Phishing Countermeasures

Fraud Investigation and Education
FIS

www.fisglobal.com

Phishing …What is it?

Phishing is a technique used to gain personal information for purposes of identity theft, using fraudulent e-mail messages that appear to come from legitimate sources. These authentic-looking messages are designed to fool recipients into divulging personal data such as account numbers and passwords, card number and Social Security numbers.

Most phishing e-mails include false statements intended to create the impression that there is an immediate threat or risk to the bank, credit/debit card, or financial account of the person who received the e-mail. Also, people who receive phishing e-mails may not realize that the senders may have used “spamming” (mass e-mailing) techniques to send the e-mail to thousands of people.

Below is an example of a phishing email along with screenshots of a series of events after clicking on the imbedded link:

From: "service@visa.com" <service@visa.com>
Sent: Tuesday, April 17, 2007 7:41 AM
To:
Subject: Your Card is Limited for Online Services!

Dear Visa Cardholder

Continuous Monitoring is an integral part of Visa's multiple layers of security. In addition to other fraud monitoring tools, we can often spot fraud based upon transactions on the card that are outside of cardholders typical purchasing pattern. This allows us to spot fraudulent activity as quickly as possible and acts as an early-warning system to identify fraudulent activity.

During a recent checkout we detected suspicious activity and your Visa card may have been compromised. Fraudulent activity made it necessary to limit your card for online services, your case ID number for this matter: AT09GP32D506 : Conform to our security requirements and in order to continue online services with your card, we most validate your identity. Please use our link below to proceed.

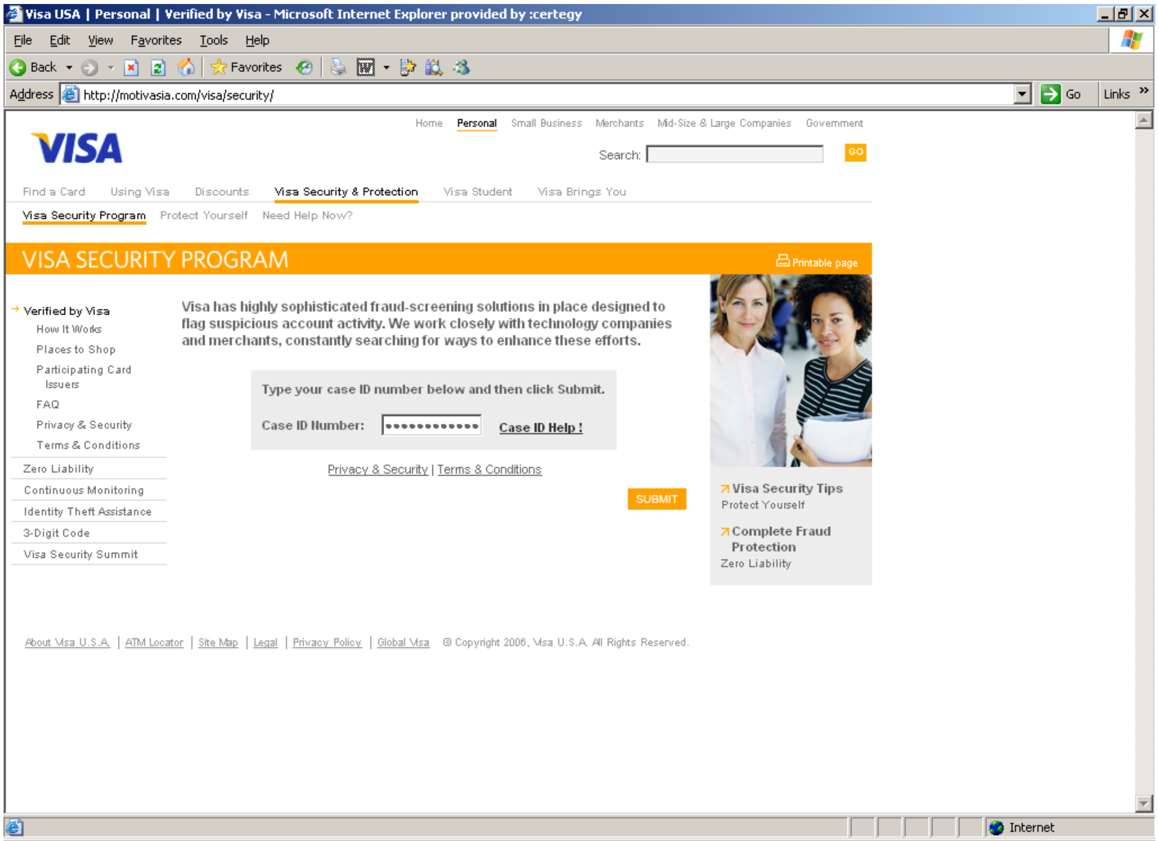
https://phishingforyourpersonalandfinancialinformation.com

Visa takes online security very seriously so that you can shop safely on the Internet. As part of our commitment to fighting fraud we have the right to investigate, prevent, or take action regarding illegal activities, suspected fraud, situations involving potential threats to the physical safety of any person, or violations of the terms and conditions for using Visa U.S.A.

(c) Copyright 1996-2007 Visa International Service Association. All Rights Reserved.

Below are screenshots of a spoofed website made to look like Visa's website after the web link was accessed from the phishing email. Let's take a look at the internet address in the URL bar. Does it say it's from Visa.com? That's right it doesn't! This shows you that no matter how authentic the webpage looks you need to verify several tokens before proceeding. (Please see 'Avoiding Phishing Scams" below for more details.)

