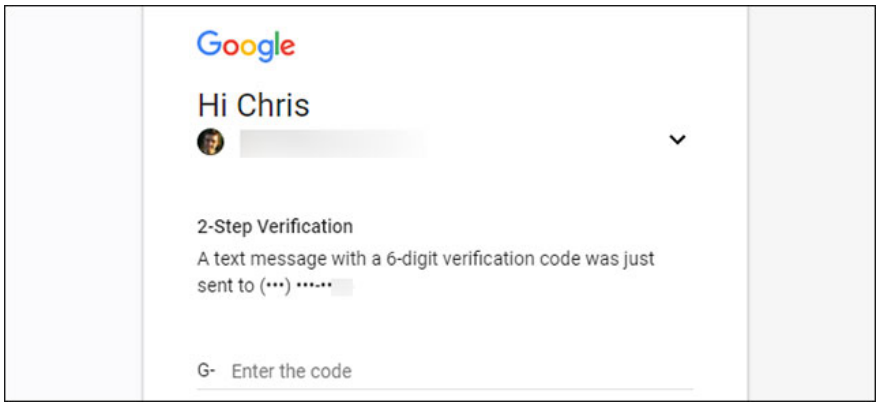
Why shouldn't SMS be used to authenticate two factors and what are alternatives?

Security experts always suggest using two-factor authentication to secure users' online accounts. Many default services are authenticated by SMS, but is this really a safe choice?

With two-factor authentication via SMS, a code will be sent to the recipient's phone and you will use it to continue logging in. But in fact, SMS has many security issues and is a less secure option when it comes to two-factor authentication. Although it should be clarified, this is still safer than not using two-factor authentication.

When not using this method, the attacker only needs a password to log in to your account. When authenticating by SMS, someone will need both a password and a code sent in the message. Of course, SMS is still safer than not needed at all. If that's the only option, just use SMS. However, you should know why experts recommend against using SMS when you have other options, and the alternatives they suggest.



Many services require two-factor authentication to ensure safety

Changing the sim will help the attacker get your phone number

This is the way to authenticate by SMS: When you log in, you will receive a text message to the phone number previously provided. You enter the code in the message and log in. It sounds very safe. But is it only you who can get that phone number and can you see that code on your phone alone? The answer is no.

If someone knows your phone number or personal information such as the last 4 digits of the phone number you use to secure your society, it will be easy to find by companies, the government will leak data In addition, they can contact the phone company and change the number. This is called changing sim (SIM swap), similar to when you buy a new phone and change the phone number to it. The attacker assumes that you will provide some

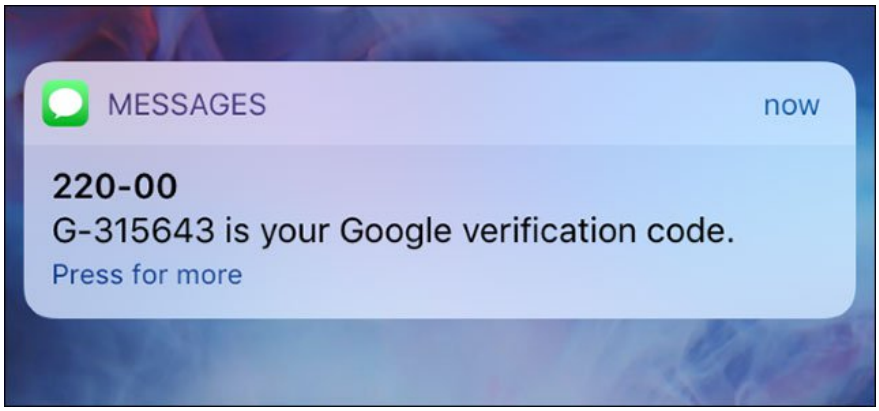
personal information, the phone company will reset their phone with your number, so they will get the code sent to that phone number.

In the UK there have been reports of such a situation when an attacker steals the user's phone number and accesses their bank account. New York also warned of this form of phishing. At the core, this is a form of phishing attack by tricking the phone company.

SMS messages can be interfered in many ways

It is possible to steal SMS messages. Politicians and journalists in harsh countries all want to be careful because the government can read SMS messages. This happened in Iran when the hackers said they had hacked into their Telegram account via SMS.

Attackers take advantage of the problem at SS7, roaming connection system, to read SMS messages anywhere. There are many other ways that SMS messages may leak, including using fake radio stations, SMS messages are not designed for security, so they cannot trust them completely.



SMS messages are sent to the phone for authentication

In other words a skilled hacker and a bit of information can hack your phone, access online accounts. That is why the US National Institute of Standards and Technology no longer encourages the use of SMS to authenticate two factors.

Alternatives: create code snippets on your device

When the method to authenticate two non-SMS-based elements is safer because phone companies can't let anyone else get that code. Popular options are now applications like **Google Authenticator** or **Authy** with similar features.

These applications will create code snippets right on your phone. Even if the attacker has transferred your phone number to their phone, they cannot get the code. The data needed to create this code will only be available on your phone. Users do not even need to use these codes because Twitter, Google and Microsoft also check the two-factor authentication method using the application and allow logging on the device by logging in to the application on the phone. .

There are also token devices. Big companies like Google and Dropbox have used the new standard for two-factor authentication tokens named U2F. They are more secure than relying on outdated mobile companies or phone networks.

A device token authenticates two elements

If you are required to use SMS, you can create a Google Voice number and send it to a service that requires SMS authentication. Then log in to your Google account and view messages on the Google Voice website or application. Note that Google Voice does not support in Vietnam but if you are in another country, you can use it.

You finished reading the article "**Why shouldn't SMS be used to authenticate two factors and what are alternatives?**" 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.