* Cybersquatting is registering, selling or using a domain name with the intent of profiting from the goodwill of someone else's trademark. It generally refers to the practice of buying up domain names that use the names of existing businesses with the intent to sell the names for a profit to those businesses.

There are three main components of cybersquatting definition.

**1. The Domain Name Is Identical or Confusingly Similar to A Registered Trademark**

But what is considered to be an identical or confusing similar domain? There’s no fixed definition of “confusingly similar” as it’s a pretty subjective term. Generally, court or arbitration committee decides whether a domain in question can confuse or deceive people on case-by-case basis.

Another part of this point is “registered trademark.” A person or company can seek legal remedy only after registering its brand as a trademark.

If the business/person is **already famous** but before they register the trademark, if someone else buys the domain with an intention to sell it to the brand owner in the future at a premium price, it also falls into cybersquatting.

For an example of how a cybersquatting case can play out, check out the [Wayne Rooney case.](https://www.wipo.int/wipo_magazine/en/2006/06/article_0008.html)

**2. The Domain Is Obtained in Bad Faith**

While dealing with a cybersquatting case, courts also consider the intension of the domain registrant.  If the cybersquatter’s intention is one or more of the following, it’s included in bad faith’s definition:

* Sell the domain to the original trademark owner at a premium price.
* Attract traffic on the website to earn money from advertisements or affiliate marketing.
* Use the cybersquatted domain to spread [malware](https://sectigostore.com/blog/different-types-of-malware/) or run [phishing](https://sectigostore.com/blog/common-types-of-phishing-attacks-how-to-recognize-avoid-them/) scams
* Sell domain name to the competitors.
* Ruin a person or company’s reputation.
* Show disagreement with the original site’s cause or mission.
* Start a similar business and leverage the established brand’s goodwill to deceive their customers.

**3. The Registrant Has No Apparent or Legitimate Interest in the Domain Name**

Sometimes people **unintentionally** end up buying domain names that resemble famous businesses or celebrities. Some words look unique or abstract in one language but are popular and trademark in other language.

For example, locolo.app is a startup in Estonia for renting products while locolo.in is an online grocery delivery platform in India. In the same way, in the U.S., Princeton.edu represents New Jersey’s Princeton University. But in India, Princeton.in represents a club!

Although both businesses in each scenario share the same domain name with different top-level domains (TLDs), they are otherwise entirely unrelated and don’t have any intention to capitalize on their counterparts’ reputations. Such examples are considered as having a **genuine interest in the domains** because **they have established businesses** or organizations using the names.

Now that we know what cybersquatting is in a general sense, let’s explore the eight different types of cyberquatting.

Types of Cybersquatting

**1. Typosquatting**

[Typosquatting](https://sectigostore.com/blog/what-is-typosquatting/) is one of the most common types of cybersquatting. In this situation, the cybersquatter intentionally buys misspelled domain names of popular brands. The goal is to create an illegitimate website that people will land on when they make a typing error (i.e., misspell or hit one or more wrong keys when typing a domain name.

Typosquatting involves adding or omitting any numbers, letters or periods in the original spelling of a domain. It also includes swapping the order of letters or words in a domain as well. Basically, typosquatting includes any such spelling variant that people might mistype.

For example:

* Twiitter.com,
* Twittr.com,
* Twittor.com,
* Twitter.cm, and
* wwwtwitter.com (omitting the period between “www” and “twitter”).

When popular sites have millions of visitors, even if a small fraction of people make a typo, the typosquatters receive lots of free traffic on their illegitimate websites.

**2. TLDs Exploitation Cybersquatting**

Top-level domains (TLDs) are the last part of a domain name like .com, .ca, .tech, .org, and more. There are more than [2,000](https://data.iana.org/TLD/tlds-alpha-by-domain.txt) TLDs available in the market. Although big companies like Microsoft, Amazon, Facebook, etc. keep a large portfolio of such domains, it’s not feasible for small and medium-sized businesses to buy the domain names containing their brand name in all the TLD variants.

