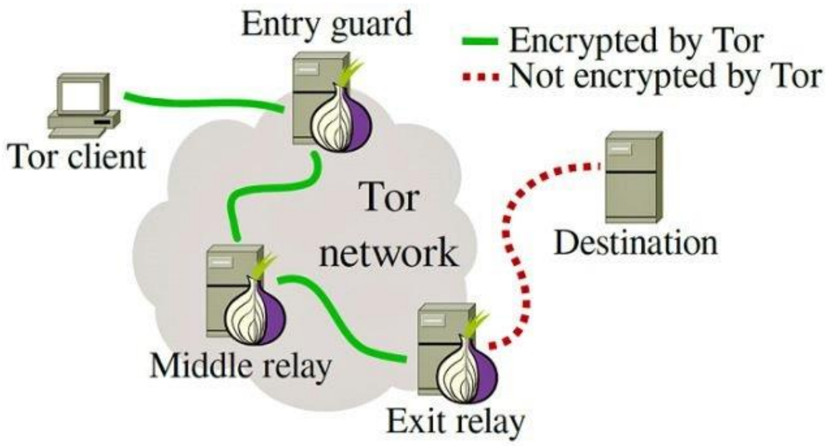
E-COMMERCE & DIGITAL SECURITY
Assignment-13
N Ravinder Reddy
Roll No: 2406CYS106

Q. 1) What is ToR and discuss attacks that are possible on it. Install ToR on your system and compare and contrast it with a regular search engine like Google.

Ans:

Tor (an acronym for The Onion Router) is essentially a network that masks online traffic. Tor browser is an open-source platform managed by volunteers and, due to its onion routing, creates anonymity for users who access websites and servers through this network. The browser is often used legitimately by journalists and other users who need to protect their identities, for example, while investigating the opposition in a legal dispute, or researching competitors.

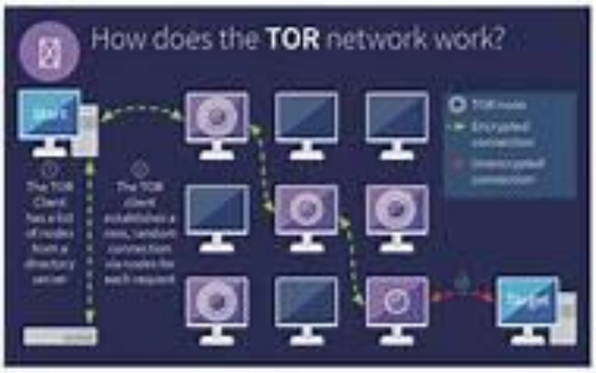


In the simplest terms, Tor browser is a software that allows users to browse the internet with a relatively high degree of privacy. The network and browser take their name from the fact that they direct all web activity through several routers—called nodes—much like going through the layers of an onion, making it difficult to track and identify users.

Layer upon layer

Sitting atop the ordinary Internet, the Tor network consists of Internet-connected computers on which users have installed the Tor software. If a Tor user wants to, say, anonymously view the front page of The New York Times, his or her computer will wrap a Web request in several layers of encryption and send it to another Tor-enabled computer, which is selected at random. That computer — known as the guard — will peel off the first layer of encryption and forward the request to another randomly selected computer in the network. That computer peels off the next layer of encryption, and so on.

The last computer in the chain, called the exit, peels off the final layer of encryption, exposing the request’s true destination: the Times. The guard knows the Internet address of the sender, and the exit knows the Internet address of the destination site, but no computer in the chain knows both. This routing scheme, with its successive layers of encryption, is known as onion routing, and it gives the network its name: “Tor” is an acronym for “the onion router.”


How does the TOR network work?
TOR node
Encrypted connection
Unencrypted connection
The TOR Client has a list of nodes from a directory server
The TOR client establishes a new, random connection via nodes for each request

In addition to anonymous Internet browsing, however, Tor also offers what it calls hidden services. A hidden service protects the anonymity of not just the browser, but the destination site, too. Say, for instance, that someone in Iran wishes to host a site archiving news reports from Western media but doesn’t want it on the public Internet. Using the Tor software, the host’s computer identifies Tor routers that it will use as “introduction points” for anyone wishing to access its content. It broadcasts the addresses of those introduction points to the network, without revealing its own location.

If another Tor user wants to browse the hidden site, both his or her computer and the host’s computer build Tor-secured links to the introduction point, creating what the Tor project calls a “circuit.” Using the circuit, the browser and host identify yet another router in the Tor network, known as a rendezvous point, and build a second circuit through it. The location of the rendezvous point, unlike that of the introduction point, is kept private.

However, there is a close association between Tor and the dark web because the Tor browser is often used for illicit activity, even though there was never any intention for Tor to enable criminality. Although the Tor browser is legal in many countries, some do not allow residents to access the network.

So how does Tor work? In its simplest form, a Tor browser use onion routing to direct and encrypt all traffic, offering users a high level of anonymity. The network transmits traffic through three layers of international network nodes called onion routers:

- Entry nodes, which form the first layer of encryption and enable the connection to the Tor network.
- A series of middle nodes fully encrypt web traffic to ensure anonymity.
- Exit nodes, which further encrypt data before it reaches the final server.

Because onion routing effectively encrypts and relays data through multiple network layers, the Tor browser is highly effective at protecting user data and concealing IP addresses.

There are several questions worth asking about Tor, including “What does a Tor browser do?” and how its use differs from regular browsers. The Tor browser is primarily a way to browse the web anonymously. As such, the main reason it is used is to avoid surveillance and ensure privacy while online. However, many people also use Tor to access services that regular browsers cannot reach, such as .onion sites which only function on the onion network, such as DuckDuckGo, a privacy-enhanced search engine, which offers a .onion version of its search engine, which doesn't track user data, providing a more private search experience.

