Wireless network and security

If communication takes place between any two earth stations through a satellite, then it is called as **satellite communication**. In this communication, electromagnetic waves are used as carrier signals. These signals carry the information such as voice, audio, video or any other data between ground and space and vice-versa. This tutorial is meant to provide the readers an overview of Satellite Communication and how it works.

In general terms, a **satellite** is a smaller object that revolves around a larger object in space. For example, moon is a natural satellite of earth.

We know that **Communication** refers to the exchange (sharing) of information between two or more entities, through any medium or channel. In other words, it is nothing but sending, receiving and processing of information.

If the communication takes place between any two earth stations through a satellite, then it is called as **satellite communication**. In this communication, electromagnetic waves are used as carrier signals. These signals carry the information such as voice, audio, video or any other data between ground and space and vice-versa.

Soviet Union had launched the world's first artificial satellite named, Sputnik 1 in 1957. Nearly after 18 years, India also launched the artificial satellite named, Aryabhata in 1975.

## **Need of Satellite Communication**

The following two kinds of propagation are used earlier for communication up to some distance.

* **Ground wave propagation** − Ground wave propagation is suitable for frequencies up to 30MHz. This method of communication makes use of the troposphere conditions of the earth.
* **Sky wave propagation** − The suitable bandwidth for this type of communication is broadly between 30–40 MHz and it makes use of the ionosphere properties of the earth.

The maximum hop or the station distance is limited to 1500KM only in both ground wave propagation and sky wave propagation. Satellite communication overcomes this limitation. In this method, satellites provide **communication for long distances**, which is well beyond the line of sight.

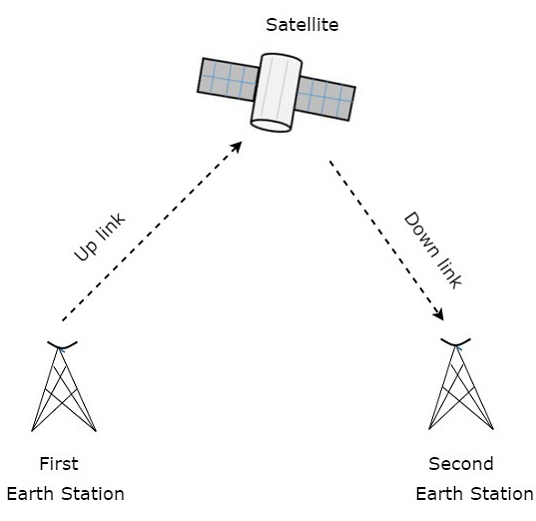
Since the satellites locate at certain height above earth, the communication takes place between any two earth stations easily via satellite. So, it overcomes the limitation of communication between two earth stations due to earth’s curvature.

## **How a Satellite Works**

A **satellite** is a body that moves around another body in a particular path. A communication satellite is nothing but a microwave repeater station in space. It is helpful in telecommunications, radio and television along with internet applications.

A **repeater** is a circuit, which increases the strength of the received signal and then transmits it. But, this repeater works as a **transponder**. That means, it changes the frequency band of the transmitted signal from the received one.

The frequency with which, the signal is sent into the space is called as **Uplink frequency**. Similarly, the frequency with which, the signal is sent by the transponder is called as **Downlink frequency**. The following figure illustrates this concept clearly.



The transmission of signal from first earth station to satellite through a channel is called as **uplink**. Similarly, the transmission of signal from satellite to second earth station through a channel is called as **downlink**.

**Uplink frequency** is the frequency at which, the first earth station is communicating with satellite. The satellite transponder converts this signal into another frequency and sends it down to the second earth station. This frequency is called as **Downlink frequency**. In similar way, second earth station can also communicate with the first one.

The process of satellite communication begins at an earth station. Here, an installation is designed to transmit and receive signals from a satellite in an orbit around the earth. Earth stations send the information to satellites in the form of high powered, high frequency (GHz range) signals.

The satellites receive and retransmit the signals back to earth where they are received by other earth stations in the coverage area of the satellite. Satellite's **footprint** is the area which receives a signal of useful strength from the satellite.

## **Pros and Cons of Satellite Communication**

In this section, let us have a look at the advantages and disadvantages of satellite communication.