Cybersquatters exploit this situation and buy matching domains of a popular business with different TLDs. Cybersquatters make an inappropriate site using such a misspelled domain and coerce the business owners to buy the domain at a premium price to protect their brands’ reputations. Some cybersquatters make phishing sites using such domains to mislead the original site’s customers.

**3. Gripe Sites Cybersquatting**

Not all cybersquatters are out to make a profit — some have other agendas. Some people take the path of cybersquatting to:

* Ruin a business/person’s reputation,
* Take personal revenge,
* Publish their extremist political, religious, or social beliefs, or
* Mock or make a satire on the original site’s values or mission.

They post content on such cybersquatting websites that contradict the original site’s values or put it in an embarrassing situation.

Examples: microsoftsucks.com (To show hatred for Microsoft) and GodHatesFigs.com (parody of GodHatesFags.com). To see more, be sure to check out our article on [cybersquatting examples](https://sectigostore.com/blog/cybersquatting-examples/).

Although a rare practice, some businesses buy the “typo-domains” of their competitors and make an inappropriate website or write stuff that is harmful to the competitor brand’s image and redirect traffic to their own website.

**4. Look-Alike Domain Cybersquatting**

Cybersquatters buy similar-looking domain names of original brands by adding special characters, numbers, or common words in it. Sometimes they interchange the words if the domain name is long.

Let’s look at a few examples of these methods of cybersquatting:

* **Adding extra characters**: Amazon-site.com, Amazonshopping.com, Amazon-official.com, Amazon1.com, Amaz0n.com, Ama-zon.com, Microsofty.com,
* **Reordering the words:** guardianthe.com (instead of theguardian.com), retailnotme.com (instead of retailmenot.com), businessfox.com (instead of foxbusiness.com), and newsfox.com (instead of foxnews.com)

**5. Misleading Subdomain Cybersquatting**

Attackers sometimes split a domain name into two parts, buy a domain of the latter part and add a subdomain of the former part. Not sure what we mean? Let’s consider a quick example with the domain www.britannica.com.

In this scenario, the original domain is www.britannica.com. If a typosquatter divides it into two parts — let’s say, *britan* and *nica* —they buy a domain named nica.com and make a subdomain **britan.nica.com** to try to trick people.

Cybersquatters also buy random domain names and make subdomains containing famous brand names. For example, **amazon.randomsite.com** or **facebook.anydomain.com**.

Non-tech savvy people might not be aware of the fact that virtually anyone can make a subdomain of any word (or number). It is the **primary domain** that is written before TLD (.com, .in, .org, .edu, etc.) that represents the legitimacy of the domain name.

So, in the case of **facebook.anydomain.com**, the **Facebook** word is used just as a subdomain and that doesn’t represent the legitimacy of the primary domain. The primary domain is anydomain.com. In other words, you can’t buy facebook.com, but you might be able to buy any other available domain name and make subdomain using “Facebook” word.

**6. Celebrity Name Cybersquatting**

Cybersquatters buy domains of celebrities’ names before the celebrities themselves decide to do so. If celebrities already have websites, perpetrators buy similar or close-matching domain names. They attract traffic by misleading fans and make revenue through third-party advertising or selling merchandise embedded with a celebrity’s brand name/images.

Often, cybersquatters make phishing sites and lure fans to share their personally identifiable information (PII) like email addresses, phone numbers, dates of birth, or even their physical addresses. Some cybersquatters’ goals are to sell such domain names to the celebrity at a premium rate.

Celebrities like [Paris Hilton](https://domainnamewire.com/2010/08/16/paris-hilton-upset-about-cybersquatters/), [Madonna](https://edition.cnn.com/2000/TECH/computing/10/16/madonna.cybersquatter.reut/), and [Jennifer Lopez](https://www.wipo.int/amc/en/domains/decisions/html/2009/d2009-0057.html) have been victims of cybersquatting in the past.

**7. Expiration Date Exploitation Cybersquatting**

Some cybersquatters keep an eye on target domain names and their expiration dates. If the domain owner fails to renew the domain name, the perpetrators grab the opportunity and register the domain in their names.

