

Assignment 13

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.

The Dark Web Browser: What Is Tor, Is It Safe, and How to Use It

The Tor Browser takes online privacy to extremes. With an encrypted and anonymous connection, Tor helps you access the unindexed part of the internet known as the dark web. But how does this dark web browser work, and is it safe? Learn more about Tor and its pros and cons — then get Avast Secure Browser for cleaner and faster private browsing.

What is Tor Browser?

Tor (The Onion Router) is a network that anonymizes web traffic to provide truly private web browsing. The Tor Browser hides your IP address and browsing activity by redirecting web traffic through a series of different routers known as nodes. Because Tor hides browsing activity and blocks tracking, it's used by whistle blowers, journalists, and others who want to protect their privacy online.

Tor anonymizes web traffic with a special **encryption** technique originally developed by the US Navy to help protect American intelligence communications. Today, Tor is an open-source, privacy platform available to everyone. Though some countries — like China — have banned its use outright.

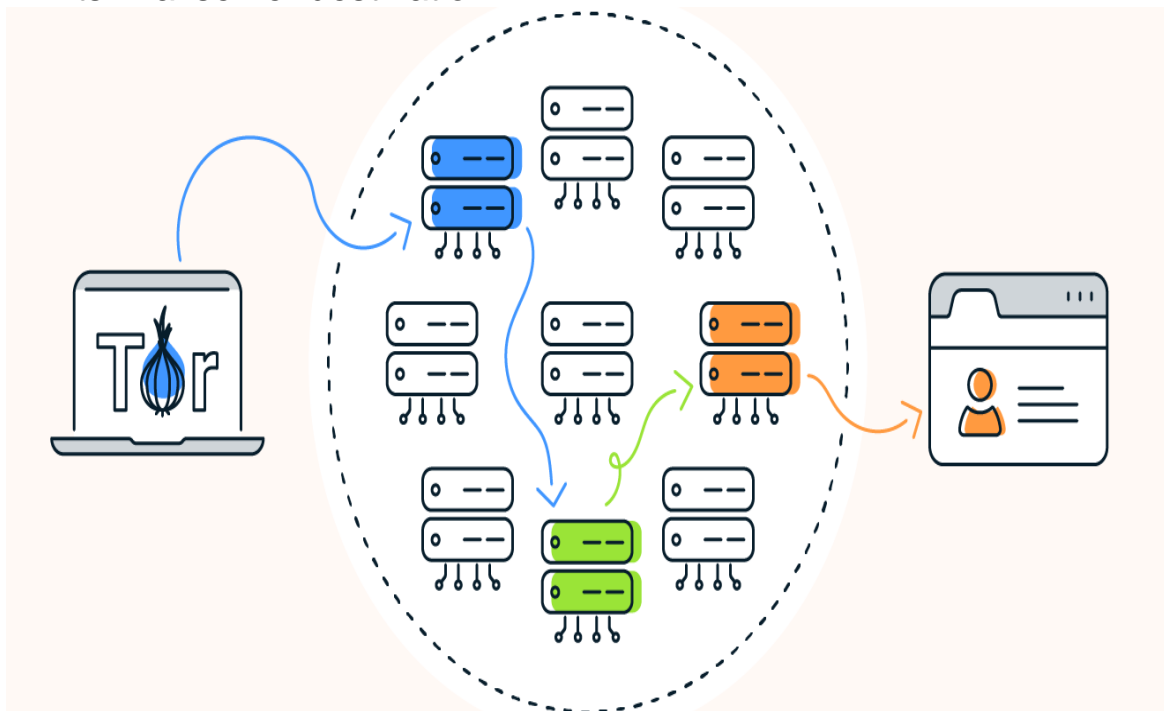
Besides a **web browser**, Tor also provides onion services via its onion network to enable anonymity for websites and servers. A [dot] onion web address, which is exclusively accessible via the Tor Browser, protects the identity of both the website and visitors. With a complex, encrypted connection that offers up anonymity for both hosts and visitors, Tor is often used to create and access the **dark web**. As such, Tor is the very definition of a dark web browser.

How does Tor, the dark web browser, work?

Tor uses **onion routing** to encrypt and reroute web traffic through Tor's onion network. After your data is secured inside multiple layers of encryption, your web traffic is transmitted through a series of network nodes, called onion routers. Each router (or node) **“peels away”** a layer of encryption until the data reaches its final destination, fully decrypted. Tor anonymously transmits encrypted data across three layers of international proxies that make up the Tor circuit.

Let's take a closer look at the three layers of network nodes:

1. **Entry/Guard node:** First, Tor Browser randomly connects to a publicly known entry node. The entry node introduces your data into the Tor circuit.
2. **Middle nodes:** Here your data is fully encrypted. Then it's sent through a series of nodes which decrypt your data one layer at a time. To ensure anonymity, each middle node knows only the identity of the preceding and the subsequent middle nodes.
3. **Exit node:** Once the last layer of encryption is peeled off, the decrypted data leaves the Tor network via an exit node and reaches its final server destination.



Tor Browser sends web traffic through an entry node (blue), middle node

(Green), and exit node (orange) to encrypt and decrypt traffic.

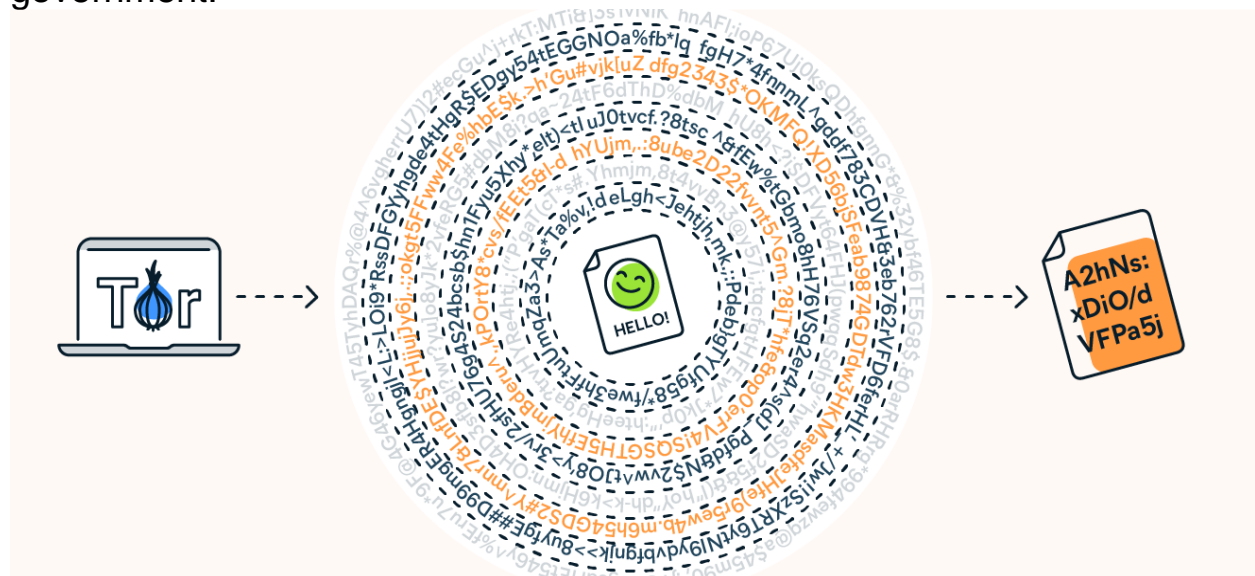
Sounds complicated, right? That's because it is. But fortunately knowing how to use Tor Browser doesn't require a PhD in computer science — it's surprisingly easy and user-friendly.

Does Tor Browser hide your IP and how?

Tor Browser's onion routing technology is extremely effective at concealing your **IP address** from network surveillance or traffic analysis. In addition to relaying your data through network nodes to hide your location and identity, onion routing uses **multi-layered encryption** to provide even more robust privacy protection.

Because Tor-encrypted data needs to be "peeled" through more than 7,000 independent network relays before it's fully decrypted, by the time internet traffic reaches its destination, its origin is completely obscured.

This elaborate process shows how secure Tor is at protecting data and **hiding your IP address** from websites, your ISP, and even the government.



Your web traffic goes through thousands of layers of decryption when connecting to the internet via Tor Browser.

Is Tor Browser anonymous?

Tor Browser is anonymous in terms of hiding your location and browsing activity — but there are limits. Although they can't see your browsing activity or Tor encrypted data, your ISP can still see that you're using Tor. You can also be identified if you log in to an online account or provide details to a website while using Tor.

What is the difference between Tor Browser and a proxy server?

A **proxy server** acts as an intermediary between you and web sites and services. While proxies hide your IP address and location, they don't encrypt internet traffic, meaning your data is still exposed in transit. Tor Browser is much more secure thanks to onion routing and multi-layer encryption, which anonymizes your location and protects your data from hackers, web trackers, and other snoops.

Using a proxy server in combination with Tor Browser can help to hide the fact that you've connected to Tor, but it won't confer any additional **cybersecurity** benefits.

Tor is not the same as a **VPN**, though both tools provide encryption and reroute your web traffic to another network. A key difference between Tor and a VPN is that a VPN's network is operated by a central service provider, while the Tor network is decentralized and run by volunteers.

In addition, Tor and VPNs take different approaches to rerouting data. A VPN sends your web traffic to a server, which transmits it to the internet. Tor's onion routing method reroutes your data through a series

of independent nodes. Though Tor is slower, the process of rerouting data through nodes makes it more difficult to trace your activity back to you.