In addition, because Tor is closely linked with the dark web, some users use this for particular types of research, and also to carry out illegal activities.

Benefits of a Tor browser

The Tor browser does have several advantages, which is why some internet users can benefit from using it. However, not all of these will be relevant to regular internet users. Here are some of the main reasons why some users choose to use a Tor onion browser:

- The browser is a free, open-source program
- IP addresses and browsing history are masked
- Enjoy heightened network security because the Tor browser operates on secure, encrypted networks
- Easy access to non-indexed pages, especially through search engines

Disadvantages of Tor browser

Aside from security concerns and wondering "is the Tor browser safe," there are some other potential disadvantages of using this software. Below are a few things to keep in mind before deciding to use the Tor onion browser.

- Because of the way it routes traffic, Tor connections are very slow, especially when compared to VPNs, and downloading large files is not practical.
- Activity may not be completely anonymous, and it is possible to decrypt a user's identity
- Some countries and companies can block the Tor browser, and its usage can even be illegal in certain countries.
- The use of this browser can be suspicious, even if it is legal
- Not all websites function on Tor

To begin with, we present a simple explanation of the Internet layers down to the Dark Web, while explaining these layers in detail is out of the scope of this review. First, the Surface Web (Open Web or Clear Web in other synonyms) represents all websites that are publicly and easily accessible because search engines can index them. Alternatively, numerous websites are inaccessible because search engines cannot index them, forming the Deep Web (or the Invisible Web). In the latter, one needs to type the URL of the website directly in the address bar of the web browser, or the website itself is visible but its content needs a password to access it [14].

Researchers should differentiate Deep Web from Dark Web. -e Deep Web is part of the web that search engines cannot access for different reasons related to the operational functions of the websites. Researchers estimate this part at more than 90% of the entire web, whereas the Dark Web is part of the

Deep Web that uses special encryption software to hide users' identities and IP addresses [15]. -us, the most difficult-to-access part of the Deep Web is the Dark Web or the Darknet in another synonym. -is anonymization leads to the predominance of malicious and criminal activities in that hidden and encrypted environment [15]. Various crimes and heinous actions are prevalent in this part of the web, including novice and professional hackers either for fun deeds or for making gains through extortion, sabotaging networks, or stealing organizations' data, in addition to many crimes such as children pornography and pedophile networks, drugs and arms trade, human trafficking, terrorism and recruitment of extremists, planning terrorist attacks, murderers for hire, hacked digital media trade, counterfeit documents, fraud, and many others [15, 16]. -e Dark Web provides the ability to hide the user's identity, network traffic, and data exchanged through it. Users outside the Dark Web cannot access it using standard web browsers but through special software, such as -e Onion Router (TOR), Invisible Internet Project (I2P), and Freenet [15, 17].

Researchers consider dark networks the primary host for various criminal activities. For example, marketplaces on the Dark Web are evidence of Crime-as-aService (CaaS), as they provide most of the items commonly found in conventional black markets [18]. Trades on Dark Web marketplaces are anonymized as well, where members complete their transactions using cryptocurrencies, such as Bitcoin and Monero [16]. In this regard, some cybercriminals act as cryptocurrency providers to make it easier for others to perform criminal activities [19].

In terms of cybersecurity threats, hacking communities are active on Dark Web platforms, where hackers exchange 2 Journal of Computer Networks and Communications experiences and share information, in addition to circulating hacking tools, malware, ransomware, breached data, and planning large-scale cyberattacks resembling a pattern of an organized crime [16]. Alternatively, Dark Web marketplaces are fraught with hacking products and tools for organizing attacks. Additionally, vendors offer breached personal data, such as credit cards, bank accounts, PINs, credentials, and other Personal Identifiable Information (PII). -ese marketplaces also provide botnets for renting to perform Distributed Denial of Service (DDoS) and fraud and spam services such as e-mail lists for sending phishing e-mails [14].

Dark Web marketplaces include sellers and buyers with different levels of technical expertise. For example, a small class of highly experienced professional sellers creates and sells sophisticated hacking tools and malware, whereas other less-experienced members buy from or collaborate with them to organize massive attacks or breached data exploitation in a Crime-as-a-Service (CaaS) paradigm. -is example of crime indicates that technical professionalism is no longer an essential component to conduct cybercrime [14]. In this context, some professional vendors offer security services to others to provide an extra level of protection and privacy against law enforcement agencies' operations. -us, if a cyberattack is detected, the identity of the perpetrator remains unknown [14].

In this regard, studies have shown that many successful cyberattacks relied on the cohesion of the mutual relationships between the hackers, which they established in the long term of cooperation, especially with the different levels of skills they possess. -ese levels entail them cooperating to implement the attacks and achieve their pursued gains. -erefore, these networks and marketplaces form what look like peership or colleagueship networks [19]. Moreover, many cybercrime marketplaces operate alongside hacking forums. Sellers advertise their products on these forums along with a description of the product features, price details, payment methods, terms of services, and contact information of the seller. For the latter, sellers and buyers tend to use other encrypted communication media such as private messaging apps or direct messaging features included in the forum [14].

Dark Web marketplaces play a significant role in providing hacking-related items. From the existence of markets for hackers, one can infer that the focus of such business on the Dark Web is financial gains, which are sometimes monopolized by the professional minority that dominates the market [20]. Some forums maintain a level of professionalism by establishing a reputation system to prevent intruders or, in the case of researchers, from gathering information. -e reputation system is based on giving professional and active users in the community more privileges as their professionalism and trustworthiness levels increase, such as getting more reputation points and permission to access other sections in the forum [3]. TOR also allows hosting websites, thus masking the location of the hosting servers, or TOR Hidden Services, and they can only be accessed through TOR [14].