Thankfully, the likelihood of such renewal failures to occur for big companies is rare because they typically receive a couple of reminders before the domains’ expiration dates. However, it still does happen. But this scenario typically affects startups and small companies. This could be because the businesses’ founders are:

* In an indecisive stage,
* Deciding whether to continue their businesses, or,
* May have temporary halted their businesses for another reason.

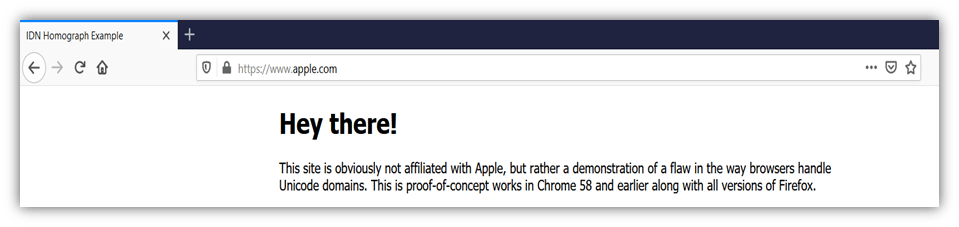
Whenever the company owners decide to restart their businesses, if cybersquatting occurs, they are forced to buy back their domains from cybersquatters at premium rates.

**8. Homograph Attacks**

This next type of cybersquatting is incredibly malicious. In homograph attacks, cybercriminals use punycode (a subset of Unicode characters) to convert regular domain names (which traditionally consist of ASCII numbers, letters, and special characters) into domain names that visually look legitimate. So, in this type of attack, bad actors intentionally create domains using punycode that you can’t distinguish visually from real website domains.

[Xudong Zheng](https://www.xudongz.com/blog/2017/idn-phishing/) shows how he was able to buy a domain that looks like “apple.com” by using punycode. He bought the domain “xn--80ak6aa92e.com,” which appears virtually identical to “apple.com” in the URL bar.

Pretty scary, right? Thankfully, Chrome and Internet Explorer now have security mechanisms that detect homographic domains. But if you click on [this link](https://www.xn--80ak6aa92e.com/) and open it with Firefox or Chrome 58 (or earlier), you can still see the fake apple.com website. Here’s a screenshot of the example below:



But since Chrome had addressed this issue, this is the message you’ll now see on later versions of their browser:

https://searchsecurity.techtarget.com/definition/cyberwarfare

The generally accepted definition of cyberwarfare is the use of [cyber attacks](https://searchsecurity.techtarget.com/definition/cyber-attack) against a nation-state, causing it significant harm, up to and including physical warfare, disruption of vital computer systems and loss of life.

However, there has been some debate among experts regarding [what acts specifically qualify as cyberwarfare](https://www.computerweekly.com/opinion/Drawing-the-line-for-cyber-warfare). While the United States Department of Defense (DOD) states that the use of computers and the internet to conduct warfare in cyberspace is a threat to national security, why certain activities qualify as warfare, while others are simply cybercrime, is unclear.

Although cyberwarfare generally refers to cyber attacks perpetrated by one nation-state on another, it can also describe attacks by terrorist groups or hacker groups aimed at furthering the goals of particular nations. While there are a number of examples of suspected cyberwarfare attacks in recent history, there has been no formal, agreed-upon definition for a cyber act of war, which experts generally agree would be a cyber attack that directly leads to loss of life.

### What kinds of cyber weapons are used in warfare?

Examples of acts that might qualify as cyberwarfare include the following:

* viruses, phishing, computer worms and [malware](https://searchsecurity.techtarget.com/definition/malware) that can take down [critical infrastructure](https://whatis.techtarget.com/definition/critical-infrastructure);
* distributed denial-of-service ([DDoS](https://searchsecurity.techtarget.com/definition/distributed-denial-of-service-attack)) attacks that prevent legitimate users from accessing targeted computer networks or devices;
* hacking and theft of critical data from institutions, governments and businesses;
* spyware or [cyber espionage](https://searchsecurity.techtarget.com/definition/cyber-espionage) that results in the theft of information that compromises national security and stability;
* [ransomware](https://searchsecurity.techtarget.com/definition/ransomware) that holds control systems or data hostage; and
* propaganda or disinformation campaigns used to cause serious disruption or chaos.