What is Tor Browser used for?

Tor Browser is primarily used as a method of **anonymous browsing**. From journalists and civil society organizations seeking to escape spying or political repression, to regular individuals with online privacy concerns, Tor Browser users are a diverse group. But criminals also take advantage of Tor's anonymity to carry out illegal activities both on and off the dark web.

Can I be tracked while using Tor?

Despite its impressive privacy features, there are still ways that you can be tracked while using Tor. Onion routing is a sophisticated means to prevent tracking your location, but there's no such thing as perfect online anonymity.

Although your internet traffic is encrypted on Tor, your ISP can still see that you're connected to Tor. Plus, **Tor cannot protect against tracking at the entry and exit nodes of its network**. Anyone who owns and operates the entry node will see your real IP address. And at the exit node, your decrypted traffic is vulnerable to interception. You can reinforce Tor's weak spots by pairing it with a VPN that provides end-to-end encryption.

That means your web traffic will be fully encrypted at the entry and exit nodes of the Tor network, and using VPN-over-Tor will keep your real IP address safe from any prying eyes lurking at those gateways.



Use Tor alongside a VPN to ensure your web traffic is fully encrypted.

Reasons to use Tor

One of the main reasons to use Tor is the high level of privacy provided by the onion network. Not only do Tor's security protocols allow users to access sites safely and hide their IP address, but the browser is

open-source, free, and simple to use, especially considering the complex protection it provides.

Is Tor Browser legal?

Tor Browser is legal to use in most countries, although there may be a stigma attached to using it, because Tor is often associated with dark web criminality. But despite its sometimes seedy reputation, the dark web is host to many legitimate resources, like the dark web Wikipedia, secure email services, and research databases. If you're not engaged in illicit activities, it's not a crime to use the dark web to protect your privacy.

Still, Tor usage can call undue attention to your web activity, which could be counter-productive if you're seeking privacy. ISPs have been known to **throttle internet speeds** and even contact customers about Tor usage. Your government may also track your activities if you use Tor.

In some countries, Tor itself is outlawed. China has banned anonymous browsing — making Tor illegal to use. Other countries like Russia and Venezuela actively try to block their citizens from using Tor. If you're interested in anonymous browsing, first check whether Tor or VPNs are legal in your country.

Is Tor Browser safe?

The Tor Browser is generally considered safe and secure thanks to onion routing protocol that encrypts your data and hides your IP address. But Tor does have some vulnerabilities, and as with any browser, Tor users remain vulnerable to online threats, ranging from malware to phishing scams.

Knowing how to safely use Tor means using it alongside other cybersecurity tools, so **set up a VPN** to benefit from end-to-end encryption. And make sure your network's protected by a **firewall** and the **best antivirus software**.

Tor Browser and the dark web

For many, Tor is synonymous with the **dark web** — the unindexed part of the internet that's only accessible with certain browsers. The connection between Tor and the dark web started with the **Silk Road, the first dark web market** where customers could buy drugs and other illegal goods. When in operation, the notorious online marketplace could only be accessed through Tor.

As a browser that enables anonymity to both website hosts and visitors, the appeal of Tor to dark web participants is obvious. And though the dark web is not just a haven for illicit activity, accessing the dark web via the onion browser is popular with criminals.

But Tor was not designed with criminality in mind, or intended to be the "dark web browser." Tor is a legitimate and effective online

privacy tool that's used by a variety of users who value their online privacy and data security.

The disadvantages of Tor Browser

Although Tor is a sophisticated privacy tool, it has several disadvantages — some of which counteract its cybersecurity advantages.

Here are the disadvantages of using Tor:

- **Slow Speeds:** Tor is a slow browser. Onion routing encrypts web traffic and sends it through a series of network nodes — this is great for privacy, but the elaborate process results in slow speeds compared to other browsers. Although there are ways of making Tor faster, you can't significantly boost speeds.
- **Stigma:** Tor has acquired the unfortunate stigma of dark web illegality. ISPs and governments may take note of people who use the browser. For people seeking privacy, Tor may bring them the opposite.
- **Blocking:** Some network administrators block Tor. Some websites also keep track of and block web traffic coming from Tor exit nodes. But you can mask node usage by using Tor bridges or a VPN.
- **Vulnerabilities:** Though Tor is designed for anonymity, the onion network is vulnerable at the entry and exit nodes. Since internet traffic is not encrypted at these points, your data is liable to interception, and your IP address could be exposed.

Other dark web browsers

Though the Tor Browser has strong ties with dark web browsing, it also has competition. There are other browsers that can also access the dark web. Though Tor enables anonymity, these other browsers have their own advantages.

Here are the other dark web browsers:

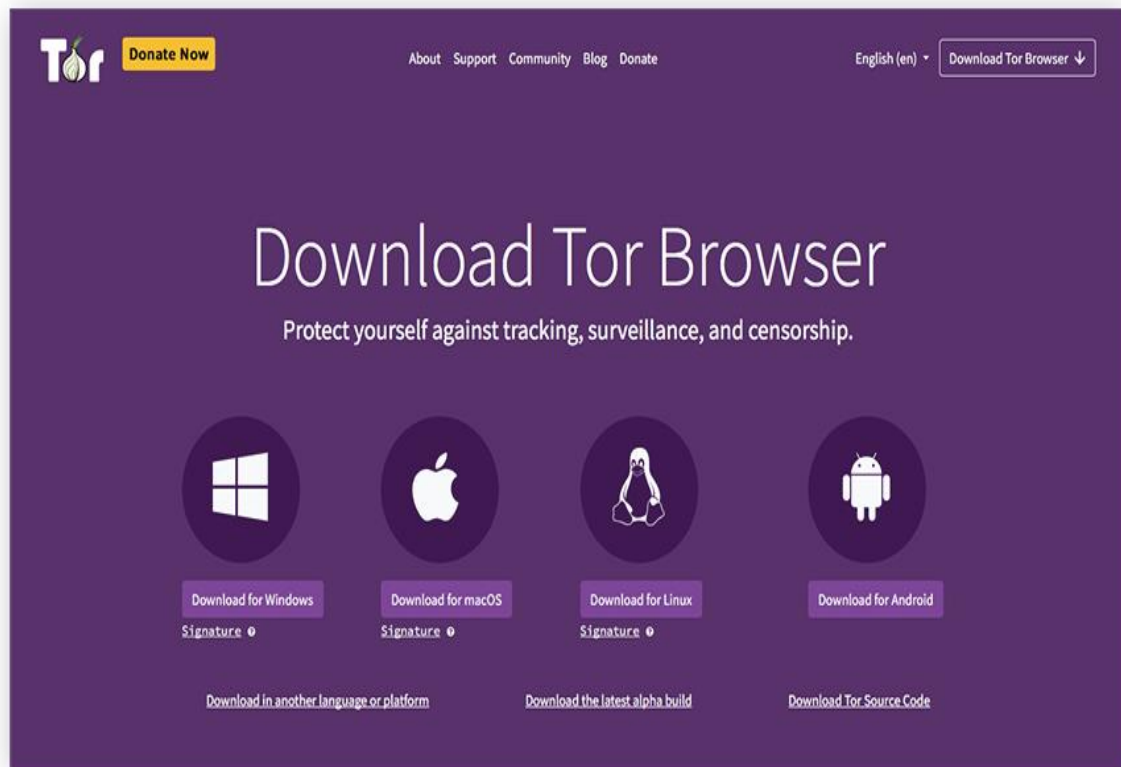
- **Subgraph OS:** This open-source operating system is designed to be resistant to surveillance and other snoops. It's been mentioned by whistleblower Edward Snowden as showing potential.
- **Firefox:** Though this popular and accessible browser can access the dark web, it lacks safety features.
- **Water fox:** Based on Firefox, the Waterfox browser is fast and features tracking protection to safeguard your privacy.
- **I2P - Invisible Internet Project:** Similar to Tor, this is a fully-encrypted, private network layer.

How to use Tor Browser on Windows and Mac

Tor is currently available for Windows, Mac, and Linux. It's a Firefox-based app that's downloaded and installed on your computer. After installation, you can use Tor to access the public internet as well as .onion websites.

