9 December 2010

Visa Warns Merchants of E-mail Phishing Scams

U.S., Canada, LAC

Visa has detected an increase in e-mail “phishing” scams directed toward merchants. These scams utilize fraudulent e-mails that appear to originate from legitimate financial institutions, transaction processors or other business entities that routinely conduct business with merchants.

Through these e-mail scams, criminals attempt to convince merchants to provide sensitive information such as merchant account information, passwords, login credentials or other payment transaction information, which can be used by criminals to commit fraud.

In most of these e-mail phishing cases, the merchant is asked to click on an Internet hyperlink embedded in the e-mail. This link connects to the criminal’s fraudulent website or computer server and may lead to the installation of malicious software (known as “malware”) on the merchant's computer.

E-mail Phishing Message Example and Phishing Scam Indicators

Merchants and acquirers are encouraged to review both the example phishing e-mail message and the list of phishing scam indicators provided below. Together, these tips can help merchants identify and report suspicious e-mails.

From: support-x@yourprocessor.net
To:
Subject: Urgent Alert
Date: Mon, 15 Nov 2010

Your Processor’s Graphic

<Your Processor> urgent Alert.
Your online password has expired. Please login to renew it.
If you fail to do so, your account will be locked.

1. **Look Closely at the Sender’s E-mail Address.** Although the “From” line in the example e-mail above closely resembles a valid e-mail address, a closer look reveals unusual characters or constructs that can help confirm that the address is fraudulent. For example, the “-x” after the word “support” indicates that the address may not be legitimate. Merchants should be aware that suspicious e-mails can often appear to come from legitimate sources.

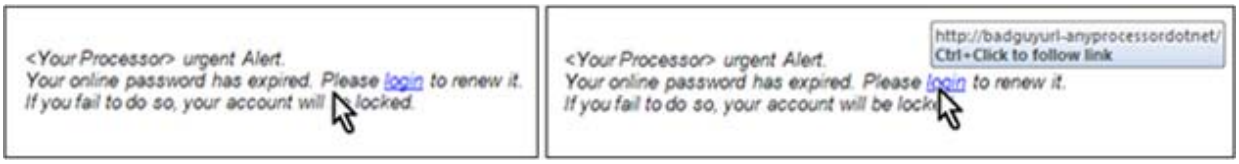
2. **Check E-mail Images and Graphics.** Images used in fraudulent e-mails are often broken (i.e., not present), out of place or incorrect. These problems typically occur when a fraudulent message attempts to reference an image from a legitimate entity’s website and fails. Sometimes the fraudsters may not fully understand the payment card industry and incorrectly provide co-branded images (such as the Visa Verified by Visa logo and the MasterCard SecureCode logo) on the same phishing message.

3. **Pay Attention to Message Format and Text.** Message length, grammar, word choice and sentence structure play a part in the success of a phishing e-mail. In the example above, the brevity of the message and the lack of personalization (e.g., the merchant's name is not used; the sender's contact information is not provided) could indicate that the e-mail is fraudulent. Merchants should be aware that e-mails can arrive in different languages and with small mistakes or errors. Those e-mails that seem out-of-place or have glaring errors typically require more validation.

4. **Pay Attention to Message Tone; Look for Consequences Resulting From Lack of Action.** Be aware of the tone used in the e-mail message. Does it demand the merchant's attention and indicate that there will be consequences if the merchant does not take action? If so, this could indicate that the e-mail is fraudulent.

5. **Consider Whether the Message Received Seems Out of Character.** Merchants' relationships with their financial institutions develop over time. Through the course of business, merchants may learn that their financial institutions like to conduct business and exchange information in a particular way. In the example above, the merchant might ask, "Would my financial institution or transaction processor send a message like this?" Or is it more likely that the merchant would receive a phone call or be asked to address the issue in person?

6. **Be Wary of Embedded Hyperlinks**. Hovering or moving your computer mouse pointer over an embedded hyperlink should reveal the associated web URL.



If you don't recognize the web URL or if the URLs don't match, there may be reason for suspicion. Even embedded links for sites that you know or recognize may contain clues indicating fraud (such as hidden characters or other slight modifications), which can be easy to miss. Instead, open a new browser window and type the web URL into the browser. Do not copy and paste the URL included in the e-mail into your browser.

E-mail messages that request personal information or demand urgent action on the part of the merchant should be approached with suspicion. To confirm the origin of any suspicious e-mail and verify that requests for sensitive information are legitimate, contact customer service using the telephone number provided by your acquiring bank or transaction processor, or located in your vendor contract agreement.

Merchant and Acquirer Impact

Neither Visa nor its personnel will ever ask for personally identifiable information (e.g., passwords, national identification numbers (such as Social Security numbers) or Personal Account Numbers (PANs)) via e-mail or telephone.

Any merchant that receives a suspected or actual phishing e-mail should report the incident to their financial institution and to Visa. To notify Visa, send an e-mail to phishing@visa.com with the phishing e-mail attached.

For More Information

For more information on how to combat phishing scams, please contact your financial institution or visit the Anti-Phishing Working Group website.