How to Catch a Phish

An email phishing scam or "phish" is a fraudulent email that attempts to trick the reader to submit valuable personal or payment information. A phish may also include links or pop ups that, if clicked, can potentially install harmful software onto your computer.

For more information on the latest scams to the smartest prevention tips, visit **www.VisaSecuritySense.com**.

Watch for these clues in your inbox:

Look but don't click! Scrolling your mouse over the embedded link reveals that it points to a suspicious webpage rather than a Visa site. While the "From:" field in the email indicates this email is from a "usa.Visa.com" web address, this link (as shown below) leads to a strange domain ending in ".be".

http://verified.visa.com.aam.data.default.landing.aam.partner.default.resize-yes.cyclepassion-borgloon.be/
Click to follow link

Top 5 Tips to Avoid Email Phishing Scams

1. Consider all email requests for personal or payment information to be suspicious.
2. Be cautious about clicking on links in unsolicited email that you receive.
3. Check the legitimacy of any email inquiry requesting your personal or payment information by looking up the company's phone number separately and calling to verify the request.
4. Watch for typos and bad grammar. These are warning signals that an email may be fraudulent.
5. Use spam blockers and keep your anti-virus software up to date.

The "From:" line appears to be from a valid Visa email address, but that doesn't guarantee the legitimacy of an email. Fraudsters can make an email appear to originate from someone or somewhere other than the actual source, a tactic known as "spoofing."

The subject line uses ominous or threatening language to compel the recipient to take immediate action. Invoking a sense of urgency or fear is a common phishing tactic.

This message was sent with High importance.

From: Visa.com [mailto:service@usa.visa.com] Sent: Friday, Feb. 10, 2012 1:40 AM
To: undisclosed-recipients
Subject: Your Credit Card has been Suspended

VISA

Dear Valued Customer,

Your Credit Card has been Suspended, as an error was detected in your Credit Card information. The reason for the error is not certain, but for security reasons, we have suspended your Credit Card temporarily.

We need you to update your information for further use of this Credit Card.

To Lift this Suspension:

Click Here

and follow the Steps to re-activate your Credit Card.

NOTE: If this is not resolved within 72 hours, we will be forced to suspend your Credit Card Permanently as it may be used fraudulently. The purpose of this verification is to ensure that your Credit Card account has not been fraudulently used.

Thanks,

Customer Support Service.

Copyright © 1999-2012 Verified by Visa® All Rights Reserved.

You'll notice that there is a lack of formal addressing, salutation or personalization unlike what you would expect from most legitimate businesses.

Read the email closely. While the language appears consistent, several words are in upper case when they shouldn't be (e.g., "Credit Card"). Typos and bad grammar should be a clear warning signal that the email is likely fraudulent.

This phish again uses threatening language urging the recipient to take immediate action. If you receive such an email, look up the company's customer service line separately and call to inquire about the purported account problem first.

The lack of closing details, including how to contact the company if more information is needed, also strongly suggest a phish. A legitimate business would provide a customer contact phone number, especially for an important matter such as account suspension.

Note: This is just one example of a phishing scam, but there are countless variations that may exhibit different warning signs.