**Answer**

**Q: Cybercrime and cyber fraud:**

|  |  |
| --- | --- |
| Cybercrime on the other hand can be executed for many reasons including political, passion and even opportunistically, purely because a vulnerability was there. | Fraud is a crime carried out for financial gain |
| **cybercrime=hacking someone's personal account is cybercrime** | **cyber fraud=making people fool &taking Their money is cyber fraud** |
|  |  |

**Q: Phishing and methods:**

Phishing is an attack in which the threat actor poses as a trusted person or organization to trick potential victims into sharing sensitive information or sending them money. As with real fishing, there's more than one way to reel in a victim: Email phishing, smishing, and vishing are three common types.

**Email phishing**

Email phishing is one of the most common types of phishing. It has been widespread since the early days of e-mail.

**Vishing (voice call phishing)**

With phone-based phishing attempts, sometimes called voice phishing or “[vishing](https://blog.malwarebytes.com/glossary/vishing/" \t "_blank),” the phisher calls claiming to represent your local bank, the police, or even the IRS. Next, they scare you with some sort of problem and insist you clear it up immediately by sharing your account information or paying a fine. They usually ask that you pay with a wire transfer or with prepaid cards, so they are impossible to track.

**Smishing (SMS or text message phishing)**

SMS phishing, or “[smishing](https://blog.malwarebytes.com/cybercrime/mobile/2021/04/what-is-smishing-the-101-guide/),” is vishing's evil twin, carrying out the same kind of scam (sometimes with an embedded malicious link to click) by means of SMS texting.

**Catphishing**

Catfishing or catphishing? Either way, it's phishing with a romantic twist.

*Catphishing* (spelled with a “ph”) is similar, but with the intent of gaining rapport and (consequently) access to information and/or resources that the unknowing target has rights to.

**Spear phishing**

[Phishing vs. spear phishing](https://blog.malwarebytes.com/101/2021/12/spear-phish-whale-phish-regular-phish-whats-the-difference/): While most phishing campaigns send mass emails to as many people as possible, spear phishing is targeted. [Spear phishing](https://blog.malwarebytes.com/social-engineering/2020/01/spear-phishing-101-what-you-need-to-know/) attacks a specific person or organization, often with content that is tailor made for the victim or victims.

**Whale phishing**

Whale phishing is what it probably sounds like: Phishing that targets high-profile victims. This can include celebrities, politicians, and C-level businesspeople. Typically, the attacker is trying to trick these well-known targets into giving our their personal information and/or business credentials. Whaling attacks usually involve social engineering efforts to trick the victim into believing the deception.

**Protect from Phishing:**

* Don't open e-mails from senders you are not familiar with.
* Don't ever click on a link inside of an e-mail unless you know exactly where it is going.
* To layer that protection, if you get an e-mail from a source you are unsure of, navigate to the provided link manually by entering the legitimate website address into your browser.
* Lookout for the digital certificate of a website.
* If you are asked to provide sensitive information, check that the URL of the page starts with “HTTPS” instead of just “HTTP.” The “S” stands for “secure.”It's not a guarantee that a site is legitimate, but most legitimate sites use HTTPS because it's more secure. HTTP sites, even legitimate ones, are vulnerable to hackers.
* If you suspect an e-mail isn't legitimate, take a name or some text from the message and put it into a search engine to see if any known phishing attacks exist using the same methods.
* Mouse over the link to see if it's a legitimate link.

**Q: Passive attack and active attack:**

| BASIS FOR COMPARISON | ACTIVE ATTACK | PASSIVE ATTACK |
| --- | --- | --- |
| Basic | Active attack tries to change the system resources or affect their operation. | Passive attack tries to read or make use of information from the system but does not influence system resources. |
| Modification in the information | Occurs | does not take place |
| Harm to the system | Always causes damage to the system. | Do not cause any harm. |
| Threat to | Integrity and availability | Confidentiality |
| Attack awareness | The entity (victim) gets informed about the attack. | The entity is unaware of the attack. |
| Task performed by the attacker | The transmission is captured by physically controlling the portion of a link. | Just need to observe the transmission. |
| Emphasis is on | Detection | Prevention |

