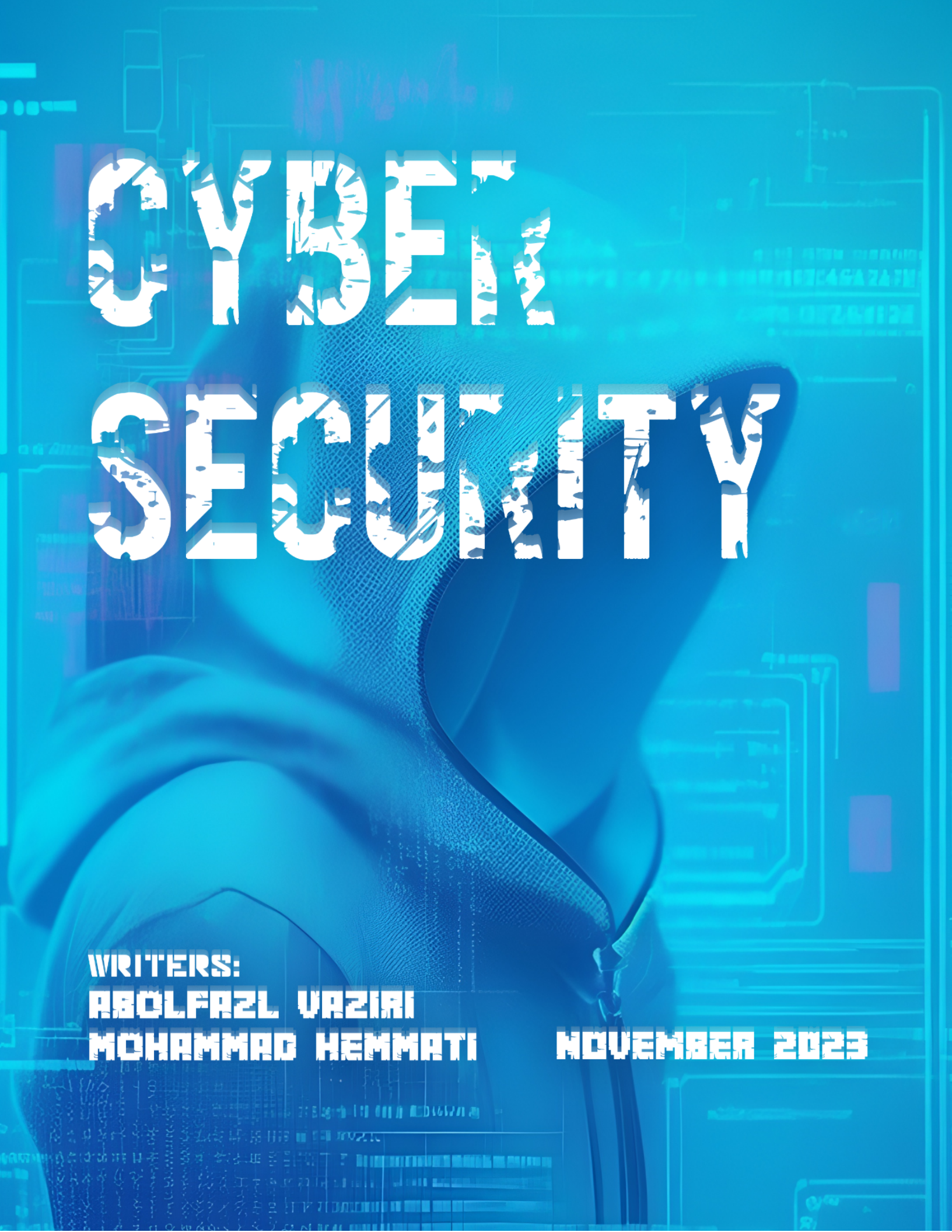


CYBER SECURITY

WRITERS:
ABOLFAZL VAZIRI
MOHAMMAD HEMMATI

NOVEMBER 2023

به نام یزدان پاک

Contents:

Introduction

Nowadays, cyberspace has become a vital part of our lives. From sending messages and personal information to managing bank accounts and shopping online, everything is available online. This phenomenon takes advantage of communication and internet technology and has caused our life to be experienced more deeply in cyberspace.

However, along with these unique possibilities, risks and threats have also arisen for our cyberspace. In fact, with the expansion of the use of cyberspace, security threats have also increased greatly, and we need more awareness and preparation to deal with them.

In this book, we will examine and be aware of security threats in cyberspace. From easy passwords, which are one of the common weaknesses in cyberspace security, to suspicious links and high-risk social networks that can be exposed to all kinds of attacks and cyber risks, we comprehensively examine them.

Our goal in presenting this book is to increase your awareness of the dangers associated with using cyberspace. By reading this book, you will be able to know and apply the best security methods and solutions to protect your personal information, user accounts and devices. Our goal in this book is to strengthen your security in cyberspace and reduce the risks associated with its misuse.

We do our best to strengthen your security in cyberspace and reduce the risks associated with its misuse.

Therefore, although cyberspace offers unique opportunities to our lives, we must also pay attention to its security risks and threats. In this book, we will comprehensively examine these threats to familiarize you with them and provide solutions and guidance so that you can act better and safer in cyberspace, as well as strengthen your security and protect your personal information and user accounts.