Following are the **advantages** of using satellite communication:

* Area of coverage is more than that of terrestrial systems
* Each and every corner of the earth can be covered
* Transmission cost is independent of coverage area
* More bandwidth and broadcasting possibilities

Following are the **disadvantages** of using satellite communication −

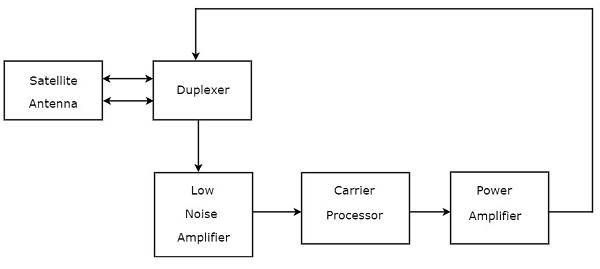
* Launching of satellites into orbits is a costly process.
* Propagation delay of satellite systems is more than that of conventional terrestrial systems.
* Difficult to provide repairing activities if any problem occurs in a satellite system.
* Free space loss is more
* There can be congestion of frequencies.

## **Applications of Satellite Communication**

Satellite communication plays a vital role in our daily life. Following are the applications of satellite communication −

* Radio broadcasting and voice communications
* TV broadcasting such as Direct To Home (DTH)
* Internet applications such as providing Internet connection for data transfer, GPS applications, Internet surfing, etc.
* Military applications and navigations
* Remote sensing applications
* Weather condition monitoring & Forecasting
* The subsystem, which provides the connecting link between transmitting and receiving antennas of a satellite is known as **Transponder**. It is one of the most important subsystem of space segment subsystems.
* Transponder performs the functions of both transmitter and receiver (Responder) in a satellite. Hence, the word ‘Transponder’ is obtained by the combining few letters of two words, Transmitter **(Trans)** and Responder **(ponder)**.

## **Block diagram of Transponder**

* Transponder performs mainly **two functions**. Those are amplifying the received input signal and translates the frequency of it. In general, different frequency values are chosen for both uplink and down link in order to avoid the interference between the transmitted and received signals.
* The **block diagram** of transponder is shown in below figure.
* 

We can easily understand the operation of Transponder from the block diagram itself. The function of each block is mentioned below.

* **Duplexer** is a two-way microwave gate. It receives uplink signal from the satellite antenna and transmits downlink signal to the satellite antenna.
* **Low Noise Amplifier** (LNA) amplifies the weak received signal.
* **Carrier Processor** performs the frequency down conversion of received signal (uplink). This block determines the type of transponder.
* **Power Amplifier** amplifies the power of frequency down converted signal (down link) to the required level.

**Satellite image Security** is playing a vital role in the field of communication system and Internet. This work is interested in securing transmission o images on the Internet, in public or local networks. To enhance the security of transmission in network communication, a hybrid encryption algorithm based on Advanced Encryption Standard (AES) and Rivest Shamir Adleman (RSA) algorithms is proposed. AES algorithm is used for data transmission because of its higher efficiency in block encryption and RSA algorithm is used for the encryption of the key of the AES because of its management advantages in key cipher. Our encryption system generates a unique password every new session of encryption. Cryptanalysis and various experiments have been carried out and the results were reported in this paper, which demonstrate the feasibility and flexibility of the proposed scheme.

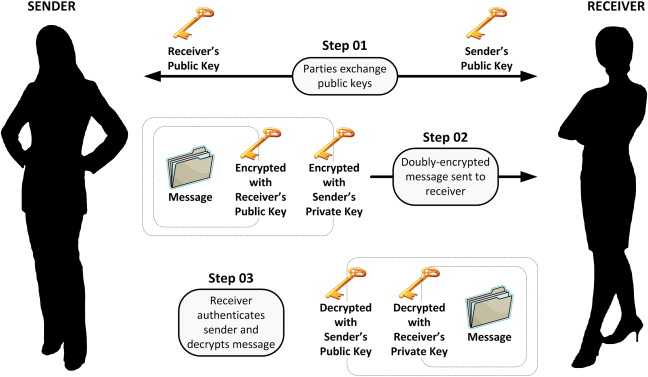
**General Satellite Encryption and Issues**