**Q: How does perception make people least suspect cyber security threats through mobile devices? What measures do you recommend against this situation?**

* Do not keep any kind of sensitive data in your device like credit/debit card number and it's pin, any personal image or document which is too personal, etc.
* Have a screen lock.
* Do not hand your device to someone else, or do not let the device get disappeared even for a short duration of time if already been handed over to someone else.
* Only use the official store for downloading and installing apps. Like play store for android. And do not trust any other sources.
* Have an anti-virus. Yes, even phones can have it.
* Do not let anyone else use your wifi if you are using any at home or office. And hide the ssid of your wifi.
* Do not connect and perform transactions or perform any kind of private actions over public wifi.
* Do not use phones like xiaomi, vivo, oppo. As it is said that they use Chinese servers and the Chinese are getting each and every data of us.
* While installing any app make sure you look at the permission it asks for. Like contacts, gallery, Facebook, mail etc.

**Q: Proxy server and anonymizer:**

**Proxy Server**

It is a server (a computer system or an application) that acts as an intermediary for requests from clients seeking resources from other servers. A client connects to the proxy server, requesting some service, such as a file, connection, web page, or other resource available from a different server and the proxy server evaluates the request as a way to simplify and control its complexity.

**Types of proxy** – A proxy server may reside on the user’s local computer, or at various points between the user’s computer and destination servers on the Internet.

* A proxy server that passes requests and responses unmodified is usually called a gateway or sometimes a tunneling proxy.
* A forward proxy is an Internet-facing proxy used to retrieve from a wide range of sources (in most cases anywhere on the Internet).
* A reverse proxy is usually an Internet-facing proxy used as a front-end to control and protect access to a server on a private network. A reverse proxy commonly also performs tasks such as load-balancing, authentication, decryption or caching

**Anonymizer**

An anonymizer or an anonymous proxy is a tool that attempts to make activity on the Internet untraceable. It is a proxy server computer that acts as an intermediary and privacy shield between a client computer and the rest of the Internet. It accesses the Internet on the user’s behalf, protecting personal information by hiding the client computer’s identifying information.

**Types**

* Protocol specific anonymizers – Sometimes anonymizers are implemented to work only with one particular protocol. The advantage is that no extra software is needed. The operation occurs in this manner: A connection is made by the user to the anonymizer. Commands to the anonymizer are included inside a typical message.
* Protocol independent anonymizers – Protocol independence can be achieved by creating a tunnel to an anonymizer. The technology to do so varies. Protocols used by anonymizer services may include SOCKS, PPTP, or OpenVPN. In this case either the desired application must support the tunneling protocol, or a piece of software must be installed to force all connections through the tunnel. Web browsers, FTP and IRC clients often support SOCKS for example, unlike telnet.

**Q: Hacker, crackers, phreakers:**

1. **Hackers**

* He is the one who is curious about workings of any computer software.
* Very often they are no other than unit of smart programmers.
* They have advanced knowledge of operating system and programming language.
* They require data concerned with variety of security holes, so they can exploit and damage or steal knowledge.

2. **Crackers**

* They are the ones who break into different systems with malicious intent.
* They carry out activities like making unauthorized access, destroying necessary information, stopping services provided by server, etc.
* Crackers can easily be identified because their actions are malicious.

**3.Phreakers**

* They are the ones who gain illegal access to the telephone system.
* They are considered to be the original computer hackers as they are the ones who break into telephone system illegally and make long distance calls.
* Phreaker word is a combination of, “Phone” + “Freak”.
* Earlier, Phreakers whistled or used an instrument to mimic tones of phone system operators to route calls and identify payments to avoid paying for an expensive call. Thus, they basically attack phone systems to obtain free phone access or using the phone line to transmit viruses and access, steal and destroy data
* Now, they break into company’s system and manipulate data.

