INFORMATION
TECHNOLOGY ACT, 2000

The Government of India enacted the Information Technology (I.T.) Act with some major objectives to deliver and facilitate lawful electronic, digital, and online transactions, and mitigate cyber-crimes.

Salient Features of I.T Act

The salient features of the I.T Act are as follows

- Digital signature has been replaced with electronic signature to make it a more technology neutral act.
- It elaborates on offenses, penalties, and breaches.
- It outlines the Justice Dispensation Systems for cyber-crimes.
- It defines in a new section that cyber café is any facility from where the access to the internet is offered by any person in the ordinary course of business to the members of the public.
- It provides for the constitution of the Cyber Regulations Advisory Committee.
- It is based on The Indian Penal Code, 1860, The Indian Evidence Act, 1872, The Bankers' Books Evidence Act, 1891, The Reserve Bank of India Act, 1934, etc.
- It adds a provision to Section 81, which states that the provisions of the Act shall have overriding effect. The provision states that nothing contained in the Act shall restrict any person from exercising any right conferred under the Copyright Act, 1957.

Scheme of I.T Act

The following points define the scheme of the I.T. Act

- The I.T. Act contains **13 chapters** and **90 sections**.
- The last four sections namely sections 91 to 94 in the I.T. Act 2000 deals with the amendments to the Indian Penal Code 1860, The Indian Evidence Act 1872, The Bankers' Books Evidence Act 1891 and the Reserve Bank of India Act 1934 were deleted.
- It commences with Preliminary aspect in Chapter 1, which deals with the short, title, extent, commencement and application of the Act in Section 1. Section 2 provides Definition.
- Chapter 2 deals with the authentication of electronic records, digital signatures, electronic signatures, etc.
- Chapter 11 deals with offences and penalties. A series of offences have been provided along with punishment in this part of The Act.
- Thereafter the provisions about due diligence, role of intermediaries and some miscellaneous provisions are been stated.
- The Act is embedded with two schedules. The First Schedule deals with Documents or Transactions to which the Act shall not apply. The Second Schedule deals with electronic signature or electronic authentication technique and procedure. The Third and Fourth Schedule are omitted.

Application of the I.T Act

As per the sub clause (4) of Section 1, nothing in this Act shall apply to documents or transactions specified in First Schedule. Following are the documents or transactions to which the Act shall not apply −

- **Negotiable Instrument** (Other than a cheque) as defined in section 13 of the Negotiable Instruments Act, 1881;
- A **power-of-attorney** as defined in section 1A of the Powers-of-Attorney Act, 1882;
- A **trust** as defined in section 3 of the Indian Trusts Act, 1882;
- A **will** as defined in clause (h) of section 2 of the Indian Succession Act, 1925 including any other testamentary disposition;
- Any **contract** for the sale or conveyance of immovable property or any interest in such property;
- Any such class of documents or transactions as may be notified by the Central Government.

Amendments Brought in the I.T Act

The I.T. Act has brought amendment in four statutes vide section 91-94. These changes have been provided in schedule 1-4.

- The first schedule contains the amendments in the Penal Code. It has widened the scope of the term "document" to bring within its ambit electronic documents.
- The second schedule deals with amendments to the India Evidence Act. It pertains to the inclusion of electronic document in the definition of evidence.
- The third schedule amends the Banker's Books Evidence Act. This amendment brings about change in the definition of "Banker's-book". It includes printouts of data stored in a floppy, disc, tape or any other form of electromagnetic data storage device. Similar change has been brought about in the expression "Certified-copy" to include such printouts within its purview.
- The fourth schedule amends the Reserve Bank of India Act. It pertains to the regulation of fund transfer through electronic means between the banks or between the banks and other financial institution.

Intermediary Liability

Intermediary, dealing with any specific electronic records, is a person who on behalf of another person accepts stores or transmits that record or provides any service with respect to that record.