One of the problems common to all forms of satellite encryption relates to signal degradation. Satellite signals are typically sent over long distances using comparatively low-power transmissions, and must frequently contend with many forms of interference, including terrestrial weather, solar and cosmic radiation, and many other forms of electromagnetic noise. Such disturbances can cause errors or gaps to emerge in the signal that carries a satellite transmission from its source to its destination. Depending on the encryption algorithm chosen, this situation can be particularly problematic for encrypted satellite transmissions, since the entire [encrypted message](https://www.sciencedirect.com/topics/computer-science/encrypted-message) may be irretrievably lost if even a single bit of data is out of place. To resolve this problem, a checksum or cryptographic [hash function](https://www.sciencedirect.com/topics/computer-science/hash-function) may be applied to the encrypted message to allow errors to be identified and reconciled upon receipt. This approach comes at a cost however – appending checksums or [error-correcting code](https://www.sciencedirect.com/topics/computer-science/error-correcting-code) to an encrypted message increases the length of the message, and by extension increases the time required for the message to be transmitted. The result, of course, is that a satellite’s actual overall communications capacity is commonly lower than its theoretical capacity, due to the extra burden that is placed on its limited resources by this [communications overhead](https://www.sciencedirect.com/topics/computer-science/communication-overhead).

Another common problem associated with two-way encrypted satellite communications relates to establishing the identity of the sender of a message. Most modern satellites, for example, are designed to receive and respond to signals that control their onboard functions. Such satellites need to be certain that the control signals they receive from the ground originate from an authorized source. In addition to control signals, senders of other types of satellite transmissions commonly need to be authenticated as well. An intelligence agency receiving a satellite transmission from one of its operatives, for example, needs to establish that the transmission is genuine. To establish the identity of the sender, the message needs to be encrypted in such a way that from the recipient’s perspective, only a legitimate sender could have encoded the message. The sender, of course, also wants to ensure that the message is protected while in transit, and thus desires that only an authorized recipient would be able to decode the message upon receipt. Both parties to the communication must therefore agree to use an encryption algorithm that serves to identify the authenticity of the sender while affording a sufficient level of protection to the message while it is in transit to its destination. Although keyless encryption algorithms may satisfy these two criteria, such algorithms are usually avoided in satellite communications, since the satellite may become useless if the keyless encryption algorithm were to be compromised, and satellites are expensive to replace. This problem also extends to the terrestrial equipment used to encrypt satellite signals prior to transmission and decrypt those signals after receipt. Keyed encryption algorithms are therefore typically used to protect information transmitted via satellite. Even keyed methods of encryption can be problematic when it comes to satellite communications, however.

To gain insight into the problems associated with keyed encryption, one might first consider the case of a symmetrically keyed encryption algorithm, wherein the same key is used to both encode and decode a message. If party *A* wants to communicate with party *B* via satellite using this method, then both *A* and *B* must agree on a secret key in advance of the communication. As long as the key remains secret, it also serves to authenticate both parties. If party *A* also wants to communicate with party *C*, however, then *A* and *C* must agree on their own unique secret key, otherwise party *B* could masquerade as *A* or *C*, and vice-versa. A keyed encryption approach to two-way satellite communication thus requires that each party establish a unique secret key with every other party with whom they would like to communicate. To further compound this problem, each party must obtain all of its secret keys in advance, because possession of an appropriate key is a necessary prerequisite to establishing a secure communications channel with another party.

To resolve these issues, an asymmetrically keyed encryption algorithm may be adopted, wherein the key used to encrypt a message is different from the key used to decrypt the message. Such an approach requires each party to maintain only two keys, one of which is kept private, and the other of which is made publicly-available. If party *A* wants to send party *B* a secure transmission, *A* first asks *B* for her public key, which can be transmitted over an unsecured connection. Party *A* then encodes a secret message using *B’s* public key. The message is secure because only *B’s* private key can decode the message. To authenticate herself to *B*, party *A* needs only to re-encode the entire message using her own private key before transmitting the message to *B*. Upon receiving the message, *B* can establish whether it was sent by *A*, because only *A’s* private key could have encoded a message that can be decoded with *A’s* public key. This process is depicted in Figure 38.4 below.