### What are the goals of cyberwarfare?

According to the Cybersecurity and Infrastructure Security Agency, the goal of cyberwarfare is to "weaken, disrupt or destroy" another nation. To achieve their goals, cyberwarfare programs target a wide spectrum of objectives that might harm national interests. These threats range from propaganda to espionage and serious disruption with extensive infrastructure disruption and loss of life to the citizens of the nation under attack.

Cyberwarfare is similar to cyber espionage, and the two terms are sometimes confused. The biggest difference is that the primary goal of a cyberwarfare attack is to disrupt the activities of a nation-state, while the primary goal of a cyber espionage attack is for the attacker to remain hidden for as long as possible in order to gather intelligence. The two activities are often used together. For example, cyber espionage can be used to build intelligence that helps a nation-state prepare for declaring a physical or cyber war.

### What are the types of cyberwarfare attacks?

The threat of cyberwarfare attacks grows as a nation's critical systems are increasingly connected to the internet. Even if these systems can be properly secured, they can still be hacked by perpetrators recruited by nation-states to find weaknesses and exploit them. Major types of cyberwarfare attacks include the following.

#### Destabilization

In recent years, cybercriminals have been attacking governments through critical infrastructure, including such entities as transportation systems, banking systems, power grids, water supplies, dams and hospitals. The adoption of the internet of things makes the [manufacturing industry increasingly susceptible](https://searcherp.techtarget.com/answer/Why-is-cybersecurity-critical-for-modern-manufacturing) to outside threats.

From a national security perspective, destabilizing critical digital infrastructure inflicts damage on vital modern services or processes. For example, an attack on the energy grid could have massive consequences for the industrial, commercial and private sectors.

#### Sabotage

Cyber attacks that sabotage government computer systems can be used to support conventional warfare efforts. Such attacks can block official government communications, contaminate digital systems, enable the theft of vital intelligence and threaten national security.

State-sponsored or military-sponsored attacks, for example, may target military databases to get information on troop locations, weapons and equipment being used.

#### Data theft

Cybercriminals hack computer systems to steal data that can be used for intelligence, held for ransom, sold, used to incite scandals and chaos, or even destroyed.

The Center for Strategic and International Studies (CSIS) maintains a timeline record of cyber attacks on government agencies and defense and high-tech companies, as well as economic crimes with losses of more than $1 million. In CSIS timelines dating back to 2006, many of the recorded cyber incidents involve hacking and data theft from nation-states.

* **Cyberterrorism** is the use of the Internet to conduct violent acts that result in, or threaten, the loss of life or significant bodily harm, in order to achieve political or ideological gains through threat or intimidation.
* It is also sometimes considered an act of Internet terrorism where terrorist activities, including acts of deliberate, large-scale disruption of computer networks, especially of personal computers attached to the Internet by means of tools such as computer viruses, computer worms, phishing, and other malicious software and hardware methods and programming scripts.

Cyberterrorism essentially consists of using computer technology to engage in terrorism. Since “crime” and “terrorism” are similar in certain respects, and since both target societies’ ability to maintain internal order, we must begin by differentiating the two.

[15](https://www.cairn.info/revue-internationale-de-droit-penal-2006-3-page-453.htm#pa15)Basically, crime is “personal” while terrorism is “political.” Crimes are committed for individual, personal reasons, the most important of which are personal gain and the desire (need) to harm others psychologically and/or physically.

[16](https://www.cairn.info/revue-internationale-de-droit-penal-2006-3-page-453.htm#pa16)Terrorism often results in the infliction of “harms” indistinguishable from those caused by crime (e.g., death, personal injury, property destruction), but the “harms” are inflicted for very different reasons. A U.S. statute, for example, defines “terrorism” as (i) committing acts constituting “crimes” under the law

U.S. statute, for example, defines “terrorism” as (i) committing acts constituting “crimes” under the law of any country (ii) to intimidate or coerce a civilian population, to influence government policy by intimidation or coercion or to affect the conduct of government by mass destruction, assassination or kidnapping.  [**[9]**](https://www.cairn.info/revue-internationale-de-droit-penal-2006-3-page-453.htm#no10)

Email spoofing is a form of cyber attack in which a hacker sends an email that has been manipulated to seem as if it originated from a trusted source. Email spoofing is a popular tactic used in [phishing](https://searchsecurity.techtarget.com/definition/phishing) and [spam](https://searchsecurity.techtarget.com/definition/spam) campaigns because people are more likely to open an email when they think it has been sent by a known sender. The goal of email spoofing is to trick recipients into opening or responding to the message.