Security Threats

One of the main security threats is Malware. Malware is malicious software used by cyber attackers to achieve their goals. They can infiltrate users' computers through spam emails or receiving suspicious files.

There are many types of malware, including:

Viruses: There are programs that attach themselves to other files and infect the system using malicious codes.

Trojans: These types of malware look like genuine and safe software. But in fact, cyber attackers use various methods to trick users into installing Trojans on their systems. Trojans can collect information or damage the system.

Spyware: These programs secretly record users' activities so that cyber attackers can exploit that information. For example, spyware can capture credit card details.

Ransomware: These malwares lock user files and data and pose security threats by providing decryption keys and payment drops.

Advertising software (Adware): These software are used to display various advertisements, but sometimes they may contain malware.

Botnet networks: These networks consist of computers infected with malware that cyber attackers use to carry out illegal activities without users' permission.

In addition to malware, there are other cyber security threats that we will mention below:

- **Phishing attacks:** In this type of attack, cyber attackers try to obtain sensitive user information, such as usernames, passwords, and banking information, using deception and fraud methods.

- **Denial of Service attacks (DOS):** In this type of attack, services and sites are overloaded with a large number of virtual requests from the attackers.
- **System intrusion and control:** In this type of attack, cyber attackers target users' systems and gain complete control over the system and access to sensitive information by penetrating them.
- **Physical Intrusion:** In some cases, cyber attacks can also be carried out through physical access to systems and equipment.

We will discuss some of these topics further.

Password

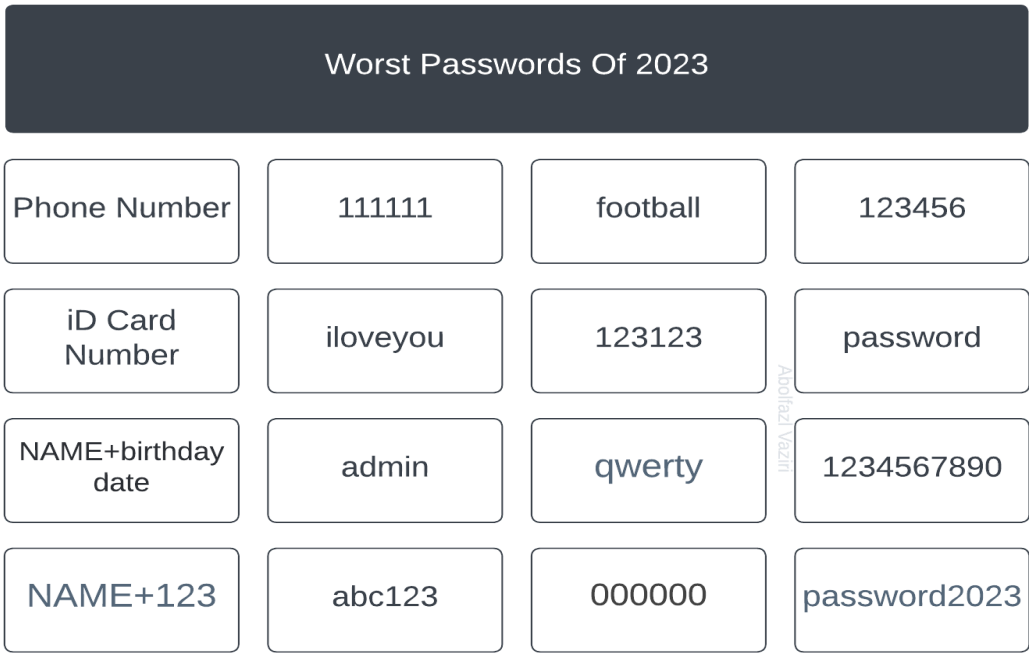
Passwords play a very important role in protecting information security and are one of the main factors in preventing unauthorized access to accounts and sensitive information. When a hacker tries to gain access to a system or user account, they use various methods such as brute force attacks and password guessing based on collected personal information. By using a strong password, the probability of success of these attacks is greatly reduced.

A strong password should have the following characteristics:

Suitable length: Password must contain at least 8 to 12 characters. The longer the password, the more resistant it is to attacks.

Variety of characters: The password must contain a combination of upper and lower case letters, numbers and symbols (@#$.%^,*). Using a variety of characters increases the level of complexity of the password.

Not using predictable words: Passwords should not be common and predictable words like "password" or "123456".



Non-use of personal information: The password should not be guessable personal information such as name, date of birth, phone number and address.

Periodic change: The password should be changed regularly to increase the possibility of blocking unauthorized access to the account. For this, you can set specific dates to remind you to change the password periodically. Also, if you doubt the validity of the password, you can change it earlier than the date.

Not using the same password: Each user account must have a unique password. so that if the password of an account is discovered, there is no ability to access other points and accounts.

Avoid sharing your password with others: Under no circumstances should you share your password with others.

> **The password is like a toothbrush!**
>
> - Choose the best password.
> - Replace every once in a while.
> - Never give it to others under any circumstances.
>
> "Jadi"

Use a two-factor password if possible: If there is a two-factor password feature in the mentioned program or website, be sure to activate it, this feature acts as a double layer of security.