Here's how to use Tor on Windows and Mac:

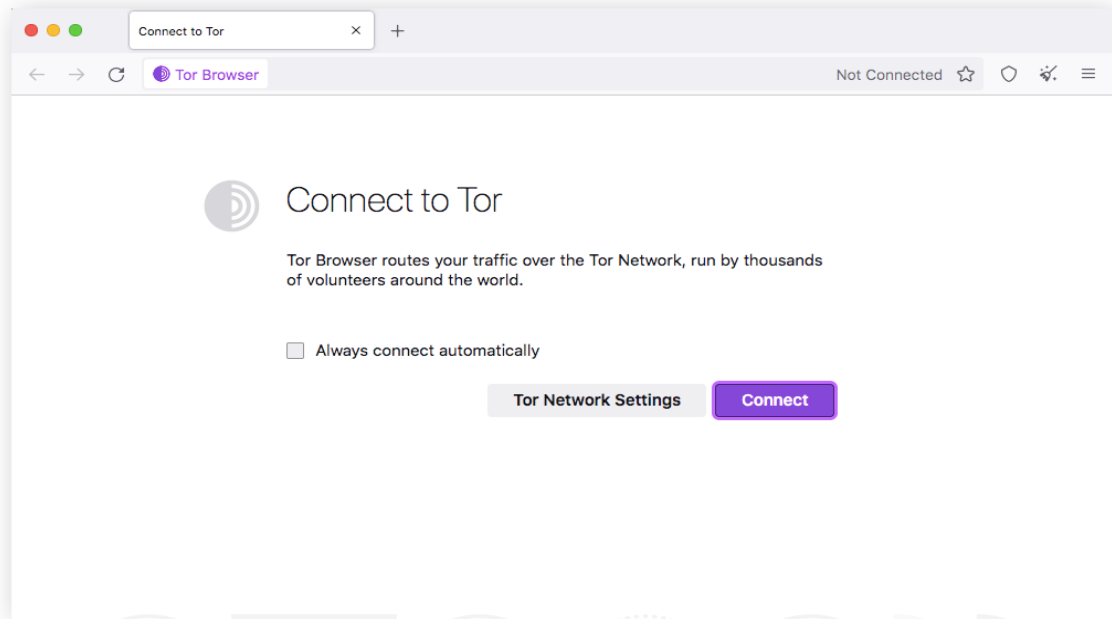
1. On the Tor project website, go to the Tor Browser download page.
2. Click on the download link for your OS.



3. Once downloaded, install the Tor Browser application.



4. Launch the Tor Browser application and connect to the Tor network.



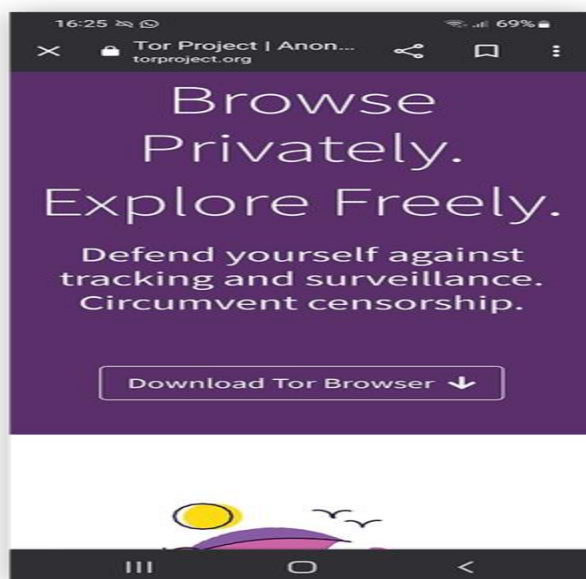
Now that you've got Tor set up on your computer, you may want to [change your default browser](#) for maximum privacy. Check out our review of the [best browsers for security and privacy](#).

How to use Tor on mobile

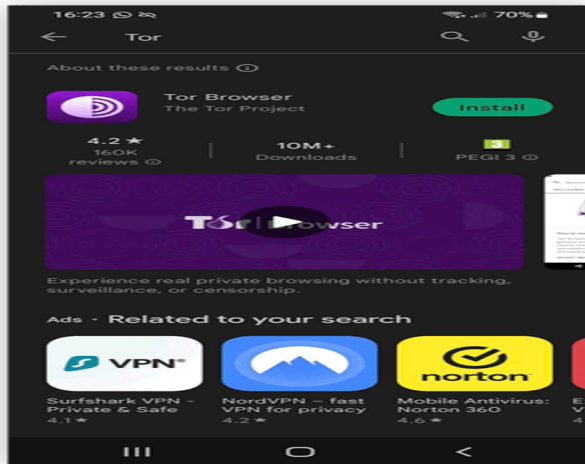
Tor is available on mobile only for Android devices, as there's no Tor Browser for iPhone. The mobile Tor Browser is an application you can download on the Tor project website and the Google Play store.

Here's how to access Tor on your Android device:

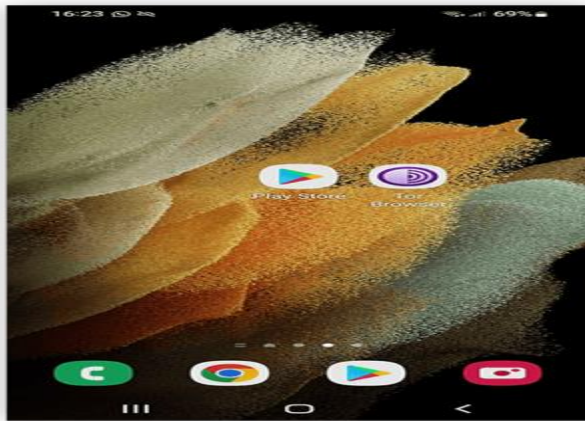
1. On the Tor project website, go to the Tor Browser download page. Or, find and download the app in the Google Play store.



2. Download the app on your Android device.



3. Click the app icon on your home screen to launch the browser.



Browse securely and privately online

Though Tor is a powerful tool for anonymous browsing, it's not without flaws. Tor is slow and can be vulnerable to attacks. And Tor may attract unwanted attention from your government or ISP. If you're looking for a secure and private alternative that's also much easier to use than Tor, get Avast Secure **Browser**.

Light, fast, and easy-to-use, Avast Secure Browser is designed to provide ironclad online privacy, while stopping hackers from stealing your data, blocking malicious links, and warning you about dangerous websites. Avast Secure Browser also forces websites to use encryption and integrates seamlessly with a VPN for ultimate security and privacy.

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.

What is SQL Injection (SQLi) and How to Prevent It

SQL Injection (SQLi) is a type of an **injection attack** that makes it possible to execute malicious SQL statements. These statements control a database server behind a web application. Attackers can use SQL Injection vulnerabilities to bypass application security measures. They can go around authentication and authorization of a web page or web application and retrieve the content of the entire SQL database. They can also use SQL Injection to add, modify, and delete records in the database.

An SQL Injection vulnerability may affect any website or web application that uses an SQL database such as MySQL, Oracle, SQL Server, or others. Criminals may use it to gain unauthorized access to your sensitive data: customer information, personal data, trade secrets, intellectual property, and more. SQL Injection attacks are one of the oldest, most prevalent, and most dangerous web application vulnerabilities. The OWASP organization (Open Web Application Security Project) lists injections in their **OWASP Top 10** 2017 document as the number one threat to web application security.



How and Why Is an SQL Injection Attack Performed

To make an SQL Injection attack, an attacker must first find vulnerable user inputs within the web page or web application. A web page or web application that has an SQL Injection vulnerability uses such user input directly in an SQL query. The attacker can create input content. Such content is often called a malicious payload and is the key part of the attack. After the attacker sends this content, malicious SQL commands are executed in the database.

SQL is a query language that was designed to manage data stored in relational databases. You can use it to access, modify, and delete data. Many web applications and websites store all the data in SQL databases. In some cases, you can also use SQL commands to run operating system commands. Therefore, a successful SQL Injection attack can have very serious consequences.

- Attackers can use SQL Injections to find the credentials of other users in the database. They can then impersonate these users. The impersonated user may be a database administrator with all database privileges.
- SQL lets you select and output data from the database. An SQL Injection vulnerability could allow the attacker to gain complete access to all data in a database server.
- SQL also lets you alter data in a database and add new data. For example, in a financial application, an attacker could use SQL Injection to alter balances, void transactions, or transfer money to their account.
- You can use SQL to delete records from a database, even drop tables. Even if the administrator makes database backups, deletion of data could affect application availability until the database is restored. Also, backups may not cover the most recent data.
- In some database servers, you can access the operating system using the database server. This may be intentional or accidental. In such case, an attacker could use an SQL Injection as the initial vector and then attack the internal network behind a firewall.

There are several types of SQL Injection attacks: **in-band SQLi** (using database errors or UNION commands), **blind SQLi**, and **out-of-band SQLi**. You can read more about them in the following articles: [Types of SQL Injection \(SQLi\)](#), [Blind SQL Injection: What is it](#).

To follow step-by-step how an SQL Injection attack is performed and what serious consequences it may have, see: [Exploiting SQL Injection: a Hands-on Example](#).

Simple SQL Injection Example

The first example is very simple. It shows, how an attacker can use an SQL Injection vulnerability to go around application security and authenticate as the administrator.

The following script is pseudo code executed on a web server. It is a simple example of authenticating with a username and a password. The example database has a table named **users** with the following columns: **username** and **password**.

```
# Define POST variables
uname = request.POST ['username']
passwd = request.POST['password']

# SQL query vulnerable to SQLi
sql = "SELECT id FROM users WHERE username=" + uname + " AND
password=" + passwd + ""

# Execute the SQL statement
database.execute(sql)
```

These input fields are vulnerable to SQL Injection. An attacker could use SQL commands in the input in a way that would alter the SQL statement executed by the database server. For example, they could use a trick involving a single quote and set the **passwd** field to:

```
password' OR 1=1
```

As a result, the database server runs the following SQL query:

```
SELECT id FROM users WHERE username='username' AND password='password' OR 1=1'
```

Because of the **OR 1=1** statement, the **WHERE** clause returns the first **id** from the **users** table no matter what the **username** and **password** are. The first user **id** in a database is very often the administrator. In this way, the attacker not only bypasses authentication but also gains administrator privileges. They can also comment out the rest of the SQL statement to control the execution of the SQL query further:

```
-- MySQL, MSSQL, Oracle, Postgre SQL, SQLite
' OR '1'='1' --
' OR '1'='1' /*
-- MySQL
' OR '1'='1' #
-- Access (using null characters)
' OR '1'='1' %00
' OR '1'='1' %16
```

Example of a Union-Based SQL Injection



One of the most common types of SQL Injection uses the UNION operator. It allows the attacker to combine the results of two or more SELECT statements into a single result. The technique is called *union-based* SQL Injection.