**Why email spoofing is important**

Although most spoofed emails can be easily detected and can be remedied by simply deleting the message, some varieties can cause serious problems and pose security risks. For example, a spoofed email may pretend to be from a well-known shopping website, asking the recipient to provide sensitive data, such as a password or credit card number.

Alternatively, a spoofed email may include a link that installs malware on the user's device if clicked. A common [example of business email compromise](https://searchsecurity.techtarget.com/feature/Explore-5-business-email-compromise-examples-to-learn-from) (BEC) involves spoofing emails from the chief executive officer (CEO) or chief financial officer (CFO) of a company requesting a wire transfer or internal system access credentials.

**Reasons for email spoofing**

In addition to phishing, attackers use spoofed email for the following reasons:

* Hide the fake sender's real identity.
* Bypass spam filters and blocklists. Users can minimize this threat by blocklisting internet service providers (ISPs) and [Internet Protocol (IP) addresses](https://whatis.techtarget.com/definition/IP-address).
* Pretend to be a trusted individual -- a colleague or a friend -- to elicit confidential information.
* Pretend to be a reliable organization -- for example, posing as a financial firm to get access to credit card data.
* Commit [identity theft](https://searchsecurity.techtarget.com/definition/identity-theft) by impersonating a targeted victim and requesting personally identifiable information (PII).
* Damage the sender's reputation.
* Launch and spread malware hidden in attachments.
* Conduct a [man-in-the-middle (MitM) attack](https://internetofthingsagenda.techtarget.com/definition/man-in-the-middle-attack-MitM) to seize sensitive data from individuals and organizations.
* Obtain access to sensitive data collected by third-party vendors.

**What's the difference between phishing, spoofing and domain impersonation?**

Cybercriminals often use spoofing as part of a phishing attack. Phishing is a method used to obtain data by faking an email address and sending an email that looks like it is coming from a trusted source that could reasonably ask for such information. The goal is to make victims click on a link or download an attachment that will install malware on their system.

Spoofing is also related to domain impersonation, in which an email address that is similar to another email address is used. In domain impersonation, an email may come from an address such as customerservice@amaz0n.co, while, in a spoofing attack, the fake sender's address will look genuine, such as customerservice@amazon.com.

**How email spoofing works**

Email spoofing can be easily achieved with a working Simple Mail Transfer Protocol ([SMTP](https://whatis.techtarget.com/definition/SMTP-Simple-Mail-Transfer-Protocol)) server and common email platform, such as Outlook or Gmail. Once an email message is composed, the scammer can forge fields found within the message header, such as the FROM, REPLY-TO and RETURN-PATH addresses. When the recipient gets the email, it appears to come from the forged address.

This is possible to execute because SMTP does not provide a way to authenticate addresses. Although protocols and methods have been developed to combat email spoofing, adoption of those methods has been slow.

### best ways to stop email spoofing

Users and businesses can prevent email spoofers from accessing their systems in a variety of ways.

#### 1. Deploy an email security gateway

Email security gateways protect businesses by blocking inbound and outbound emails that have suspicious elements or do not meet security policies a business puts in place. Some [gateways offer additional functions](https://searchsecurity.techtarget.com/buyershandbook/What-secure-email-gateways-can-do-for-your-enterprise), but all can detect most malware, spam and phishing attacks.

#### 2. Use antimalware software

Software programs can identify and block suspicious websites, detect spoofing attacks and stop fraudulent emails before they reach user inboxes.