Unfortunately, even this approach to secure two-way satellite communication is not entirely foolproof. To understand why, consider how a malicious party *M* might interject himself between *A* and *B* in order to intercept the secure communication. To initiate the secure transmission, *A* must request *B’s* public key over an unsecure channel. If this request is intercepted by *M*, then *M* can supply *A* with his own (that is, *M’s*) public key. *A* will then encrypt the message with *M’s* public key, after which she will re-encrypt the result of the first encryption operation with her own private key. *A* will then transmit the encrypted message to *B*, which will once again be intercepted by *M*. Using *A’s* public key in conjunction with his own private key, *M* will be able to decrypt and read the message. *A* will not know that the message has been intercepted, and *B* will not know that a message was even sent. Note that intercepting a secure communication is particularly easy for *M* if he owns or controls the satellite through which the message is being routed. In addition to the risk of interception, asynchronously keyed encryption algorithms are typically at least 10,000 times slower than synchronously keyed encryption algorithms – a situation that may place an enormously large burden on a satellite’s limited computational resources. Until a means is developed of dynamically and securely distributing synchronous keys, satellite-based encryption will always require trade-offs among security, computational complexity, and ease of implementation.

**Instant messaging**

The [Internet](https://computer.howstuffworks.com/internet/basics/internet-infrastructure.htm) has revolutionized the way we communicate. [E-mail](https://computer.howstuffworks.com/e-mail-messaging/email.htm) has been the most rapidly adopted form of communication ever known. Less than two decades ago, not many people had heard of it. Now, many of us e-mail[instead of writing letters or even calling people on the phone](https://computer.howstuffworks.com/e-mail-messaging/email.htm). People around the world send out billions of e-mail messages every day.

But sometimes even e-mail isn't fast enough. You might not know if a person you want to e-mail is online at that moment. Also, if you're e-mailing back and forth with someone, you usually have to click through a few steps. This is why **instant messaging** (IM) has become so popular.

With IM, you can keep a list of people you interact with. You can IM with anyone on your **buddy list** or **contact list** as long as that person is online. You type messages to each other into a small window that shows up on both of your screens.

Most IM programs provide these features:

* **Instant messages** - Send notes back and forth with a friend who is online
* **Chat** - Create a chat room with friends or co-workers
* **Web links** - Share links to your favorite Web sites
* **Video** - Send and view videos, and chat face to face with friends
* **Images** - Look at an image stored on your friend's [computer](https://computer.howstuffworks.com/pc.htm)
* **Sounds** - Play sounds for your friends
* **Files** - Share files by sending them directly to your friends
* **Talk** - Use the Internet instead of a phone to actually talk with friends
* **Streaming content** - Real-time or near-real-time [stock](https://money.howstuffworks.com/personal-finance/financial-planning/stocks.htm) quotes and news
* **Mobile capabilities** - Send instant messages from your [cell phone](https://electronics.howstuffworks.com/cell-phone.htm)

In this article, you will learn about the history of instant messaging and how it works. You will also learn what the major IM programs are, what makes them different from each other and what the future holds for IM.

In the early 1990s, people began to spend more and more time on the Internet. Creative software developers designed **chat-room** software and set up chat rooms on Web servers. In a chat room, a group of people can type in messages that are seen by everyone in the "room." Instant messages are basically a chat room for just two people.­

**Internet privacy**

Internet **privacy** is a subset of data **privacy**. **Privacy** concerns have been start from the beginnings of large-scale **computer** sharing. **Privacy** can entail either personally identifiable information (PII) or non-PII information such as a site visitor's behavior on a website.

What is privacy and security on the Internet?

**Privacy**: It helps to block websites, **internet** browsers, cable companies, and **internet** service providers from tracking your information and your browser history. **Security**: It helps protect you from other people accessing your personal information and other data.

What is Internet privacy and why is it important?

**Internet privacy** is the right to keep sensitive data and information produced as a result of using the web, **private**. ... The thing about the **Internet** is that to interact with most websites, some information is **necessary**.

Why is privacy and security important?

The amount of information that companies must keep **secure** is increasing. As a result of technological advances, companies are constantly gaining more data about their clients and customers. They must ensure that data **security** and **privacy** remain a priority to protect against costly breaches

.

What does Digital Privacy mean?

**Digital Privacy is** a collective definition that encompasses three sub-related categories; information **privacy**, communication **privacy**, and individual **privacy**. ... While our data **is** exposed through **digital** mediums, such as social media, we also more sensitized to **privacy** issues.

Why is Internet privacy so important?

Protect your identity and personal **privacy** from theft  
  
Your identity is extremely valuable. Being able to prove you are you is **important** for most aspects of life – from applying for a home loan to getting a passport. ... That's why it's extremely **important** to protect your personal **privacy** online.

Can you have privacy without security?

**You can have security without privacy**, but **you can**'t **have privacy without security**. **Privacy** includes the laws and regulations requiring companies to protect your data, and **security** is the technical method used to protect that data.

