fake websites. Be cautious of links or attachments in emails or messages, especially from unknown or untrusted sources.
- **Strange URLs:** Phishing attacks often use fake websites that look similar to the real ones, but have slightly different URLs. Look for strange URLs or slight variations in the URL that may indicate a fake website.

**How To Stay Protected Against Phishing?**

Until now, we have seen how a user becomes so vulnerable due to phishing. But with proper precautions, one can avoid such scams. Below are the ways listed to protect users against phishing attacks:

- **Authorized Source:** Download software from authorized sources only where you have trust.
- **Confidentiality:** Never share your private details with unknown links and keep your data safe

from hackers.

- **Check URL:** Always check the URL of websites to prevent any such attack. it will help you not get trapped in Phishing Attacks.
- **Avoid replying to suspicious things:** If you receive an email from a known source but that email looks suspicious, then contact the source with a new email rather than using the reply option.
- **Phishing Detection Tool:** Use phishing-detecting tools to monitor the websites that are crafted and contain unauthentic content.
- **Try to avoid free wifi:** Avoid using free Wifi, it will lead to threats and Phishing.
- **Keep your system updated:** It's better to keep your system always updated to protect from different types of Phishing Attacks.
- **Keep the firewall of the system ON:** Keeping ON the firewalls helps you in filtering ambiguous and suspicious data and only authenticated data will reach to you.

**How To Distinguish between a Fake Website and a Real Website?**

It is very important nowadays to protect yourself from fake websites and real websites. Here are some of the ways mentioned through which you can identify which websites are real and which ones are fake. To distinguish between a fake website and a real website always remember the following points:

- **Check the URL of the website:** A good and legal website always uses a secure medium to protect yourself from online threats. So, when you first see a website link, always check the beginning of the website. That means if a website is started with https:// then the website is secure because https:// s denotes secure, which means the website uses encryption to transfer data, protecting it from hackers. If a website uses http:// then the website is not guaranteed to be safe. So, it is advised not to visit HTTP websites as they are not secure.
- **Check the domain name of the website:** The attackers generally create a website whose address mimic of large brands or companies like www.amazon.com/order_id=23. If we look closely, we can see that it's a fake website as the spelling of Amazon is wrong, that is amazon is written. So it's a phished website. So be careful with such types of websites.
- **Look for site design:** If you open a website from the link, then pay attention to the design of the site. Although the attacker tries to imitate the original one as much as possible, they still lack in some places. So, if you see something off, then that might be a sign of a fake website. For example, www.sugarcube.com/facebook, when we open this URL the page open is cloned to the actual Facebook page but it is a fake website. The original link to Facebook is www.facebook.com.

- **Check for the available web pages:** A fake website does not contain the entire web pages that are present in the original website. So when you encounter fake websites, then open the option(links) present on that website. If they only display a login page, then the website is fake.

**Anti-Phishing Tools**

Well, it's essential to use Anti-Phishing tools to detect phishing attacks. Here are some of the most popular and effective anti-phishing tools available:

- **Anti-Phishing Domain Advisor (APDA):** A browser extension that warns users when they visit a phishing website. It uses a database of known phishing sites and provides real-time protection against new threats.
- **PhishTank:** A community-driven website that collects and verifies reports of phishing attacks. Users can submit phishing reports and check the status of suspicious websites.
- **Webroot Anti-Phishing:** A browser extension that uses machine learning algorithms to identify and block phishing websites. It provides real-time protection and integrates with other security tools.
- **Malwarebytes Anti-Phishing:** A security tool that protects against phishing attacks by detecting and blocking suspicious websites. It uses a combination of machine learning and signature-based detection to provide real-time protection.
- **Kaspersky Anti-Phishing:** A browser extension that provides real-time protection against phishing attacks. It uses a database of known phishing sites and integrates with other security tools to provide comprehensive protection.

# Spamming

**What is Spamming?**

Spamming in cybersecurity is the act of sending unsolicited messages, often with commercial or malicious purposes, to a large number of people. E-mails, texts & instant messages can be used as forms of communication. Spamming can be used to spread malware, steal personal information, or promote scams & phishing schemes. It can also be used to overload networks & servers, causing them to crash. It is important for individuals to be cautious when opening emails or messages from unknown senders, & to avoid clicking on suspicious links or providing personal information.