#### 3. Use encryption to protect emails

An email signing certificate encrypts emails, allowing only the intended recipient to access the content. In asymmetric encryption, a public key encrypts the email, and a private key owned by the recipient then decrypts the message. An additional digital signature can ensure the receiver that the sender is a valid source. In environments without broad encryption in place, users can [learn to encrypt email attachments](https://searchsecurity.techtarget.com/answer/How-secure-is-an-email-with-a-pdf-attachment).

#### 4. Use email security protocols

Infrastructure-based [email security protocols can reduce threats and spam](https://searchsecurity.techtarget.com/answer/What-are-the-most-important-email-security-protocols) by using domain authentication. In addition to SMTP and SPF, businesses can use DomainKeys Identified Mail (DKIM) to provide another layer of security with a digital signature. Domain-based Message Authentication, Reporting and Conformance (DMARC) can also be implemented to define the actions that should be taken when messages fail under SPF and DKIM.

#### 5. Use reverse IP lookups to authenticate senders

A reverse IP lookup confirms the apparent sender is the real one and verifies the email's source by identifying the domain name associated with the IP address.

Website owners can also consider publishing a domain name system (DNS) record stating who can send emails on their domain's behalf. Messages are then inspected before the email body is downloaded and can be rejected before causing any harm.

#### 6. Train employees in cyber awareness

On top of software-based anti-spoofing measures, businesses must encourage user caution, [teaching employees about cybersecurity](https://searchsecurity.techtarget.com/tip/Cybersecurity-employee-training-How-to-build-a-solid-plan) and how to recognize suspicious elements and protect themselves. Simple educational programs can equip users with email spoofing examples and give them the ability to spot and handle spoofing tactics, along with procedures to follow when a spoofing attempt is discovered. [Training should be ongoing](https://www.computerweekly.com/opinion/How-effective-security-training-goes-deeper-than-awareness) so that the materials and methods can be updated as new threats emerge.

#### 7. Watch out for possible spoofed email addresses

The email addresses users communicate with are often predictable and familiar. Individuals can learn to watch out for unknown or odd email addresses and to verify an email's origin before interacting with it. Attackers often use the same tactics multiple times, so users must remain vigilant.

#### 8. Never give out personal information

In many situations, even if spoofed emails get into an inbox, they only cause real damage when a user responds with personal information. By making it a common practice never to divulge personal information in emails, users can significantly limit the effects email spoofing could have.

#### 9. Avoid strange attachments or unfamiliar links

Users should also steer clear of suspicious attachments and links. As a best practice, they can examine every element of an email, looking out for telltale signs, like misspellings and unfamiliar file extensions, before going ahead and opening a link or attachment.

* Spam is any kind of unwanted, unsolicited digital communication that gets sent out in bulk.
* Often spam is sent via email, but it can also be distributed via text messages, phone calls, or social media.
* The proliferation of spam email presents a harmful, costly, and evolving threat to Internet users.
* Governments can help reduce the impact of spam by deterring offenders via effective laws and enforcement measures, multistakeholder antispam efforts, the adoption of best practices, and citizen education about the dangers of spam

Search engine spamming

* Excessive manipulation to influence search engine rankings, often for pages which contain little or no relevant content.
* Spamming involves getting a site more exposure than it deserves for its keywords, leading to unsatisfactory search experiences.
* Optimization involves getting a site the exposure it deserves on the most targeted keywords, leading to satisfactory search experiences.
* Irrelevancy – targeting keywords unrelated to the site/page.
* Hidden Text – putting keywords where visitors will not see them, used to increase keyword count.
* Hidden Links – putting links where visitors will not see them, used to increase link popularity.
* Doorway Clutter – mass production of low-quality doorway pages, sometimes of the machine-generated variety.