Does Internet privacy matter?

**Online privacy** is important for numerous reasons. You don't want to share details of your personal life with strangers and it's hard to be sure what personal information is gathered and by whom: information collected by one company might be shared with another

We typically define security as the protection against unauthorized access, with some including explicit mention of integrity and availability. Security controls are put in place to control who can access the information, while privacy is more granular, controlling what and when they can access specific data. For example, if you bank with a national financial institution, all of the tellers in the country may be provisioned (i.e., granted security access) to access your account detail. This provides the flexibility for you, the customer, to visit a branch in your hometown, a branch on the west coast during a business trip or a Florida branch when vacationing. But privacy is another layer. While the teller may be provisioned to view all customers' account detail, privacy only allows access when a business need exists; such as a customer walking into a branch in another city to access their accounts. But privacy disallows that same teller viewing their neighbors account balance or perhaps the balance of a famous person, just because they are interested – despite their access privileges granting them access.

So the business application of the terms privacy and security are very different, with significant overlap. The old adage reads, "You can't have privacy without security, but you can have security without privacy." Let's exam why this might be true, but first address the amount of data being compiled, the improved abilities to leverage that data for business decisions, and new internet-enabled devices that are collecting the data – often without consumers' knowledge.

**Identity Management**

The broad aim of identity management (IdM) is to manage the resources of an organization (such as files, records, data, and communication infrastructure and services) and to control and manage access to those resources in an efficient and accurate way. Consequently, identity management is both a technical and process-orientated concept. The concept of IdM has begun to be applied in identities-related applications in enterprises, governments, and Web services since 2002. As the integration of heterogeneous wireless networks becomes a key issue in towards the next generation (NG) networks, IdM will be crucial to the success of NG wireless networks. A number of issues, such as mobility management, multi-provider and securities require the corresponding solutions in terms of user authentication, access control, and so forth. IdM in NG wireless networks is about managing the digital identity of a user and ensuring that users have fast, reliable, and secure access to distributed resources and services of an next generation network (NGN) and the associated service providers, across multiple systems and business contexts.

objectives As IdM can be used in different areas such as enterprise, government, Web services,

define the identity of an entity (a person, place, or thing).

• It should store relevant information about entities, such as names and credentials, in a secure, flexible, customisable store.

• It should make the information accessible through a set of standard interfaces.

• It should provide a less complex, distributed, and high performance infrastructure for identity management.

• It should help to manage relationships between the enterprise and the resources and other entities in a defined context.

**Main Aspects**

Authentication

Authentication is the process by which an entity provides its identity to another party, for example, by showing photo ID to a bank teller or entering a password on a computer system. This process is broken down into several methods which may involve something the user knows (e.g., password), something the user has (e.g., card), or something the user is (e.g., fingerprint, iris, etc.). Authentication can take many forms, and may even utilise combinations of these methods.

Authorisation

Authorisation is the process of granting access to a service or information based on a user’s role in an organisation. Once a user is authenticated, the system then must ensure that a particular user has access to a particular resource.

Access Control

Access control is used to determine what a user can or cannot do in a particular context (e.g., a user may have access to a particular resource/file, but only during a certain time of day, e.g., work hours, or only from a certain device, e.g., desktop in the office).

**Identity management** (**ID management**) is the organizational process for identifying, authenticating and authorizing individuals or groups of people to have access to applications, systems or networks by associating user rights and restrictions with established identities.

What is IAM process?

Identity and access management (**IAM**) is a framework of business **processes**, policies and technologies that facilitates the management of electronic or digital identities. With an **IAM** framework in place, information technology (IT) managers can control user access to critical information within their organizations.

**identity management** (**IdM**), also known as **identity and access management** (**IAM** or **IdAM**), is a framework of policies and technologies for ensuring that the proper people in an enterprise have the appropriate access to technology resources. IdM systems fall under the overarching umbrellas of [IT security](https://en.wikipedia.org/wiki/Computer_security) and [data management](https://en.wikipedia.org/wiki/Data_management). Identity and access management systems not only identify, authenticate, and authorize individuals who will be utilizing IT resources, but also the hardware and applications employees need to access. Identity and [access management](https://en.wikipedia.org/wiki/Access_management) solutions have become more prevalent and critical in recent years as regulatory compliance requirements have become increasingly more rigorous and complex.

