The most common ways that hackers use to hack your Facebook account

The issue of security and information safety on the internet is always a hot issue that many people are concerned about. To protect your account on the internet, you should equip yourself with basic knowledge

Facebook is the largest social network in the world today, this is the target that hackers most frequently attack in the world for many different purposes. Even if you set a very strong password or add multiple layers of security, your Facebook account is still not really safe.

Below are some of the most common methods hackers use to attack Facebook accounts and how to avoid them.

Attack Facebook account using Phishing method

The most basic concept Phishing is a phishing attack method, in the field of computer security, is a malicious act of forgery to obtain sensitive information such as usernames, passwords and card details. credit by masquerading as a trusted entity in an electronic transaction.

As for attacking Facebook, Phishing is one of the most common attack methods used by hackers who hijack Facebook accounts. Hackers will create fake login pages that look like the original Facebook page. It then asks the victim to log in to the fake Facebook page. The victim's "Email Address" and "Password" are saved in the hacker's data file at the time the victim logs in to the fake site. The hacker will then access this data file to get the victim's login information.

The disadvantage of this method is that when 2-step security layers are enabled or verified with other devices, it is also difficult to get login information to get a Facebook account. However, losing information and passwords is also very dangerous.

Recently, bad guys have been continuously using deception methods, tagging Facebook users in attractive and curious content.

Bad guys use many virtual accounts to share a lot of curious content to trick Facebook users into logging into phishing sites to collect information from Facebook users.

How to prevent Facebook account attacks using Phishing methods

1. Just log in to your Facebook account by typing the exact domain name facebook.com in the browser address bar
2. Do not access emails that ask you to log in to your Facebook account
3. Use some browsers or AVs that warn of Facebook Phishing such as: Chrome

Use Keylogging

Keylogging method is the easiest way to hack Facebook password. This method is sometimes so dangerous that even a person with good knowledge of computers can fall into the trap. A keylogger is basically a small spy program that, once installed on a victim's computer, records everything the victim does on their computer. This activity log is then sent back to the attacker by FTP or directly to the hacker's email address.

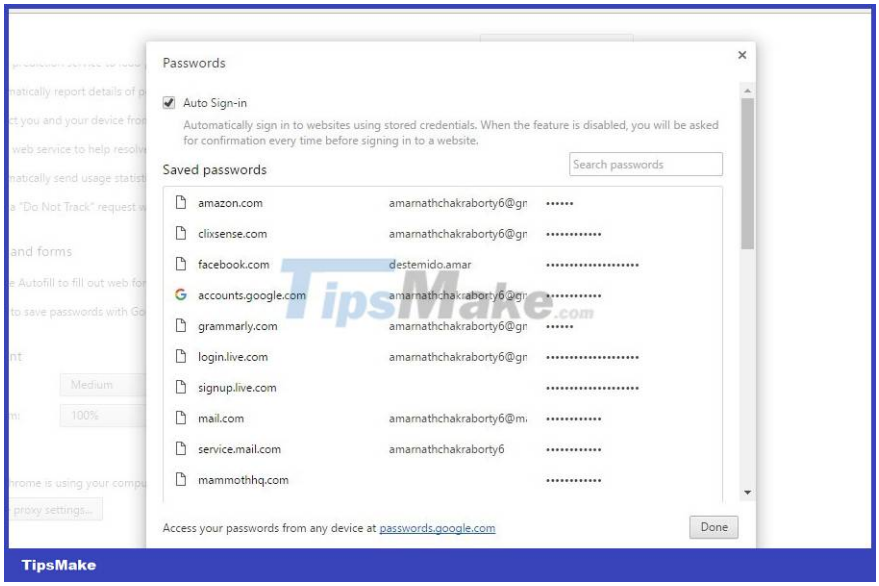
How to prevent Keylogging

1. Always download software from trustworthy websites
2. Scan your USB drive before use with good AV software
3. Having a good antivirus and internet security program will keep keyloggers at bay

Passwords are saved in the browser

Computer browsers often ask us to save our username and password when we log into any account in the browser. So anyone can hack your Facebook account from your browser's password manager

For example: chrome://settings/passwords you can find all the information saved on chrome



Prevention

1. Do not choose the function to save passwords in browsers on unfamiliar computers, and do not hand over computers with passwords saved in browsers to others.
2. Always use strong passwords and enable 2-layer security by phone and email or require verification of devices connected to your Facebook account.