**What is Brute Force Attack?**

A brute force attack uses trial-and-error to guess the password, login info, or encryption keys with the hope of eventually guessing a combination correctly. The attacker systematically checks all possible passwords and passphrases until the correct one is found. A brute force attack accounted for 5% of confirmed security breaches to gain unauthorized access to a system. It is a simple attack method and has a high success rate.

**Wardialing?**

War dialing refers to the use of various kinds of technology to automatically dial many phone numbers, usually in order to find weak spots in an IT security architecture. Hackers often use war dialing software, sometimes called "war dialers" or "demon dialers," to look for unprotected modems. Narrowing down the list of phone numbers answered by modems cuts down the amount of time it takes to do this.

**1. What is reconnaissance**

Reconnaissance definition states that it is a significant instrument as a starting point of numerous data hacking and for penetration testing. The cycle includes gathering data about the target machine that could be utilized to discover its blemishes, weaknesses, and security vulnerabilities.

**2. The two phases of reconnaissance in ethical hacking are**

* Active reconnaissance
* Passive reconnaissance

**A) Active reconnaissance**

Dynamic reconnaissance is the kind of reconnaissance where you assemble data about the framework/application by straightforwardly connecting with the framework. At the point when you utilize Active reconnaissance, there is a high possibility that some data like your IP address is known by the framework you are attempting to accumulate the data about.

**B) Passive reconnaissance**

On account of Passive reconnaissance, you assemble data without interfacing with the framework/application you are attempting to think about. You accumulate data through web indexes or freely available reports. At the point when you utilize Passive reconnaissance, it is highly unlikely that the framework would know your IP address.

**3. The subprocesses of reconnaissance ethical hacking are**

* Footprinting
* Enumeration
* Scanning

**A) Footprinting**

Footprinting is gathering data about the target system which can be utilized to hack the system. To get this data, a programmer may utilize different strategies with variation apparatuses. Maximum time is spent in Footprinting. Information such as Firewall, OS used, and Security configurations in the target system, IP address, Server configurations, VPN, URLs, Network map.

**B) Enumeration**

The enumeration in data security is the way toward extricating client names, network assets, machine names, and different administrations from the target system.  The assembled data is utilized to distinguish the weaknesses or frail focuses on the security of the victim and afterward attempts to misuse it.

**C) Scanning**

Scanning is one of the most famous procedures that assailants use to find services that can be used to misuse the frameworks. All the machines associated with the LAN, through a modem or into notable ports are discovered in scanning.

**What is Patriotic hacking?**

* Patriotic hacking is a term for computer hacking or system cracking in which citizens or supporters of a country, traditionally industrialized Western countries but increasingly developing countries, attempt to perpetrate attacks on, or block attacks by, perceived enemies of the state .

**What is cyber defamation?**

* Cyber defamation is also known as internet defamation or online defamation in the world of internet and its users. Cyber defamation is a new concept but it virtually defames a person through new medium. The medium of defaming the individual’s identity is through the help of computers via internet.

----------------------------------------------------------------

**Q:What is Cyberstalking?**

Cyberstalking is a type of [cybercrime](https://intellipaat.com/blog/what-is-cybercrime/) that uses the internet and technology to harass or stalk a person. It can be considered an extension of cyberbullying and in-person stalking. However, it takes the form of text messages, e-mails, social media posts, and other mediums and is often persistent, deliberate, and methodical.

Example:

* Posting  offensive, suggestive, or rude comments online
* Joining the same groups and forums as the victim
* Releasing the victim’s confidential information online

**Types of Stalker:**

**I.** **Rejected Cyberstalkers:** These offenders either feel misunderstood hoping to reverse the breakup or feel angry and seeking revenge because their attempts at reconciliation with the victim has failed in the past.

**ll Resentful Cyberstalkers:** This type of cyberstalker can be dangerous given their perceived motivation for stalking.  Fear and distress experienced by the victim are the goals of this type of cyberstalker. For this type of profile, the cyberstalker believes the victim both deserves and requires being frightened because they have caused them and/or others anguish and distress.