It addresses the need to ensure appropriate access to resources across increasingly heterogeneous technology environments and to meet increasingly rigorous compliance requirements.

The terms "identity management" (**IdM**) and "identity and access management" are used interchangeably in the area of identity access management.[[5]](https://en.wikipedia.org/wiki/Identity_management#cite_note-5)

[Identity-management systems](https://en.wikipedia.org/wiki/Identity_management_systems), products, applications and platforms manage identifying and ancillary data about entities that include individuals, computer-related hardware, and [software applications](https://en.wikipedia.org/wiki/Software_application).

IdM covers issues such as how users gain an [identity](https://en.wikipedia.org/wiki/Digital_identity), the roles and, sometimes, the permissions that identity grants, the protection of that identity and the technologies supporting that protection (e.g., [network protocols](https://en.wikipedia.org/wiki/Protocol_(computing)), [digital certificates](https://en.wikipedia.org/wiki/Public_key_certificate), [passwords](https://en.wikipedia.org/wiki/Password), etc.).

## Identity Management Cyber Security Threats

Traditional IT cyber security countermeasures are not adequate to protect against attacks in today's world. Consider for a moment, countermeasures can often trigger network compromises, denial of services, and security breaches themselves. Cyber security risks most likely come from penetrators who are:

* dissatisfied employees, contractors and insiders who damage systems and steal intellectual property.
* Terrorists seeking low cost, low risk and high gain hacking opportunities.
* Professional cyber thieves who steal and sell information.
* groups who use the Internet for cyber warfare(**Cyber warfare** involves the actions by a nation-state or international organization to attack and attempt to damage another nation's computers or information networks through, for example, computer viruses or denial-of-service attacks.) IP theft.

Insiders usually possess legitimate reasons to misuse computer systems, extend their privileges, and impersonate other users. Outsiders use the Internet, remote access, and partner network tunnels to penetrate your network and even facilities. Attackers exploit vulnerabilities, wherever they exist, using a variety of techniques and tools to probe networks, publicize targets, stifle operations, gain business advantage and promote causes.

identity management offers comprehensive IT risk management software and services that protect employees, companies, shareholders, customers and vendors.

**Identity Theft**

What exactly is identity theft?

**Identity theft** and **identity** fraud are terms used to refer to all types of crime in which someone wrongfully obtains and uses another person's personal data in some way that involves fraud or deception, typically for economic gain

**Identity theft** is the deliberate use of someone else's [identity](https://en.wikipedia.org/wiki/Personally_identifiable_information), usually as a method to gain a financial advantage or obtain credit and other benefits in the other person's name, and perhaps to the other person's disadvantage or loss. The person whose identity has been assumed may suffer adverse consequences, especially if they are held responsible for the perpetrator's actions. Identity theft occurs when someone uses another's personally identifying information, like their name, identifying number, or [credit card number](https://en.wikipedia.org/wiki/Credit_card_number), without their permission, to commit fraud or other crimes. The term *identity theft* was coined in 1964. Since that time, the definition of identity theft has been defined throughout both the U.K. and the United States as the theft of personally identifiable information, generally including a person's name, date of birth, social security number, driver's license number, bank account or credit card numbers, [PINs](https://en.wikipedia.org/wiki/Personal_identification_number), [electronic signatures](https://en.wikipedia.org/wiki/Electronic_signature), fingerprints, [passwords](https://en.wikipedia.org/wiki/Password), or any other information that can be used to access a

**Examples of Identity Theft**

* Stolen Checks. If you have had checks stolen or bank accounts set up fraudulently, report it to the check verification companies. ...
* ATM Cards. ...
* Fraudly Change of Address. ...
* Social Security Number Misuse. ...
* Passports. ...
* Phone Service. ...
* Driver **License** Number Misuse. ...

What are the four types of identity theft?

**Types of Identity Theft**

* Financial **Identity Theft**. Financial **identity theft** is by far the most common **type of identity theft**. ...
* Medical **Identity Theft**. ...
* Criminal **Identity Theft**. ...
* Child **Identity Theft**.

**Identity theft** can happen to anyone and lead to a number of problems. It can damage your credit and disqualify you from loans, stall your tax refund, and drain your bank account — to name but a few outcomes. In more **severe** cases, it can even get you wrongfully arrested

How do they do identity theft?

**Identity** thieves can steal your personal information directly or indirectly by: Stealing your wallets and purses containing identification cards, credit cards and bank information. Stealing your mail including credit and bank statements, phone or utility bills, new checks, and tax information.