Hack Facebook via email

Another common method that hackers use is to attack email accounts linked to Facebook accounts. After taking over the email account, the hacker will reset the Facebook password

Prevention

1. Use strong passwords for your email accounts
2. Enable 2-step authentication in your Gmail account
3. Never enter email accounts on strange or phishing websites

Attack via phone

Smartphones make it easy for millions of Facebook users to access their accounts using dedicated phone apps on Android or iOS. If the hacker can access the victim's cell phone, he can access their Facebook account. The simplest thing is that they will install popular tracking software such as Spy Phone Gold and Mobile Spy.

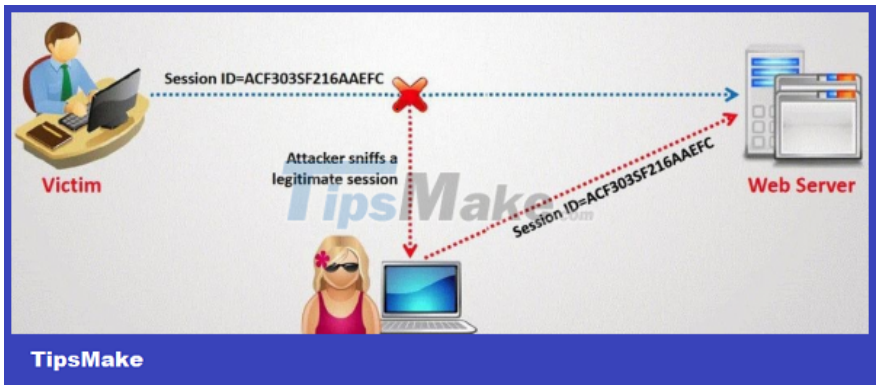
Prevention

1. Use a reliable antivirus and mobile security program for your mobile phone
2. Do not install applications from unknown sources
3. Uninstall suspicious applications on your device

5. Hack facebook account using Session Hijacking method

In computer science, session hijacking, sometimes also called a cookie attack, is the exploitation of a valid computer session — sometimes also called a session key — to gain unauthorized access to information or services within computer system. Session Hijacking, a common form of attack targeting social network users such as Facebook or Gmail mailboxes.

Session Hijacking is a form of attack on the session between the client and the server by stealing the user's cookies after they have passed the authentication step with the server, then taking control of this session. Session is a term that refers to a connection session between two computers on a network system, usually maintained by values ??such as session lifetime, browser cookie information or appropriate tokens. You can review the introduction to the session and the three-way handshake process in previous chapters.



If you are accessing Facebook over an (insecure) HTTP connection, session hijacking may occur. A hacker can steal a victim's browser cookies in a session hijacking attack, which are used to authenticate users on a website and access the victim's account. Session hijacking is widely used on LAN and Wi-Fi connections.

To prevent Session Hijacking attacks, we need to prevent eavesdropping. Once hackers cannot eavesdrop, they cannot attack the user's session. One of the solutions to avoid sniffers is to encrypt data and encrypt transmission lines with techniques such as using Secure Shell (SSH instead of regular Telnet) when administering remotely or applying Secure Socket Layer (SSL uses for communication over HTTPS).

In addition, we can prevent hackers from interacting with the transmission line, which also helps eliminate the risk of this attack, with effective solutions such as using a virtual private network (VPN), or applying IPSEC. Many opinions also say that when accessing the internet in public environments, using DCOM 3G devices also significantly reduces the risk of data loss.

Here are some recommendations to prevent Session Hijacking:

1. Use encryption.
2. Apply safety protocols.
3. Limit input connections.
4. Reduce remote access.
5. Has strong authentication mode.
6. Training for users, improving information security awareness.
7. Use different access credentials for different accounts.

Sidejacking using Firesheep

Sidejacking attacks were very popular in late 2010, however it is still widely used by many hackers using the Firesheep method. The Firesheep method is used when the hacker and the victim are on the same WiFi network. The sidejacking method is basically how a hacker hijacks an HTTP session, but it is more targeted at WiFi users.