Password management program: Using password management tools and programs to store and generate strong and secure passwords greatly helps to keep you safe.

- **Bitwarden:** For online use
- **KeePassXC:** For offline use and installable

Using a strong password can protect your accounts and personal information from hackers. Also, using strong passwords is recommended as a healthy habit when using the online space.

Links

One of the digital security problems that is gaining a wider scope day by day is the spread of infected links. Infected links that are spread between users through email, social networks and messengers and contain malware and infected or phishing sites.

Many of the links you receive appear to be standard or truncated links that you cannot tell if they are infected or healthy by their appearance. Therefore, never try to distinguish the security of the sites from the appearance of the links.

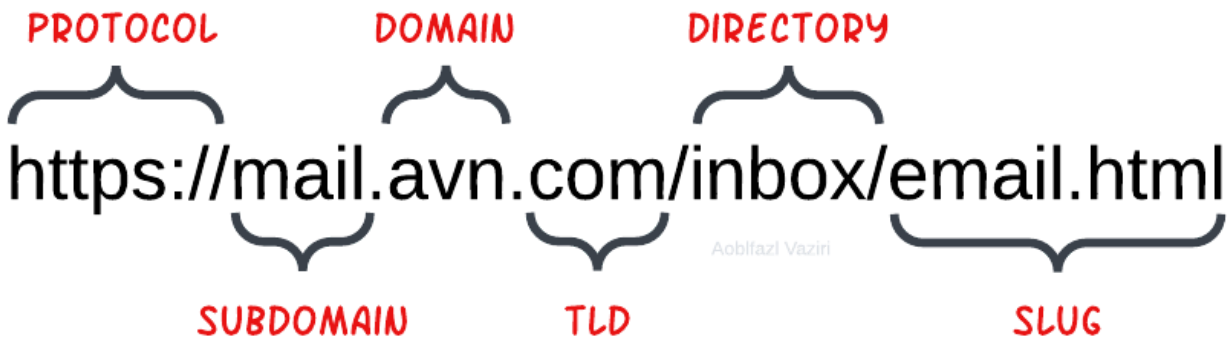
When you receive a link, by all means check its security first before you click on it and create a security problem for yourself.

To check the security of links, you can use free online services in this field. Using these sites is very simple, just put the link in the search field of these sites and press the Enter button to start the search. Finally, if the result is good, you can click on the desired link.

One of the free online services to check the security of links is VirusTotal. Using this service, you can upload the desired link and check it. Also, you can use extensions and security software available for your browser and device to detect suspicious links in advance and prevent you from entering dangerous sites.

One of the main ways to secure links is to learn and be aware of the signs and symptoms of suspicious links. These signs can include suspicious URLs, misspellings, random letters and numbers, unusual lengths, and the presence of special characters. When in doubt, avoid clicking on these signs.

Links consist of several parts, which we will try to review very simply:



Protocol: One of the most important parts of a link is the protocol. In the past, the HTTP protocol was used to communicate, but due to insufficient security, the majority of secure sites in the world currently use the secure HTTPS protocol, and this is enough to know that one of the signs Malicious links use the HTTP protocol.

Subdomain & Domain: Each link contains a domain or subdomain+domain, which must have a correct name:

True	False
https://www.digikala.com	https://wvw.digicala.com
https://adliran.ir	http://adlran.ir
https://Irancell.ir	https://Irancell.xyz
https://career.snapp.ir	http://career.snap.ir

Domain extension (TLD): According to the country or type of business, the domain extension is different, for example, for the country of Iran we use .ir and all internal institutions and organizations use this domain extension, and as you can see in the above table, "https://irancell.xyz" is an invalid link.

Malicious links can have the potential to seriously harm your security and privacy. Hackers use malicious links to access your personal information, attack your systems, and generally engage in illegal activities.

Below are some of the importance and threats related to malicious links:

Theft of personal information: By clicking on a malicious link, hackers can gain unauthorized access to your personal information. This information can include your passwords, bank account numbers, credit card information, and other sensitive information.

Penetration into systems and networks: Malicious links can be used to hack into your systems and gain full control of the system. This can lead to unauthorized access to personal and sensitive information, theft of business information, service interruption and damage to your systems. This allows them to use your resources and information or even access other systems on the network.

Installing viruses and malware: By clicking on a malicious link, viruses and malware may be automatically installed on your system. These software can collect your information, gain complete control over your system or operate anonymously.

Trojans and keyloggers: Malicious links may be used to install Trojans and keyloggers. Trojans give hackers complete control over your system, and keyloggers record and send your activities to hackers, including login information to sites and online accounts.

Publish passwords: Hackers can steal your passwords and give them to others by using malicious links.

Abuse of online accounts: Hackers may gain access to your online accounts using malicious links and use them to send unauthorized emails, spread fraudulent information, or perform other malicious activities.

To avoid malicious links and detect them, you can do the following:

1. **Taking care of emails and messages:** Do not click on suspicious links in unknown emails and messages. Also, carefully check emails and messages that ask for your online account information or ask you to click on a link sent to you and make sure it's authentic.