**III**. **Intimacy Seekers:**This type of cyberstalker does not have ill will towards their victim and simply wants to engage in a loving relationship with them. Intimacy seekers view their victims as their soulmate destined to be together at all costs. Within their mind, they believe it is their job and purpose to make sure destiny of a loving relationship is fulfilled. Intimacy seeking cyberstalkers are often the segment of men or women who harass celebrities and public figures.

**IV. Incompetent Suitors:**These people who fit this profile are cyberstalkers deeply enamored with their victim. Their interest for the victim at times can reach a state of fixation whereby their entire waking life is focused on the endeavor of one day becoming a couple. They tend to lack social, communication or courting skills and may feel entitled that their fantasy of a loving relationship is inevitable.

**V. Predatory Cyberstalkers:**Of the six types, the predatory cyberstalker can be the most dangerous and determined. This type of cyberstalker is motivated by a perverted sexual need. They engage in actively planning an attack along with fantasizing about sexual acts with their victim.

**VI. Ghost Cyberstalkers:**Not included in Dr. Mullen’s five stalker profiles, the ghost cyberstalker is unique to the Information Age. They are online assailants who their target cannot identify. Using [Cyberstealth](https://ipredator.co/cyberstealth/" \t "_blank), the ghost cyberstalker repeatedly makes direct or indirect threats of physical harm and inspires fear.

**Q:What is email spoofing?**

Email spoofing is the act of sending emails with **a forged sender address**. It tricks the recipient into thinking that someone they know or trust sent them the email. Usually, it’s a tool of a phishing attack, designed to take over your online accounts, send malware, or steal funds.

Spoofed email messages are easy to make and easy to detect. However, more malicious and targeted varieties can cause significant problems and pose a huge security threat.

Reasons:

* **Phishing.** Almost universally, email spoofing is a gateway for phishing. Pretending to be someone the recipient knows is a [tactic](https://cybernews.com/security/social-engineering/) to get the person to click on malicious links or provide sensitive information.
* **Identity theft.** Pretending to be someone else can help a criminal gather more data on the victim (e.g. by asking for confidential information from financial or medical institutions).
* **Avoiding spam filters.** Frequent switching between email addresses can help spammers avoid being blacklisted.
* **Anonymity.**Sometimes, a fake email address is used to simply hide the sender’s true identity.

**Q: What is spamming in Internet Security?**

Internet Security - Spamming. Spam is a form of email which is used to send to different email accounts and in general contains advertising about any product or services. But the real problem is when they contain malwares that can damage the user’s data.

Generally, they are sent to a massive list of emails for the mail purpose that a small percentage of users might open them and respond. They are used to such treatment because they are cheap in infrastructure investment, not too much time consuming and simple.

**Techniques Used by Spammers**

In this section, we will discuss the different techniques used by the spammers.

* **Domain Spoofing** − The spammer sends an email on behalf of a known domain so the receivers think that they know this person and open it.
* **Poisoning Filters** − A filter can be poisoned by adding text with the same color of the background to reduce the scoring of the filters.
* **Directory Harvesting** − In directory harvesting, spammers generate email addresses by using known email addresses from corporates or ISP (Internet Service Provider).
* **Social Engineering** − Spammers send promotional emails to different users such as offering huge discounts and tricking them to fill their personal data.
* **Junk Tags** − Spam Words can be hidden by including invalid HTML tags within the words.

**Q: What is cyber bullying, exactly?**

Cyberbullying is the act of intimidating, threatening, or coercing people online through the use of social media, email, text messages, blog posts, or other digital or electronic methods. Also called digital harassment, cyberbullying usually involves the use of derogatory, aggressive, or threatening language. To mask their real identity, cyberbullies often hide behind fake digital personas.

Common example:

* Harassment
* Sexual harassment
* Trolling (The term trolling actually comes from fishing)
* Outing/Doxing (Outing, or doxing, refers to sharing someone’s personal information online without their consent. )
* Fraping (Fraping means breaking into someone’s social media accounts or create a fake account)
* Dissing (When a cyberbully spreads rumors or posts humiliating photos, videos, or screenshots of their victim, that’s referred to as dissing.)