Cyberdefamation

* The tort of cyber defamation is an act of intentionally insulting, defaming or offending another individual or a party through a virtual medium.
* It can be both written and oral.
* Today Internet has given us an opportunity to share our opinions globally.
* We can easily post something and it gets viral just in few minutes.
* But today what people fail to understand is that stating an OPINION is different from stating a FACT**.**
* MODIFICATION Pictures which are modified to degrade the reputation of another person are also clear case of defamation.
* FACT The statement should be presented as a fact not as an opinion.
* PUBLICATION The statement of fact should be published on the social media ground, and then only one can file a complaint for defamation.
* OPINIONS an opinion is not a defamatory statement. But at times, few opinions are considered as fact by the court if they have caused an actual damage to another party.
* Cyber Defamation in Corporate World can take place in various forms
* A disgruntled employee of a Company may post some defamatory remarks about the Company on a popular blog site or may send some slanderous email, defaming the company or any of its important managerial personnel, to the clients of the company across the globe;
* A competitor may divert the client and/or customers of a Company visiting the website of the Company to any other website which may give some misleading information about the Company.
* Unlike other form of defamation Cyber defamation can cause huge damage to a Company in a very short span of time owning to a worldwide accessibility of internet and its ever increasing number of users.

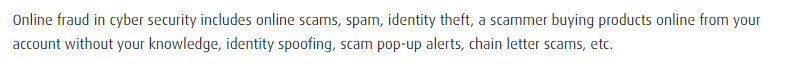
Internet Time Theft

* It refers to the theft in a manner where the unauthorized person uses internet hours paid by another person.
* The authorized person gets access to another person's ISP user ID and password, either by hacking or by illegal means without that person’s knowledge.
* Time theft at work occurs when an employee accepts pay from their employer for work that they have not actually done, or for time they have not actually put into their work.
* Cyber theft is a part of cybercrime which means theft carried out by means of computers or the Internet.

Cyber espionage

* Cyber espionage (cyberespionage) is a form of cyber attack that is carried out against a competitive company or government entity. The goal of cyber espionage, which may also be referred to as cyber spying, is to provide the attacker with information that gives them advantages over competing companies or governments.
* As of this writing, cyber espionage is used most often in the media in reference to advanced persistent threats ([APT](https://searchsecurity.techtarget.com/definition/advanced-persistent-threat-APT)s) launched by one nation-state against another for political gain. When the attacker's motives are financial as well as political, the cyber attack is likely to be characterized as being an example of economic espionage.
* Bad actors who engage in cyber espionage typically want to remain undetected for long periods of time. This means that this type of attack is often quite complicated and expensive to carry out.

Hacking

* Hacking is the activity of identifying weaknesses in a computer system or a network to exploit the security to gain access to personal data or business data.
* An example of computer hacking can be: using a password cracking algorithm to gain access to a computer system.
* It is not enough to have isolated computers systems; they need to be networked to facilitate communication with external businesses.
* This exposes them to the outside world and hacking.
* System hacking means using computers to commit fraudulent acts such as fraud, privacy invasion, stealing corporate/personal data, etc.
* Cyber crimes cost many organizations millions of dollars every year.
* Businesses need to protect themselves against such attacks.
* A **Hacker** is a person who finds and exploits the weakness in computer systems and/or networks to gain access. Hackers are usually skilled computer programmers with knowledge of computer security.
* **Ethical Hacker (White hat):**A security hacker who gains access to systems with a view to fix the identified weaknesses. They may also perform penetration Testing and vulnerability assessments.
* **Cracker (Black hat):**A hacker who gains unauthorized access to computer systems for personal gain. The intent is usually to steal corporate data, violate privacy rights, transfer funds from bank accounts etc.
* Ethical Hacking is identifying weakness in computer systems and/or computer networks and coming with countermeasures that protect the weaknesses. Ethical hackers must abide by the following rules.
  + Get written permission from the owner of the computer system and/or computer network before hacking.
  + Protect the privacy of the organization been hacked.
  + Transparently report all the identified weaknesses in the computer system to the organization.
  + Inform hardware and software vendors of the identified weaknesses.
* Text