The following is an example of this technique. It uses the web page **testphp.vulnweb.com**, an intentionally vulnerable website hosted by Acunetix.

The following HTTP request is a normal request that a legitimate user would send:

```
GET http://testphp.vulnweb.com/artists.php?artist=1 HTTP/1.1
Host: testphp.vulnweb.com
```

← → ↻ testphp.vulnweb.com/artists.php?artist=1

TEST and Demonstration site for Acunetix Web Vulnerability Scanner

[home](#) | [categories](#) | [artists](#) | [disclaimer](#) | [your cart](#) | [guestbook](#) | [AJAX Demo](#)

search art

[Browse categories](#)
[Browse artists](#)
[Your cart](#)
[Signup](#)
[Your profile](#)
[Our guestbook](#)
[AJAX Demo](#)

Links
[Security art](#)
[Fractal Explorer](#)



artist: r4w8173

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Donec molestie. Sed aliquam sem ut arcu. Phasellus sollicitudin. Vestibulum condimentum facilisis nulla. In hac habitasse platea dictumst. Nulla nonummy. Cras quis libero. Cras venenatis. Aliquam posuere lobortis pede. Nullam fringilla urna id leo. Praesent aliquet pretium erat. Praesent non odio. Pellentesque a magna a mauris vulputate lacinia. Aenean viverra. Class aptent taciti sociosqu ad litora torquent per conubia nostra, per inceptos hymenaeos. Aliquam lacus. Mauris magna eros, semper a, tempor et, rutrum et, tortor.

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Donec molestie. Sed aliquam sem ut arcu. Phasellus sollicitudin. Vestibulum condimentum facilisis nulla. In hac habitasse platea dictumst. Nulla nonummy. Cras quis libero. Cras venenatis. Aliquam posuere lobortis pede. Nullam fringilla urna id leo. Praesent aliquet pretium erat. Praesent non odio. Pellentesque a magna a mauris vulputate lacinia. Aenean viverra. Class aptent taciti sociosqu ad litora torquent per conubia nostra, per inceptos hymenaeos. Aliquam lacus. Mauris magna eros, semper a, tempor et, rutrum et, tortor.

[view pictures of the artist](#)

[comment on this artist](#)

[About Us](#) | [Privacy Policy](#) | [Contact Us](#) | ©2006 Acunetix Ltd

The **artist** parameter is vulnerable to SQL Injection. The following payload modifies the query to look for an inexistent record. It sets the value in the URL query string to **-1**. Of course, it could be any other value that does not exist in the database. However, a negative value is a good guess because an identifier in a database is rarely a negative number.

In SQL Injection, the **UNION** operator is commonly used to attach a malicious SQL query to the original query intended to be run by the web application. The result of the injected query will be joined with the result of the original query. This allows the attacker to obtain column values from other tables.

```
GET http://testphp.vulnweb.com/artists.php?artist=-1 UNION SELECT 1, 2, 3 HTTP/1.1
```

Host: testphp.vulnweb.com



The following example shows how an SQL Injection payload could be used to obtain more meaningful data from this intentionally vulnerable site:

GET `http://testphp.vulnweb.com/artists.php?artist=-1 UNION SELECT 1, pass, cc FROM users WHERE uname='test'` HTTP/1.1

Host: testphp.vulnweb.com



How to Prevent an SQL Injection

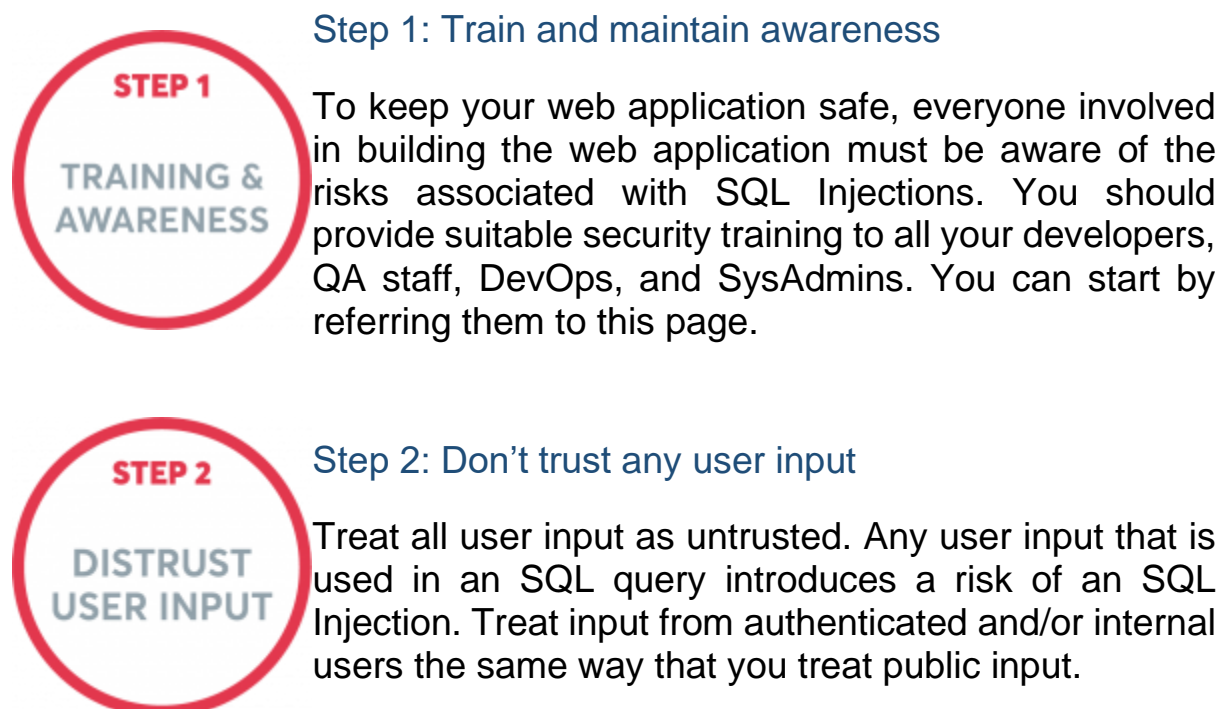
The only sure way to prevent SQL Injection attacks is input validation and parametrized queries including prepared statements. The application

code should never use the input directly. The developer must sanitize all input, not only web form inputs such as login forms. They must remove potential malicious code elements such as single quotes. It is also a good idea to turn off the visibility of database errors on your production sites. Database errors can be used with SQL Injection to gain information about your database.

If you discover an SQL Injection vulnerability, for example using an Acunetix scan, you may be unable to fix it immediately. For example, the vulnerability may be in open source code. In such cases, you can use a web application firewall to sanitize your input temporarily.

How to prepare SQL Injections (SQLi)-generic tips

Preventing SQL Injection vulnerabilities is not easy. Specific prevention techniques depend on the subtype of SQLi vulnerability, on the SQL database engine, and on the programming language. However, there are certain general strategic principles that you should follow to keep your web application safe.





Step 3: Use whitelists, not blacklists

Don't filter user input based on blacklists. A clever attacker will almost always find a way to circumvent your blacklist. If possible, verify and filter user input using strict whitelists only.



Step 4: Adopt the latest technologies

Older web development technologies don't have SQLi protection. Use the latest version of the development environment and language and the latest technologies associated with that environment/language. For example, in PHP use PDO instead of MySQLi.



Step 5: Employ verified mechanisms

Don't try to build SQLi protection from scratch. Most modern development technologies can offer you mechanisms to protect against SQLi. Use such mechanisms instead of trying to reinvent the wheel. For example, use parameterized queries or stored procedures.



Step 6: Scan regularly (with Acunetix)

SQL Injections may be introduced by your developers or through external libraries/modules/software. You should regularly scan your web applications using a web vulnerability scanner such as Acunetix. If you use Jenkins, you should install the Acunetix plugin to automatically scan every build.

An SQL injection needs just two conditions to exist – **a relational database that uses SQL, and a user controllable input which is directly used in an SQL query.**

In the example below, it shall be assumed that the attacker's goal is to exfiltrate data from a database by exploiting an SQL injection vulnerability present in a web application.

Supplying an SQL statement with improper input, for example providing a string when the SQL query is expecting an integer, or purposely inserting a syntax error in an SQL statement cause the database server to throw an error.

Errors are very useful to developers during development, but if enabled on a live site, they can reveal a lot of information to an attacker. SQL errors tend to be descriptive to the point where it is possible for an attacker to obtain information about the structure of the database, and in some cases, even to enumerate an entire database just through extracting information from error messages – this technique is referred to as *error-based SQL injection*. To such an extent, database errors should be disabled on a live site, or logged to a file with restricted access instead.

Another common technique for exfiltrating data is to leverage the UNION SQL operator, allowing an attacker to combine the results of two or more SELECT statements into a single result. This forces the application to return data within the HTTP response – this technique is referred to as *union-based SQL injection*.

The following is an example of such a technique. This can be seen on **testphp.vulnweb.com**, an intentionally vulnerable website hosted by Acunetix.