**Q: Types of Wireless and Mobile Device Attacks?**

**1.SMiShing :**Smishing become common now as smartphones are widely used. SMiShing uses Short Message Service (SMS) to send fraud text messages or links.

2.**War driving :**  
War driving is a way used by attackers to find access points wherever they can be. With the availability of free Wi-Fi connection

3.**WPA attack :**  
Wi-Fi Protected Access (WPA) and then WPA2 came out as improved protocols to replace WEP. WPA2 does not have the same encryption problems because an attacker cannot recover the key by noticing traffic.

4. **Bluejacking :**  
Bluejacking is used for sending unauthorized messages to another Bluetooth device. Bluetooth is a high-speed but very short-range wireless technology for exchanging data between desktop and mobile computers and other devices.

5. **Replay attacks :**  
In Replay attack an attacker spies on information being sent between a sender and a receiver. Once the attacker has spied on the information, he or she can intercept it and retransmit it again thus leading to some delay in data transmission. It is also known as playback attack.

**Q: Difference b/w virus and worm**:

|  |  |  |  |
| --- | --- | --- | --- |
| r.No. | Basis of Comparison | WORMS | VIRUS |
| 1. | Definition | A Worm is a form of malware that replicates itself and can spread to different computers via Network. | A Virus is a malicious executable code attached to another executable file which can be harmless or can modify or delete data. |
| 3. | Host | It doesn’t need a host to replicate from one computer to another. | It requires a host is needed for spreading. |
| 4. | Harmful | It is less harmful as compared. | It is more harmful. |
| 5. | Detection and Protection | Worms can be detected and removed by the Antivirus and firewall. | Antivirus software is used for protection against viruses. |
| 7. | Execution | Worms are executed via weaknesses in the system. | Viruses are executed via executable files. |
| 8. | Comes from | Worms generally comes from the downloaded files or through a network connection. | Viruses generally comes from the shared or downloaded files. |
| 14. | Speed | Its spreading speed is faster. | Its spreading speed is slower as compared to worms. |

**Q: Difference b/w steganography and cryptograpy**:

|  |  |  |
| --- | --- | --- |
| **Key** | **Steganography** | **Cryptography** |
| Type | Steganography refers to Cover Writing. | Cryptography refers to Secret Writing. |
| Popularity | Steganography is less popular than Cryptography. | Cryptography is more popular than Steganography. |
| Integrity | Structure of data remains same. | Structure of data can be altered. |
| Attack | Attack in Steganography is termed as Steganalysis. | Attack in Cryptography is termed as Cryptanalysis. |
| Security Principles | Steganography supports Confidentiality and Authentication. | Cryptography supports Confidentiality, Authentication, Data integrity and Nonrepudiation. |
| Parameter | Steganography requires a parameter like key. | Cryptography may not need any key. |

**Q: Blind SQLi Explained:-**

This is a type of SQLi injection attack in which the adversary sends malicious queries to the server then uses its response to make inferences about the application’s configuration. Blind SQLi attacks are mainly performed on websites vulnerable to SQL injection and show generic information for each error message. This type of attack is known as Blind/Inferential SQLi.

**Prevention – Best Practices**

* **Parameterize SQL statements**
* **Utilize secure coding practices**
* **Use an automated vulnerability scanner.**

## Q: Whaling

Whaling is again a type of email phishing attack where top officials like CEO, COO, CTO, etc. are targeted. The attacker sends a mail with a malicious link that looks to come from an authentic source.

**differences between Spear Phishing and Whaling.:-**

| **Sr. No.** | **Key** | **Spear Phishing** | **Whaling** |
| --- | --- | --- | --- |
| 1 | Targets | Spear Phishing targets a specific group of people. | Whaling targets top officials of an organization. |
| 2 | Focus | Spear phishing focuses on stealing login credentials/ sensitive information. | Whaling focuses on fetching trade secrets which can affect a company's performance. |
| 3 | Designing | Spear Phishing emails are prepared for a group of people. | Whaling emails are highly customized for specific persons. |
| 4 | Target | Spear Phishing targets low profile individuals. | Whaling targets high profile individuals. |
| 5 | Prevention | To prevent spear phishing, we should educate people about such an attack | To prevent whaling attack, education, awareness helps and each URL should be checked before opening. |

## Q: What Is Identity Theft? What are the different type of identity theft?

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.

