What is cybercrime? How to prevent cybercrime?

We live in an era of Internet globalization. The Internet invades every corner of the street, is present in every living room and appears in every breath of life. In addition to the obvious benefits, as well as the enormous positive role in the overall development of all humanity, the global internet is becoming a 'fertile ground' for all kinds of criminals to thrive. flourish with incalculable harm.

We are living in an era of internet globalization. The Internet invades every corner of the street, is present in every living room and appears in every breath of life. In addition to the obvious benefits, as well as the enormous positive role in the overall development of all humanity, the global internet is becoming a 'fertile ground' for all kinds of criminals to thrive. flourish with incalculable harm. According to the report of the International Criminal Police Organization, criminals using high technology (cybercrime) ranked second in the most dangerous crimes today, that is, only after the crime of terrorism. Statistics show that 90% of traditional criminals have moved to the network environment or used high-tech equipment. So what are cybercriminals really like? What to do to prevent cybercrime? We will find out later.

1. The world lost $ 400 billion every year for cybercrime

Cybercrime

1. Definition of cybercrime
2. Classification of cybercrime
3. Prevent cybercrime

Definition of cybercrime

Cybercrime can be defined as any criminal activity involving any networked device (computer, smartphone, etc.) or the network itself. In the concept of cybercrime, a computer device can both be the target of a criminal, but

can also be used as a tool to commit a criminal offense.

According to the provisions of the Criminal Code (Penal Code) of the Socialist Republic of Vietnam, cybercrime is the act of using cyberspace, information technology or electronic means to conduct acts guilty.

From there it can be seen that, by taking advantage or using computer technology in the wrong direction, cybercriminals will access sensitive personal data of users (payment card data, login information, etc.), trade secrets of companies, government agencies, valuable information . or use the internet for any other malicious purpose. Cyber ??criminals often use malicious code (malware) and various tricks to exploit security holes and cause damage to the subject. Behaviors that constitute the definition of cybercrime can include network attacks, cyber terrorism, cyber espionage, cybercrime; causing problems, attacks, intrusion, hijacking, distorting, interrupting, stalling, paralyzing or damaging important national security information systems.

1. The provisions of the Criminal Code relate to the field of information technology and telecommunications networks

Classification of cybercrime

First, it must be affirmed that the common point of all cyber criminals is that they are computer experts, network security masters, but use their knowledge to serve bad intentions. However, cybercrime can also be categorized into many different forms, depending on the area of ??activity as well as how to commit the offense. If you understand how each type of cyber crime works, it will be easier for us to respond to and provide remote security methods, to ensure maximum security for the information system we are managing. physical. It is possible to classify cybercriminals into some main types as follows:

Identity **theft:** English also known as Identity Theft, is a term used to describe cybercrime using a method of impersonating another person, to create fraud in financial interests. More specifically, when hackers access a person's personal information and then use the same information to steal identity or access the victim's bank account . it is called onion. Identity theft.

In addition, in identity theft, hackers also often make sales or purchase transactions related to the victim's identity on the dark web. These data may include financial data, health-related data, social security, addresses, phone numbers, etc., in short, personal information that can later be used for fraudulent activities. The most common source for stealing other people's identity information is the data from the websites of businesses, organizations, service providers, or it can also be data from personal websites themselves.

1. The 4 true stories show how scary identity theft can be

Credit card fraud: A form of fraudulent use of high technology to steal credit card information of users in the financial and banking sectors. More specifically, when hackers make attacks on system retailers, POS terminals, or even banks and steal credit card data (Visa, MasterCad, ATM . or information) Bank information) of customers is considered credit card fraud. The stolen credit card data can then be sold by crooks on the dark web, or can even be used to steal money directly from the accounts of the people involved. For years, credit card fraud is one of the most common forms of cybercrime.

Cryptojacking: This is a relatively new form of cyber crime that appears and goes hand in hand with the development and development of the electronic money market. Cryptojacking is a term that refers to the way cyber criminals use to make money with your hardware. By using scripts, hackers can exploit electronic money through browser platforms. When the victim opens a website in his browser, cryptojacking malware can use the CPU to the maximum for cryptocurrency. To do so, hackers will first hack a system to install electronic money mining software, then they will use JavaScript code to conduct electronic money mining in the browser. In other

words, crooks will run an electronic money digging software on your hardware without your own permission. These attackers take electronic money and sell it to make a profit, but you will encounter problems when using the CPU at a high level.

1. Detecting new electronic phishing malware, redirecting payment transactions to attackers

Cyberextortion: A cyber attack combined with the need for money - that is the most closely defined definition of cyberextortion. However, there are many different methods to perform a cyberextortion case. A typical ransomware attack is also considered cyberextortion. An act in which hackers blackmail victims by threatening to publish their own private videos on social networks or pornographic sites is also defined as cyberextortion. In addition, hackers can also use DDoS attacks to blackmail businesses, as well as threaten the release of commercial documents or important data (such as contract terms, unregistered patents). , or unreleased TV episodes, etc.) are also considered a case of cyberextortion.

1. New ransomware appeared not to send Bitcoin, money, but . nude photos !!!

Ransomware **:** Ransomware is a term used to name the type of malware that encrypts all data in a computer system or network, and then issues a ransom request to decoding data. Ransomware attacks are becoming one of the most popular forms of cybercrime today, targeting both casual and corporate users. Typical recent ransomware attacks include Shamoon 2.0, StoneDrill, or WannaCry.