**How Spamming Works?**

Typically, spamming is a part of online marketing strategy that aims to attract potential customers by sending emails & texts to a massive number of email addresses & phone numbers. The process of spamming starts by acquiring email addresses & phone numbers, which can be done through various means such as purchasing email lists or using software to extract them from websites.

Once the email addresses & phone numbers are obtained, the spammer creates an email or a message, often with a catchy subject line that could interest the recipient, & includes a link or attachment that leads to a scam website or malware download.

The success of spamming relies on the sheer volume of emails being sent. Even if only a small percentage of recipients fall for the scam, it can still yield significant gains for the spammer. Moreover, spamming can be done on a massive scale with minimal cost & effort, making it a popular tactic among cybercriminals.

What is Spamming is an important question as it creates a problem for many people & businesses. Spamming is not only harmful to individuals but also affects an organization's productivity, as employee's time is wasted sorting through irrelevant emails & more. Therefore, it is crucial to be careful while opening an email or a message from an unknown sender to protect your digital security & avoid being a victim of spamming.

**Types of Spam in Cybersecurity**

With the evolution of technology, cybercriminals have adopted various tactics to exploit the vulnerabilities of individuals & organizations. Through spam messages, cybercriminals typically reach their targets.

What is spam messages, you ask? In simple terms, spam messages are unsolicited & unwanted messages sent to a large group of people with the intent to deceive, steal information, or spread malware. Spam messages can take different forms. Let us see the various types of spamming in cyber security:

1. **Email Spam**: This type of spam is sent through email. Cybercriminals send phishing emails that appear to be from legitimate sources, but contain malicious links or requests for personal information.
2. **Instant Messaging Spam**: Instant messaging spam is sent through messaging platforms such as WhatsApp & Telegram. They often contain tempting offers such as job openings, contests or lottery wins that are too good to be true.
3. **Social Media Spam**: There are several types of social media spam, like fake profiles, fake likes, spam comments, & malicious links that can trick users into downloading malware.
4. **Comment Spam**: Often found in the comments section of blogs, comment spam are mostly

automated messages that can include unrelated links or promotional content.

5. **SMS Spam**: This type of spam messages are sent in bulk to mobile phones. They may contain fake lottery wins, offers for free stuff or requests to click a link that will download malware to the phone.
6. **Voice Call Spam**: Cybercriminals use robocalls to make unsolicited calls to mobile or landline phones to promote products, spread scams or demand payments.
7. **Forum & Blog Spam**: Spam comments on blogs & forums are mostly irrelevant, & could contain links that lead to malware downloads.

**Impact of Spamming**

Cybercriminals use spamming as a tool to deceive people into clicking on links or downloading malicious attachments. What is spam, & how is it harmful? Spamming can be defined as the unsolicited & unwanted content sent electronically to a large number of people. This content can be malicious, irrelevant, or inappropriate & is often used as a tool for cybercriminals to gain access to personal information, identities & commit cyber crimes.

One of the major impacts of spamming in cybersecurity is that it can cause network congestion, clog up servers, & reduce internet speed. It can also consume a lot of storage space on your devices, making them slow & less efficient.

Spam also plays a vital role in phishing attacks, where cybercriminals send fraudulent messages posing as legitimate messages coming from banks, social media, & e-commerce websites. They may ask for sensitive information, from login credentials, credit card numbers, to other financial information. Furthermore, spamming can result in the distribution of malware-infected attachments, such as Trojan & ransomware that encrypt your devices & demand money to unlock them. This malware can also facilitate cyber espionage, leading to the theft of valuable intellectual property or state secrets. In addition, it can lead to reputational damage & loss of trust in the organization that has been compromised.

All in all, People should be well-educated about what is spamming in cyber security as it is a severe problem that has significant consequences. Using spamming, cybercriminals can spread malware, viruses, & other malicious content that result in cybercrime attacks, financial losses, and identity theft. It is vital to stay informed & take necessary steps to protect oneself from spamming. What is spamming in cyber security? It is a threat that must not be ignored. By enrolling in a certified course, individuals can conveniently acquire this knowledge and enhance their skills. For further information, explore the **course details of Ethical Hacking** to discover comprehensive opportunities for upskilling.