### KEY TAKEAWAYS

* Identity theft occurs when someone steals your personal information and credentials to commit fraud.
* There are various forms of identity theft, but the most common is financial.
* Identity theft protection is a growing industry that keeps track of people's credit reports, financial activity, and Social Security Number use.

**Types of Identity Theft:-**

**Financial Identity Theft**

In financial identity theft, someone uses another person's identity or information to obtain credit, goods, services, or benefits. This is the most common form of identity theft.

**Social Security Identity Theft**

If identity thieves obtain your Social Security Number, they can use it to apply for credit cards and loans and then not pay outstanding balances. Fraudsters can also use your number to receive medical, disability, and other benefits.

**Medical Identity Theft**

In medical identity theft, someone poses as another person to obtain free medical care.

**Synthetic Identity Theft**

Synthetic identity theft is a type of fraud in which a criminal combines real (usually stolen) and fake information to create a new identity, which is used to open fraudulent accounts and make fraudulent purchases. Synthetic identity theft allows the criminal to steal money from any credit card companies or lenders who extend credit based on the fake identity.

**Child Identity Theft**

In child identity theft, someone uses a child's identity for various forms of personal gain. This is common, as children typically do not have information associated with them that could pose obstacles for the perpetrator.

**Q: What is a DNS redirect?**

A DNS redirect is a technique where a client computer is directed to contact a different server than the one it initially requested. The result is that the client may end up on a different domain than they originally intended. There are several common scenarios where you can use DNS redirects to do good:

* Protect your website and users from malicious activity
* Funnel users to a different website than the one they intended to visit for marketing or testing purposes
* Direct traffic from one domain name to another if the original domain changes ownership
* Direct traffic from an old to a new website if the organization decides to move everything over

**Q: What is Cyber Law?**

Cyber law, also known as Internet Law or Cyber Law, is the part of the overall legal system that is related to legal informatics and supervises the digital circulation of information, e-commerce, software and information security. It is associated with legal informatics and electronic elements, including information systems, computers, software, and hardware. It covers many areas, such as access to and usage of the Internet, encompassing various subtopics as well as freedom of expression, and online privacy.

**Why are cyber laws needed?**

There are many security issues with using the Internet and also available different malicious people who try to unauthorized access your computer system to perform potential fraud. Therefore, similarly, any law, cyber law is created to protect online organizations and people on the network from unauthorized access and malicious people. If someone does any illegal activity or breaks the cyber rule, it offers people or organizations to have that persons sentenced to punishment or take action against them.

***Trojan Horse*.**

A program that appears to perform desirable and necessary functions but also performs other functions that the end user does not know about and most probably doesn't need is known as a *Trojan horse*.

A broad category that includes rootkits, illicit servers, viruses, worms or a combination of all of these is better known as *malicious code*. One of the many means to deliver such a payload to the target host is known as a *Trojan horse*.

* Remote Access
* Data Sending
* Destructive
* Denial of Service
* proxy
* FTP
* Security Software Disablers
* Document

**Q: What Is SQL Injection? How to prevent it?**

SQL Injection is a code-based vulnerability that allows an attacker to read and access sensitive data from the database. Attackers can bypass security measures of applications and use SQL queries to modify, add, update, or delete records in a database. A successful SQL injection attack can badly affect websites or web applications using relational databases such as MySQL, Oracle, or SQL Server. In recent years, there have been many security breaches that resulted from SQL injection attacks.

**Prevent:**

1. Use prepared statements and parameterized queries - Parameterized statements ensure that the parameters passed into the SQL statements are treated safely.
2. Object-relational mapping - Most development teams prefer to use Object Relational Mapping frameworks to translate SQL result sets into code objects more seamlessly.
3. Escaping inputs - It is a simple way to protect against most SQL injection attacks. Many languages have standard functions to achieve this. You need to be aware while using escape characters in your code base where an SQL statement is constructed.

