Things you need to pay attention to computers at the office

Currently many companies provide computers or smartphone devices for employees to serve daily tasks. And to be able to secure your personal information and safety for your company, you should pay attention to the following.

There are many companies that provide adequate equipment for computers or smartphones for employees. Or even those computers have preinstalled programs and applications for work. And according to the habit, we will proceed to log in personal accounts like Facebook to check messages, login Instagram account, .

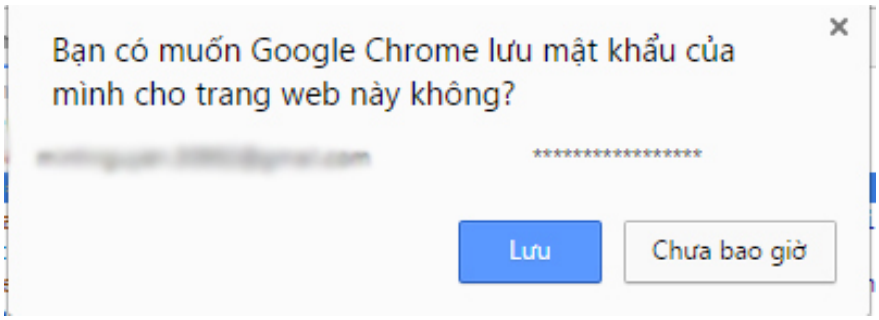
However, many cyber security experts have warned that employees who store personal information with work on the same computer, can pose a commercial risk to both you and the company. In addition to avoiding access to malicious websites, links containing viruses, you should also pay attention to some of the rules that should not be stored in the computer at the office below.

1. Do not save passwords at office computers:

It's not too much to say that the time you use your computer at the company is much more than your personal computer device. And it is easy to understand when you save your login password for websites or personal accounts in certain folders on your computer, or automatically click save account when logging in on the browser.

Quite a few companies have policies to check computer data, email and Internet of employees and maybe, every personal account password is not as safe as you think. Every website you visit through the Internet, equipment is under the management of the company and they have the right to inspect and monitor our access, including onsite or offsite.

It's best to remember the passwords for each website or save them in your personal book, if you don't remember them. In addition, the web browser will also automatically suggest saving login information. And if you accidentally click OK, the account and password are saved. The best way is to disable this suggestion. Please refer to how to proceed in the Guide to turn off the proposal to save passwords on the Web browser.



2. Attention to speech when group chat:

Usually for easy exchange within the group, companies will proceed to install the software. And while talking to colleagues you need to control all the words in the group, even jokes because it will make others uncomfortable. All messages in group chat can be retained on the server (server) and will be restored as email.

3. No public WiFi connection on company computers:

Maybe on the weekend you bring your company home to work and then go to a coffee shop, for example. Of course you will connect to free WiFi at that cafe to surf the Internet, go to Facebook or even send job data.

However, the use of public WiFi such as bookstores, restaurants, and airports can bring risks to users, especially the loss of accounts or disclosure of "confidential" corporate documents. . We can log into fake network lines that are disguised as real, so bad guys can easily steal any information for some bad purpose.

4. Limited access to remote computers:

In order to assist users to connect with each other remotely, especially in support issues on computers, remote control software like TeamViewer helps a lot. With these software, anyone can access your computer anywhere.

