How do hackers attack your Facebok account and how to prevent this process?

Hackers can attack your Facebook account in many different ways, such as attacking email addresses, phishing .... To better understand how hackers attack your Facebook account and solutions to prevent this process, please refer to the following article of Network Administrator.

Facebook is one of the most popular social networking sites today with over 500 million users. Therefore, it is not controversial for hackers to attack users' Facebook accounts.

Hackers can attack your Facebook account through various ways, such as attacking the email address you use to create a Facebook account, Phishing . To better understand how hackers use to attack your Facebook account and solutions to prevent this process, please refer to the following article of Network Administrator.

If unfortunately your Facebook account has been hacked, you can consult some ways to get back your hacked Facebook account here.

1. Attack email address

All that a hacker needs is your name, then access the profile to find the email address you use to create your Facebook account and take steps to attack your Facbook account.

Regarding the password issue, if you create a weak password, then the hackers will easily guess the password or can answer the security questions to get your Facebook account password.

How to protect your email address safe?

To secure your email address, follow the steps below:

1. Hide your Email address with everyone by going to **Edit profile** => **Contact Information** => selecting the icon next to the email address => selecting **Only me** (only me) **.**

2. Change your primary email address with a different email address only you know by visiting **Account Settings** => **Email** => Change your primary email address with a new email address only you know and delete the email address first.

3. To increase security, on the **Account Settings** page, select **Secure browsing** and **Send me an email when a new computer or mobile device logs into this account** , then click **Save** .

2. Phishing

Phishing is one of the simplest ways to "trick" users into providing their login information.

All the hackers need to do is set up a website similar to designing the Facebook homepage, attaching the server sided script (server scripting language) to track the username (username) and login password. store in their 1 login. Send users the email saying that someone has tagged them in a certain photo on Facebook and sent the user a link containing phishing.

In some cases, some Facebook spam apps like apps tell you who viewed your Facebook profile . will automatically send links to phishing sites. This is a new trend that phishers use to "steal" user login information.

How to protect your Facebook account from Phishing?

All you need to do is' stay away from 'strange' links. In addition, before logging in, check the URL in the address bar.

Stay away from websites and blogs that require logging in through your Facebook account. Instead, log in only on the Facebook home page. During the search process, always use Safe Search (safe search).

3. Keylogging through Keylogger

Keylogger is a type of virus, a computer program originally written to monitor and record all actions taken on the keyboard into a log file (log) to let the installer use it.

How to prevent keylogger?

To prevent keyloggers, it is best to install an "effective" antivirus program on your computer and update it regularly. Never click on any "strange" link and avoid downloading unknown software to your device and installing it.

Also avoid installing free toolbar and other spam software. Always "scan" the USB drive and Pendrive before plugging in the computer to use.

4. Social Egineering

Social Engineering is a non-technical method of breaking into a company network or network. It is the process of deceiving users of the system, or convincing them to provide information that can help us defeat the security department.

Social Egineering involves using any trick to trick users into being vulnerable. This involves sending fake emails from Facebook, informing you that to change your password to 12345678 you will have to answer security questions .

How to prevent Social Engineering?

Using the best and most difficult security questions is never to reveal an answer to anyone. In addition, one thing that you need to keep in mind is that Facebook or any other company will never ask you to change your login password to a password string 12345678 or similar passwords . Therefore Always think carefully before making any requests from Facebook.

Refer to some of the following articles:

1. Instructions for setting up auto reply to messages on Facebook Fanpage

1. How to know if someone has read your message on Facebook Message?

1. How to identify an unauthorized login IP address of your Facebook account

Wish you have moments of fun!