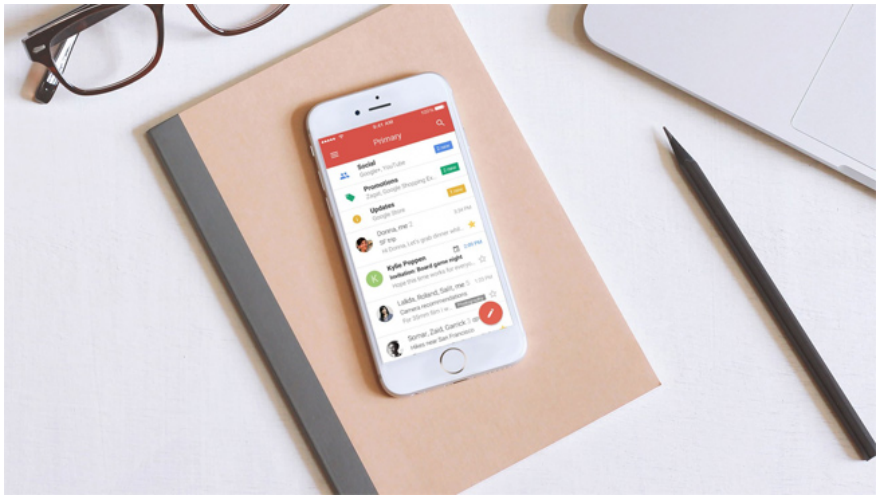
Some security methods for online services

Online accounts such as Facebook, email, Messenger, etc. all now become targets for account steals, as they can quickly steal your personal data in just a few minutes. sleepy So how to keep safe when online?

Online accounts that are used every day have always become fat items for hackers to attack and steal accounts. Whether users implement a 2-layer security method with phone numbers, such as Facebook, email, iCloud, . hackers are still capable through your phone number to steal data. So how can I keep those accounts safe and prevent the loss of personal data for online services? Join the Network Administrator to consult some ways to secure online services in the article below.

1. Do not share the phone, the email is rampant:

Today's social network becomes the spiritual food of many people but also has potential risks. You will encounter problems such as account hacking and easy hack. In case when we have shared an email address or phone number, it is even more dangerous. In addition to being constantly spammed, spam mail, someone can look up all the relevant information via phone number when searching on Google.



They can know their habits, interests, history on social networking sites, . so that they can affect your reputation. The best way is to not share the rampant phone numbers on social networking sites. Or if you've accidentally shared it, please delete it or ask the help of the website owner to help you do this.

2. Absolute security of credit cards:

Losing a credit card not only costs you money, but can also become a tool for bad guys to do illegal things. In addition to giving credit card information when you make online purchases for trustworthy websites, do not disclose any card information, especially credit card numbers.