Cyber ??Espionage: A criminal-colored attack on a government organization's network, or defense-related and gaining access to sensitive, secret data Serious nature, affecting national security is a typical example of cyber espionage. Those involved in cyber espionage are able to change or destroy sensitive data that they access by hacking. Besides, they can even use internet-connected devices, such as cameras, webcams, IoT devices . to serve as spy tools (gathering information) and related activities.

Cyberstalking: When an individual, organization, or business is harassed or harassed in many ways through the internet, they are more likely to be victims of network surveillance. More specifically, cyberstalking is a form of cyber crime that involves sneaking surveillance on someone's activity in reality or while they are online on computers as well as internet-connected devices. With a few more complex techniques, even hackers can track users even when they're offline.

A common example of cyberstalking that you may have been a victim is the case of online advertising tools that illegally access the recording or monitoring device on your computer or smartphone to save all key presses, moving locations as well as personal habits to serve the purpose of advertising promotion.

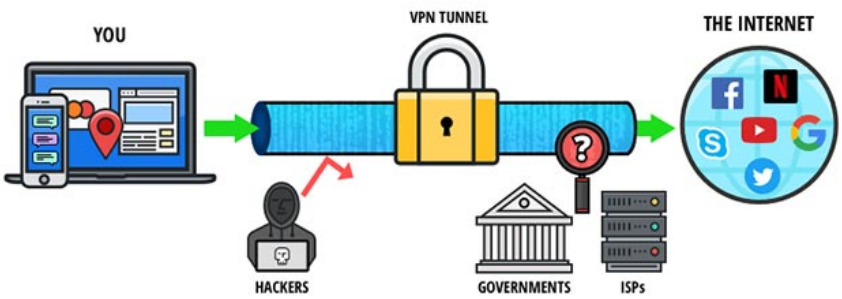
1. 5 ways to check who is following you online

Prevent cybercrime

There are some basic methods that can help prevent cybercrime at both micro and macro levels, many of which include:

Using security software: Always use any reputable and relevant security software to keep your computer, network and data secure, this is a prerequisite for operations. security as well as network security in general. Choosing the right security software will depend on the nature of the data, the importance and nature of the job / task you are doing. In general, you should start by deploying an antivirus program, and then select the endpoint security tools that are appropriate for your system.

Use encryption or VPN: Setting up encryption or using VPN (Virtual Private Network) can help secure your communications and data quite effectively in many different situations. Encryption is beneficial in that it causes hackers to only compromise encrypted data, even if they successfully hacked your communication line. Similarly, it is best to use VPN while connecting your devices to the Internet via public Wi-Fi networks.



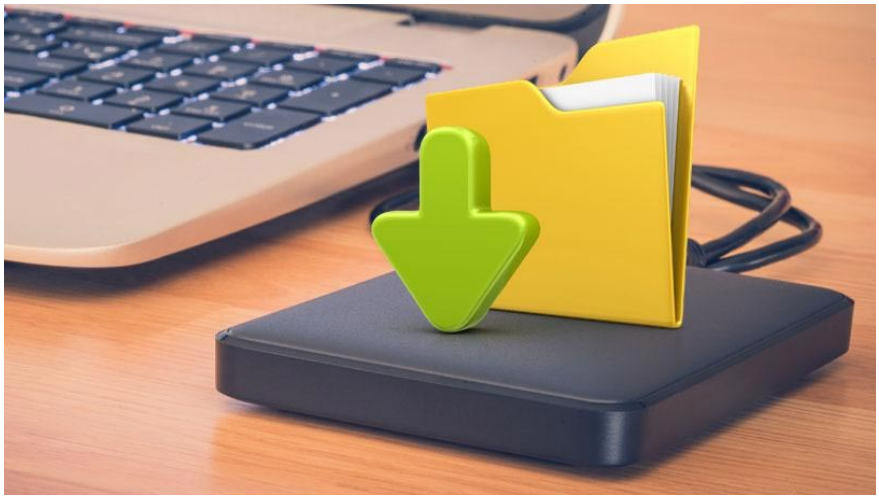
1. If using an Android phone, be careful: You may be being tracked without knowing

Focus on password management: Effective password management helps to prevent and limit cybercrime acts at the macro level. Always use strong passwords (ideally, use a combination of uppercase and lowercase letters, numbers and special characters. Besides, make sure that the password you use for accounts and services If you are concerned about not being able to remember all your passwords or schedule them effectively, you can use more security management tools. password

Regular software updates: Keep the software, applications on the system and above all, your operating system updated to the new version is one of the leading factors in system security. Never forget to update on time, delays can lead to cybercriminals finding vulnerabilities, thereby exploiting attacks. If you are confused about this, the automatic update of the operating system as well as the application will be a reasonable option.

1. Windows 10 update continuously, why?

Deploying backup operations: A requirement is also important, to always back up all the data you have on your computer as well as your network. This must especially be applied to important data and is a prerequisite task in all organizations and businesses. Also, remember to update your backups periodically.



Follow the best security practices: Absolutely no excess when you follow best practices for security practices, including being cautious with email and phishing links, keeping safe BYOD devices as well as IoT devices, ensuring physical security for your system / device by locking them when not in use, or just connecting secure USB devices, etc.

Improve knowledge of cyber security: Constantly learning, updating new knowledge about information security as well as network security because as you know, cyber crime situation changes day by day and tends to be complicated. more trash. If you are a business owner, or encourage or organize classes to improve information security for your employees.

1. What can organizations do to protect themselves from cyber attacks?

According to security experts, when you grasp the characteristics of cybercrime, it means you are holding up to 50% of the advantage in dealing with them, the rest will depend on specialized measures. the subject you are holding.

Wish you build your own great security system!

You finished reading the article "**What is cybercrime? How to prevent cybercrime?**" 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.