Learn more about sidejacking

Situation: You go to a cafe, there is free wifi service, you eagerly connect to the network, access Facebook.com (FaceBook). After a few minutes, a status line appears on your wall written by you but not by you, saying 'This FaceBook account has been infiltrated by abcxyz'. You're scared, turn off your phone, then turn it back on and access Facebook again, but some mysterious person is still posting randomly in your identity. You are confident that your computer is safe because you have installed an antivirus program that updates continuously and never downloads dirty programs that can cause your device to get infected with trojans or keyloggers. Yet your Facebook Account is still being stolen right under your nose.

What happened to my Facebook account? How was it stolen so carelessly and so quickly?

Well, chances are you've been the victim of a Session Sidejacking attack.

Session Sidejacking is not a new type of attack, if not an old one, since HTTP version 1.1 was introduced with support for session cookies.

What is Session Sidejacking?

This is a type of attack belonging to the man-in-middle attack family, the purpose of which is to eavesdrop on the transmission between users and service servers using sniff tools and then steal important data related to the user's session. user, then restore this session on a third computer.

Session Sidejacking is especially effective and easy to implement when targeting sessions on the web environment. This attack direction in the web environment and HTTP protocol is mainly aimed at stealing session cookies

1. identify the user, thereby restoring the user's current session, and then the attacker will have more extensive attack measures to capture the user's account password

In short, easy to understand, to a certain extent, the attacker will easily take over users' Facebook, gmail, and yahoo accounts using HTTP Session Sidejacking.

This article mainly talks about HTTP Session Sidejacking attacks. That is, the form of Session Sidejacking attack targets stealing session cookies and restoring them as HTTP Session.

Special: The Session Sidejacking attack method in this article does not require a network card that supports Promiscuous mode (chaotic mode).

2. This is a step forward compared to automated attack tools like Firesheep, hamster & ferret, making session Sidejacking attacks easy to perform on all existing network cards. In other words, anyone can do it

Attack environment: a multi-user wifi network that you also have access to

Description of the attack process: As mentioned above, Session Sidejacking is an attack method belonging to the Man-in-middle attack family, it is essentially a combination of 3 different attack techniques including ARP Poison Routing, Network Sniffing, Cookie injection.

The attack process will take place through the following steps:

Step 1: Connect to the wifi network, if you do not have access, you must 'Crack' and find out the password to access the Wifi network (refer to Crack wifi technique with aircrack-ng)

Step 2: Perform ARP Poison Routing, this step helps you turn your computer into an impersonated router for the purpose of sniffing data transmitted throughout the wifi network. You should learn more about APR Poisoning attack to understand how this technique works and why it can be performed.

Step 3: Sniff all data in transit on the wifi network after this network has been subjected to ARP Poison Routing

Step 4: filter out data coming from specific users, for example a user whose IP is: 192.168.1.138

Step 5: reconstruct the TCP stream of the user's website session, and extract the user's cookie data

Step 6: Perform cookie injection, to insert cookie data into the attacker's browser

Step 7: Completely restore the user's web session on the attacker's computer

0. Session: Working session. To easily imagine what a session is like, imagine you are opening a new access to the facebook.com page using your computer's browser. Your browser opens a series of TCP/UDP connections to the web server of the website www.facebook.com, at which point your session has begun, because you have initiated a connection to the website www.facebook.com. facebook.com page. But this session has not been authenticated, meaning you have not logged in yet. The website www.facebook.com does not yet know who you are, and you cannot access your data on the website www.facebook.com. Then you log in with your username and password, now you are authenticated, FaceBook knows who you are, and you can access your personal data on FaceBook. The session will end when you close the browser,

1.Session cookies: Session cookies are small pieces of data, which can be files or records in the browser's database, responsible for storing some information related to the user's session on a page. web. From the above explanation of sessions it will be clear how the website www.facebook.com (or rather the web server of www.facebook.com) maintains that it knows who you are, after you have logged in. Enter with your username and password. That's right, http://www.facebook.com/ creates several session cookies on your computer, which store some information related to your username and some form of encrypted password (understand). this way for simplicity), along with some other miscellaneous information.