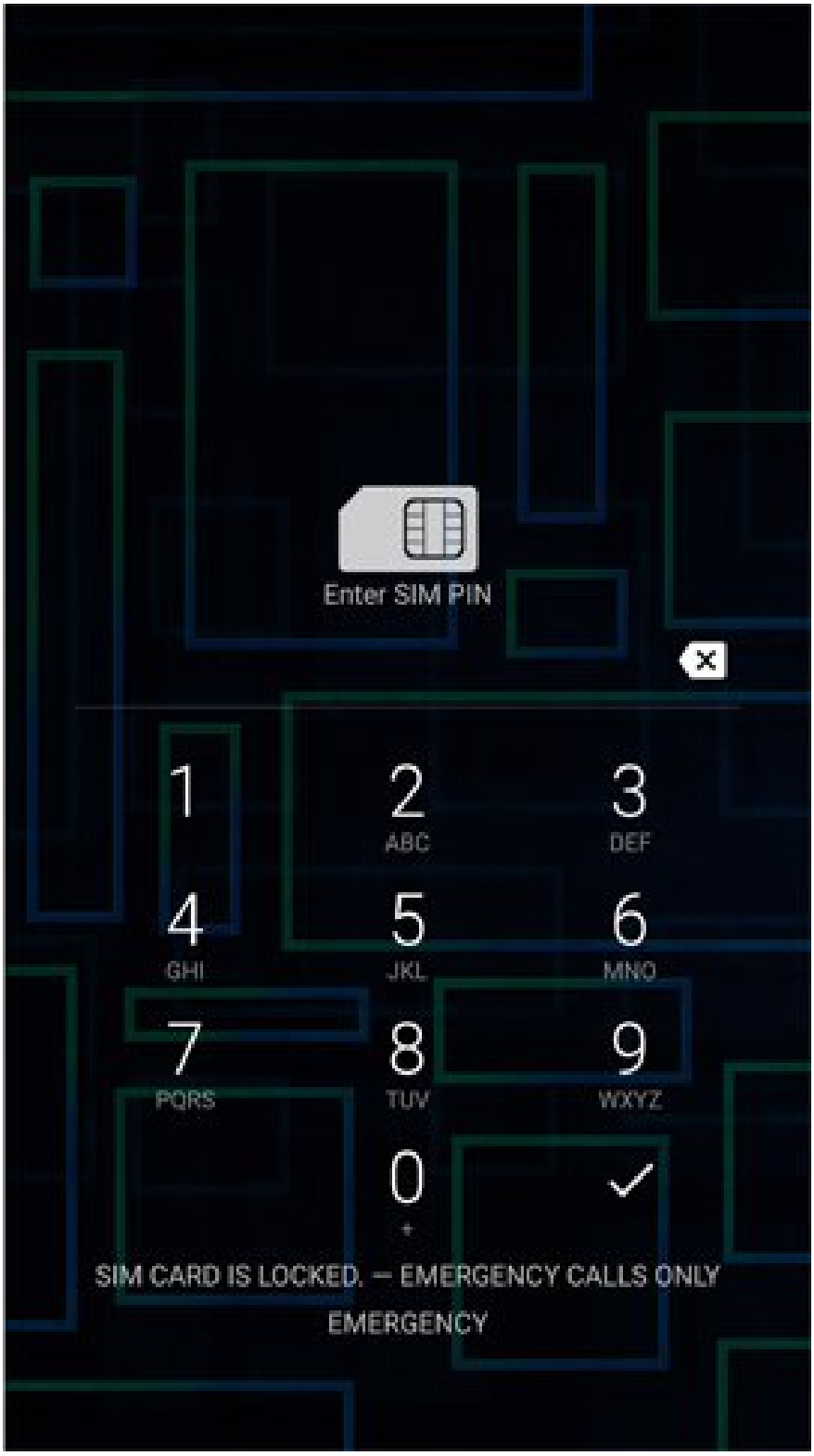
3. Proceed to setting up PIN code for SIM:

As mentioned, many people now choose to use their phone number to secure their accounts. However, your online account can still be lost if the phone is lost, when the thief can insert the SIM into another device to get the phone number.

To prevent all unauthorized actions from SIM phones, the best way is to set up a SIM PIN code. Whenever someone installs a SIM card to a new phone, it is required to enter the correct PIN code with 3 digits. If not entered correctly, the SIM will be locked and we can prevent the bad guys from knowing the phone number.

For detailed instructions on how to set a SIM PIN code, read the article How to set up a PIN for your phone SIM.