**Common Spamming Techniques**

Spamming examples are prevalent across the digital world, & spammers continuously devise new ways to deliver their messages to unsuspecting individuals. From unwanted promotional messages to fraudulent emails, spamming techniques have evolved from simple bulk emailing to sophisticated strategies that can infiltrate our personal & professional lives. Below are four common spamming techniques used by spammers to target individuals & businesses.

**1. Botnets**

Botnets, often referred to as a "zombie army," are notorious networks of compromised devices that hackers use to send out unwanted emails by exploiting security vulnerabilities. Attackers can hijack computer systems, internet of things (IoT) devices like home routers, & smartphones to create a massive network that sends spam messages out en masse. The majority of botnets are responsible for disseminating phishing scams, malware, or ransomware in emails sent from hijacked user accounts.

**2. Snowshoe Spam**

Snowshoe spam involves spreading spam messages from a large number of email accounts & domains to evade spam filters. Attackers can rotate through various domains to distribute their group of spam emails in small chunks. By doing so, spammers can avoid detection & bypass traditional blacklists. Typically, these messages contain unimportant & trivial data that essentially wastes the time & resources of the recipient & email server.

**3. Blank Email Spam**

Blank email spam is a technique used to exploit email clients' weaknesses & i.e., leave blank spaces in critical information fields. Such areas typically include email addresses, titles, subject lines, and, in some instances, the message body itself. The technique is popular as most email clients display incoming messages as blank messages & makes it difficult for users to identify or report spam.

**4. Image Spam**

Image spam is a technique where ads & unwanted messages are inserted as images into emails. Incorporating pictures or graphics to evade spam filters & trick the users into believing that the email is legitimate & makes it look more authentic & engaging. The image will typically contain a hyperlink that takes the recipient to a dubious website where attackers prey on users to steal their data or deceive them into downloading malware.

**How to Protect Yourself from Spam?**

Spam, or unsolicited messages, can be a real headache for many people. They often end up in our email inbox & can be anything from annoying advertisements to phishing scams. However, with the right precautions, you can protect yourself from spam & avoid falling victim to cyber threats. In this section, we explore six expert tips on how to prevent spam.

**1. Use Spam Filters**

Many email providers have built-in spam filters that can help to block unwanted messages. These filters analyze incoming emails based on their content & headers & determine whether they are spam or not. They work by using algorithms that identify spam based on patterns, such as specific keywords or phrases that spammers often use.

**2. Be Cautious with Your Email Address**

Unwanted messages can be easily sent to you by spammers via your email address. To prevent this, be cautious with your email address. Only share it with people you trust & avoid posting it on social media or public forums.

**3. Avoid Clicking on Suspicious Links**

Spam emails often contain links that can lead to malicious websites or fraudulent pages. Consequently, you should avoid clicking these links if you are unsure of their legitimacy. Instead, hover your cursor over the link to see the URL, & if it looks suspicious, delete the message immediately.

**4. Opt-Out & Unsubscribe**

If you're receiving unwanted messages from legitimate companies, you can typically opt-out or unsubscribe from their mailing list. You will no longer receive emails from them after you do this. If you tap on the "unsubscribe" link, you may fall victim to a phishing scam. Be careful before clicking on anything from the sender & the URL.

**5. Installing Cybersecurity Software**

To further protect yourself from spam & other cyber threats, consider installing cybersecurity software on your device. This software can help to detect & block spam messages, while also providing additional layers of protection against malware & phishing scams.

**6. Report Spam**

Most email services have a "report spam" feature that allows you to flag unwanted messages. Reporting spam can help your email service provider to improve its spam filters & protect other users from similar messages.

So, how to stop spam emails is not an exact science, but with the above techniques, you can effortlessly reduce your chances of being directly targeted by spammers. Always keep vigilance over your email & take precautions to protect yourself & your data.

**Winding Up**

Understanding what is spamming and obtaining **KnowledgeHut's Cyber Security certification** will help protect your information. Spam emails not only clog up your inbox but also use tactics to lure victims into downloading malicious malware that can cause harm. You can prevent cyber criminals from

targeting your business or organization if you take the right steps.

If you are aware of the types of attacks & how they work, you can develop an effective plan for protecting yourself online. In addition, it is advisable to install antivirus protection on all devices connected to the Internet & be on the lookout for suspicious emails or website links.

## All the Best!