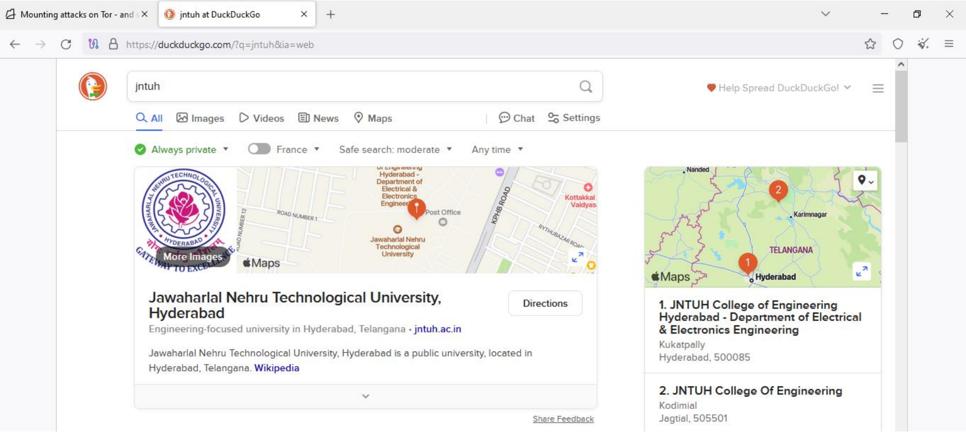
Recently, Darknets have become more complex and difficult to penetrate. TOR has added a layer of privacy in 2017 that increases the complexity of identifying both website hosts and visitors. -us, platforms on the Dark Web will be less discoverable. Moreover, website administrators become more inclined toward making sites and forums accessible by invitation only [16]. Conventional cybersecurity solutions have focused on protecting endpoint devices of all kinds; however, while they can be effective for some time, they are not a long-term remedy [16]. On the bright side, methods and techniques of artificial intelligence, machine learning, data mining, and analytics are vital tools in fighting cybercrime. Such tools assist law enforcement agencies to target and disrupt websites on Dark Web. Additionally, they provide them with the legal evidence they need to sanction perpetrators [16]. It is worth noting that not all activities on the Dark Web are illegal; many entities use encryption software for legitimate purposes, such as journalists, political activists, whistleblowers, and law enforcement agencies and researchers for research purposes [15, 16].

What are the differences between the **Tor** browser, proxy servers, and VPNs?

While the Tor browser, proxy servers, and VPNs all offer some form of anonymity, they differ slightly in how they work and the levels of protection they provide.

Proxy servers essentially function as an intermediary between a user and the websites they access. While they do obscure IP addresses and geographical locations, they do not encrypt data and online activity. Because of this, user data remains exposed and can easily be tracked and hacked. So, is Tor safe compared to proxy servers? Yes, to an extent. Despite the weaknesses outlined above, the Tor browser offers a much higher level of encryption and routing, giving users more anonymity. While using a proxy server alongside the Tor browser can help mask the use of Tor, using both a proxy server and Tor browser will not offer any further protection to users.

Virtual private networks (VPNs) are powerful networks that fully encrypt all web traffic by routing it through different servers, thereby also obscuring the user's IP address. The most significant difference between VPNs and the Tor browser is that VPN is operated by central providers who operate the network, while the latter is a decentralized network managed by volunteers. Additionally, Tor routes data through independent nodes, while VPNs route online traffic through remote servers.



jntuh

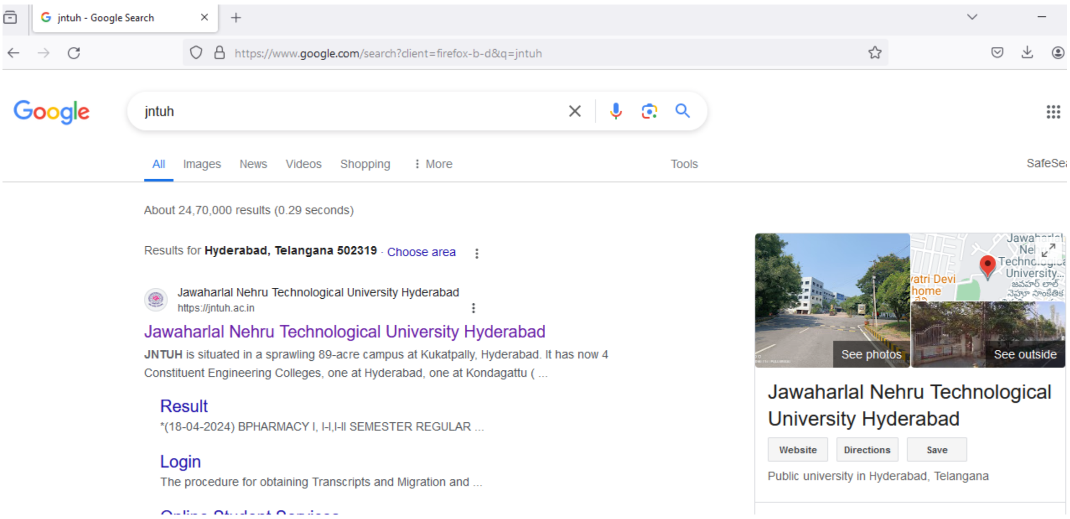
Jawaharlal Nehru Technological University, Hyderabad

Engineering-focused university in Hyderabad, Telangana · jntuh.ac.in

Jawaharlal Nehru Technological University, Hyderabad is a public university, located in Hyderabad, Telangana. Wikipedia

1. JNTUH College of Engineering Hyderabad - Department of Electrical & Electronics Engineering
Kukatpally
Hyderabad, 500085

2. JNTUH College Of Engineering
Kodimial
Jagtial, 505501



About 24,70,000 results (0.29 seconds)

Results for **Hyderabad, Telangana 502319** · Choose area

Jawaharlal Nehru Technological University Hyderabad
https://jntuh.ac.in

Jawaharlal Nehru Technological University Hyderabad

JNTUH is situated in a sprawling 89-acre campus at Kukatpally, Hyderabad. It has now 4 Constituent Engineering Colleges, one at Hyderabad, one at Kondagattu (...