The following HTTP request is a normal request that a legitimate user would send.

```
GET http://testphp.vulnweb.com/artists.php?artist=1 HTTP/1.1  
Host: testphp.vulnweb.com
```

← → ↻ testphp.vulnweb.com/artists.php?artist=1

TEST and Demonstration site for Acunetix Web Vulnerability Scanner

[home](#) | [categories](#) | [artists](#) | [disclaimer](#) | [your cart](#) | [guestbook](#) | [AJAX Demo](#)

search art

artist: r4w8173

[Browse categories](#)
[Browse artists](#)
[Your cart](#)
[Signup](#)
[Your profile](#)
[Our guestbook](#)
[AJAX Demo](#)

Links
[Security art](#)
[Fractal Explorer](#)



view pictures of the artist

[comment on this artist](#)

[About Us](#) | [Privacy Policy](#) | [Contact Us](#) | ©2006 Acunetix Ltd

Although the above request looks normal, the artist parameter in the GET request's query string is vulnerable to SQL injection.

The SQL injection payload below modifies the query to look for an inexistent record by setting the value in the URL's query string to -1 (it could be any other value that does not exist in the database, however, an ID in a database is less likely to be a negative number).

In SQL injection, the UNION operator is commonly used to allow an attacker to join a malicious SQL query to the original query intended to be run by the web application. The result of the injected query will be joined to the result of the original query, allowing an attacker to exfiltrate data out of a database by obtaining values of columns from other tables.

GET http://testphp.vulnweb.com/artists.php?artist=-1 UNION SELECT 1, 2, 3 HTTP/1.1

Host: testphp.vulnweb.com



The above example proves that the query to the database can be modified to return data which an attacker may want to extract. The following example shows how an SQL injection payload could be used to exfiltrate data from this intentionally vulnerable site.

GET http://testphp.vulnweb.com/artists.php?artist=-1 UNION SELECT 1,pass,cc FROM users WHERE uname='test' HTTP/1.1

Host: testphp.vulnweb.com

← → ↻ testphp.vulnweb.com/artists.php?artist=-1 UNION SELECT 1,pass,cc FROM users

acunetix acuart

TEST and Demonstration site for Acunetix Web Vulnerability Scanner

[home](#) | [categories](#) | [artists](#) | [disclaimer](#) | [your cart](#) | [guestbook](#) | [AJAX Demo](#)

search art

artist: test

1234-5678-2300-9000

[view pictures of the artist](#)

[comment on this artist](#)

Links
[Security art](#)
[Fractal Explorer](#)



[About Us](#) | [Privacy Policy](#) | [Contact Us](#) | ©2006 Acunetix Ltd

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

Deep fake Definition

Deep fake is a form of **artificial intelligence** (AI) that can be used to create convincing hoax images, sounds, and videos. The term "deep fake" combines the deep learning concept with something fake.

Deep fake compiles hoaxed images and sounds and stitches them together using machine learning algorithms. As a result, it creates people and events that do not exist or did not actually happen.

Deep fake technology is most notably used for nefarious purposes, such as to mislead the public by spreading false information or propaganda. For example, deep fake videos could show a world leader

or celebrity saying something they have not said, which is also referred to as “fake news” that shifts public opinion.

What Are Deep fakes Used For?

Deep fake technology can be used for a wide variety of appalling purposes, including:

Scams and Hoaxes

Cyber criminals can use deep fake technology to create scams, false claims, and hoaxes that undermine and destabilize organizations.

For example, an attacker could create a false video of a senior executive admitting to criminal activity, such as financial crimes, or making false claims about the organization’s activity. Aside from costing time and money to disprove, this could have a major impact on the business’s brand, public reputation, and share price.

Celebrity Pornography

A major threat that deep fake poses is non-consensual pornography, which accounts for up to **96% of deep fakes** on the internet. Most of this targets celebrities. Deep fake technology is also used to create hoax instances of revenge porn.

Election Manipulation

Deep fake videos have been used to spread fake videos of world leaders like Donald Trump and Barack Obama, which raises concerns that it could be used for election manipulation. For example, there were widespread concerns that deep fake videos would affect the 2020 U.S. election campaign.

Social Engineering

Deep fake technology has been used within **social engineering** scams, with audio deep fakes fooling people into believing trusted individuals have said something they did not. For example, the **CEO of a U.K. energy firm** was tricked into believing he was

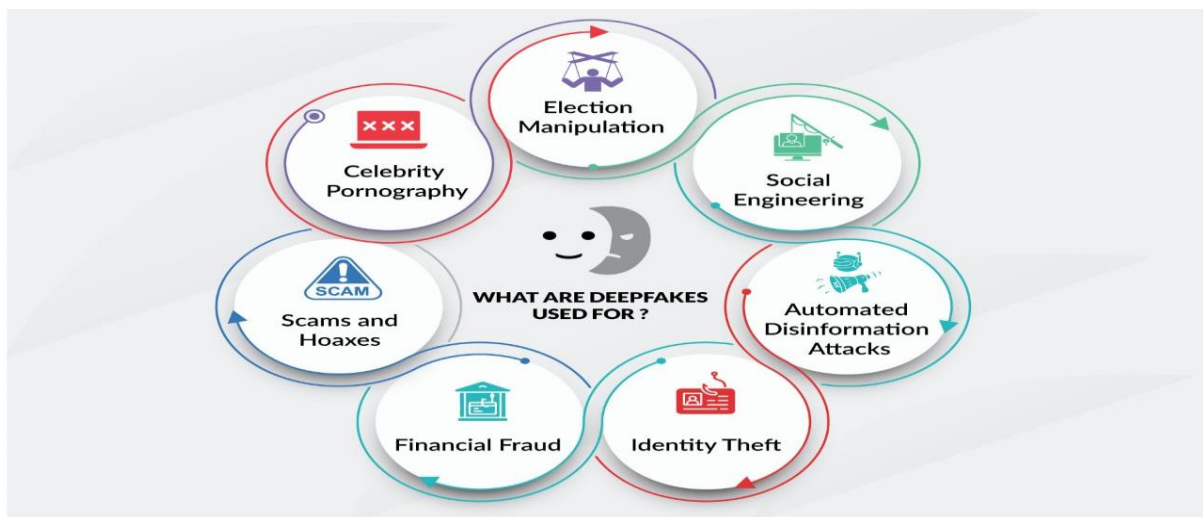
speaking to the chief executive of the company's parent company in Germany. The deep fake voice impersonated the chief executive and convinced the CEO to transfer €220,000 to a supposed Hungarian supplier's bank account.

Automated Disinformation Attacks

Deep fake can also be used to spread automated disinformation attacks, such as conspiracy theories and incorrect theories about political and social issues. A fairly obvious example of a deepfake being used in this way is a **fake video of Facebook founder Mark Zuckerberg** claiming to have "total control of billions of people's data," thanks to Spectre, the fictional organization in the James Bond novels and movies.

Identity Theft and Financial Fraud

Deep fake technology can be used to create new identities and steal the identities of real people. Attackers use the technology to create false documents or fake their victim's voice, which enables them to create accounts or purchase products by pretending to be that person.



How Was Deep fake Technology Created?

The term "deep fake" first came into the public domain in 2017, when a Reddit user with the username "deep fakes" shared doctored pornographic videos on the site. He did so by using Google's open-source, deep-learning technology to swap celebrities' faces onto the

bodies of pornographic performers. Modern deep fakes are descended from the original codes that were used to create these videos.

How Are Deep fakes Made?

There are several methods for creating deep fakes. One of the most popular is using the generative adversarial network (GAN), which trains itself to recognize patterns using algorithms, which can also be used to create fake images.

Another method is AI algorithms called encoders, which are used in face-replacement and face-swapping technology. The decoder retrieves and swaps images of faces, which enables one face to be superimposed onto a completely different body. Deep fakes use auto encoders, which go beyond the compression and decompression of classic encoders, enabling cyber criminals to create completely new images. Deep fake applications use two auto encoders, which enable images and movement to be transferred from one image onto another.

How to Spot Deep fakes

Deep fakes can be spotted by recognizing unusual activity or unnatural movement, including:

Unnatural Eye Movement

A lack of eye movement is a good sign of deep fakes. Replicating natural eye movement is challenging as peoples' eyes usually follow and react to the person they are speaking with.

A Lack of Blinking

A lack of blinking is also a flaw with deep faked videos. Replicating the natural, human action of regular blinking is difficult with deep fake technology.

Unnatural Facial Expressions and Facial Morphing

Deep fake technology involves morphing facial images, with faces simply being stitched from one image over another. This typically results in unusual or unnatural facial expressions.

Unnatural Body Shape

If a person's body does not look to have a natural shape, then it is most likely fake. Deep fake technology largely focuses on faces rather than the entire body, which leads to unnatural body shapes.

Unnatural Hair

Fake images cannot generate realistic individual characteristics, such as frizzy or messed-up hair.

Abnormal Skin Colours

Deep fakes are unable to replicate the natural colours of images and videos. This leads to them showing abnormal skin colours.

Awkward Head and Body Positioning

Deep fake images will often feature inconsistent or awkward-looking head and body positioning. Examples of this include jerky movements and distorted images when people move or turn their heads.

Inconsistent Facial Positions

Deep fake images will often feature inconsistent or awkward-looking head and body positioning. Examples of this include jerky movements and distorted images when people move or turn their heads.

Odd Lighting or Discoloration

Similar to the reasons for unnatural skin tones, deep fake images are also prone to discoloration, misplaced shadows, and unusual lighting.