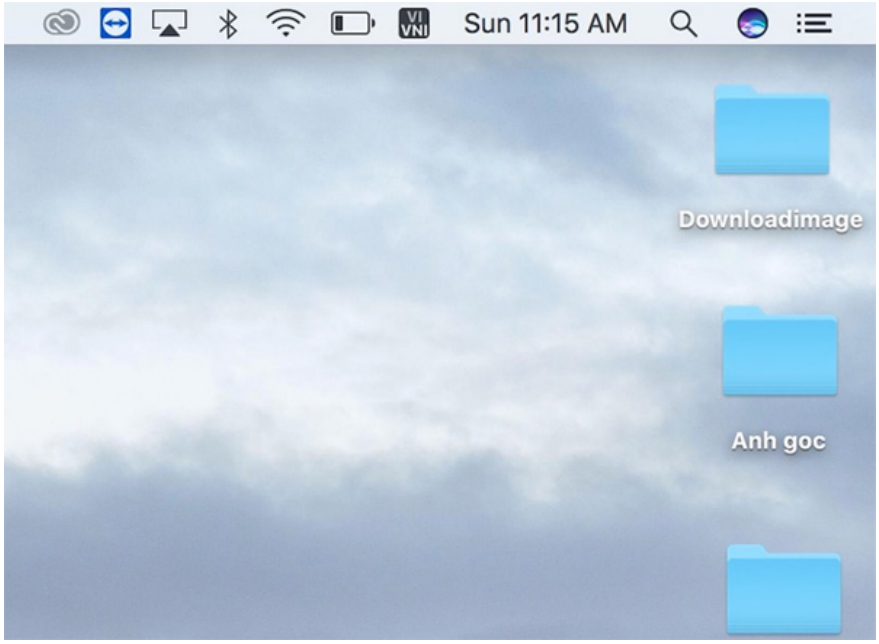
But remember, when we want to give anyone access to a computer outside the office, we need permission from our superiors. Especially for those who have no expertise in IT, it is even more impossible. Every device on the

company is not your personal property, so we are not allowed to let anyone access the remote computer without consent.

5. Say no to storing personal data:

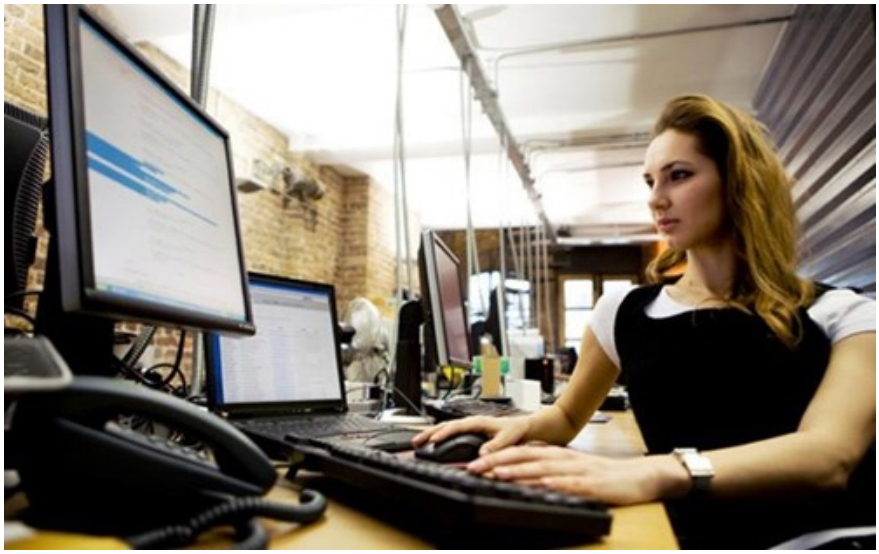
In addition to the work-related content that you store on your computer, we can create multiple folders with personal information such as favorite songs, photos of yourself or friends, .

However, we should change this habit now. In case you no longer work at the company or take a long time off, the personal data will accidentally be exposed.



6. Do not use company computers for additional jobs:

As mentioned, all the work you do on the device will be observed remotely and if, you use it for extra work, you need to be careful. This can have big, unnecessary consequences and we are forced to explain to management or human resources. It's best to use the company's equipment to serve the company's work only.



The above are some of the notes when we work with a company computer. Remember, computers are property of the company and the company has the right to regulate everything you do on this computer. Absolutely do not allow anyone to access your computer remotely, without the consent of management. All information or personal data is best recorded in the personal book to avoid unfortunate circumstances.

Hope the above article is useful to you!

You finished reading the article "**Things you need to pay attention to computers at the office**" 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.