2. **Check the URL address:** Check the URL carefully before clicking on the link. Make sure that the URL matches the original source and that no changes have been made to it. Also, make sure the secure HTTPS protocol is used.

3. **Using vulnerability detection tools:** Use vulnerability detection and prevention tools such as firewall, antivirus and antimalware. These tools can detect malicious links and prevent you from entering dangerous pages. Sometimes the initial influence takes place through the people around you!

4. **Education and awareness:** Educate yourself and the people you care about to recognize suspicious and malicious links. Provide them with explanations about the performance of phishing and cyber attacks.

These methods can help you avoid malicious links and protect your online security. Also, it is important to always perform security updates and use trusted and reliable sources to access information.

Social Networks & Messengers

The security of social media accounts and messengers is very important and having a secure account can prevent many risks.

Unauthorized access to your social media account and messengers can lead to identity theft, publication of personal information, publication of bank account information, erasure of important information, and abuse of your account by attackers. Your accounts can also become the target of deceptive attempts such as phishing and hacking into other accounts.

Losing an account can cost you money, damage your reputation, and lose contact with friends and family.

It should be noted that some people should be warned that they work in the form of security and safety of cyberspace with titles such as Instagram security, WhatsApp, etc. 90% of these people are fraudsters and do not have any technical knowledge and did not perform any action on your account and finally set a relatively strong password for your account... Securing social networks like Instagram can only be implemented in one way, that is Creating a robot connected to the account and defining a series of security configurations that are activated based on the behavior and changes of the account and prevent penetration into the account.

You can apply these things to increase the security of your social network and messenger accounts:

1. **Strong password:** Use a strong and unique password for your accounts. The password must contain upper and lower case letters, numbers and symbols and have at least 8 characters. Also, avoid using a password derived from your personal information (such as your date of birth or last name).
- In the password section, we mentioned more things that you can read again.

2. **Two-step authentication:** Enable two-step authentication for your accounts. This feature allows you to enter an additional factor, such as a code sent to your mobile

phone, in addition to your password when logging into your account. This gives you more security against unauthorized access to accounts.

3. **Access check:** In the account settings of social networks and messengers, pay attention to active sessions in your account. There may be unauthorized access to your account, remove the connected unauthorized device. Also, periodic review to check for unusual activities in your account is very important.

4. **Personal Information:** Avoid posting too much personal information on your social media accounts and messengers. Do not post information such as your home address, phone number, banking information, and other sensitive information, and the photo or video you posted may inadvertently contain important information. This information may be used by attackers for targeting and exploitation.

5. **Private messages:** Always be careful that the messages and requests you receive are from reliable sources. Do not receive suspicious requests such as requests for money or personal bank account information through social networks and messengers.

6. **Software updates:** Make sure that the software and programs used to access your messenger and social network accounts are updated. These updates may include security improvements and by installing them you can avoid security vulnerabilities in older versions.

7. **Awareness and learning:** By studying and being aware of new methods of cyber attacks and methods of protection against them, you can get ahead of your account security. Studying and keeping up-to-date on security threats and how to deal with them is very important.

By applying these recommendations, you can improve the security of your social media and messenger accounts. It is also better to check your accounts regularly and if you see any suspicious activity or unauthorized access, delete it and cut off its access.

Phishing attacks

Phishing is an internet attack method used by attackers to obtain sensitive and important information from target users. In this type of attack, attackers fraudulently ask users to provide sensitive personal information, such as passwords, credit card numbers, banking information, and so on, typically through emails, text messages, phone calls, or fake web pages.

Information theft: By accessing personal and sensitive information, attackers can steal your identity and use it to forge documents, or by accessing bank and credit card information, attackers can withdraw money from your bank accounts, make unauthorized purchases or transactions.

Damage to the security of other accounts: Attackers may also access and hack your other accounts using the information they receive from you.

Phishing occurs widely and some common scenarios are:

1. Sending fake text messages to mobile phone numbers with bank claims and requests to send personal information.
2. Creating fake web pages that are similar to the real pages of banking sites and reliable sites such as google and ask for user information.
3. Fraudulent phone calls from scam numbers, asking for sensitive information or claiming virtual prizes.

Types of phishing:

Email Phishing: By sending fake and misleading emails, attackers encourage users to enter their personal information on fake pages.

Voice Phishing: In this method, attackers deceive users with fake phone calls and receive personal and sensitive information from them.

SMS Phishing: In this attack, fake text messages are sent to mobile phone numbers and users are asked to click on a link or download a file.

Web Phishing: Attackers create fake web pages and trick users into providing personal information. In this scenario, the attacker sometimes does not need the victim's action, and only by clicking and opening the link from the victim's side, the attacker obtains the information and data he needs.

Ways to prevent phishing are:

1. **Educating yourself and others:** Educating yourself and the people around you about phishing methods, identifying signs of fraud and suspicious behavior can help against these types of attacks.

2. **Care of personal information:** Always be careful not to send your personal information directly in response to fake emails, messages or phone calls.

3. **Website address check:** Before entering your personal information on the website, make sure that the website address in your browser is correct and matches the actual website address.