Bad Lip-syncing

Deep fake videos will likely feature lip-syncing that does not align with the words being spoken by the people in the video.

Deep fakes vs. Shallow fake

Shallow fakes are videos that appear out of context or are edited using more simplistic tools. A good example of shallow fake is a **speech by Nancy Pelosi**, the U.S. Speaker of the House, edited to make her voice sound slurred, implying she was drunk.

How to Combat Deep fakes

Steps have already been taken to combat deep fakes and prevent the images and videos from being shared online.

Social Media Rules

Facebook has hired researchers from universities to help it build a deep fake detector, which enforces its ban on deep fakes. Twitter has policies in place to prevent fake content and is working to tag deepfake images that are not immediately removed. YouTube also vowed to block any deep fake content related to the 2020 U.S. election and census.

Research Lab Technologies

Researchers have been working on data science solutions that detect deep fakes. Many of these have quickly become ineffective as the attackers' technology evolves and creates more convincing results.

Filtering Programs

Filtering programs are also working to prevent deep fakes. AI firm Deep Trace's program acts in the same way as an antivirus or spam filter and diverts fake content into a quarantine zone, while Reality Defender, from AI Foundation, aims to tag manipulated content before it can do any damage.

Corporate Best Practices

One of the best ways to prevent deep fakes is for employees to understand the signs of fake images and videos. Corporate best practices include advising users on the telltale signs of cyber attacks and fraudulent online activity.

U.S. Legislation

Laws have already been passed in several U.S. states to criminalize deep fake pornography and prevent the technology's use around elections. A deep fake legislation was also introduced into the National Defence Authorization Act (NDAA) in December 2019.

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

Cyber Crime - What is, Types and Prevention

Any criminal activity carried out over the internet is referred to as cybercrime. With 4.5 million attacks in July 2020, India was the country with the highest number of attacks, making it vital to raise awareness about cybercrime.

The first incident of cybercrime was documented in 1973. A computer was used by a teller at a New York bank to pilfer over two million dollars. The first email spam was sent in 1978.

Cyber Crime Meaning

Let us start with the definition of cybercrime. Cybercrime refers to criminal conduct committed with the aid of a computer or other electronic equipment connected to the internet. Individuals or small groups of people with little technical knowledge and highly organized worldwide criminal groups with relatively talented developers and specialists can engage in cybercrime.

Cybercriminals or hackers who want to generate money, commit a majority of cybercrimes. Individuals and organizations are both involved in cybercrime. Aside from that, cybercriminals might utilize computers or networks to send viruses, malware, pornographic material, and other unlawful data.

To make money, cybercriminals engage in a range of profit-driven criminal acts, including stealing and reselling identities, gaining access to financial accounts, and fraudulently utilizing credit cards to obtain funds.

Types of cybercrime include:

1. Email and internet fraud.
2. Identity fraud (where personal information is stolen and used).
3. Theft of financial or card payment data.
4. Theft and sale of corporate data.
5. Cyber extortion (demanding money to prevent a threatened attack).
6. Ransomware attacks (a type of cyber extortion).
7. Crypto jacking (where hackers mine crypto currency using resources they do not own).
8. Cyber espionage (where hackers access government or company data).

9. Interfering with systems in a way that compromises a network.
10. Infringing copyright.
11. Illegal gambling.
12. Selling illegal items online.
13. Soliciting, producing, or possessing child pornography.

Cybercrime involves one or both of the following:

- Criminal activity *targeting* computers using viruses and other **types of malware**.
- Criminal activity *using* computers to commit other crimes.
Cybercriminals that *target* computers may infect them with malware to damage devices or stop them working. They may also use malware to delete or steal data. Or cybercriminals may stop users from using a website or network or prevent a business providing a software service to its customers, which is called a Denial-of-Service (DoS) attack.
Cybercrime that *uses* computers to commit other crimes may involve using computers or networks to spread malware, illegal information or illegal images.

Cybercriminals are often doing both at once. They may target computers with viruses first and then use them to spread malware to other machines or throughout a network. Some jurisdictions recognize a third category of cybercrime which is where a computer is used as an accessory to crime. An example of this is using a computer to store stolen data.

Cybercrimes Examples

1. Malware attacks

A malware attack is where a computer system or network is infected with a computer virus or other type of malware. A computer compromised by malware could be used by cybercriminals for several purposes. These include stealing confidential data, using the computer to carry out other criminal acts, or causing damage to data.

A famous example of a malware attack was the WannaCry ransomware attack, a global cybercrime committed in May 2017. **WannaCry** is a type of ransomware, malware used to extort money by holding the victim's data or device to ransom. The ransomware targeted a vulnerability in computers running Microsoft Windows.

When the WannaCry ransomware attack hit, 230,000 computers were affected across 150 countries. Users were locked out of their files and sent a message demanding that they pay a [Bit coin ransom](#) to regain access.

Worldwide, the WannaCry cybercrime is estimated to have caused \$4 billion in financial losses. To this day, the attack stands out for its sheer size and impact.

2. Phishing

A [phishing](#) campaign is when spam emails, or other forms of communication, are sent with the intention of tricking recipients into doing something that undermines their security. Phishing campaign messages may contain infected attachments or links to malicious sites, or they may ask the receiver to respond with confidential information. A famous example of a phishing scam took place during the [World Cup in 2018](#).

According to our report, [2018 Fraud World Cup](#), the World Cup phishing scam involved emails that were sent to football fans. These spam emails tried to entice fans with fake free trips to Moscow, where the World Cup was being hosted. People who opened and clicked on the links contained in these emails had their personal data stolen.

Another type of phishing campaign is known as [spear-phishing](#). These are targeted phishing campaigns which try to trick specific individuals into jeopardizing the security of the organization they work for.

Unlike mass phishing campaigns, which are very general in style, spear-phishing messages are typically crafted to look like messages from a trusted source. For example, they are made to look like they have come from the CEO or the IT manager. They may not contain any visual clues that they are fake.

3. Distributed DoS attacks

[Distributed DoS attacks \(DDoS\)](#) are a type of cybercrime attack that cybercriminals use to bring down a system or network. Sometimes connected IoT (Internet of Things) devices are used to launch DDoS attacks.

A DDoS attack overwhelms a system by using one of the standard communication protocols it uses to spam the system with connection requests. Cybercriminals who are carrying out cyber extortion may use

the threat of a DDoS attack to demand money. Alternatively, a DDoS may be used as a distraction tactic while another type of cybercrime takes place.

A famous example of this type of attack is the [2017 DDoS attack on the UK National Lottery website](#). This brought the lottery's website and mobile app offline, preventing UK citizens from playing. The reason behind the attack remains unknown, however, it is suspected that the attack was an attempt to blackmail the National Lottery.

Stolen credit card information

The most common cybercrime is when a person's credit card information is stolen and used unlawfully to acquire or purchase goods or services over the Internet. The stolen information is observed to be sold on the dark web to make fraudulent purchases or withdrawals, or used to commit identity theft. The consequences of stolen credit card information can result in severe financial losses, damaged credit ratings, and legal issues.

Hacking into a Government Website

Another type of cybercrime is tampering with sensitive government data. Hacking into a government website refers to unauthorized access to a government's computer system or network. Considered a highly illegal and unethical act that involves exploiting vulnerabilities in the system's security to gain access to sensitive information, and manipulate the system for malicious purposes. Such actions can lead to severe consequences, such as fines, imprisonment, and damage to national security.

Account Takeover (ATO) Fraud

Account Takeover (ATO) Fraud is a form of identity theft in which a fraudster manages to gain access to a victim's bank or credit card

accounts and uses them to make unauthorized transactions. Yahoo experienced a serious data breach from 2013 to 2016 that resulted in the theft of three billion user accounts. The attackers gained access to private information and passwords that were used to access user accounts on other online services. Most of this data is available even today on the dark web.

Compromised IoT devices

In 2016, over one million connected devices in the IoT were compromised by attackers who took advantage of existing software vulnerabilities. It is the largest DDoS attack to date and one that caused outages in the global DNS affecting popular services including Netflix, PayPal, Twitter, and many more.

Loss of control and access to content

The **WannaCry** attack, which was allegedly launched by North Korea, in 2017, unleashed ransomware that locked down content on user devices. This **ransomware** rapidly spread itself and infected 300,000 computers worldwide. The victims had to pay hundreds of dollars to restore their data.

Impact of cybercrime

Generally, cybercrime is on the rise. According to **Accenture's State of Cybersecurity Resilience 2021 report**, security attacks increased 31% from 2020 to 2021. The number of attacks per company increased from 206 to 270 year on year. Attacks on companies affect individuals too since many of them store sensitive data and personal information from customers.

A single attack – whether it's a data breach, malware, ransomware or DDoS attack - costs companies of all sizes an average of \$200,000, and many affected companies go out of business within six months of the attack, according to **insurance company Hiscox**.

Javelin Strategy & Research published an [Identity Fraud Study in 2021](#) which found that identity fraud losses for the year totalled \$56 billion.

For both individuals and companies, the impact of cybercrime can be profound – primarily financial damage, but also loss of trust and reputational damage.