  Description automatically generatedComputer sabotage involves deliberate attacks intended to disable computers or networks for the purpose of disrupting commerce, education and recreation for personal gain, committing espionage, or facilitating criminal conspiracies, such as drug and human trafficking.
* Committing computer sabotage can be as simple as deliberately infecting a computer with a virus to keep authorized users from logging in.
* Although not always, much computer sabotage involves the use of malware, such as bots, worms, viruses and other spyware, which enables hackers to gain illegal access to personal and corporate computers.
* Apart from theft of services and wire fraud, such sabotage facilitates pedophiles who stalk children online at school and at home, identity thieves who duplicate fake IDs for illegal immigrants, and home invasion rings and other criminals who use malware to identify potential victims.
* An email bomb is an attack against an email inbox or server designed to overwhelm an inbox or inhibit the server’s normal function, rendering it unresponsive, preventing email communications, degrading network performance, or causing downtime.
* The intensity of an email bomb can range from an inconvenience to a complete denial of service.
* Typically, these attacks persist for hours or until the targeted inbox or server implements a mitigation tactic to filter or block the attacking traffic.
* Such attacks can be carried out intentionally or unintentionally by a single actor, group of actors, or a botnet.

Computer network intrusion

* A network intrusion refers to any unauthorized activity on a digital network.

Network intrusions often involve stealing valuable network resources and almost always jeopardize the security of networks and/or their data

* Multi-Routing- This refers to when the intruders use multiple sources to intrude which helps them avoid detection. This is also known as asymmetric routing;
* Buffer Overflow Attacks- The Buffer overflow attack refers to when certain sections of the computer’s memory code is rewritten so that they can be used as a part of the intrusion later on;
* Traffic Flooding- This type of attacks are when the intruders flood the victim’s systems with traffic that they cannot handle in order to cause chaos and confusion. When the systems have too large traffic in order to screen, then they can easily get away undetected;
* Trojan Horse Malware- Trojan Horse Malware gives provides a network backdoor to the attackers so that they get an unfettered access to the network;
* Worms- This type of virus is most common and effective. Worms usually spread through email or instant messaging and can spread throughout the network.
* Password Sniffing is a hacking technique that uses a special software application that allows a hacker to steal usernames and passwords simply by observing and passively recording network traffic.
* This often happens on public WiFi networks where it is relatively easy to spy on weak or unencrypted traffic.
* They are often used by IT professionals as a tool to identify weak applications that may be passing critical information unencrypted over the Local Area Network (LAN).
* IT practitioners know that users download and install risky software at times in their environment, running a passive password sniffer on the network of a business to identify leaky applications is one legitimate use of a password sniffer.
* Such activities should be sanctioned by a senior leader in the company and the use of this software should be governed by more than one individual to prevent the abuse of any findings.
* Credit card fraud is the unauthorized use of a credit or debit card, or similar payment tool (ACH, EFT, recurring charge, etc.), to fraudulently obtain money or property.
* Credit and debit card numbers can be stolen from unsecured websites or can be obtained in an identity theft scheme.
* Don’t give out your credit card number online unless the site is secure and reputable..
* Don’t trust a site just because it claims to be secure.
* Before using the site, check out the security/encryption software it uses.
* Make sure you are purchasing merchandise from a reputable source.
* Obtain a physical address rather than simply a post office box and a telephone number and call the seller to see if the telephone number is correct and working.
* Send an e-mail to the seller to make sure the e-mail address is active, and be wary of those that utilize free e-mail services where a credit card wasn’t required to open the account
* Check with the Better Business Bureau from the seller’s area.
* Check out other websites regarding this person/company.
* Don’t judge a person or company by their website; flashy websites can be set up quickly.
* Be cautious when responding to special investment offers, especially through unsolicited e-mail.
* Be cautious when dealing with individuals/companies from outside your own country.
* Make sure the transaction is secure when you electronically send your credit card number.
* Keep a list of all your credit cards and account information along with the card issuer’s contact information.
* Identity theft is the crime of obtaining the personal or financial information of another person to use their identity to commit fraud, such as making unauthorized transactions or purchases.
* Identity theft is committed in many different ways and its victims are typically left with damage to their credit, finances, and reputation.
* Identity thieves increasingly use computer technology to obtain other people's personal information for identity fraud.
* To find such information, they may search the hard drives of stolen or discarded computers; hack into computers or computer networks; access computer-based public records; use information-gathering malware to infect computers; browse social networking sites; or use deceptive emails or text messages.
* Crime targeted at individuals.
* Crime targeted at property.
* Crime targeted at organizations.
* Single event of cybercrime.
* Series of events