Phishing is known as one of the most important methods of attacking online security due to the fake and fraudulent methods used in it. It’s danger is that unsuspecting people may easily trust these fake devices and enter their sensitive information.
On the other hand, phishing is always associated with sophisticated and advanced tools, and attackers constantly create new methods to attract the attention and information of their target users.

Application

For the security of programs, there are certain methods and solutions that you can use to prevent malicious attacks and intrusions.

In the following, we describe some of the solutions:

Get programs from reliable sources: Be sure to download apps from official and reliable sources such as App Store or Google Play. These sources usually run security checks on the apps and make sure that the downloaded files are malware-free.

Use the official version and update regularly: Always use the official version of the programs and do not install unofficial and so-called Crack versions because these versions are usually developed by third parties and may contain malware or malicious programs and spyware, here you should go to unofficial versions of the program. He pointed out such as WhatsApp, Instagram, Telegram, etc. and emphasized that all these versions are unofficial and invalid and are designed only to collect information and spy on users. monitor and even have unauthorized access to their devices, so please do not install unofficial versions of the programs under any circumstances and always update the programs provided by the original developers. These updates usually include security fixes that fix security issues and weaknesses and help keep apps safe from malicious attacks.

Check program permissions: When installing an app, check the permissions requested by it. If a program asks for unnecessary and unusual permissions, it is better to avoid installing that program. For example, if an online game requests access to your calls or camera resources, it may be suspicious and you should be careful.

Using locks and encryption: If your app stores sensitive information such as passwords, banking information, or other personal information, make sure you use security locks such as passwords or fingerprints to access the app. Also, some programs provide the ability to encrypt information to protect it in case of unauthorized access.

Checking program access: After installing an app, check what access the app has in the settings section of your phone. For example, does the app have access to the camera, call sources, geolocation, etc.? If the accesses of the application do not match with the use of the function and its actual need, the application may have unauthorized access and is suspicious.

Android	Settings > Apps > APP-Name > Permissions
iOS	Settings > APP-Name > Allow To Access

These are just a few of the ways you can increase the security of your apps. Also, you should always consult app developers and reputable security sources for further guidance.

Safe Storage Of Information

If your personal documents and information, bank accounts, sensitive organizational documents and other important information become available to hackers or abusers, you may face serious risks, including identity theft, lost financial assets and internet fraud. If your data is damaged, without proper backup, sensitive information and important documents may be lost and cannot be recovered.

Data encryption: Use encryption for protection It is very effective for sensitive documents and information. With encryption, your data is encrypted with a key or password and can only be accessed using that same key or password. Well-known encryption programs such as BitLocker for the Windows operating system and FileVault for the macOS operating system or the VeraCrypt program for all operating systems can be useful in this regard.

Regular backups: Creating a backup copy of important documents and information can prevent data loss in case of loss or damage. You can use external backup methods such as external drives or cloud services such as Dropbox, Google Drive and OneDrive.

- Automate the backup process as much as possible.

Use a strong password: To protect information, you must use a strong password to log in. Strong passwords should be a combination of upper and lower case letters, numbers and symbols, and it is best to use a unique password for each of your accounts.

Antivirus software: Using antivirus and antimalware software protects your computer from malicious programs and cyber attacks. These softwares regularly scan the system and identify and eliminate any threats.

Update operating system and programs: To stay secure, it's important to keep your operating system and apps up to date. Authentication and security fixes in updates can fix existing vulnerabilities and prevent the loss of your data at risk.

Restrict access: Restricting access to important information can prevent unauthorized access. Make sure that you set the access settings for files and folders containing sensitive information on your computer correctly and that only those who need access have access to them.

physical protection: Finally, physical protection is also very important. Make sure your data is in a safe place and protect your smart devices with encryption and lock patterns so your data is safe if lost or stolen. If needed, you can use locks or other physical protection systems.

By applying these methods, you can improve the security of your documents and information and prevent their loss or unauthorized access.

VPN

VPN is a technology used to create a secure and encrypted connection between a device and a computer network, as well as to increase security and privacy in Internet communications. With a VPN, you can tunnel your connection through a VPN server so that your data is encrypted and your traffic is hidden from your real IP address.

But you should pay attention to the following:

Free VPN: Some free and built-in VPNs may carry risks. To provide their free service, these tools usually use methods such as displaying annoying ads, collecting and selling user information, or even weak encryption.

A reputable manufacturing company: When choosing a VPN, pay attention to the reliability and validity of the service provider. Research whether the VPN provider is reliable and trustworthy, and whether protecting your privacy is a priority for them.
Using a VPN from a reputable and reliable manufacturing company will help you benefit from quality service and proper security. Reputable VPN companies usually use strong encryption protocols and provide reliable servers in different locations around the world. By using a VPN from a reputable company, your information is encrypted and protected from unauthorized access, and your traffic passes through secure servers, which ensures that your information is secure and confidential.

Security and encryption: Make sure the VPN service uses strong encryption and uses reputable security VPNs such as WireGuard, OpenVPN or IPSec.

Paid subscription: Using VPNs that require a paid subscription to use them usually provides a better and more secure service.

Download from a reliable VPN site or official market: When downloading a VPN, it is better to use official and reliable sites and markets. These sources ensure that you get and install the original version without any unwanted modifications.