According to the above mentioned definition, it includes the following −

- Telecom service providers
- Network service providers
- Internet service providers
- Web-hosting service providers
- Search engines
- Online payment sites
- Online auction sites
- Online market places and cyber cafes

Highlights of the Amended Act

The newly amended act came with following highlights −

- It stresses on privacy issues and highlights information security.
- It elaborates Digital Signature.
- It clarifies rational security practices for corporate.
- It focuses on the role of Intermediaries.
- New faces of Cyber Crime were added.

Digital Signature

A digital signature is a technique to validate the legitimacy of a digital message or a document. A valid digital signature provides the surety to the recipient that the message was generated by a known sender, such that the sender cannot deny having sent the message. Digital signatures are mostly used for software distribution, financial transactions, and in other cases where there is a risk of forgery.

Electronic Signature

An electronic signature or e-signature indicates either that a person who demands to have created a message is the one who created it.

A signature can be defined as a schematic script related with a person. A signature on a document is a sign that the person accepts the purposes recorded in the document. In many engineering companies digital seals are also required for another layer of authentication and security. Digital seals and signatures are same as handwritten signatures and stamped seals.

Digital Signature to Electronic Signature

Digital Signature was the term defined in the old I.T. Act, 2000. **Electronic Signature** is the term defined by the amended act (I.T. Act, 2008). The concept of Electronic Signature is broader than Digital Signature. Section 3 of the Act delivers for the verification of Electronic Records by affixing Digital Signature.

As per the amendment, verification of electronic record by electronic signature or electronic authentication technique shall be considered reliable.

According to the **United Nations Commission on International Trade Law (UNCITRAL),** electronic authentication and signature methods may be classified into the following categories –

- Those based on the knowledge of the user or the recipient, i.e., passwords, personal identification numbers (PINs), etc.
- Those bases on the physical features of the user, i.e., biometrics.
- Those based on the possession of an object by the user, i.e., codes or other information stored on a magnetic card.
- Types of authentication and signature methods that, without falling under any of the above categories might also be used to indicate the originator of an electronic communication (Such as a facsimile of a handwritten signature, or a name typed at the bottom of an electronic message).

According to the UNCITRAL MODEL LAW on Electronic Signatures, the following technologies are presently in use –

- Digital Signature within a public key infrastructure (PKI)
- Biometric Device
- PINs
- Passwords
- Scanned handwritten signature
- Signature by Digital Pen
- Clickable “OK” or “I Accept” or “I Agree” click boxes

Offences & Penalties

The faster world-wide connectivity has developed numerous online crimes and these increased offences led to the need of laws for protection. In order to keep in stride with the changing generation, the Indian Parliament passed the Information Technology Act 2000 that has been conceptualized on the United Nations Commissions on International Trade Law (UNCITRAL) Model Law.

The law defines the offenses in a detailed manner along with the penalties for each category of offence.

Offences

Cyber offences are the illegitimate actions, which are carried out in a classy manner where either the computer is the tool or target or both.

Cyber-crime usually includes the following −

- Unauthorized access of the computers
- Data diddling
- Virus/worms attack
- Theft of computer system
- Hacking
- Denial of attacks
- Logic bombs
- Trojan attacks
- Internet time theft
- Web jacking
- Email bombing
- Salami attacks
- Physically damaging computer system.

The offences included in the I.T. Act 2000 are as follows –

- Tampering with the computer source documents.
- Hacking with computer system.
- Publishing of information which is obscene in electronic form.
- Power of Controller to give directions.
- Directions of Controller to a subscriber to extend facilities to decrypt information.
- Protected system.
- Penalty for misrepresentation.
- Penalty for breach of confidentiality and privacy.
- Penalty for publishing Digital Signature Certificate false in certain particulars.
- Publication for fraudulent purpose.
- Act to apply for offence or contravention committed outside India Confiscation.
- Penalties or confiscation not to interfere with other punishments.
- Power to investigate offences.