Identity theft is when someone steals your personal information and uses it without your permission. There are several [forms of identity theft](https://www.experian.com/blogs/ask-experian/20-types-of-identity-theft-and-fraud/), and each one can affect you in a different way.

There's no way to protect yourself against identity theft completely. But if you're diligent in learning how your information can be at risk and what fraudsters can do with it, you'll be better equipped to protect your data and act quickly if someone does manage to steal it.

## **How Identity Theft Happens**

[Identity theft](https://www.experian.com/blogs/ask-experian/how-does-identity-theft-happen/) is a broad term that applies any time someone steals your personal information, such as your Social Security number, and uses it to create a new account, make a purchase or commit other fraud.

Due to the nature of technology and the internet, your personal information is always at risk. If you're not carefully monitoring your credit file, you may not notice you've been victimized until the damage is already done.

Here are 10 of the most common ways identity thieves get hold of your data:

### 1. Data Breaches

A [data breach](https://www.experian.com/blogs/ask-experian/what-is-a-data-breach/) happens when someone gains access to an organization's data without authorization. The most common types of information stolen in data breaches include full names, Social Security numbers(In the United States, a Social Security number is a nine-digit number issued to U.S. citizens, permanent residents, and temporary residents under section 205 of the Social Security Act) and credit card numbers.

In 2018, there were 1,244 data breaches in the U.S., and more than 446 million records were exposed, according to the Identity Theft Resource Center.

Because people have so many accounts with various businesses and other organizations, it's virtually impossible to keep your information safe from a data breach, but there are steps you can take to minimize your risk.

### 2. Unsecure Browsing

For the most part, you can browse the internet safely, especially if you stick to well-known websites. But if you share any information on an unsecure website or a website that's been compromised by hackers you could be putting your sensitive information directly in the hands of a thief.

Depending on your browser, you may get an alert if you try to access a risky website.

### 3. Malware Activity

[Malware](https://www.experian.com/blogs/ask-experian/what-is-malware/) is malicious software that's designed to perform all sorts of havoc. Fraudsters may use malware is to steal your data or spy on your computer activity without you knowing.

### 4 Credit Card Theft

One of the simplest forms of identity theft is credit card theft. If a thief can gain access to your credit card information, they can use it to make unauthorized purchases.

Common ways credit card theft occurs are through a data breach, physical theft, credit card skimmers and via online retail accounts where card information is stored.

### 5. Mail Theft

Since long before the internet, identity thieves have been combing through the mail to find documents that held personal information. Bank and credit card statements and any other document you send or receive through the postal system can be intercepted and used to gain access to your data.

The mail you throw away also can leave you vulnerable, so be sure to shred any old mail that may contain personal information.

### 6. Phishing and Spam Attacks

Some scammers use email and text messages and other forms of electronic communication to steal your sensitive information. The message often looks like it's coming from a reputable source and asks victims to give up one or more types of information.

For example, a bogus email made to look like it's from your bank may include a link that directs you to a spoof website that looks just like the one it's mimicking. Once there, the website may ask you for a username and password, or to input credit card information or your Social Security number. If something seems suspicious, it might be an attempt at identity theft.

### 8. Wi-Fi Hacking

If you use your computer or phone on a public network—airport, department store or coffee shop Wi-Fi—hackers may be able to "eavesdrop" on your connection.

This means that if you type in a password, bank account or credit card number, Social Security number or anything else, an eavesdropper can easily intercept it and use it for their own purposes.

### 9. Mobile Phone Theft

Smartphones are a treasure trove of information for identity thieves, especially if your apps allow you to log in automatically without a password or fingerprint. If someone manages to steal and unlock your phone, it could allow them to view the information found in your apps, as well as in your emails, text messages, notes and more.

Make sure your phone locks with a secure passcode, biometric screening is set up properly and your passwords aren't stored in plain text anywhere on your phone.

### 10. Card Skimming

Some thieves use a [skimming device](https://www.experian.com/blogs/ask-experian/how-to-protect-yourself-against-credit-card-skimmers-at-gas-stations/) that easily can be placed over a card reader on an ATM or a fuel pump without looking out of the ordinary. When somebody swipes a debit or credit card at a compromised machine, the skimmer reads the information from the card's magnetic stripe and either stores it or transmits it. A criminal can then use this information to make purchases.

