Microsoft shows how to avoid trapping phishing

Microsoft has issued a warning and recommended ways to protect users of e-mail services ...

Microsoft has issued a warning and recommended ways to protect users of e-mail services.

Recently, a large number of e-mail accounts from Hotmail, Gmail to Yahoo have been attacked by phishing emails (phishing). According to the latest Microsoft Security Report, over 97% of e-mails sent on the Internet are unwanted e-mails, mainly phishing e-mails containing malicious code or is spam.

Artwork of Times

Below are Microsoft's recommendations for how to avoid fraudulent "old" tricks of scammers, and what to do when your online accounts are stolen.

How to identify a phishing email?

Any email that requires you to provide the name, date of birth, personal security code, username and password of the mail account, or other personal information, regardless of who it is sent from, it is almost certainly a phishing email.

The e-mails have a plain text, typographical errors or phrases like 'this is not a joke' (this is not a joke) or "forward this message to your friends" (please forward the message) This message to your friends) is usually an e-mail scam.

Phishing e-mails also often have logos that look like official logos or information directly taken from legitimate Web sites, which can also contain details about yourself that thieves steal. Information found on social networking sites you join.

Some of the phrases you need to know if you think an e-mail message is a phishing email are: "Verify your account." (Please confirm your account information '; "If you do not respond within 48 hours, your account will be closed.") (If you do not reply within 48 hours, your account will be closed); "You have won the lottery." (You won the lottery.)

What should you do when you think you have received a phishing email?

Please take a moment to check your e-mail. Most importantly, NEVER click on the links in that e-mail or provide personal information. Because your computer will be attacked by malware simply after you accidentally visit a fake website. Sites such as snopes.com often list a list of popular phishing emails. Visit the website of the company you received e-mail from and contact customer service via phone or online to verify the validity of the e-mail.

Be sure to make sure you have a reliable password for your account by using more than 7 characters and a combination of uppercase and lowercase letters, numbers and special symbols such as @ or #. Another useful advice is to periodically change the password for your existing accounts.

Report phishing messages to help identify their new formats. If you use Windows Live Hotmail and receive a fake e-mail, you can select the drop-down menu next to the 'Junk' folder, and select the 'Report phishing scam' tab. And remember, no matter what you do, don't reply to the address. You can also notify fake e-mail to Anti-Phishing Working Group via the following address:

reportphishing@antiphishing.org.

What to do when you answer a fake e-mail and have provided your personal information?

1. Notice the incident to the relevant agencies:

2. If you have sent your credit card information, contact your credit card service company immediately. The company offers to know the sooner it happens, the easier it is for them to protect your account.

3. Contact the company that you think their names have been taken advantage of. Please remember to contact them directly, not through the email address you received. Or call that company's customer service department.

4. Please change the password of all your online accounts immediately. Many people use the same password for many different accounts. Start with the password of the credit card account or your personal information. If you suspect someone has accessed your e-mail account, change your password immediately. Review your credit card statement, ask your card provider and bank to provide you with a monthly statement and notice unclear expenses, requirements or activities that you don't require. .

5. Finally, make sure to use the most up-to-date security products, such as anti-spam and fake mail services, spam filters in your web browser and other services that help you. warn and protect you against phishing attacks.