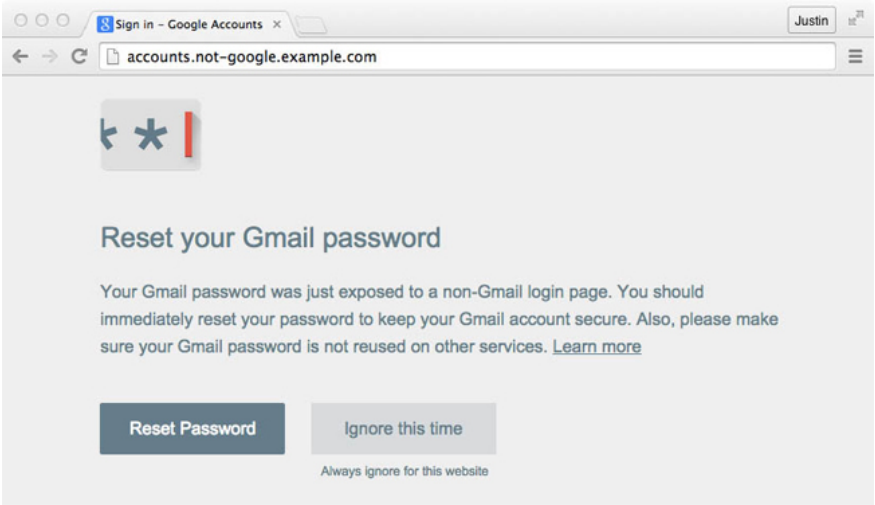

SIM bị Khóa
08:05
Nhập PIN
Còn lại 3 lần
1
2 ABC
3 DEF
4 GHI
5 JKL
6 MNO
7 PQRS
8 TUV
9 WXYZ
0
Hủy



4. Check website carefully when entering password:

Passwords are considered to be the most basic way for us to secure online accounts. Therefore, be careful when sharing passwords through any means such as email, messages, SMS.

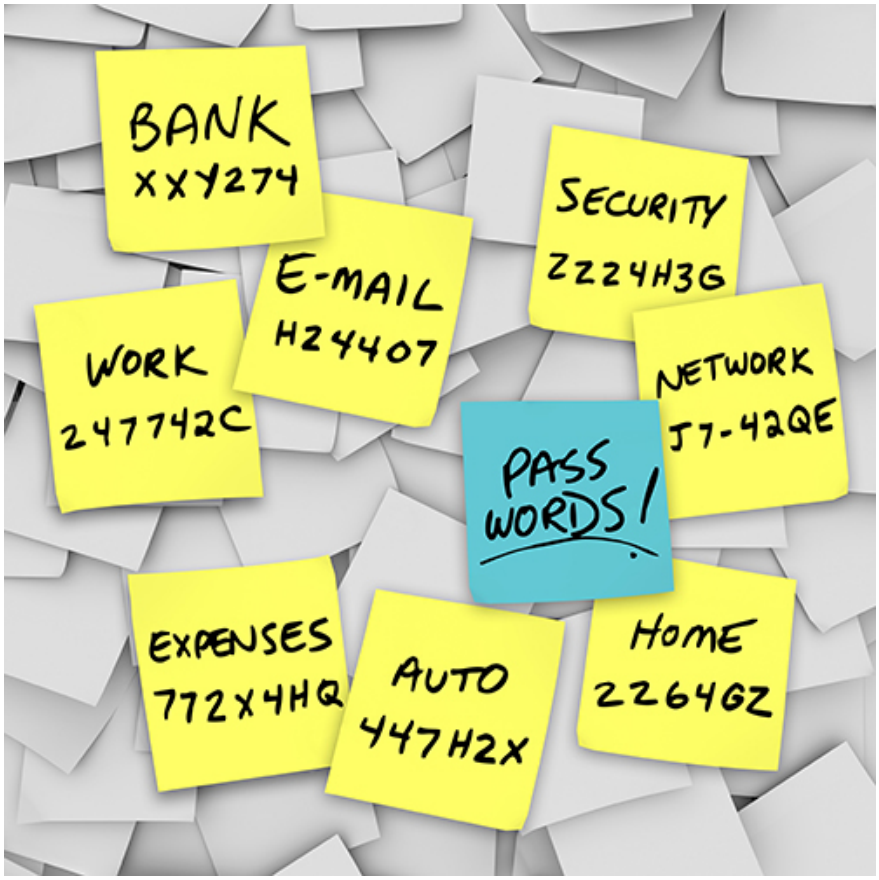
If the user is not careful, thoroughly checking that you have entered the password quickly, you will probably lose your account quickly. For example, with phishing SMS like "We detect harmful transactions, enter the password to cancel the transaction". In addition, there are now many cases of disguising the original and standard domain names, thereby stealing the user's password. Therefore, you should thoroughly check the domain name before proceeding to enter the account password.



5. Use different passwords for online accounts:

Typically, users will tend to set a password for all online accounts that are owned. This makes it easier for you to remember your account passwords, not having to worry about losing your account when you accidentally forget your password.

