What is Deafing Credential?

The following article will explain how credential dumping works and how to protect yourself from this attack.

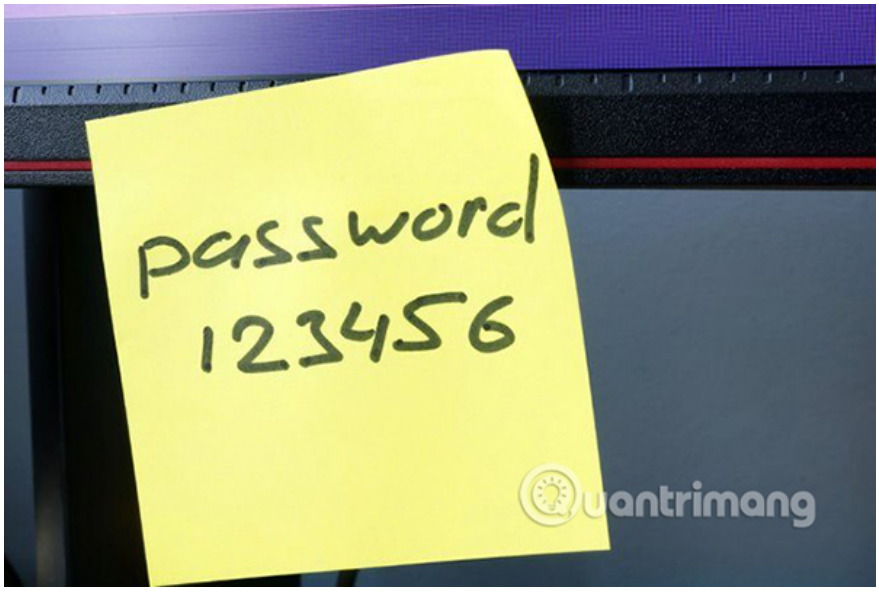
It is bad enough for hackers to hack into one of your accounts or steal your login information. But sometimes, hackers can use a stolen password to steal many other passwords. If your computer is on a network, they can also take advantage of this to steal passwords of other users.

This is done by hackers using a credential dumping technique. The following article will explain how credential dumping works and how to protect yourself from this attack.

Learn about Credential Dumping and how to protect yourself with 4 simple tips

1. What is Credential dumping?
2. How does Credential dumping affect you?
3. How do I protect myself from credential dumping?
    1. 1. Do not save the password on the computer
    2. 2. Use the online password manager
    3. 3. Activate Microsoft Defender
    4. 4. Use two-factor authentication

What is Credential dumping?



Recently, security researchers talked about the danger of credential dumping. This is a technique used by hackers to access multiple accounts from one user.

Credential dumping starts when hackers access a victim's computer. From this computer, they can extract usernames and passwords for many other accounts. This information may include login information for bank accounts, email accounts or login details for other machines or networks.

This can help hackers easily steal someone's identity and hijack all their accounts. Hackers can also use this technique to retrieve login information for other users on the network, spreading vulnerabilities from a single machine to the entire system.

How does Credential dumping affect you?

It is possible that hackers have gained access to multiple passwords when they enter a computer, due to the way the operating system handles passwords. Your operating system does not want to bother you by asking for a password at all times, so once you have entered the password, it will be saved in the computer memory for later use.

If hackers can access a file called **Security Account Manager** , they can see a list of passwords stored on that computer. The password is hashed, meaning that each character is converted to another icon to hide. This is the same process used for passwords on secure websites. But if the hash is not strong enough, each stored password can be broken. After that, the hacker will have access to all the different accounts of that user.

If another user has logged in on the same machine, hackers can also find their password. If business users have problems, they can call IT support, ask the network administrator to come and check their computers. When network administrators log on to the compromised machine, hackers can also steal the administrator's login information and cause additional damage.

How do I protect myself from credential dumping?

You can see the threat caused by the credential dumping. But there are a few simple steps you can take to protect yourself and your device from this technique:

1. Do not save the password on the computer

A bad habit that many people make is to store all the passwords in an unencrypted text file on the hard drive. They know that not using the same password for many websites and passwords must be very difficult to guess. So they use random passwords. But remembering them all is an impossible task, so they write them into a file and save them on the computer.

The reason why this becomes a problem is that if an attacker accesses that text file, they will have access to all your passwords on every web page. This is a big security risk and makes the credential dumping attack very easy, so you should pay special attention to this issue.

2. Use the online password manager

So if you should not store passwords on your computer, what should you do with them? It is best to use a reliable online password manager like LastPass or 1Password.

The online password manager works by storing your login information online. This data is encrypted before uploading to the Internet, so you can access your password from any device. This has the advantage of protecting you from credential dumping. But it can also be a disadvantage. If someone finds the password manager password that you use, they can access all your accounts.

In fact, the online password manager is an option considered by many to be the best security measure. But you need to be very careful with your main password and make sure you never write it out anywhere, both on your computer or on paper. This is the password you really need to remember.

3. Activate Microsoft Defender

If you are a Windows user, you must make sure Microsoft Defender, a Microsoft antivirus solution, is activated. There is also a version of Microsoft Defender for Mac.

Microsoft said that Defender will protect users against credential dumping by protecting the lsass.exe process, the goal of many credential dumping attacks. When you activate Defender, it will automatically run in the

background to protect your computer.

Defender is enabled by default on Windows computers. To check, go to **Settings** in Windows, then go to **Update & Security** . Select **Windows Security** from the left menu. Now click on the **Open Windows Defender Security Center option** . Here, check if **Virus & threat protection** and **Account protection** are enabled.

4. Use two-factor authentication

One of the best ways to protect yourself from password theft is to use two-factor authentication, whenever possible. This means that when logging in to a website, you must first enter your username and password. Then, if the password is correct, you must enter a second authentication information.

Normally, you will enter the code generated by the application on the phone. Alternatively, you can enter the code sent to your phone via SMS.

The idea is that even if an attacker knows the password, they don't have access to your phone or email. The only way to access your account is when you have both your password and access to your device.

The annoying thing about two-factor authentication is that you have to activate it individually on every site you use. But you should definitely enable two-factor authentication on your most essential websites, such as email accounts, online banking, PayPal or other payment services.

Credential dumping is a technique used by hackers to steal passwords for multiple accounts, when they have access to a computer. It may happen due to the way the operating system stores passwords.

You can protect yourself from this threat by using the password manager, enabling Microsoft Defender and using the two-factor authentication feature.

To learn more about how passwords can be compromised, see the article summarizing **TipsMake.com** 's current popular network attacks **.**