Result

*(18-04-2024) BPHARMACY I, I-I,I-II SEMESTER REGULAR ...

Login

The procedure for obtaining Transcripts and Migration and ...

Online Student Services

Jawaharlal Nehru Technological University Hyderabad

Public university in Hyderabad, Telangana

2) Use the web site http://testphp.vulnweb.com/ for the following. Perform sql injection on it and retrieve the user table and its contents.

Q. 3) What are Deepfakes? Discuss how they are being used for Impersonation attacks. Explain how they can be countered.

Ans:

Deepfakes portmanteau of "deep learning" and "fake are synthetic media that have been digitally manipulated to replace one person's likeness convincingly with that of another. It can also refer to computer-generated images of human subjects that do not exist in real life. While the act of creating fake content is not new, deepfakes leverage tools and techniques from machine learning and artificial intelligence, including facial recognition algorithms and artificial neural networks such as variational autoencoders (VAEs) and generative adversarial networks (GANs) In turn the field of image forensics develops techniques to detect manipulated images.

Impersonation attacks involve cybercriminals posing as a person or organization (often a trusted individual or brand) to defraud a business of funds, steal credentials or data, or deliver malicious payloads, such as malware. Impersonation attacks delivered via email can be an effective way for cybercriminals to achieve these aims.

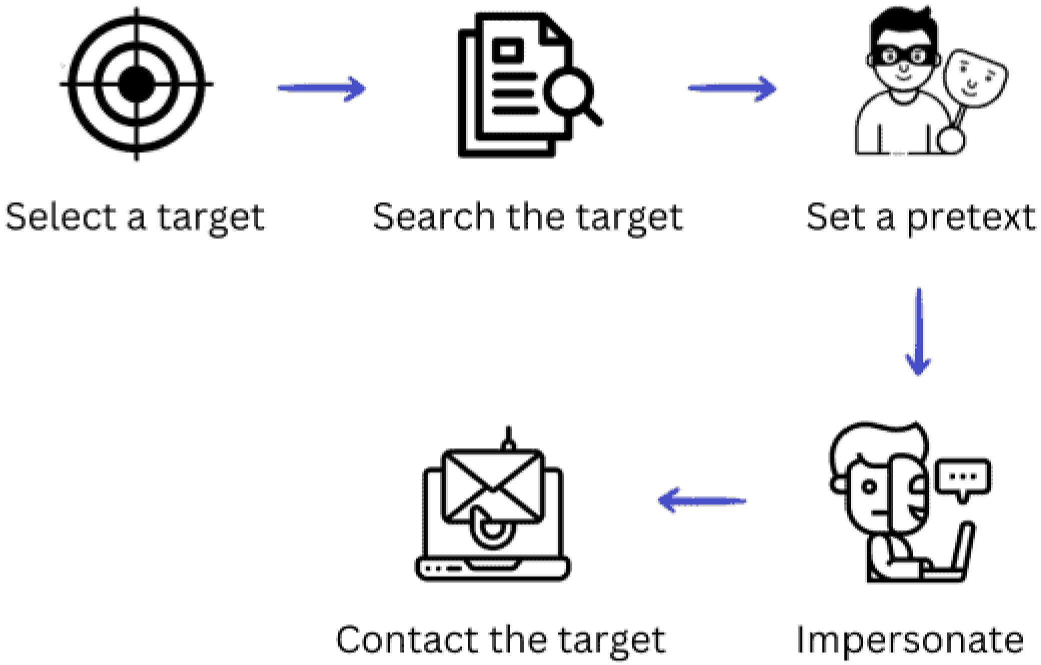
the technical definition of impersonation attacks and the main pattern when executing them. Then, we'll explain the most common forms of impersonation attacks and give measures to prevent them.

Impersonation is a type of cyberattack where an adversary illicitly identifies as a known person or trusted associate to gain unauthorized access to sensitive resources.

Mainly, the attacker pretends to be someone else and tricks the target into divulging information such as login credentials or into executing actions such as paying invoices and clicking malicious links.

Impersonation attacks are attacks on authentication. Basically, they rely on social engineering and phishing tactics. In the following, we'll talk about the steps of an impersonation attack and its potential forms.

An impersonation attack is composed of a target, a story, and an impersonated account:



They typically follow these steps:

- target selection
- researching the target
- setting the pretext
- actual impersonation
- contacting the target

- The attacker begins by choosing a target person, usually from a specific company or organization.
- They pick an executive or an employee with access to critical data. Generally, it will be someone working in the accounting, legal, or HR departments.

The attacker studies the target person’s role, responsibilities, and coworkers using online platforms such as LinkedIn and the company website.

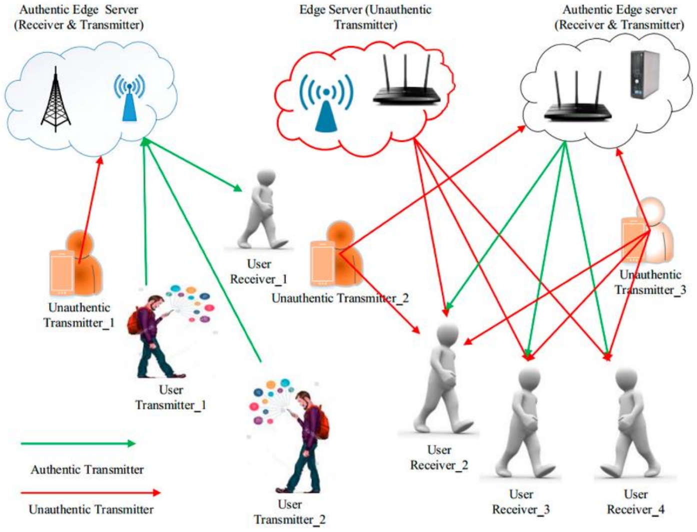
The attacker can even go further to find out about the target’s hobbies, address, and family through social media. Their goal is to draw a complete profile of the target to successfully set the trap afterward.