How to report a cybercrime

India

Fake calls/sms/QR/links/apps claiming to be from bank

To report dial 1930 or visit www.cybercrime.gov.in

HOW TO FILE A COMPLAINT

The complaint regarding commission of cybercrime can be made to the in-charge of the cybercrime cells which are present almost in every city. To file a complaint alleging commission of a cybercrime the following documents must be provided:

1. In case of hacking the following information should be provided:

1. Server Logs
2. Copy of defaced web page in soft copy as well as hard copy format, if your website is defaced
3. If data is compromised on your server or computer or any other network equipment, soft copy of original data and soft copy of compromised data.
4. Access control mechanism details i.e.- who had what kind of the access to the compromised system
5. List of suspects – if the victim is having any suspicion on anyone.
6. All relevant information leading to the answers to following questions –
 - What? (what is compromised)
 - Who? (who might have compromised system)
 - when?(when the system was compromised)
 - why?(why the system might have been compromised)
 - where?(where is the impact of attack-identifying the target system from the network)
 - How many?(How many systems have been compromised by the attack)

2. In case of e-mail abuse, vulgar e-mail etc. the following information should be provided:

1. Extract the extended headers of offending e-mail and bring soft copy as well hard copy of offending e-mail.
2. Please do not delete the offending e-mail from your e-mail box.

3. Please save the copy of offending e-mail on your computer's hard drive.

Where to Report a Cyber Fraud?

1. Visit the nearest police station immediately.

2. To report cybercrime complaints online, visit the National Cyber Crime Reporting Portal. This portal can be accessed at <https://cybercrime.gov.in/>. In this portal, there are two sections. One section is to report crimes related to Women and Children (where reports can be filed anonymously as well). Another section is to report other types of cyber-crimes. You can also file a complaint offline by dialing the **helpline number 155260**.

3. In case you receive or come across a fraud sms, e-mail, link, phone call asking for your sensitive personal information or bank details, please report it on Maharashtra Cyber's web portal by visiting www.reportphishing.in

4. Refer to the latest advisories which are issued by CERT-IN on <https://www.cert-in.org/>

4. Report any adverse activity or unwanted behaviour to CERT-IN using following channels **E-mail: incident@cert-in.org.in**
Helpdesk: +91 1800 11 4949

Provide following information (as much as possible) while reporting an incident.

- Time of occurrence of the incident
 - Information regarding affected system/network
 - Symptoms observed
6. To report lost or stolen mobile phones, file a First Information Report (FIR) with the police. Post filing the FIR, inform Department of Telecommunications (DoT) through the **helpline number 14422** or file an online complaint on Central Equipment Identity Register (CEIR) portal by visiting <https://ceir.gov.in>.

After verification, DoT will blacklist the phone, blocking it from further use. In addition to this, if anyone tries to use the device using a different SIM card, the service provider will identify the new user and inform the police.

US:

File a report with the Internet Crime Complaint Center (IC3) as soon as possible. [Visit ic3.gov](https://www.ic3.gov) for more information.

UK:

Contact [Action Fraud](#) as soon as possible – find out more on their website here.

EU:

[Europol](#) has a useful website here which collates the relevant cybercrime reporting links for each EU member state.

UAE:

You can find information about how to report cybercrime in the UAE [on this official website here](#).

Australia:

The [Australian Cyber Security Centre](#) has information about how to report a cybercrime here.

How to protect yourself against cybercrime

Given its prevalence, you may be wondering how to stop cybercrime? Here are some sensible tips to protect your computer and your personal data from cybercrime:

1. Keep software and operating system updated

Keeping your software and operating system up to date ensures that you benefit from the latest security patches to protect your computer.

2. Use anti-virus software and keep it updated

Using anti-virus or a comprehensive internet security solution like [Kaspersky Premium](#) is a smart way to protect your system from attacks. Anti-virus software allows you to scan, detect and remove threats before they become a problem. Having this protection in place helps to protect your computer and your data from cybercrime, giving you piece of mind. Keep your antivirus updated to receive the best level of protection.

3. Use strong passwords

Be sure to use **strong passwords** that people will not guess and do not record them anywhere. Or use a reputable password manager to generate strong passwords randomly to make this easier.

4. Never open attachments in spam emails

A classic way that computers get infected by malware attacks and other forms of cybercrime is via email attachments in spam emails. Never open an attachment from a sender you do not know.

5. Do not click on links in spam emails or untrusted websites

Another way people become victims of cybercrime is by clicking on links in spam emails or other messages, or unfamiliar websites. Avoid doing this to stay safe online.

6. Do not give out personal information unless secure

Never give out personal data over the phone or via email unless you are completely sure the line or email is secure. Make certain that you are speaking to the person you think you are.

7. Contact companies directly about suspicious requests

If you are asked for personal information or data from a company who has called you, hang up. Call them back using the number on their official website to ensure you are speaking to them and not a cybercriminal. Ideally, use a different phone because cybercriminals can hold the line open. When you think you've re-dialled, they can pretend to be from the bank or other organization that you think you are speaking to.

8. Be mindful of which website URLs you visit

Keep an eye on the URLs you are clicking on. Do they look legitimate? Avoid clicking on links with unfamiliar or URLs that look like spam. If your internet security product includes functionality to secure online transactions, ensure it is enabled before carrying out financial transactions online.

9. Keep an eye on your bank statements

Spotting that you have become a victim of cybercrime quickly is important. Keep an eye on your bank statements and query any unfamiliar transactions with the bank. The bank can investigate whether they are fraudulent.

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

Online payment fraud is a serious and growing problem in the digital world. It refers to any fraudulent or unauthorized transaction that occurs online using a payment method such as a credit card, debit card, Net Banking, UPI or wallet. Online payment fraud can occur in various ways, such as phishing, data theft, identity theft or chargeback fraud.

In this article, we will discuss the different types of online payment fraud, their impact on businesses and customers, and the strategies to prevent and mitigate them. But before that, let's dive deep into what payment fraud is.

What is Payment Fraud?

Payment fraud is a type of financial fraud or online payment scam where fraudsters use unauthorised methods to steal money or sensitive financial information. It can happen in various ways, but it often involves scammers stealing credit card / bank details, making fake cheques, or using stolen IDs to make unauthorized purchases.

The following features characterise online payment fraud:

- It is often carried out by organized criminal groups or networks that use sophisticated tools and techniques to steal and use payment information.
- It exploits the vulnerabilities and loopholes in online payment systems and processes, such as weak security measures.
- It targets businesses and customers across various industries and segments such as e-commerce, travel, gaming, education, healthcare, etc.

6 Different Types of Payment Frauds

The most common types of online payment fraud occur via phishing or spoofing, data theft, identity theft and chargeback. We have explained these in detail below.

1. Online Phishing or Spoofing

Online phishing involves accessing your personal information through fraudulent emails or websites claiming to be legitimate. This information can include usernames, passwords, credit card numbers, or bank account numbers.

The most widely used method for online phishing is to redirect you from an email or SMS to an 'official' website, where you are asked to update your personal information. Thus, you are tricked into revealing

personal information that you would ideally not reveal to anyone. You can also be redirected to make a payment on a website that looks legitimate but is created to capture your card details so they can be used later.

According to reports, India is the third-most targeted country for online phishing attacks, after the US and Russia.

2. Data Theft

Data theft is the illegal copying or accessing of digital information, such as personal, financial, or confidential data. Data thieves can use various methods, such as phishing, hacking, or social engineering, to obtain data from individuals or organisations. The stolen data can be used for identity theft, fraud, ransomware, or other malicious purposes. Data theft can cause serious harm to the victims, such as financial loss, reputational damage, legal issues, or emotional distress.

To prevent data theft, it is essential to use strong passwords, encryption, antivirus software, and secure networks. To protect customer data, online platforms use advanced security techniques such as tokenisation and encryption. Razorpay is a leader in data security and has achieved the ISO-27001 certification, which demonstrates adherence to the highest data protection standards.

3. Identity Theft

Identity theft is a malicious act where your personal information such as driver's license, PAN or Aadhaar details are illicitly obtained and exploited for fraudulent financial activities. This includes unauthorised transactions and the establishment of counterfeit accounts, thereby inflicting financial and emotional distress. Recovering from identity theft is a burden some and time-consuming process, often involving legal and financial complexities.

This crime results in financial loss and can even damage your reputation. Identity theft victims are forced to spend significant time and resources rectifying the aftermath, often requiring legal and financial assistance. To combat this issue, it is essential to prioritise personal data security through enhanced awareness and robust security measures.

4. Chargeback Fraud or Friendly Fraud

Let's say a customer makes an online purchase. Later, they claim that the purchase was made fraudulently and ask for friendly fraud chargebacks – even though they made it themselves! In simple terms, a friendly fraud chargeback is an order from a bank to a business, asking it to return the amount paid for a possible fraudulent purchase. The business processes the transaction since it seems legitimate, only to be issued with a chargeback later on.

Chargeback online payment frauds cause GMV losses and are a hassle for businesses. [Razorpay's Chargeback Guide](#) can help you understand why friendly fraud chargebacks happen and what steps can be taken against these charges.

5. Card-not-present (CNP) fraud

Perpetrators exploit stolen cardholder data to make remote online purchases. This is often acquired through phishing, malware, data breaches or social engineering. In this scenario, merchants face chargeback risks.

6. Account takeover (ATO) fraud

Fraudsters infiltrate online accounts by stealing credentials or exploiting security weaknesses. They can then enable unauthorised transactions, account modifications and fund transfers, affecting your financial security.

How to Prevent Payment Fraud?