Example

Offences under the Information Technology Act 2000 Section 65, Tempering with computer source documents

Whoever knowingly or intentionally conceals, destroys or alters or intentionally or knowingly cau7ses another to conceal, destroy or alter any computer source code used for computer, computer program, computer system or computer network, when the computer source code is required to be kept or maintained by law for the being time in force, shall be punishable with imprisonment up to three year, or wit6h fine which may extend up to two lakh rupees, or with both.

Explanation – For the purpose of this section "computer source code" means the listing of programs, computer commands, design and layout and program analysis of computer resource in any form.

Object – the object of the section is to protect the "intellectual property" invested in the computer. It is an attempt to protect the compute source documents (codes) beyond what is available under the copyright Law.

Essential ingredients of the section

Knowingly or intentionally concealing

Knowingly or intentionally destroying

Knowingly or intentionally altering

Knowingly or intentionally causing others to conceal

Knowingly or intentionally causing another destroy

Knowingly or intentionally causing another to alter

This section extends towards the Copyright Act and helps the companies to protect their source code or their programs.

Penalties – section 65 is tried by any magistrate.

This is cognizable and non - bailable offence.

Penalties – Imprisonment up to 3 years and/or

Fine – Two lakh rupees.

The following table shows the offence and penalties against all the mentioned section of the I.T. Act-

Section	Offence	Punishment	Bailability and Cognizanability
65	Tampering with Computer Source Code	Imprisonment up to 3 years or fine up to Rs 2 lakhs	Offence is Bailable, Cognizable and triable by Court of JMFC.
66	Computer Related Offences	Imprisonment up to 3 years or fine up to Rs 5 lakhs	Offence is Bailable, Cognizable and
66-A	Sending offensive messages through Communication service, etc...	Imprisonment up to 3 years and fine	Offence is Bailable, Cognizable and triable by Court of JMFC
66-B	Dishonestly receiving stolen computer resource or communication device	Imprisonment up to 3 years and/or fine up to Rs. 1 lakh	Offence is Bailable, Cognizable and triable by Court of JMFC
66-C	Identity Theft	Imprisonment of either description up to 3 years	Offence is Bailable, Cognizable and triable by

		and/or fine up to Rs. 1 lakh	Court of JMFC
66-D	Cheating by Personation by using computer resource	Imprisonment of either description up to 3 years and /or fine up to Rs. 1 lakh	Offence is Bailable, Cognizable and triable by Court of JMFC
66-E	Violation of Privacy	Imprisonment up to 3 years and /or fine up to Rs. 2 lakh	Offence is Bailable, Cognizable and triable by Court of JMFC
66-F	Cyber Terrorism	Imprisonment extend to imprisonment for Life	Offence is Non-Bailable, Cognizable and triable by Court of Sessions
67	Publishing or transmitting obscene material in electronic form	On first Conviction, imprisonment up to 3 years and/or fine up to Rs. 5 lakh On Subsequent Conviction imprisonment up to 5 years and/or fine up to Rs. 10 lakh	Offence is Bailable, Cognizable and triable by Court of JMFC
67-A	Publishing or transmitting of material containing sexually explicit act, etc... in electronic form	On first Conviction imprisonment up to 5 years and/or fine up to Rs. 10 lakh On Subsequent Conviction imprisonment up to 7 years and/or fine up to Rs. 10 lakh	Offence is Non-Bailable, Cognizable and triable by Court of JMFC
67-B	Publishing or transmitting of material depicting children in sexually explicit act etc., in electronic form	On first Conviction imprisonment of either description up to 5 years and/or fine up to Rs. 10 lakh On Subsequent Conviction imprisonment of either description up to 7 years and/or fine up to Rs. 10 lakh	Offence is Non Bailable, Cognizable and triable by Court of JMFC
67-C	Intermediary intentionally or knowingly contravening the directions about Preservation and retention of information	Imprisonment up to 3 years and fine	Offence is Bailable, Cognizable.
68	Failure to comply with the directions given by Controller	Imprisonment up to 2 years and/or fine up to Rs. 1 lakh	Offence is Bailable, Non-Cognizable.
69	Failure to assist the agency referred to in sub section (3) in regard interception or monitoring or decryption of any information through any	Imprisonment up to 7 years and fine	Offence is Non-Bailable, Cognizable.