The attacker creates a false asset to fool the target. It can be a spoofed email or a fake social media account.

Pretending to be someone else by imitating or compromising an original account is at the core of an impersonation attack.

At this point, the attacker has already set a convincing outreach story based on the research carried out on the target profile.

Then, they approach the target via email, phone call, or any other communication medium to commit fraud. They’ll ask the target to provide credentials, pay a fake receipt or download a counterfeit app.


Authentic Edge Server (Receiver & Transmitter)
Edge Server (Unauthentic Transmitter)
Authentic Edge server (Receiver & Transmitter)
User Receiver_1
Unauthentic Transmitter_1
Unauthentic Transmitter_2
Unauthentic Transmitter_3
User Transmitter_1
User Transmitter_2
User Receiver_2
User Receiver_3
User Receiver_4
Authentic Transmitter
Unauthentic Transmitter

There are various forms of impersonation attacks.

Email Impersonation

Let’s start with the most famous impersonation attack, which is email impersonation. During this attack, the hacker pretends to be someone else (a coworker, a manager, or a friend) and uses a false or hijacked email address. Emails often include malicious links or attachments leading the target to phishing websites or malware installation.

The attacker may also manipulate the target into replying with sensitive information. For example, they can address the target by name, use familiar company language, or share finite details about a recent company event to make the targetted person trust them.

A common example of email impersonation is CEO fraud, also called business email impersonation, in which the attacker impersonates a high-rank executive or manager in the company.

Cousin Domain

Here, the attacker fabricates a fake website or email with an address that looks similar to the official website. Usually, they choose a trusted and known website or a brand to lure the victim. Also called a lookalike domain, this attack is created by different means, such as misspelling words and replacing some letters with numerals.

In short, the attacker makes slight and almost invisible changes to the domain code to seem legitimate. For example: baelldung.com instead of baeldung.com.

Account Takeover

An account takeover means logging into an account with stolen credentials gained by credential stuffing, using malware and various keylogger software, or buying passwords on the dark web. Poor password management also helps the attacker access and steal logging details.

The attacker can use the stolen accounts to send a phishing story to the victim's social media contacts. More dangerously, the stolen accounts can be financial and banking accounts. The adversary can make purchases or blackmail the target with money.

IP Spoofing

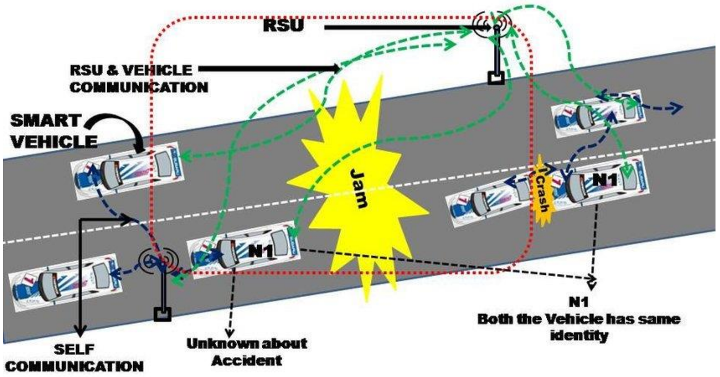
Here, the attacker changes the IP address of a source packet or hides it. In general, spoofing can take various forms. In addition to IP spoofing, there are also website spoofing and extension spoofing.

The former creates a website layout with a design that appears almost similar to the original website, fooling the target into giving away its personal information. The latter disguises a file and hides its true format to make the victim run an executable malicious file.

Man in the Middle

The man-in-the-middle (MITM) attack intercepts two communicating parties and impersonates one of them to get illicit access to confidential resources.

For example, the adversary eavesdrops on network traffic between a user and a club membership website. Then, they pose as the website and steal the login credentials.



NODE IMPERSONATION ATTACK

Vishing and Smishing

Phishing attacks also trick people into divulging sensitive and confidential information.

Smishing and vishing are two common types of phishing attacks. They use social engineering strategies. The former uses SMS texts for scams, whereas the latter exploit voice communication as phone calls and voicemails.

How to Protect from Impersonation?

Impersonation attacks can be challenging to detect and prevent since they exploit human nature. Still, there are technical and non-technical countermeasures we can implement to reduce the risk:

- Use strong passwords and multi-factor authentication to secure accounts
- Email authentication protocols such as SPF, DKIM, and DMARC
- Encrypt data and limit access to resources
- Scan for suspicious activity using automated security tools and AI-based threat detection tools
- Raise security awareness of employers in a company by training them regularly on social engineering tactics and inciting them to report any doubtful activity

Q. 4) Discuss about different types of Cyber crimes. Explain how a person can report to the concerned officials and take protection.

Ans:

Cybercrime or a computer-oriented crime is a crime that includes a computer and a network. The computer may have been used in the execution of a crime or it may be the target. Cybercrime is the use of a computer as a weapon for committing crimes such as committing fraud, identity theft, or breaching privacy. Cybercrime, especially through the Internet, has grown in importance as the computer has become central to every field like commerce, entertainment, and government. Cybercrime may endanger a person or a nation's security and financial health. Cybercrime encloses a wide range of activities, but these can generally be divided into two categories:

1. Crimes that aim at computer networks or devices. These types of crimes involve different threats (like viruses, bugs etc.) and denial-of-service (DoS) attacks.
2. Crimes that use computer networks to commit other criminal activities. These types of crimes include cyberstalking, financial fraud or identity theft.