Some of the other methods used to prevent SQL Injection are:

* Password hashing
* Third-party authentication
* Web application firewall
* Purchase better software
* Always update and use patches
* Continuously monitor SQL statements and database

## Q:What is Vishing?

This is referred to as "voice phishing."

Vishing, like *phishing* and *smishing*, depends on convincing victims that answering the caller is the proper thing to do. The caller will frequently impersonate the government, the tax department, the police, or the victim's bank.

Cybercriminals make victims feel as though they don't have any choice but to deliver the information requested by using threats and persuasive language.

**Q:What is software piracy?**

Software piracy is the unauthorized downloading, copying, use, or distribution of software. Downloading and using software without paying for it is a common tactic of pirated software users. However, software piracy also includes distributing software on multiple machines when a license was only purchased for one, as well as copying software and redistributing it.

Take a moment to learn more about what software piracy is, the ramifications of pirated software use, as well as how to spot and ultimately avoid pirated software when it crosses your path.

**5 Steps on Prevent Software Piracy**

1. Release a “[Freemium](https://en.wikipedia.org/wiki/Freemium" \l ":~:text=Freemium%2C%20a%20portmanteau%20of%20the,the%20free%20version%20of%20the" \t "_blank)” version of your piece of software or product. A freemium version of your application can help bring in customers who might normally pirate your software.
2. Use a license key to activate your application. We’ve used [Keygen.sh](https://keygen.sh/) with good success.
3. Go to Google and look for a pirated version of your application. Submit a DMCA request to have the URL or Site removed from the Google search index. This is a powerful way to reduce the discovery and download of the pirated version of your application.
4. Contact the site that is pirating your software, and reach out to the site owner and ask for removal. This is often overlooked, but an extremely powerful way to limit the piracy of your application. Some pirate sites have a “remove request” option as well.

5. Last but not least, push updates more frequently with updated features. Often, pirated software will not update automatically. These updates with new features and services can push users using pirated software to move a paid and secured version of the application.

**Q: Introduction of Information Technology Act, Objectives and Features(IT act 2000)**

The Information Technology Act, 2000 was notified on Oct 17, 2000. It was the law that deals with law-breaking and electronic commerce in India and during this article, we are going to verify the objectives and options of the knowledge Technology act 2000. In 1996, the international organization Commission on International Trade Law (UNCITRAL) adopted the model law on electronic commerce (e-commerce) to bring uniformity within the law in several countries. Further, the overall Assembly of the international organization counselled that each one country should think about this model law before creating changes to its laws. India became the 12th country to alter cyber law once it passed the knowledge Technology Act, 2000. While the primary draft was created by the Ministry of Commerce, Government of India because of the E-Commerce Act, 1998, it was redrafted because of the ‘Information Technology Bill, 1999’, and passed in could 2000.

**Pros of the I.T. Act, 2000:**

1. Before the enactment of the I.T. Act, 2000, the usual means of communication such as emails and texts were not considered as a legal form of communication and due to this, they were not admissible as evidence in a court of law. But after the enactment of I.T. Act, 2000 electronic formats and communication got legal recognition, and now they are admissible as evidence in a court of law.
2. With the introduction of the I.T. Act, 2000, now companies can carry out e-commerce and e-business and promote online transactions commercially using the legal infrastructure provided by this Act.
3. Digital signatures and authentications have been legalised after the I.T. Act, 2000, which is a great assistance to carry out transactions online as they help in verifying the identity of an individual on the internet.
4. The I.T. Act, 2000, provides for corporate to have statutory remedies if anyone hacks and breaks into their computer systems or networks and causes any kind of damages. The I.T. Act, 2000 provides for monetary damages, by the way, compensation, as a remedy for such crimes.
5. The I.T. Act, 2000 has defined, recognised and penalised various cyber crimes such as hacking, spamming, identity theft, phishing and many more. Prior to this Act, cybercrimes were not included in any legislation, and there was no legal remedy for such crimes.
6. The Act allows companies to issue digital certificates by becoming Certifying Authorities.
7. This Act also allows the Government to issue notices on the internet through e-governance.