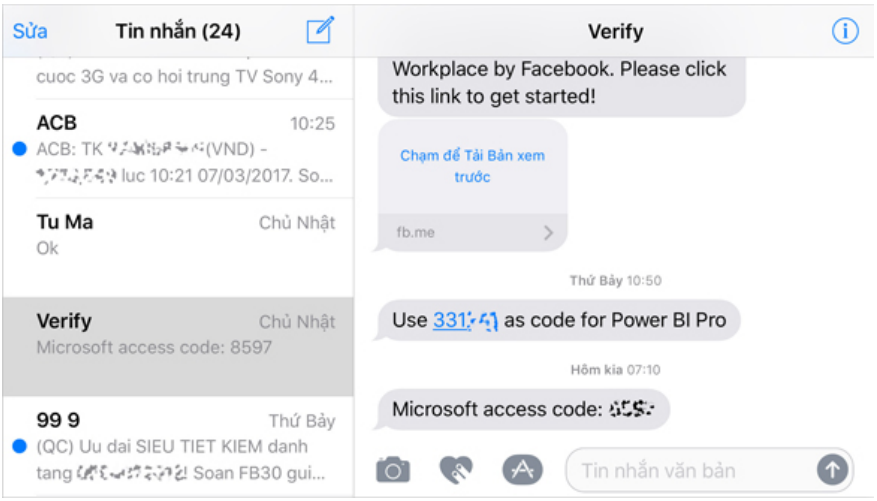
However, it is also because of that convenience that hackers can easily control accounts, as they can detect passwords of other accounts. So how to solve this problem, when you can not set each account a separate password?



It is best to classify the accounts you own. Important email accounts, account registration, exchange with customers or colleagues, you should put together a pass. Bank withdrawal accounts choose 1 password and other emails choose another password.

6. Be wary of OTP phone numbers:

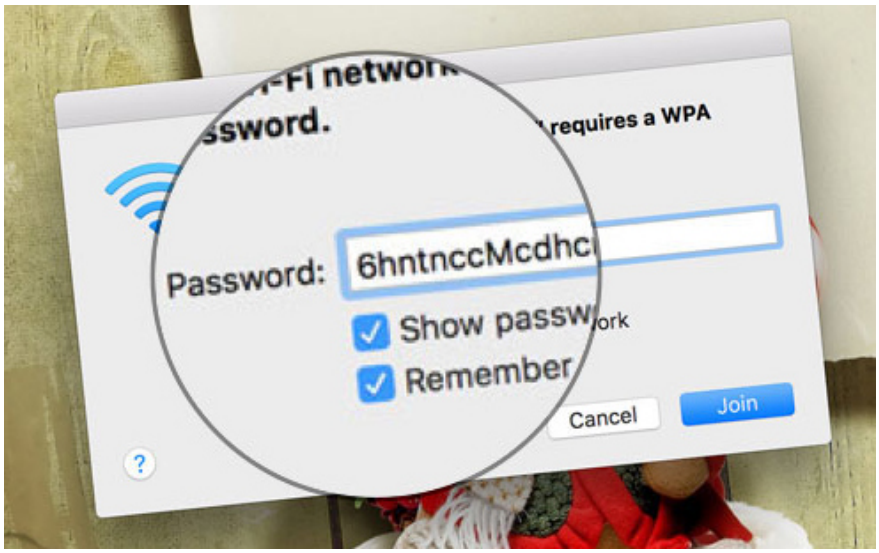
OTP is the authentication code sent to your phone number and the user is required to enter that code to use the account. However, there will be many cases where you receive a code reset message, in the form of a personal number of 10 to 11 digits, it is definitely a fake form, completely different from the 4 to 6 digital switchboard. Ideally, when you receive a message, you should contact the service company to check all received messages.



7. Using difficult to guess password ranges:

Currently most websites that create accounts will encourage or even require users to set passwords including lowercase, uppercase and number, even with special characters. So you should consider when setting a password with unpredictable characters, to partly limit the loss of passwords. But don't be too troublesome because you probably won't remember them.

Also avoid setting passwords related to birthdays and house numbers, etc. Because hackers will rely on it to guess the password. Regularly changing passwords is also a safe way for our account.



Hope the above article is useful to you!

You finished reading the article "**Some security methods for online services**" 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.