Classification of Cyber Crime: Cyber Terrorism – Cyberterrorism is the use of the computer and the internet to perform violent acts that result in loss of life. This may include different types of activities either by software or hardware to threaten life of citizens. In general, terrorism can be defined as an act of terrorism committed through the use of cyberspace or computer resources.

1. Cyber Extortion – Cyber extortion occurs when a website, e-mail server or computer system is subjected to or threatened with repeated denial of service or other attacks by malicious hackers. These hackers demand huge money in return for assurance to stop the attacks and to offer protection.

2. Cyber Warfare – Cyber warfare is the use or targeting in a battle space or warfare context of computers, online control systems and networks. It involves both offensive and defensive operations concerning to the threat of cyber attacks, espionage and sabotage.

3. Internet Fraud –
   Internet fraud is a type of fraud or deceit which makes use of the Internet and could include hiding of information or providing incorrect information for the purpose of deceiving victims for money or property. Internet fraud is not considered a single, distinctive crime but covers a range of illegal and illicit actions that are committed in cyberspace.

4. Cyber Stalking –
   This is a kind of online harassment wherein the victim is subjected to a barrage of online messages and emails. In this case, these stalkers know their victims and instead of offline stalking, they use the Internet to stalk. However, if they notice that cyber stalking is not having the desired effect, they begin offline stalking along with cyber stalking to make the victims' lives more miserable.

Cybercrime helpline number for reporting a cybercrime in India

A cybercrime helpline number has been issued for the victims of cybercrimes in India. The helpline number for the victims of cybercrime is '**1930**'. Any person who wants to report a case can dial the helpline number and report the commission of the cyber offence.

In the majority of cases of cybercrime, it is crucial that the victims register the complaint as soon as possible, thus, leading to easy and faster tracking of cyber criminals. The helpline number serves this purpose, and it should be used for the immediate reporting of these offences.

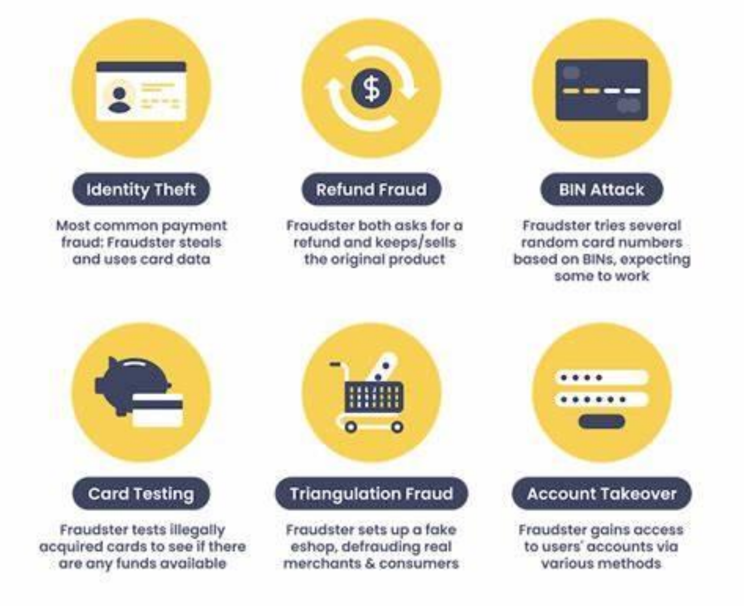
How to file a cyber crime complaint offline

Cyber laws have been introduced to punish the offenders, and in order to successfully implement these laws, cybercrime cells have been set up. It is always advisable to seek legal help in such sensitive matters. Cybercrime complaints can be filed offline as well as in an online mode with the cyber crime cells. The procedure for filing a cybercrime complaint is similar to the filing of a written application with any government office. There is no set format for filing such a complaint. However, some essential contents (as stated below) are to be included while filing an offline complaint.

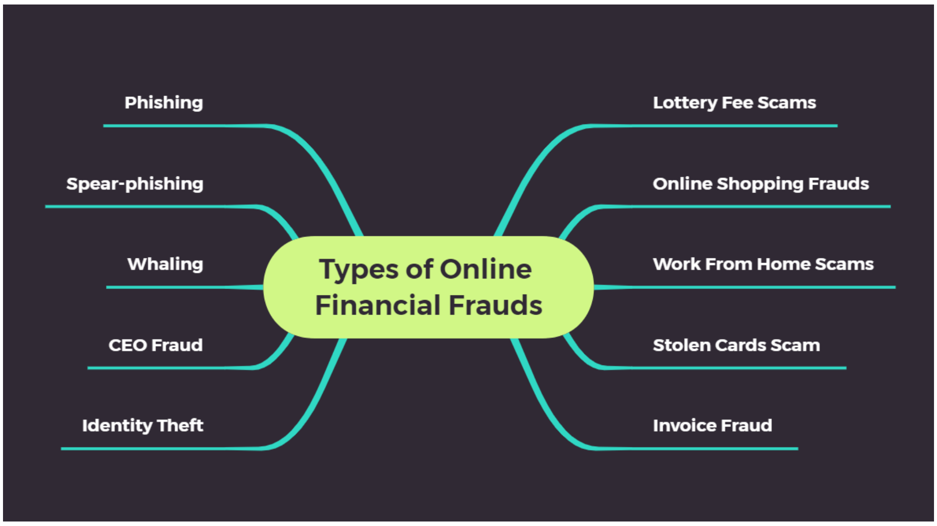
Q. 5) Discuss about various online payment frauds and how can they be prevented?