	computer resource		
69-A	Failure of the intermediary to comply with the direction issued for blocking for public access of any information through any computer resource	Imprisonment up to 7 years and fine	Offence is Non-Bailable, Cognizable.
69-B	Intermediary who intentionally or knowingly contravenes the provisions of sub-section (2) in regard monitor and collect traffic data or information through any computer resource for cyber security	Imprisonment up to 3 years and fine	Offence is Bailable, Cognizable.
70	Any person who secures access or attempts to secure access to the protected system in contravention of provision of Sec. 70	Imprisonment of either description up to 10 years and fine	Offence is Non-Bailable, Cognizable.
70-B	Indian Computer Emergency Response Team to serve as national agency for incident response. Any service provider, intermediaries, data centers, etc., who fails to prove the information called for or comply with the direction issued by the ICERT.	Imprisonment up to 1 year and/or fine up to Rs. 1 lakh	Offence is Bailable, Non-Cognizable
71	Misrepresentation to the Controller to the Certifying Authority	Imprisonment up to 2 years and/ or fine up to Rs. 1 lakh.	Offence is Bailable, Non-Cognizable.
72	Breach of Confidentiality and privacy	Imprisonment up to 2 years and/or fine up to Rs. 1 lakh.	Offence is Bailable, Non-Cognizable.
72-A	Disclosure of information in breach of lawful contract	Imprisonment up to 3 years and/or fine up to Rs. 5 lakh.	Offence is Cognizable, Bailable
73	Publishing electronic Signature Certificate false in certain particulars	Imprisonment up to 2 years and/or fine up to Rs. 1 lakh	Offence is Bailable, Non-Cognizable.
74	Publication for fraudulent purpose	Imprisonment up to 2 years and/or fine up to Rs. 1 lakh	Offence is Bailable, Non-Cognizable.

CYBER LAW IN INDIA

In Simple way we can say that cyber crime is unlawful acts wherein the computer is either a tool or a target or both.

Cyber crimes can involve criminal activities that that are traditional in nature, such as theft, fraud, forgery, defamation and mischief, all of which are subject to the Indian Penal Code. The abuse of computers has also given birth to a gamut of new age crimes that are addressed by the Information Technology Act, 2000

Cybercrime refers to all the activities done with criminal intent in cyberspace. Because of the anonymous nature of the internet, miscreants engage in a variety of criminal activities. The field of cybercrime is just emerging and new forms of criminal activities in cyberspace are coming to the forefront with each passing day.

Cybercrimes can be basically divided into three major categories −

- Cybercrimes against persons,
- Cybercrimes against property, and
- Cybercrimes against Government.

Cybercrimes committed against persons include various crimes like transmission of child pornography, harassment using e-mails and cyber-stalking. Posting and distributing obscene material is one of the most important Cybercrimes known today.

Cybercrimes against all forms of property include unauthorized computer trespassing through cyberspace, computer vandalism, transmission of harmful programs, and unauthorized possession of computerized information.

Cyber Terrorism is one distinct example of cybercrime against government. The growth of Internet has shown that the medium of cyberspace is being used by individuals and groups to threaten the governments as also to terrorize the citizens of a country. This crime manifests itself into terrorism when an individual hacks into a government or military maintained website.

We can categorize Cyber crimes in two ways:

The Computer as a Target: using a computer to attack other computers.

e.g. Hacking, Virus/Worm attacks, DOS attack etc.

The computer as a weapon: using a computer to commit real world crimes.

e.g. Cyber Terrorism, IPR violations, Credit card frauds, EFT frauds, Pornography etc.