2. Promiscuous mode (promiscuous mode): Promiscuous mode is a special operating mode of the wireless network card. In this mode, the Wireless Card allows itself to receive all packets within its reach (its reception range), regardless of whether the packet is sent to it or not. In other words, the wireless network card is allowed to secretly read packets sent to other wireless cards on the network (very impolite). This mode has not been included by manufacturers in regular wireless network cards since 2005 because it is used for more bad purposes than good purposes (for example, cracking wifi network passwords). such as). Therefore, currently, in addition to buying a specialized wireless card that supports this feature, it is difficult for you to perform techniques related to Network Sniff and APR Poisoning. However, The difficult reveals the clever, many leading network experts (or extremely skilled hackers) have introduced the Pcap library. The Pcap library supports a number of advanced techniques such as Monitor mode - RFMon (Wireless card only), Port mirroring, Network taps., helping to perform Sniff and APR Poisoning tasks on network cards that do not support Supports Promiscuous mode

3. Sniff: Capture packets. This is a common task in analyzing network traffic flows. This sniffing task can be imagined as person A sending a letter to person B. On the way the letter is delivered from person A to person B, person C secretly copies the content of the letter and then continues to bring it to person B. Persons A and B did not know that the letter had been copied and read secretly.

Replace people A, B, C with computers A, B, C and letters with packets, 'on the mail route' with 'on the network', you will see that the example I give is actually very similar.

Prevention

1. Avoid cookie leaks over HTTP
2. Exit the website when you are done
3. Avoid opening WiFi networks
4. Use VPN

DNS spoofing

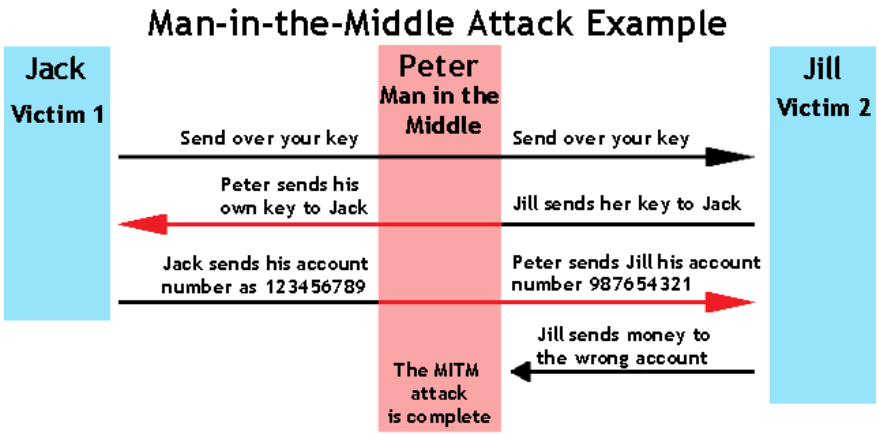
If the hacker penetrates the victim's network or both the victim and the hacker are on the same network. The DNS Spoofing method may be used by hackers to change the original Facebook page into a fake page, thereby accessing the victim's Facebook account.

Prevention

1. Configure the most secure DNS to prevent spoofing
2. Manage DNS servers with a protection system
3. Patch holes
4. Split DNS has access to each different server.

Attack in between

In cryptography and computer security, a man-in-the-middle attack, also known as Man-in-the-middle attack, is an attack in which the attacker secretly forwards and can do change communication between two parties who believe they are directly communicating with each other



If the victim and hacker are on the same LAN and on a switch-based network, the hacker can be between the client and the server or can act as the default gateway, thereby capturing all the information in between. .

The attacker must be able to intercept all relevant information traveling between the two victims and inject new information. This is simple in many cases; For example, an attacker within range of an unencrypted wireless (Wi-Fi) access point could insert himself as a "man-in-the-middle". .