To protect against **online payment frauds**, businesses must implement following effective strategies:

Transaction Monitoring

1. Continuously employ advanced real-time monitoring techniques like condition monitoring, digital experience monitoring and computational monitoring to scrutinise all transactions, identifying and flagging any irregularities or suspicious patterns.
2. Utilise cutting-edge algorithms like the random forest, support vector machine and logistic regression to analyse transaction data swiftly and accurately. This ensures a proactive approach to fraud detection and risk mitigation.
3. Maintain a vigilant watch over financial activities, leveraging anomaly detection methods like isolation forest and K-means to identify deviations from established norms swiftly. This proactive surveillance allows for timely investigation and intervention, enhancing the security and integrity of the system. It ultimately fosters a safe and trusted transaction environment for all stakeholders involved.

Restrict Access to Sensitive Data

1. Stringently restrict access to sensitive customer data, employing robust security protocols and access controls.
2. Implement encryption and multi-factor authentication to fortify storage mechanisms. This safeguards customer information from unauthorised access and potential breaches.
3. Adhere to best industry practices like using authentication, authorisation and encryption, along with compliance standards like the Personal Data Protection Act (PDPA) in India to uphold data

privacy and security standards. This mitigates risks associated with data leaks or cyber threats.

4. Utilise secure storage solutions and regularly update security measures to adapt to evolving cyber threats. This instils confidence in customers regarding the protection of their private information and reinforces trust in the organisation's commitment to data security and privacy.

Encryption

1. Encrypt data using industry-leading encryption protocols, including strong encryption algorithms like Transport Layer Security (TLS) or Secure Sockets Layer (SSL), to establish secure communication channels. This ensures the utmost data security during transmission, rendering it unintelligible to unauthorised parties and mitigating the risk of eavesdropping or tampering.
2. Continuously update encryption standards and stay informed about emerging threats to adapt and strengthen encryption methods. This bolsters the overall security posture and guarantees the confidentiality and integrity of data exchanged over networks.

Authentication Procedures

1. Integrate multi-factor authentication (MFA) as a robust identity verification measure to ensure user security.
2. Mandate users to authenticate their identity using at least two independent factors, such as a password, biometric scan, smart card, or one-time verification code. This dual or multi-step verification process significantly enhances security by adding layers of protection, making it exponentially more difficult for unauthorised individuals to gain access.
3. Regularly update and strengthen MFA mechanisms in response to evolving cyber threats, maintaining a proactive stance in safeguarding user identities and preventing unauthorised access to sensitive systems and information.

Stay informed about Fraud Trends

1. Stay vigilant by learning about the ever-evolving landscape of fraud and cyber threats.
2. Continuously monitor the latest fraud trends, techniques and tactics employed by malicious actors within the digital realm. This proactive approach allows for the swift adjustment of security measures to stay ahead of potential threats.
3. Collaborate with industry experts, engage in information sharing within cyber security communities and participate in threat intelligence networks to gather insights into emerging fraud patterns. Utilise this knowledge to adapt security protocols, update detection mechanisms, and reinforce protective measures. This will effectively

help thwart new and sophisticated fraudulent activities and preserve the trust and integrity of systems.

The Effect of Payment Fraud on Businesses

As per the current terms and conditions, a credit card issuer (i.e., the bank) does not consider the cardholder liable for any fraudulent activity for both card-present and card-not-present online payment frauds.

Therefore, online payment frauds involving credit cards have a significant effect on the business community and a merchant's bottom line. Every time a customer issues a chargeback, it leads to a loss of both inventory and GMV. This is especially true for retail establishments, where the profit margins are usually small.

The 'subscription' industry continues to have the highest rate of online **payment fraud** for **two main reasons**:

1. Subscriptions are essentially a card-dependent service, wherein the USP of the service is that one does not have to make manual payments. It is easy to claim that one's card was used without knowledge in such a scenario.
2. Hackers use subscription services to 'test' cards. Online subscription services usually provide a one-month free trial, but one needs a credit card to initiate the trial period. Since the value is negligible, such payments usually go unnoticed by the card owner. If the card details are incorrect, the subscription business shares a detailed authorisation error, thus making it easy for the hacker to modify their strategy and continue using the card.

Who is affected by Online Payment Fraud?

Payment fraud primarily affects businesses and merchants who bear the financial burden of chargebacks and inventory losses. **Payment fraud** has wide-ranging consequences for businesses, leading to financial losses, damaged reputation, and eroding customer trust. To mitigate these challenges, businesses must invest in robust fraud prevention and detection measures to protect their bottom line and reputation in an environment where online payment fraud remains a significant threat.

Online payment fraud also impacts customers and payment service providers. Customers face wide ranging impacts including financial losses and potential identity theft.

Payment service providers can lose money and credibility, facing compliance challenges under regulations like PSD2. PSD2 introduced Strong Customer Authentication (SCA) and Liability Shift, impacting who covers losses in fraudulent transactions. This has implications for both sellers and payment service providers. Payment fraud's consequences ripple throughout the online payment eco system.

How Razorpay Helps Businesses Reduce Fraud and Mitigate Risk
Razorpay is committed to helping businesses reduce fraud and mitigate risk during online transactions. We employ sophisticated systems for detecting both 'merchant fraud' and 'customer fraud.'

Systems for detecting 'merchant fraud'

Razorpay utilises advanced algorithms and pattern recognition to identify fraudulent merchant activities. This includes –

1. **KYC checks:** Adhering to strict KYC norms even before we on board a business is an integral part of online payment fraud mitigation. We have an in-house 'Risk and Activation' team that runs background checks on new businesses and vets them before they are on boarded onto our [payment gateway](#).
2. We take this check one level higher by monitoring all suspicious and potentially fraudulent businesses and the transactions that originate from them.
3. **Transaction monitoring:** Razorpay Payment Gateway has an inbuilt 'risk' logic. A sudden spike in transaction velocity (number of transactions per minute / hour / day), volume (amount transacted for), or pattern (international orders for a local brand) is an indicator of online payment fraud. Our systems immediately flag such transactions for further investigation. The logic pathway can easily differentiate between standard day-to-day transactions and those that carry a high probability of risk.

Systems for detecting 'customer fraud'

Our platform employs robust mechanisms to detect suspicious customer behaviour and unauthorised transactions. This includes –

1. **Checking for hotlisted cards:** Every time a card is used for payment, our gateway connects with the card provider to check if the card has been hotlisted. (Hotlisting means that the card has been blocked temporarily / permanently). This is done in real time so that a verified transaction is still completed within seconds, while a suspicious one gets flagged.
2. **Pattern-based transaction monitoring:** We use geographical and pattern-based transaction monitoring to identify suspicious transactions. This helps in preempting and preventing chargeback and other types of fraud. We have a hit ratio of being able to identify 85% of fraudulent cases in advance.

Online Fraud Prevention: The Present and the Future

Online payment fraud is a growing concern as more transactions are being conducted online. While it is impossible to eliminate fraud completely, there are measures in place to minimise the risk. Here are some current measures being used –

3D Secure (3DS) protocol:

VISA developed this protocol to keep its customers safe. It has been adopted by other card companies like American Express, MasterCard and JCB International. It is a more robust, secure and mobile-friendly specification that allows for frictionless transactions. It also mitigates fraud and shifts the liability of chargebacks from businesses to the customer's bank.

Two-factor authentication (2FA):

This is mandatory for all cardholders and card-issuing banks in India. The Reserve Bank of India (RBI) has mandated online alerts for all card transactions, even those where the cardholder physically swipes their card at a PoS system.

De-activation request:

You have the option to issue a de-activation request immediately and hotlist your card for all transactions considered suspicious.

FCORD initiative:

The Indian government has appointed a nodal agency for dealing with phone fraud, called the FCORD initiative. Razor pay is in touch with the Ministry of Home Affairs (MHA), which has designated the FCORD as the nodal agency for reporting and preventing cybercrime frauds in India.

While it will take time to achieve a zero-fraud system, companies are constantly building new processes to minimise online payment fraud risk. It is important to remain vigilant and adopt these measures. While 3D Secure and 2FA provide vital security measures, innovative techniques like machine learning and link analysis enhance fraud detection. Staying informed about emerging fraud trends and using test rules for scenario simulation further strengthen defense against this persistent threat. Let us understand these innovative solutions in detail

—

Machine learning:

This is a branch of artificial intelligence that enables systems to learn from data and improve their performance. This enables faster and more accurate fraud detection and prevention.

Link analysis:

This technique uses network history to identify connections and relationships between entities, such as customers, merchants, transactions, devices, etc. This can help uncover hidden patterns and anomalies in data and reveal complex fraud schemes.

Test rules:

You can create and apply these rules to transactions to simulate different scenarios and outcomes. This can help you evaluate the

effectiveness of your fraud prevention measures and optimise them for better results.

Stay updated about new fraud trends:

As online payments become more popular and diverse, new types of fraud may arise, such as mobile payment fraud, social media payment fraud, cryptocurrency payment fraud, etc. You need to stay aware of these trends and adapt your strategies accordingly.

Conclusion

Online payment fraud is a pervasive and ever-evolving threat in the digital world. Businesses and individuals must remain vigilant to protect themselves from various types of payment fraud. Razor pay's commitment to fraud prevention, along with the continuous advancement of technology, offers hope for a safer online payment environment in the future.

The bottom line remains: If you are building an e-commerce website, remember to follow all the protocols mentioned above and minimise the risk of online payment fraud. Alternatively, find a payment gateway (hello there!) with stringent security protocols already in place. We're just a click of a button away!