Downloading and installing VPN from unknown and unreliable channels and groups on social networks may bring security risks. These types of sources may offer modified or infected versions of VPNs that can lead to the theft of your information, installation of malicious programs, or unauthorized access to your device.

Knowledge of local laws: Familiarize yourself with the laws and regulations related to the use of VPN in your country and note that the use of VPN may not be legal or have restrictions in some countries and environments. Therefore, before using a VPN, be aware of your local laws and avoid using it in areas where it is not legal.

In general, using a VPN can increase your security and privacy in Internet communications, but be careful to choose a reliable service provider, use paid VPNs, and take care of personal information.

Android Devices

Android devices contain sensitive personal information such as contacts, messages, conversation history, photos, videos, and online account information. If your personal information and bank accounts are stored on your Android device, thieves can gain access to your information through malicious software or unauthorized access to the device and commit identity theft or financial abuse.

Android devices may be constantly in contact with the Internet and various applications. If these devices are damaged or compromised by malware, your information is at risk and hackers may gain access to your personal information or bank accounts.

Counterfeit software: In the market of Android applications, there are also fake and malicious software. Installing unknown and fake software can lead to loss of personal information, illegal device access, viruses and spyware. Try to only download and install software from official sources like Google Play Store. These sources usually review software for security.

Vulnerabilities of the operating system: Like other systems, the Android operating system may also have security vulnerabilities. If your device manufacturer doesn't provide security updates for the operating system or you don't install critical updates, your device is vulnerable to attacks. Try to keep your operating system and apps up to date to get the latest security updates.

Not using screen lock and password: Not using an Android device screen lock and not using a strong password will allow those who have the opportunity to physically access your device to gain access to your information. Try to always enable the screen lock on your device and use a strong password. You can also use fingerprint recognition or facial recognition features.

Internet connection care: Avoid connecting to public and anonymous Wi-Fi networks, as these networks may be designed for spying and attacks.

Email check: Make sure the email account connected to the Android device is secure and its two-step authentication is enabled, the email connected to your Android device has permission to access some resources of the device, and through it you can also access connected programs.

iOS Devices

To further secure your iPhone devices and prevent security risks, you can take the following steps:

Operating system update: Make sure that the iOS operating system on your iPhone device is up to date. Operating system updates include security fixes that help prevent potential vulnerabilities. It is important to check and apply updates regularly.

Using Touch ID or Face ID: If your iPhone device supports fingerprint recognition or face recognition (Touch ID or Face ID), use these features to increase security. These features help you log in quickly and confidently.

Use a strong password: Use a strong password for your screen lock as well as for your online accounts. Passwords must contain upper and lower case letters, numbers and symbols and have at least 8 characters.

Two-step authentication: Enable two-step authentication for your online accounts, specifically for your iCloud account and Apple ID account. In this case, in addition to the password, you need a one-time code sent to your device or phone number to log in to the account.

Using official programs: Make sure to download and use official and valid apps from the App Store. These programs are monitored and controlled by Apple.

Information Leakage

User information leakage is one of the serious risks in the field of cyber security and can have serious consequences for sites, organizations and users. Imagine that an important organization or an important site that has many users is attacked and infiltrated and hacked, and after some time the intruder publishes the information of the users in the cyberspace, which can include the personal information of the users such as name, phone number, national code, date of birth, place of residence and even financial information of users that are given to notorious people and used for inappropriate purposes.

At first glance, you may think that this information has no value and credibility, but if you look at the passwords of your accounts, you will notice that 90% of the time you choose a password that consists of your personal information, such as your date of birth or national code or your name. and an intruder can have unauthorized access to your accounts by accessing your personal information.

Also, this information can be used for crimes in cyberspace, for example, imagine someone registers with your personal information in an organization or a site and does unethical and illegal activities. Who is the criminal? The criminal owns the identity. is to be you!

Another frequent use of this information is for fraud and social engineering. Imagine someone calls you and claims to be an employee of a bank or government agency and parrots your and your family members' information. In the end, he asks you to read the code sent to the SIM card or to click on the link sent to you or any other task... In such a situation, the person trusts him because of the accuracy of his information or his family as stated by the intruder. And he does what he is asked to do.

Unfortunately, we are always witnessing the leakage of information with a very high volume.

My personal information has been exposed, what should I do?

Recovering personal information after a disclosure is difficult, but you can do everything you can to minimize the damage.

For example, check whether you use the same passwords on different websites, and whether your personal information has been used to register unwanted accounts.
In addition, as much as possible, avoid using your phone number, date of birth, or other disclosed information as a password, so that someone who has your personal information cannot guess your password.

In general, leakage of user information poses serious risks not only for users, but also for organizations and service providers. For this reason, maintaining the security and privacy of users' information is very important, and organizations should make every effort to prevent information leakage and protect users' sensitive information.

Social Engineering

There is no patch for human stupidity!
Social engineering refers to the types of methods in which the hacker takes advantage of people without using special software or hardware and only by using their own body availability. This exploitation can be done to receive information, passwords or any type of data.

Normally in this method we don’t have Firewall, various monitors and planned hardware and software programs for going to war with people on the network. This penetration may be done with an electronic message, a conversation, a casual meeting, etc.

