Phishing --

The Fake VISA email Scam

This is not scam created by Visa; they are a victim as well. If you receive an email similar to the one below, DO NOT click on the link, and do not enter any information on the forms there.

The website that the link leads to is a spoof; a fake website, not created by Visa. When you enter the information they ask for, you will simply be handing the thieves the keys to your bank accounts. That is how spoofing and phishing works. For example, the following link may look like it goes to Visa, but we sent it to amazon.com just to prove the point that you can't believe what you see http://www.visa.com

Remember, no reputable business would send you an email requesting your personal account information. Any such email you receive asking for this information should be considered phony and brought to the attention of the business being 'phished'.

Anytime you need to go to a website for your bank, credit card companies or other personal, financial or confidential information; do not follow a link in an email; just type their address in your browser directly (such as www.visa.com)

Below is an actual phishing email that started circulating in January 2006. We have removed the link to the phisher's website. Note the poor grammar, misspellings, contractions ("don't" instead of "do not"), things that a real bank or credit card company simply wouldn't do.

Subject: Attention! Several VISA Credit Card bases have been LOST!

Good afternoon, unfortunately some processings have been cracked by hackers, so a new secure code to protect your data has been introduced by Visa. You should check your card balance and in case of suspicious transactions immediately contact your card issuing bank. If you don't see any suspicious transactions, it doesn't mean that the card is not lost and cannot be used. Probably, your card issuers have not updated information yet. That is why we strongly recommend you to visit our website and update your profile, otherwise we cannot guarantee stolen money repayment. Thank you for your attention. Click here and update your profile.

PayPal Email Scam

This is not scam created BY PayPal; they are a victim as well. If you receive an email similar to the one below, DO NOT click on the link, and do not enter any information on the forms there.

The website that the link leads to is a spoof; a fake website, not created by PayPal. When you enter the information they ask for, you will simply be handing the thieves the keys to your bank accounts. That is how spoofing and phishing works.

Remember, no reputable business would send you an email requesting your personal account

information. Any such email you receive asking for this information should be considered phony and brought to the attention of the business being 'phished'.

Anytime you need to go to a website for your bank, credit card companies or other personal, financial or confidential information; do not follow a link in an email; just type their address in your browser directly (such as www.PayPal.com)

Below is an actual phishing email that started circulating in late 2006.

Dear PayPal Customer,

Due to recent fraudulent activities on some of PayPal online accounts we are launching a new security system to make PayPal online accounts more secure and safe. Before we can activate it we will be checking all PayPal online accounts to confirm the authenticity of the holder.

We will require a confirmation that your account has not been stolen or hacked. Your account has not been suspended or frozen.

To confirm your account status please Login

-complete the required information to authenticate and reset your account

-make sure your account balance has not been changed

-make sure your details have not been changed

-review recent transactions in your account history for any unauthorized transfer

If you find any type of suspicious activities please contact us immediately. Please include in your message your account number, your account name and the unauthorized transfer date & time.

Please do not reply to this message. For any inquiries, contact Customer Service.

PayPal Team Copyright 2006

The Login link takes you not to PayPal, but to this address instead:

http://smtp.aluno.feis.unesp.br/icons/developed/%20/webscr.htm

Here is what PayPal suggests:

> ***Look for a PayPal Greeting****: PayPal will never send an email with the greeting "Dear PayPal User" or "Dear PayPal Member." Real PayPal emails will address you by your first and last name or the business name associated with your PayPal account.*

If you believe you have received a fraudulent email, please forward the entire email— *including the header information—to spoof@paypal.com. We investigate every spoof reported. Please note that the automatic response you get from us may not address you by name.*

Don't share personal information via email: *Paypal will never ask you to enter your password or financial information in an email or send such information in an email. You should only share information about your account once you have logged in to https://www.paypal.com/.*

Don't download attachments: *PayPal will never send you an attachment or software update to install on your computer.*

Mississippi Attorney General's Office Consumer Division 2013