Cyber Crime regulated by Cyber Laws or Internet Laws:

Technical Aspects

Technological advancements have created new possibilities for criminal activity, in particular the criminal misuse of information technologies such as

a. Unauthorized access & Hacking:

Access means gaining entry into, instructing or communicating with the logical, arithmetical, or memory function resources of a computer, computer system or computer network.

Unauthorized access would therefore mean any kind of access without the permission of either the rightful owner or the person in charge of a computer, computer system or computer network.

Every act committed towards breaking into a computer and/or network is hacking. Hackers write or use ready-made computer programs to attack the target computer. They possess the desire to destruct and they get the kick out of such destruction. Some hackers hack for personal monetary gains, such as to stealing the credit card information, transferring money from various bank accounts to their own account followed by withdrawal of money. By hacking web server taking control on another persons' website called as web hijacking

b. Trojan Attack:

The program that act like something useful but do the things that are quiet damping. The programs of this kind are called as Trojans. The name Trojan Horse is popular.

Trojans come in two parts, a Client part and a Server part. When the victim (unknowingly) runs the server on its machine, the attacker will then use the Client to connect to the Server and start using the Trojan.

TCP/IP protocol is the usual protocol type used for communications, but some functions of the Trojans use the UDP protocol as well.

c. Virus and Worm attack:

A program that has capability to infect other programs and make copies of itself and spread into other programs is called virus.

Programs that multiply like viruses but spread from computer to computer are called as worms.

d. E-mail & IRC related crimes:

1. **Email spoofing:**

   Email spoofing refers to email that appears to have been originated from one source when it was actually sent from another source. Please Read

2. **Email Spamming:**

   Email "spamming" refers to sending email to thousands and thousands of users - similar to a chain letter.

3. **Sending malicious codes through email:**

   E-mails are used to send viruses, Trojans etc through emails as an attachment or by sending a link of website which on visiting downloads malicious code.

4. **Email bombing:**

   E-mail "bombing" is characterized by abusers repeatedly sending an identical email message to a particular address.

5. **Sending threatening emails**
6. **Defamatory emails**
7. **Email frauds**
8. **IRC related**

   Three main ways to attack IRC are: attacks, clone attacks, and flood attacks.

e. Denial of Service attacks:

Flooding a computer resource with more requests than it can handle. This causes the resource to crash thereby denying access of service to authorized users.

Examples include

attempts to "flood" a network, thereby preventing legitimate network traffic

attempts to disrupt connections between two machines, thereby preventing access to a service

attempts to prevent a particular individual from accessing a service

attempts to disrupt service to a specific system or person.

What is Vishing?

A. Vishing is the criminal practice of using social influence over the telephone system, most often using features facilitated by Voice over IP (VoIP), to gain access to sensitive information such as credit card details from the public. The term is a combination of "Voice" and phishing.

What is Mail Fraud?

Mail fraud is an offense under United States federal law, which includes any scheme that attempts to unlawfully obtain money or valuables in which the postal system is used at any point in the commission of a criminal offense.

What is ID Spoofing?

It is the practice of using the telephone network to display a number on the recipient's Caller ID display which is not that of the actual originating station.

What is Cyber espionage?

It is the act or practice of obtaining secrets from individuals, competitors, rivals, groups, governments, and enemies for military, political, or economic advantage using illegal exploitation methods on the internet.

What is the meaning of Sabotage?

Sabotage literally means willful damage to any machinery or materials or disruption of work. In the context of cyberspace, it is a threat to the existence of computers and satellites used by military activities

Name the democratic country in which The Cyber Defamation law was first introduced.

A. South Korea is the first democratic country in which this law was introduced first.

What are Bots?

A. Bots are one of the most sophisticated types of crime-ware facing the internet today. Bots earn their unique name by performing a wide variety of automated tasks on behalf of the cyber criminals. They play a part in "denial of service" attack in internet.

What are Trojans and Spyware?