Social engineers are divided into two branches:

Engineering with technical knowledge: These people use computer attacks, but they act on the basis of social engineering, for example, by sending an e-mail or an advertising message, they force you to click on a specific link or download the desired file.

"Unbeatable opportunity! Only the first 100 people! You win the biggest iPhone X prize of the year. Just click the link below and fill out the form below to claim your prize. Don't miss out!"

Or another frequent case:

"A new complaint was registered against you in the Electronic system.
http://elctronic.ws”

In this case, by targeting a sensitive point and creating fear, the intruder did not allow the victim to think and make a decision, and the victim quickly clicked on the link without checking...maybe if this scenario is implemented again in the future by another malicious team. Again, it succeeds because it very cleverly and as quickly as possible forces a person to click on a link or download a malicious file.
When dealing with such cases, try to check the number of the sender of the message first and then check the link.

In the example above, there are signs that the link is malicious:

- **Insecure HTTP protocol**

No reliable source of**HTTP** It does not use secure protocol to communicate and all original and reliable sources**HTTPS** use!

- **Invalid domain elctronic.ws**

The domain is designed in a way that is very deceptive, the first thing that can indicate that this domain is malicious is the extension .ws and the second point that is very cleverly placed is the use of elctronic instead of electronic it will not be recognizable at first glance!

Engineering with manpower: This group of people use physical contact and conversations to establish communication and then implement their plan.

Let's start with a simple example:

the scenario: The secretary's office of a company.

- **Secretary (sadly):** I don't know how to draw a table with this software?!
+ **Influential (apparently a reference lord):** Sorry, I overheard you, actually I've been working with this software for a few years, if you let me take a look, I might be able to help.
- **Secretary (smiling women):** Of course, I don't know anything about it.

As we have seen in the scenario, the secretary of the company is not justified in any way and allows a different person to use his system.

Be careful in choosing people in your network

Give basic training to the people of your network

In the above example, instead of using a stranger, the secretary could go to a guide book or more simply, to the Internet, or if someone offers him help, the secretary can use the words "no", "no, thank you" and "no". With the meaning of rejection The request of that person was

used, most of us are unable to say the word "no" and we are left behind, this one word is one of the most effective ways to deal with social engineering attacks.

Pay attention to the following scenario:

Scenario: Mr.John got into a taxi as fast as possible to go to his workplace, on the way he realized that he left his wallet at home.

When a person is not aware of his wallet or there is no money, in the first step, he tries to visit places where there is a possibility of money, in this case, most of the people find a state of semi-concern and helplessness.
In this example, the influential person appears in the role of a savior. He tells Mr.John with a sincere tone that he will pay his rent as well (insistence from the hacker and denial from John).

In case of rejection several times, the hacker will not be disappointed, he will tell John about the lack of money and getting into the car and that another person wants to calculate the fare, but he did not accept and in the end, because of the argument with the driver A taxi was hailed from it, and at the same time, it also gives the right to the driver of the same taxi.
In these conditions, John is in a situation that is unavoidable and he will accept it with a strong possibility.

John walks in front of the company and gives the address of the office to the intruder and closes the car door and goes inside the company. the intruder enters the room, John will be happy to see the hacker(Savior) and invites him to have tea (the meeting may be done in another way, here we imagine a good meeting.)

The hacker says with thanks that he does not have access to the Internet and right now he has to fill in the registration form and he has to complete the registration through the Internet. give and…

Pay attention, the lower the person's side is, the more trust will be found!

The above example is a comprehensive and general example, and of course, it is widely used. In the above example, the sense of compensation, no matter how small, is induced in the target person. The above scenario includes the psychological motivation of mutual transactions.

Most people think that there will never be victims of such attacks.

Attack without physical presence 1:

Scenario: Calling one of the people of the network (Nadri, one of the real managers of the company), the tone of the conversation and the tone of voice is completely similar to a real person, and even Nadri's unique words and phrases are used. (There are devices in the market to change the voice.)

- **hacker:** Hello, I am Nadri
+ **Secretary:** Hello, Are you fine Mr. Nadri?
- **hacker:** Yes, thank you, I won't bother you too much, I know your are busy, just go to my office, turn on my computer and follow the steps I tell you.
+ **Secretary:** Ok

Attack without physical presence 2:

Scenario: Seeing the internet user of one of the company's employees, a person tries to get the password.

- **hacker:** Hello, support unit?
+ **Support:** Yes, tell me
- **hacker:** I have not been able to enter the network since this morning, in fact, I accidentally saved my password and now I can't remember it no matter what I try, please help me?
+ **Support:** But we can't... the hacker takes action to cut off the conversation. I must get to my boss and manager. I would be grateful if you could help me. I just started working here for a month, I don't want to disappoint my boss right away, I'm afraid that his opinion of me will change.
- **Support:** Well, of course I understand, can you give me your customer's number?

+ **hacker:** 190023
- **Support:** Your password is 12345600, remember it somewhere so you don't get into trouble again.
+ **hacker:** Thank you so much.

In the above scenario, if the caller is a lady and she adds a little desire in her tone, these steps will be done many times faster than before, the psychological stimulus in this scenario is to induce feelings.
According to his duty, the person in charge of the support department should refrain from giving the password, and according to the regulations, he asks the person to contact the support and receive the password. This can be done by acquaintance or by letter.