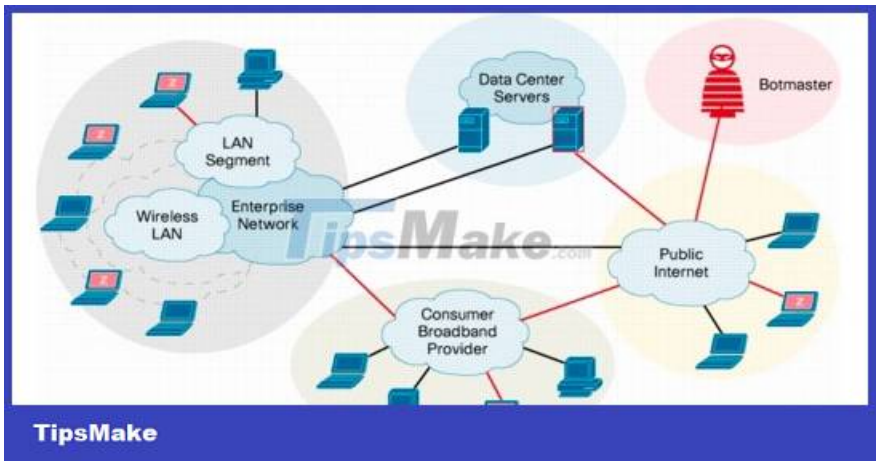
When an attack is intended to undermine mutual authentication or lack thereof, a man-in-the-middle attack can succeed only if the attacker can impersonate each endpoint to satisfy legitimate expectations from the other end. . Most encryption protocols include some form of special endpoint authentication to prevent MITM attacks. For example, TLS can authenticate one or both parties using a digital certificate provider trusted by both parties.

Prevention

1. Use a VPN service
2. Use Proxy server to access the internet
3. Use the best anti-virus software or firewall system

Botnets

Botnet is the term for a collection of software robots or bots that operate autonomously. The word is also used to refer to a network of computers using distributed computing software



Botnets are an uncommon method to hack Facebook accounts because this method takes a lot of effort and cost to build. Botnets are used to carry out more advanced attacks. A botnet is essentially a collection of compromised computers. The infection process is the same as keylogging, however, Botnets give you additional options to carry out attacks on compromised computers. Some of the most popular Botnets include Spyeye and Zeus.

Prevention

1. Always update all software on the system
2. Use strong passwords, keep secrets from sharing
3. Always keep the firewall on
4. Use USB drives with caution

Hack USB

Hackers just need to be able to insert a USB programmed with malicious code. From there, all information on the computer is stolen

Prevention

1. Plug only trusted USB devices into your computer
2. Scan USB for viruses
3. Do not buy old USB devices of unknown origin before plugging them into the computer

Social techniques

If you are using simple passwords like mobile number, date of birth, ID card number etc, then a hacker may not need to make any effort to guess the password and get into your account.

How to avoid: Never share your personal information via email, phone, or messenger chat

Hacking via Wifi network

Hackers can also hack your Wi-Fi router, if you use a weak password to set up your router's security. Hackers can hack your Wi-Fi network thereby hijacking all your internet traffic, which can allow hackers to attack and hijack your Facebook account.

Prevention

1. Do not use free Wi-Fi or public Wi-Fi
2. Change your Wi-Fi password regularly and with reasonable strength
3. If you are using public Wi-Fi, always use a VPN (virtual private network)

In addition to the above common methods, skilled hackers also use many more advanced methods to hack the entire Facebook system. They can steal Facebook account login tokens without worrying about passwords or other security methods. They can even steal the entire database of millions of Facebook users.

RIP Facebook account with FAQ, Check Point, Death notice, prisoner, sex,

FAQ is a method where bad guys use multiple accounts to report through the FAQ system, causing the victim's account to be temporarily or permanently locked. Check Point is a method for bad guys to report impersonation, inappropriate avatars.

How to fix

1. For Checkpoint or similar methods you should proceed carefully
2. This applies to both those who have submitted photos and those who have not.
3. It's best not to upload photos too quickly because it will easily be converted to FAQ form.
4. When you get caught in this situation, please go to the 2 links below to send information.
5. Link ending 890, please send a photo of your face along with your ID card (Remember to be clear, Full HD, not obscured)
6. If you have previously verified documents, please submit the correct documents.

You finished reading the article "**The most common ways that hackers use to hack your Facebook account**" edited by the **TipsMake** team. We hope this article has provided you with many useful tech tips and tricks. You can search for similar articles on tips and guides. Thank you for reading and for following us regularly.