Ans:

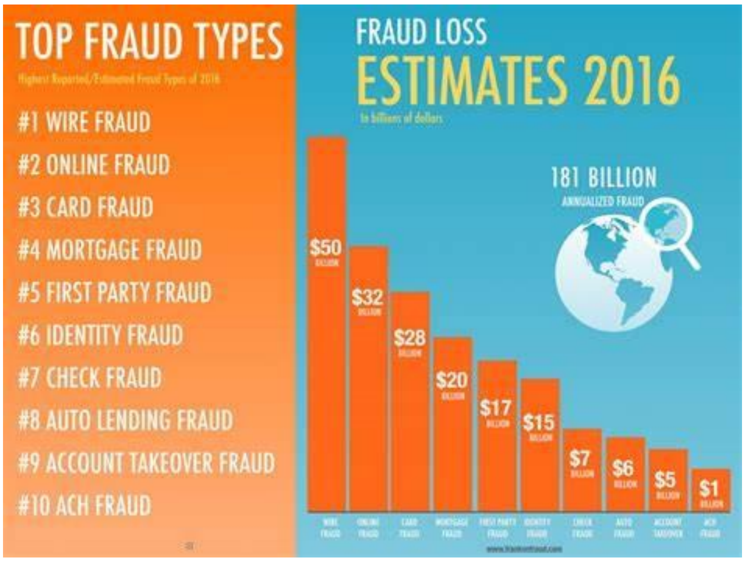
Payment fraud can threaten business finances and customer privacy, and fighting it requires defensive solutions that are as sophisticated and flexible as the tactics used by fraudulent actors.


Identity Theft
Most common payment fraud: Fraudster steals and uses card data
Refund Fraud
Fraudster both asks for a refund and keeps/sells the original product
BIN Attack
Fraudster tries several random card numbers based on BINs, expecting some to work
Card Testing
Fraudster tests illegally acquired cards to see if there are any funds available
Triangulation Fraud
Fraudster sets up a fake eshop, defrauding real merchants & consumers
Account Takeover
Fraudster gains access to users' accounts via various methods

Payment fraud can come in many different forms, from the theft of credit card numbers from an unprotected card reader to malicious, fake emails. For instance, research done in 2021 by Tessian showed that US employees receive an average of 14 emails per year that prompt them to take financially fraudulent actions. In some industries, this number is much higher, with retail workers fielding an average of 49 fraudulent emails each year.



Phishing is one of the most common types of payment fraud, accounting for 44% of all data breaches in 2020. Skimming, where fraudulent actors capture card information at cash machines or from payment terminals, costs businesses an estimated US$1 billion each year. Identity theft, where personal information is stolen and used to make fraudulent purchases, comprised 24% of nearly 6 million fraud reports in 2021, according to the FTC. And these are just some of the types of payment fraud that businesses need to fight against.



Payment fraud represents a major threat, but businesses can mitigate it with a number of effective defence tactics. Here's what you need to know about common types of payment fraud, how they work and what you can do to protect yourself, your business and your customers.

What's in this article?

- What is payment fraud?
- Types of payment fraud
- Benefits of fraud protection

What is payment fraud?

Payment fraud is a type of financial fraud that involves the use of false or stolen payment information to obtain money or goods. Payment fraud can occur in a variety of ways, but it often includes fraudulent actors stealing credit card or bank account information, forging cheques or using stolen identity information to make unauthorised transactions.

Types of payment fraud

Fraudulent actors use several methods to commit payment fraud. Here are some of the most common tactics:

Phishing

What it is:

Phishing is a type of social-engineering attack – a tactic which involves deceiving people through psychological manipulation. In phishing, fraudulent actors use fraudulent emails, text messages or websites to trick individuals into disclosing sensitive information such as log-in credentials and credit card information.

Phishing attacks are usually carried out through emails that look like they are from a trusted source, such as a bank or a reputable online retailer. The email may ask the recipient to click on a link to update their account information, verify a recent transaction or claim a prize. When the recipient clicks the link, they are directed to a fake website where they are prompted to enter their log-in credentials, credit card information or other sensitive data.

Phishing attacks can also be carried out through text messages, known as "smishing", or through social media platforms, known as "pharming". In these cases, the attacker sends a message or a link to a fraudulent website that appears to be legitimate, in order to steal personal information or infect the device with malware.

How to prevent it:

To protect against phishing attacks, be cautious when clicking links or opening attachments from unknown or suspicious sources. Stay alert for common tactics used by fraudulent actors, such as urgent or threatening language, misspelled words or suspicious links. Using antivirus software can also help protect against phishing attacks.

As with other types of payment fraud, phishing scams tend to evolve over time, becoming more advanced and appearing to be even more legitimate. Individuals and businesses should educate themselves and their employees about phishing and how to recognise and avoid these types of attacks.

Skimming

What it is:

Skimming occurs when a fraudulent actor uses a device, called a skimmer, to steal credit or debit card information. The fraudulent actor attaches a skimmer to a card reader at ATMs or point-of-sale terminals such as petrol pumps, self-service checkouts and other payment terminals. The skimmer captures the card's magnetic stripe data, which can be used to create counterfeit cards or to make fraudulent purchases.

In addition to skimmers, fraudulent actors may also use small cameras or overlays that fit over the ATM or the keypad of the payment terminal to capture the customer's PIN. This information is then used along with the stolen card data to make unauthorised withdrawals or purchases.

How to prevent it: Skimming can be difficult to detect as skimming devices are often small and inconspicuous – but it's not impossible. There are signs that can indicate the presence of a skimming device, such as loose or damaged card readers, unusual or extra devices attached to the payment terminal, or devices that look different to other payment terminals in the area.

To protect against skimming, be cautious when using payment terminals and ATMs, and inspect the device for any signs of tampering. Covering the keypad when entering a PIN can also help to protect against camera-based skimming.