Two very important points to neutralize this type of attacks:

- If your work is in accordance with the law, don't be afraid of anyone, even if that person is your boss.
- Do not trust anyone on the phone, even if that person is your father.

How Do We Know We Have Been Hacked?

Determining whether your account or system has been hacked can be challenging. But some general and technical symptoms may indicate that your user account or system has been hacked.

Unusual changes in the user account: You may notice that you have unusual activity on your account, such as sending spam messages or emails to your contacts, posting on social networks, or making suspicious transactions.

Suspicious activity in devices: If you use multiple devices, you may notice that activities and statuses on another device have changed, such as unread messages, changes to settings, or account logins from suspicious locations.

User account information: If you notice that your password or other account information has changed, but you haven't made the changes, this could be a sign that your account has been hacked.

Increase the use of system resources: If your system gets unusually warm, performance slows down, or you notice that system resources such as CPU and memory are being used abnormally, this could indicate the presence of malicious programs or attackers on your system.

Changes in files and settings: If you notice that your system files or settings have been changed without your permission, such as creating new files, changing network or operating system settings, this could be a sign that your system has been compromised.

Network activity: If you notice that your network traffic is more than normal, such as excessive sending and receiving of suspicious packets, requests to unknown services, or unusual network connections, these could be signs that your system has been hacked.

Errors and messages: If you receive unusual messages or errors, such as security messages or system errors, this could be a sign that your system has been compromised.

If you notice any of these symptoms, it is recommended that you take the following actions:

1. **change Password:** Change your account and system password with a strong and unique password.

2. **Checking and removing suspicious programs:** Check the programs and processes running on your system and remove any suspicious or unknown programs or processes.

3. **Update system and applications:** Make sure your operating system and apps are updated to the latest version available to cover new security vulnerabilities.

4. **Using antivirus software:** Using antivirus software to scan and identify suspicious programs and files and clean your system.

5. **Notification to relevant authorities:** In severe cases of hacking or intrusion, it can be useful to inform the relevant authorities such as relevant institutions and police.

However, if you suspect that your account or system has been hacked, it is recommended that you contact the relevant security technicians or IT professionals for assistance and guidance.

Physical & Wireless Connections

Connections such as external memory card connections or USB and external connections such as charging cable connections and other physical connections or wireless connections such as Bluetooth and Wifi connections to mobile phones and laptops provide many facilities for users and play an important role in our daily lives. However, with these features come some security risks that can damage your device and data if not taken care of.

Side connection security risks:

Transmission of malware and viruses: One of the main dangers of side connections is the transmission of malware and viruses. When the memory card or the source of the charging cable is infected with malware and viruses, when connected to your device, it can penetrate the device and infect or steal sensitive information. A physical connection to your device can provide the highest level of device access.

External storage devices: External storage devices such as hard drives and memory cards should also be considered. If these devices are obtained from unknown or insecure sources, they may contain malware or malicious software that infiltrates your device and compromises your information when connected to it. It is best to use reliable sources for obtaining external storage devices and regularly check and scan the devices before use.

Prevention methods:

- Not using charging ports in public and non-public places.
- Paying attention to the product packaging when buying and not getting the product without packaging or the product whose packaging has been opened.
- Use updated anti-malware programs and scan memory cards or USB before use.
- Update operating system and software regularly and implement security patches.
- Encrypt sensitive files on the device.
- Use reliable sources to buy memory cards or USB.
- Failure to run unknown or suspicious executable files.

Security risks of wireless connections:

Spying and unauthorized access: Wireless connections make it easier for spying and unauthorized access to devices. By exploiting security weaknesses in wireless connections, an attacker can infiltrate your device and manipulate or steal your personal information, passwords, files, and communications.

Man-in-the-Middle attack (MITM): In a MITM attack, attackers gain the ability to intercept your communications. They can eavesdrop on the communication between your device and the target device and learn or even change the information. This attack can occur in wireless connections and threaten the security of your communication.

Intrusion into wireless networks: Wireless networks that are improperly configured or set up using weak encryption are compromised and can be easily penetrated by attackers. Attackers can manipulate network information, disrupt communications, or even gain access to devices connected to the network, including smart devices, personal computers, surveillance cameras, and other smart devices connected to the wireless network.

Prevention methods:

- **Use strong encryption:** Make sure your wireless network is set up using strong encryption, such as WPA2 or WPA3. Strong encryption prevents attackers from infiltrating and preventing unwanted decryption of your information.

- **Set a strong password:** To access the router Set a strong password for your wireless. Do not use the router's default password and use a strong and unique password.

- **Disable unnecessary features:** Disabling unnecessary features on your wireless router can reduce security risks. For example, if you don't use the WPS feature, disable it.

- **Software and firmware updates:** Make sure your router and devices connected to your wireless network are up to date. This means fixing potential weaknesses and improving security.

- **Using a virtual private network (VPN):** Using a virtual private network (VPN) can encrypt your communications and improve your security on public networks and vulnerable wireless networks.

Overall, to reduce security risks on wireless connections, it is important to take appropriate security measures, avoid using default settings, and perform regular security updates.