Phishing tricks are becoming more and more cunning

Crime of phishing (online fraud) increasingly uses more sophisticated and cunning 'social engineering' mechanisms (which are based on users' usual reactions and habits) to steal good personal information. intellectual property c

Crime of phishing (online fraud) increasingly uses more sophisticated and cunning 'social engineering' mechanisms (which are based on users' usual reactions and habits) to steal good personal information. Intellectual property property of enterprises.

This is the most important conclusion in the 2006 Global Malware Report by security firm MessageLabs. In the field of computer security, 'social engineering' is an act of collecting or stealing other people's confidential information by forging a completely legitimate user.

'Managing victim relationships?'

Source: ***microsoft.com*** A report by MessageLabs warns: The days when users can identify phishing email scams are approaching. But that is not the complete path of cybercrime.

Now phishing criminals are developing a personalized approach to the victim by imitating customer relationship management techniques or being used in legitimate businesses. The new strategy of cyber criminals is named 'victim relationship management'.

' *The latest phishing attack using social engineering is the attack on social networking sites like MySpace to*

collect personal information ,' said Mark Sunner, chief technology engineer at MessageLabs. ' *In this attack, the victim will receive a fake personal email from their bank asking them to revise the phone area address information* .'

MessageLabs has recorded a dramatic increase in this type of attack since December 2005.

Viruses are also for fraudulent purposes

News.softpedia.com *Source* MessageLabs reports also said that spam and viruses have also increased significantly. This is an anticipated result because the virus outbreak is directly related to online spam or phishing attacks.

Cyber ??criminals often use trojans to 'recruit' more zombies - hijacked PCs - to build a system of botnets that serve spam and phishing attacks.

The pinnacle of malicious virus activities was in the summer of 2004. At this time, there were botnet systems with more than 100,000 PC zombies. However, the number of zombie PCs of botnets has dropped to 20,000 to avoid detection.

But on the contrary, more and more people have become victims of small-scale attacks with more specific goals. For example, of the 321 e-mails monitored by MessageLabs, only one e-mail is spam.

Businesses have become victims of very cunning trojans hidden in fake Microsoft Office files sent from a very reliable source. Most attacks on businesses have very specific objectives to steal property intellectual property rights or to target business spies.

What is the solution?

So how do we combat the growing threat of phishing scams? Mr. Mark Sunner affirmed: The problem here is that while cyber criminals are increasingly using complex attack techniques, security companies are still based on a business model that is 20 years old to protect them. user. In other words: Security firms have been slower than cyber criminals.

Blocking solutions need to be done at the Internet level to prevent phishing e-mails from being sent to users' mailboxes.

' *Human factor is the weakest factor in the security chain. But frankly, we were completely unfair to put such a burden of responsibility on users* , 'Sunner said. ' *We need to apply more high-level filtering solutions to prevent e-mail phishing from reaching the octopus to users* .'

Trang Dung