Regularly monitor bank and credit card statements for any suspicious transactions and report any suspected skimming to the bank or payment card issuer as soon as possible.

Paying with digital wallets or EMV chip-enabled cards can also protect against skimming, as this technology is more secure than magnetic stripe cards. Making sure that your business is set up to accept these secure payment methods is a powerful way to safeguard against skimming.

Identity theft:

What it is: Identity theft is a type of payment fraud where a fraudulent actor steals a person's personal information, such as their name, Social Security number or credit card number, and uses it to make unauthorized purchases or open accounts in the victim's name. Identity theft can have serious financial and legal consequences for the victim and can cause significant stress and anxiety.

Identity theft is an umbrella term that describes several fraud tactics. For example, phishing attacks are one type of identity theft. Data breaches, where a hacker gains access to a company's database and steals personal information on a large scale, are also a type of identity theft. Other methods of identity theft include stealing post, dumpster diving or stealing wallets or purses. Once a fraudulent actor has obtained a person's personal information, they can use it to open new credit card accounts, apply for loans or even file false tax returns.

How to prevent it: To prevent identity theft, businesses can take a number of steps. First, ensure that customer data is stored securely, using encryption and other security measures to prevent unauthorised access. Businesses should limit access to customer data to employees who specifically need it to do their jobs. They should also require strong passwords and multi-factor authentication for all accounts and systems that contain customer data.

Employee training is important for preventing identity theft and it should include security best practices such as how to identify phishing emails and create strong passwords.

Monitoring customer accounts for suspicious activity, such as unauthorised logins or changes to account information, can help businesses detect identity theft early and reduce the damage. Choosing the right payments tech stack can stop fraud detection and prevention from draining time and resources. Stripe Radar is sophisticated technology for fraud detection and prevention that is integrated into all Stripe payment products, including Terminal.

Finally, businesses should have a plan in place for responding to data breaches, including notifying affected customers and offering services to protect against identity theft.

Chargeback fraud

What it is: Chargeback fraud, also referred to as "friendly fraud", occurs when a customer disputes a legitimate transaction, either claiming that they did not make the purchase themselves or that they did not receive the product or service that they paid for. In some cases, the customer may receive a refund while keeping the product or service, resulting in a financial loss for the business. Chargeback fraud can have significant financial consequences for businesses: they may lose the revenue from the sale and be subject to chargeback fees and penalties.

Chargeback fraud can occur in a few different ways. The most common method is when a customer makes a legitimate purchase but later disputes the charge with their credit card company, claiming that the item was not as described or that they never received it. Another method is when a customer intentionally uses a stolen credit card to make a purchase and then disputes the charge as unauthorised.

How to prevent it: To protect against chargeback fraud, businesses should verify the identity of the customer and ensure that they are the rightful owner of the credit card used to make the purchase. This can include requiring a signature or CVV code for card-not-present transactions, or implementing fraud-detection tools such as address verification or IP geolocation. Businesses should also have a clear refund and return policy and a process for handling chargeback disputes. Businesses should maintain clear records of all transactions, including receipts, shipping information and customer communications, in case they need to provide evidence in a chargeback dispute.

Business email compromise

What it is: Business email compromise (BEC) is a type of payment fraud where emails trick employees into transferring money to fraudulent accounts. In a BEC scam, fraudulent actors gain access to a business email account, often through phishing or social-engineering tactics, and then use it to send emails to employees or vendors requesting bank transfers or other payments.

BEC scams can take many forms. Often, they involve a fraudulent actor who impersonates a high-level executive or vendor and requests an urgent payment or transfer. The email may look legitimate, using the company's branding and a familiar email address. However, if the employee follows the instructions in the email, they will transfer the money to a bank account controlled by the fraudulent actors.

BEC scams can be difficult to detect as they often involve social-engineering tactics that exploit human trust in authority. However, there are some signs that point to a BEC scam, such as:

- Urgent requests for payment
- Unusual payment instructions
- Emails that contain unusual grammar or spelling errors

How to prevent it: Protecting against BEC involves many of the same tactics and best practices that businesses should already be using to safeguard against other types of fraud. Educate employees on how to recognise and report suspicious emails and implement strong email security protocols, such as two-step authentication and encryption.

Businesses should also have a clear payment-approval process that includes verifying payment instructions through a secondary channel, such as a phone call or in-person conversation. It's good practice to have a clear playbook for internal requests, particularly if they involve moving money.

Finally, as with all fraud, it's important to regularly monitor bank accounts for suspicious activity and to have a plan in place for responding to a BEC scam, including contacting law enforcement and notifying customers or partners who may have been affected.

Card-not-present fraud

What it is: Card-not-present (CNP) fraud is a type of payment fraud that occurs when a fraudulent actor uses stolen credit card information to make purchases without physically presenting the card, usually online or over the phone. CNP fraud has become increasingly common with the rise of e-commerce. What's more, it can have significant financial consequences for businesses, which may be liable for chargebacks or fraudulent purchases.

CNP fraud usually occurs when a fraudulent actor obtains stolen credit card information through data breaches or other means, and then uses that information to make unauthorised purchases online. Another method is when a fraudulent actor uses social-engineering tactics, such as phishing, to obtain the card information directly from the victim.

How to prevent it: To protect against CNP fraud, businesses can take several steps, including:

- Using fraud detection tools, such as address verification or IP geolocation, to verify the identity of the customer and detect suspicious activity
- Implementing strong authentication protocols, including two-step authentication and tokenisation, to protect card information
- Maintaining clear, accessible records of all transactions, including delivery information and customer communications, in case of chargeback disputes

- Creating a thorough refund and return policy that is clearly communicated to customers, as well as a process for handling chargebacks and fraudulent transactions