Trojans and spyware are the tools a cyber-criminal might use to obtain unauthorized access and steal information from a victim as part of an attack.

What are Phishing and Pharming?

Phishing and Pharming are the most common ways to perform identity theft which is a form of cyber-crime in which criminals use the internet to steal personal information from others.

Preventing Cyber crimes

Cybercrime is considered one the most dangerous threats for the development of any state; it has a serious impact on every aspect of the growth of a country. Government entities, non-profit organizations, private companies and citizens are all potential targets of the cyber criminal syndicate.

The “cybercrime industry” operates exactly as legitimate businesses working on a global scale, with security researchers estimating the overall amount of losses to be quantified in the order of billions of dollars each year. In respect to other sectors, it has the capability to quickly react to new business opportunities, benefiting from the global crisis that – in many contexts – caused a significant reduction in spending on information security.

The prevention of cyber criminal activities is the most critical aspect in the fight against cybercrime. It’s mainly based on the concepts of awareness and information sharing. A proper security posture is the best defense against cybercrime. Every single user of technology must be aware of the risks of exposure to cyber threats, and should be educated about the best practices to adopt in order to reduce their “attack surface” and mitigate the risks.

Education and training are essential to create a culture of security that assumes a fundamental role in the workplace. Every member of an organization must be involved in the definition and deployment of a security policy and must be informed on the tactics, techniques and procedures (TTPs) belonging to the cyber criminal ecosystem.

Prevention means to secure every single resource involved in the business processes, including personnel and IT infrastructure. Every digital asset and network component must be examined through a continuous and an evolving assessment. Government entities and private companies must cooperate to identify the cyber threats and their actions—a challenging task that could be achieved through the information sharing between law enforcement, intelligence agencies and private industry.

Fortunately, like any other phenomenon, criminal activities can be characterized by specific patterns following trends, more or less strictly. Based on this consideration, it is possible to adopt an efficient prevention strategy, implementing processes of threat intelligence analysis.

Security must be addressed with a layered approach, ranging from the "security by design" in the design of any digital asset, to the use of a sophisticated predictive system for the elaboration of forecasts on criminal events.

Additionally, sharing threat information is another fundamental pillar for prevention, allowing organizations and private users to access data related to the cyber menaces and to the threat actors behind them.

At the last INTERPOL-Europol conference, security experts and law enforcement officers highlighted the four fundamentals in combating cybercrime as:

1. Prevention
2. Information Exchange
3. Investigation
4. Capacity Building

Prevention activities must be integrated by an effective incident response activity and by a recovery strategy to mitigate the effects of cyber incidents.

Once an event is occurring, it is crucial to restore the operation of the affected organization and IT systems. Recovery from cybercrime is composed of the overall activities associated with repairing and remediation of the impacted systems and processes. Typically, recovery includes the restoration of damaged/compromised data and any other IT assets.

An effective incident response procedure includes the following steps:

- **Identification** of the threat agent which hit the infrastructure.
- **Containment** of the threat, preventing it from moving laterally within the targeted infrastructure.
- **Forensic investigation** to identify the affected systems and the way the threat agent has penetrated the computer system.
- **Remediate/Recover** by restoring IT infrastructure back online and in production once forensics investigations are complete.
- **Report and share threat data** to higher management and share the data on the incident through dedicated platforms that allow rapid sharing of threat data with law enforcement and other companies.

Cybercrime Prevention Tips

1. Stay Updated

One of the easiest things you can do is keep your operating system and browser updated. Installing security patches helps protect you from these flaws. Luckily, Windows and most browsers have settings to update automatically, so you don't have to do anything other than stay protected.

2. Use Strong, Unique Passwords

Cybercrime prevention starts with using strong passwords. According to a report by Verizon, 63% of data breaches were the result of weak or stolen passwords. Just by using stronger passwords, many breaches could be prevented. It's also important to use unique passwords on every site and avoid social login to prevent hackers from getting your login information once and using it everywhere.