**Cons of the I.T. Act, 2000:**

1. The I.T. Act, 2000 may cause a conflict of jurisdiction.
2. Electronic commerce is based on the system of domain names. The I.T. Act, 2000 does not address the issues relating to domain names, rights and liabilities of domain owners.
3. The I.T. Act, 2000 does not provide for the protection of Intellectual Property Rights as issues regarding copyrights and patents are very common in relation to computer programs and networks.
4. The offences covered and defined under the I.T. Act, 2000 are not exhaustive in nature. Since, with the advancements in technologies, computer programs and networks are constantly changing and evolving, and with this advancement, the nature of cybercrimes is also evolving. This Act does not cover various kinds of cybercrimes such as cyberstalking, cyber fraud, chat room abuse, theft of internet hours and many more.
5. The I.T. Act, 2000 has not addressed issues like privacy and content regulation, which is very necessary, considering the vulnerability internet poses.
6. Lastly, the main issue with this Act is its implementation. The I.T. Act, 2000 does not lay down any parameters for its implementation and regulations.

**Q: Different type of phishing attacks:**

* Spare phishing
* Vishing
* Email phishing
* Sms phishing
* Http phishing
* Pop –up phishing
* Whaling
* Clone phishing
* Social engineering

**Q: Basic safety and security tips to prevent from cyber threat:-**

1. Clicking Without Thinking Is Reckless

2. Use Two-Factor Authentication

3. Look Out for Phishing Scams

4. Secure Your Mobile Device

5. Use a VPN

6. Choose a smart antimalware

7. Improve your browsing habits

8. Don’t fall for emails/messages from untrusted sources

**Q: types and technique of credit card fraud:-**

**PoS Fraud**

In this type of fraud, small skimming devices are attached to normal Point-of-Sale (PoS) devices to hack your data. These devices scan and store the card information while the customer completes a swipe transaction. Usually, this involves a merchant or store employee who shares these details with malicious actors. Similar attachments may also be fastened on to ATM card slots to clone card information, while a camera is secretly placed over the keypad to capture your PIN.

**Phishing and vishing**

These involve impersonating official communication from the bank which in turns acts as a bait for you to click on false links. This will usually take you to websites that look authentic.

**Keystroke logging**

Today, since most financial transactions are online, hackers have started relying on keystroke logging through malicious software to grab credit card details. This usually begins after you have clicked on a suspicious link and unknowingly installed malware on your system. The software records every key pressed on the system, eventually stealing card details, PIN and more.

**Application fraud**

This is a type of identity theft where fraudulent actors impersonate a genuine customer by using their stolen or counterfeited documents to obtain a credit card. While this might be detected after thorough background checks, if carried out, this will allow criminals to use a valid credit card with a false paper trail. A similar type of fraud involves taking over a valid [credit card](https://www.axisbank.com/retail/cards/credit-card) account by posing as the customer using a similar fake paper trail.

**Q: Botnet:-**

Since people started using computer systems, they have become victims of cyber-attack. The reason and medium of cyber-attack vary from attack to attack like phishing attack uses email, DDOS attack is network attacks etc. In most cyber-attacks, hackers use the network as a medium to exploit user information. Online security faces many hazards, and various threats are promising technologies that were abused & “Botnet” is one kind faced by the user.

The term "botnet" is the combination of two terms or words ", robot" & "network", which refer to a robot network handled by suspicious elements for exploiting the system and fetching user information. “Botnet is the combination or network of computers that are maliciously infected and under the control of a single attacking party, also known as "bot-herder".

* **Information theft** – Some attacks access sensitive data or confidential accounts to take advantage of them.
* **Financial theft** – To extort and steal money.
* **Selling data to the dark web/ access to other criminals** – To make money from this information. This database is usually required by other cyber criminals preparing an attack on a large scale or operating a large-scale scam campaign available on a payable amount, rental basis or as an outright sale.
* **Sabotage of services** – To take websites and services offline, etc.
* **Cryptocurrency scams** – Botnets are used to attain users' processing power to mine for cryptocurrency.