## **How Identity Theft Can Affect You**

Once a thief has your information, they can do several things with it, including:

* Open [fraudulent credit cards](https://www.experian.com/blogs/ask-experian/credit-education/preventing-fraud/credit-card-fraud-what-to-do-if-you-are-a-victim/).
* File phony health insurance claims.
* Use your existing bank or credit card accounts to make unauthorized purchases.
* Sell it to other thieves.
* File a fraudulent tax return or [steal your tax refund](https://www.experian.com/blogs/ask-experian/how-to-stop-identity-thieves-from-stealing-your-tax-refund/).
* Access your financial accounts and steal your money.
* Commit [child identity theft](https://www.experian.com/blogs/ask-experian/what-is-child-identity-theft/) using your child's information.

Depending on the type of theft that occurs, and how the criminal uses your information, identity theft can result in immediate financial loss, damage to your credit and emotional distress. It can also take anywhere from less than a day to several months or even years to resolve the issue.

## **How to Check for Identity Theft**

You can't completely avoid the possibility that your identity may be stolen, but you can take action to spot potential fraud before it becomes a major problem.

To [check for identity theft](https://www.experian.com/blogs/ask-experian/how-do-you-check-for-identity-theft/), keep an eye on your credit reports. While you can view each one for free every 12 months through [AnnualCreditReport.com](https://www.experian.com/blogs/ask-experian/how-do-you-check-for-identity-theft/), you can view a summary of your reports more regularly through various free and paid credit monitoring services.

As you check your report, watch for tradelines that you don't recognize or remember opening. Also, keep an eye on your credit score—a sudden inexplicable drop can be a dead giveaway that something is wrong.

Here are some other telltale signs that someone may have stolen your identity:

* You aren't receiving important mail such as bills or checks.
* You get bills for items you didn't order or statements for credit cards you didn't sign up for.
* You're denied credit, despite having an excellent credit rating.
* You have unauthorized bank transactions or withdrawals.
* You've received notice that your personal information may have been compromised in a data breach.
* Your electronic tax filing is denied.
* You receive unauthorized authentication messages by text or email for unknown accounts.
* You get an email from an organization that says your account has been recently accessed and it wasn't you.
* You receive a bill or an explanation of benefits for health care that you didn't seek.

**Biometrics**

The term Biometrics is composed of two words − *Bio* (Greek word for Life) and *Metrics* (Measurements). Biometrics is a branch of information technology that aims towards establishing one’s identity based on personal traits.

Biometrics is presently a buzzword in the domain of information security as it provides high degree of accuracy in identifying an individual.

## **What is Biometrics?**

*Biometrics is a technology used to identify, analyze, and measure an individual’s physical and behavioral characteristics.*

Each human being is unique in terms of characteristics, which make him or her different from all others. The physical attributes such as finger prints, color of iris, color of hair, hand geometry, and behavioral characteristics such as tone and accent of speech, signature, or the way of typing keys of computer keyboard etc., make a person stand separate from the rest.

This uniqueness of a person is then used by the biometric systems to −

* Identify and verify a person.
* Authenticate a person to give appropriate rights of system operations.
* Keep the system safe from unethical handling.

## **What is a Biometric System?**

*A biometric system is a technology which takes an individual’s physiological, behavioral, or both traits as input, analyzes it, and identifies the individual as a genuine or malicious user.*

## **Types of Biometric Modalities**

There are various traits present in humans, which can be used as biometrics modalities. The biometric modalities fall under three types −

* 1. Physiological
* 2. Behavioral
* 3. Combination of physiological and behavioral modality

The following table collects the points that differentiate these three modalities −

|  |  |  |
| --- | --- | --- |
| **Physiological Modality** | **Behavioral Modality** | **Combination of Both Modalities** |
| This modality pertains to the shape and size of the body. | This modality is related to change in human behavior over time. | This modality includes both traits, where the traits are depending upon physical as well as behavioral changes. |
| For example −   * Fingerprint Recognition * Hand Geometry Recognition system * Facial Recognition System * Iris Recognition System * Hand Geometry Recognition System * Retinal Scanning System * DNA Recognition System | For example −   * Gait (the way one walks) * Rhythm of typing keys * Signature | For example −  Voice Recognition  It depends on health, size, and shape of vocal cord, nasal cavities, mouth cavity, shape of lips, etc., and the emotional status, age, illness (behavior) of person |