Consider using password managers to help you keep track of your passwords. You can also use special techniques, such as a password made from the first or second letter of every word in a sentence.

3. Always Use an Updated Antivirus

Your antivirus is only as good as its last virus definition update. Antivirus has to update often to protect you from current threats. With cybercrime on the rise, new threats emerge daily. Allow your antivirus to automatically update both the core program and virus definitions.

4. Lock Down Windows

Windows has built-in security features, such as requiring a password to access a locked computer. You should always lock your computer when it's not in use, especially in public. Remember to use a strong password for your computer to prevent unauthorized access.

5. Look for HTTPS

Always look for HTTPS in the address bar of your browser when visiting any sites where you'll provide personal or financial details, such as shopping and banking sites. This identifies that the website is using a security certificate the encrypts the data sent between you and the site.

Most browsers provide details on a site's security certificate to help you determine if a site's legitimate or not. Taking those few extra seconds is just one way to take charge of cybercrime prevention.

6. Avoid Public Wi-Fi

Public Wi-Fi is a playground for hackers. Most data isn't encrypted, so it's easy to pick up credentials as you log in to email, social media, and banking sites. For best results, avoid using public Wi-Fi or use a VPN to protect your data.

7. Skip Emails and Texts You Don't Recognize

Phishing emails, texts, and social media posts are easy to avoid. If something seems odd or you don't recognize the sender, delete or avoid it. Sadly, 30% of phishing emails get opened, leading to identity theft, malware, and ransom ware. Cybercrime prevention means avoiding any messages you don't trust.

If you receive a message from a site you use that tells you that something's wrong with your account, don't click the link in the email. Instead, exit the email and visit the website directly via your browser. If you can't find any issues, contact customer service to explain the email. It's safer and prevents many phishing scams from succeeding.

8. Limit Online Sharing

Cybercriminals can learn intimate details about your life simply by how much you share on social media. They can figure out your passwords, especially those that use important dates or family and pet names in them. They know what sites and apps you use. For best results, limit your sharing. Set your social media profiles to private so only your friends see what you post.

9. Check the Site you’re Shopping On

While you might feel safer on major websites, such as Amazon, it’s a good idea to protect yourself by looking for warning signs on any site you shop on. Scammers may lure you in only to steal your information. Some signs to watch for include:

- Numerous grammatical mistakes
- Currency listed strangely, such as 100$ versus $100
- Extremely low prices – if it’s too good to be true, it probably is
- URLs with hyphens and symbols, such as shop-here-low-prices.com
- No privacy policy
- No HTTPS

If anything feels suspicious, leave the site immediately.

10. Always Monitor Your Accounts

Cybercrime prevention techniques aren’t always perfect, but you can limit the damage by monitoring your accounts. Even when you protect yourself, the sites you use may still experience a breach. Keep an eye on your credit card and bank statements and check your credit .If you do spot strange activity, contact your bank or Credit Card Company immediately. They can put a hold on your account to prevent any further charges and may even refund unauthorized charges.

11. Never Provide More Details than Necessary

Some websites ask for your entire life history. Most of this is just for marketing purposes. However, you don’t know what the site might do with that information. The only details you should ever need to provide while shopping online is your payment details and your shipping address.

Be wary of any sites that ask you for additional personal details, such as your social security number. Basically, if you don’t think a site needs certain information, skip it. If it’s required and you don’t feel comfortable providing it, move on to another website.

12. Be Careful About Downloading

A common scam is to scare you into downloading an app via a pop-up that says something is wrong with your computer or you need antivirus right now. One of the best cybercrime prevention tips to remember is to never download anything you don’t trust. This includes attachments in emails and texts. If you’re not expecting an attachment, contact the sender to see if they really did send it or not.

You should also pay close attention to any programs or apps you install. Sometimes these include extra apps that could compromise your computer. You usually have the option to opt-out of the installation for the extras. Or, you choose a different app altogether that doesn’t try to sneak any extra software on your computer.