[Infographic] 4 types of Phishing are easy to trap users

Phishing often appears as a reliable activity by legitimate companies or a reputable electronic information site like eBay, Paypal, Gmail ..

Phishing attacks are also known under familiar names - **Phishing** . Phishing often appears as a reliable activity of legitimate companies or a reputable electronic information site such as eBay, Paypal, Gmail or online banks in many different forms.

In this article, TipsMake.com introduces you to some of the most popular Phishing attacks. No matter what form, you should know the basic ways to identify and prevent. Please follow the infographic below.

Email Phishing

Email lừa đảo thường xuất hiện như một thực thể đáng tin cậy với mục đích đánh cắp dữ liệu cá nhân để kiếm tiền. Kiểu Phishing này thường đính kèm các tệp cài đặt phần mềm độc hại lên máy tính hoặc liên kết đến trang web bất hợp pháp để lừa nạn nhân chuyển giao dữ liệu cá nhân

91% các cuộc tấn công mạng tiên tiến bắt đầu bằng email

50% người nhận sẽ mở email và click vào liên kết lừa đảo

Gọi điện (Vishing)

Các cuộc điện thoại lừa đảo được tội phạm mạng thực hiện bằng cách **mạo danh các dịch vụ tài chính, ngân hàng** để dụ dỗ người dùng cung cấp thông tin chuyển tiền hoặc các thông tin nhạy cảm khác.

TIP: Hạn chế nhận cuộc gọi từ các số điện thoại lạ và không bao giờ cung cấp thông tin cá nhân qua điện thoại

Con số Vishing gây tổn hại trên toàn cầu là vào khoảng **46.3 tỷ USD mỗi năm**

Nhắn tin (SMiShing)

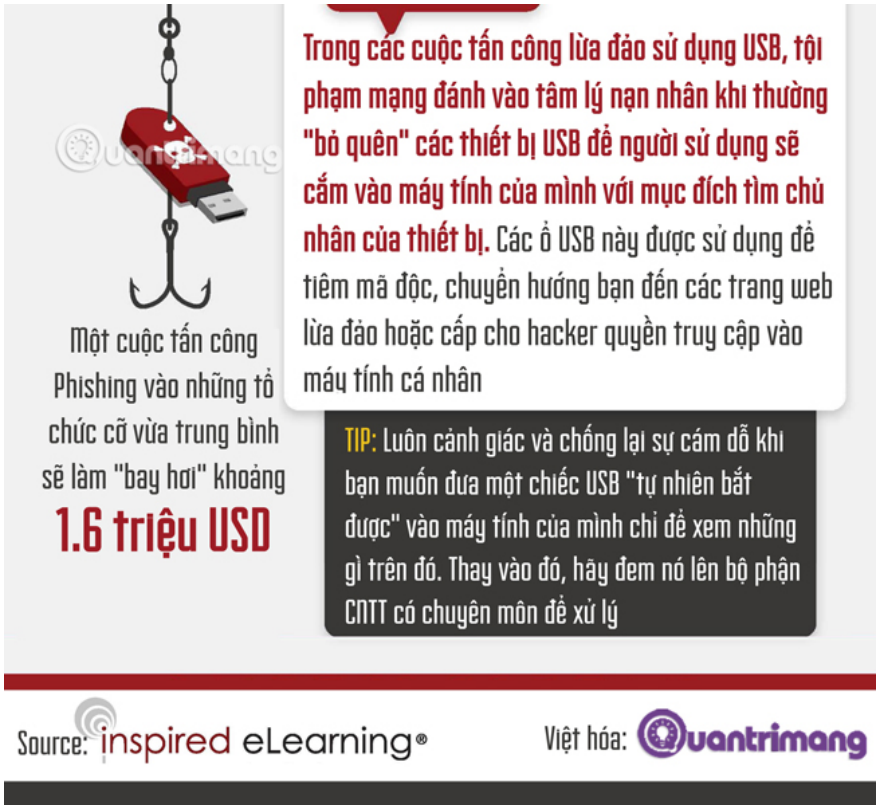
Hình thức này được thực hiện bằng cách sử dụng tin nhắn văn bản để dụ nạn nhân tải phần mềm độc hại xuống thiết bị, truy cập trang web lừa đảo hoặc gọi tới số điện thoại giả mạo.

Tin nhắn dạng SMiShing cũng có thể gợi một hành động ngay lập tức, yêu cầu thông tin bảo mật và chi tiết tài khoản cá nhân của chủ sở hữu.

32%
người dùng smartphone cài đặt phần mềm anti-virus trên điện thoại

TIP: Không trả lời tin nhắn hoặc nhấp vào bất kỳ liên kết nào. Xóa tin nhắn và chặn số người gửi ngay lập tức.

Bẫy USB



4 most popular forms of phishing

1. Email Phishing
2. Calling (Vishing)
3. Texting (SMiShing)
4. USB trap

Email Phishing

Phishing emails often appear as a trusted entity for the purpose of stealing personal data to make money. This Phishing type often attaches malware installation files to a computer or links to illegal websites to trick victims into transferring personal data.

Statistics show that up to 91% of advanced network attacks start with email, 50% of recipients will open the email and click on the phishing link. This data shows that phishing by email is an extremely effective way to be used by cyber criminals.

1. How to identify and prevent phishing attacks via fake email

Calling (Vishing)

Fraudulent phone calls made by cybercrime by **impersonating financial and banking services** to entice users to provide money transfer information or other sensitive information.

Global damage Vishing figures are about **$ 46.3 billion per year** .

TIP: Limit receiving calls from strange phone numbers and never provide personal information over the phone.

Texting (SMiShing)

This is done by using text messages to lure victims to **download malware onto their phones, access phishing websites or call fake phone numbers.** The SMiShing message can also be towing, prompting the victim to trust leading to an immediate action such as asking for the owner's security information and personal account details.

A recent survey by Pew Research reported that only 32% of smartphone users have installed anti-virus software on their phones. So the possibility of telephone phishing attacks still reaches its goal is quite high.

TIP: Do not reply to the message or click on any link. Delete messages and block the number of senders immediately.

USB trap

In fraudulent attacks using USB, cybercriminals hit the victim's psychology when they often "forgot" USB devices so **that users would plug into their computers** for the purpose of finding the owner of the device. . These USB drives are used to inject malicious code, redirect you to phishing sites or give hackers access to personal computers.

A Phishing attack on medium-sized organizations will "evaporate" about $ 1.6 million each time.

So stay alert and resist the temptation when you want to get a "naturally caught" USB device into your computer just to see what's on it. Instead, bring it to the specialized IT department for processing.

Be careful and protect yourself from Phishing attacks!