

Identify popular online scams so as not to lose money unfairly

Phishing via Facebook, Zalo, phone calls ... is quite common, although it has been warned but there are still many people who are 'trapped'. Find out the tricks, phishing tricks of scammers through the following article to not lose money unfairly and avoid unwanted nuisance.

Phishing via Facebook, Zalo, phone calls . is quite common, although it has been warned but there are still many people who are "trapped". Find out the tricks, phishing tricks of scammers through the following article to not lose money unfairly and avoid unwanted nuisance.

1. Cheat promotion, win

We can receive fraudulent winning messages via email, via SMS, via Facebook, Zalo, and even phone calls directly to you. The prize value is quite big like winning SH motorbike, phone, or big amount . but most of 99% of these messages or emails are fraudulent.



How to detect scams is as follows:

1. Service you do not participate in but still win.
2. Information on where to receive the prize, the time to receive the prize is not clear or is an inappropriate company.
3. The winner must forward a sum of money to verify, to authenticate .
4. Letter of winning notification is sent from personal mail.

If receiving messages of notification of winning prizes, consumers need to carefully consult information from multiple sources, not to give money to the subject through recharging or money transfer via bank account. If you are harassed many times, threatened, or forced to receive rewards, you should report it to the authorities for resolution.

2. Pretend to be a fraud by telling you to commit a crime

Many people receive messages, emails or phone calls saying that they were investigated for a crime, sounding very serious like drug trafficking to scare. After that, scammers often ask the victim to transfer some money into a bank account or take money to pay in an unknown place as evidence. After investigating if innocent, the victim will be refunded. Even scammers also fake police uniforms to take home to work with similar content.

If they fall into the above situation, they need to calmly ask the sector to take measures such as calling or reporting to the nearest police agency. Even if you are under investigation, the police never call the person to work, even if it is a real police, it is against the law. In accordance with the law, to get testimony or work with people or police officers, they must give an invitation, summons to the office.



1. Warning: The new Facebook virus, a malicious code that is spreading rapidly through Messenger

3. If you do not share / like this status, you will be cursed

When surfing Facebook, sometimes we will see statuses like 'if not shared you will be cursed or you are insensitive'. In fact, this is a deceptive trick for the post status to have a virtual reputation and then take advantage of selling and selling cosmetics, selling ice cream mixes.

4. Texting thanks to recharge cards / phone transfers

Fraudsters who have taken a nick from a friend or relative will text or borrow a phone card for a large amount of money because they are busy or ill to buy.

5. Phishing for spreading viruses and malware

Many Internet users have access to malicious or 'funny' websites that download malicious files that spread the virus. Most recently, the malicious code spread through Facebook Messenger, the virus-infected device became a tool to dig cryptocurrency.



To avoid getting malware, we need to be alert when receiving any file that requires downloading from strangers or even friends. This file often names sex_video or sexy_girl and the like.

6. Call your relatives who have an accident

Scammers call to inform our relatives of a traffic accident and suggest that we send money through our accounts to cover hospital costs. If then call the person who is supposed to have an accident but cannot, the victim will panic, worry and will follow their request.

In addition to the above popular methods, there are many other frauds used by bad guys to make money. If you still know how other scams can be shared, let everyone know to prevent it.

See more:

1. 4 ways to protect personal information should everyone know and use when surfing the web
2. Be wary of phishing when logging on to Facebook and how to protect your Facebook account
3. Watch out for phishing attacks that can steal Apple ID passwords very hard to detect
4. 3 golden rules to avoid fake attacks

You finished reading the article "**Identify popular online scams so as not to lose money unfairly**" 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.