(In the picture below the phisher asks for the case id number that was provided in the phishing email.)



Visa USA | Personal | Verified by Visa - Microsoft Internet Explorer provided by :certegy

Address http://motivasia.com/visa/security/

VISA SECURITY PROGRAM

Visa has highly sophisticated fraud-screening solutions in place designed to flag suspicious account activity. We work closely with technology companies and merchants, constantly searching for ways to enhance these efforts.

Type your case ID number below and then click Submit.

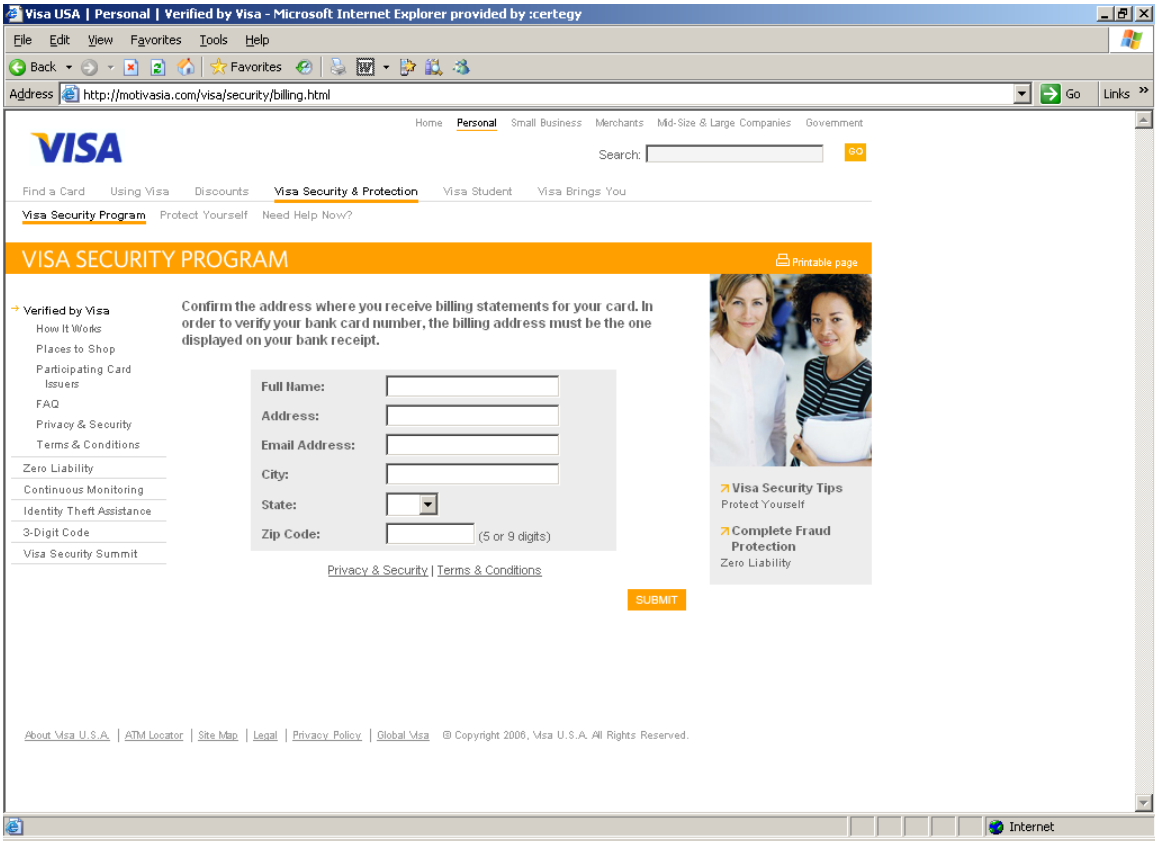
Case ID Number: ●●●●●●●●●●●●● Case ID Help !

Privacy & Security | Terms & Conditions

SUBMIT

About Visa U.S.A. | ATM Locator | Site Map | Legal | Privacy Policy | Global Visa © Copyright 2006, Visa U.S.A. All Rights Reserved.

(After the case id has been entered, the next screen shown below populates asking you to confirm your name and address)


Visa USA | Personal | Verified by Visa - Microsoft Internet Explorer provided by :certegy
File Edit View Favorites Tools Help
Back
Favorites
Address
Go
Links
Home
Personal
Small Business
Merchants
Mid-Size & Large Companies
Government
VISA
Search:
GO
Find a Card
Using Visa
Discounts
Visa Security & Protection
Visa Student
Visa Brings You
Visa Security Program
Protect Yourself
Need Help Now?
Printable page
Verified by Visa
How It Works
Places to Shop
Participating Card Issuers
FAQ
Privacy & Security
Terms & Conditions
Zero Liability
Continuous Monitoring
Identity Theft Assistance
3-Digit Code
Visa Security Summit
Visa Security Tips
Protect Yourself
Complete Fraud Protection
Zero Liability
Privacy & Security | Terms & Conditions
SUBMIT
About Visa U.S.A. | ATM Locator | Site Map | Legal | Privacy Policy | Global Visa
© Copyright 2006, Visa U.S.A. All Rights Reserved.
Internet

http://motivasia.com/visa/security/billing.html

VISA SECURITY PROGRAM

Confirm the address where you receive billing statements for your card. In order to verify your bank card number, the billing address must be the one displayed on your bank receipt.

Full Name:

Address:

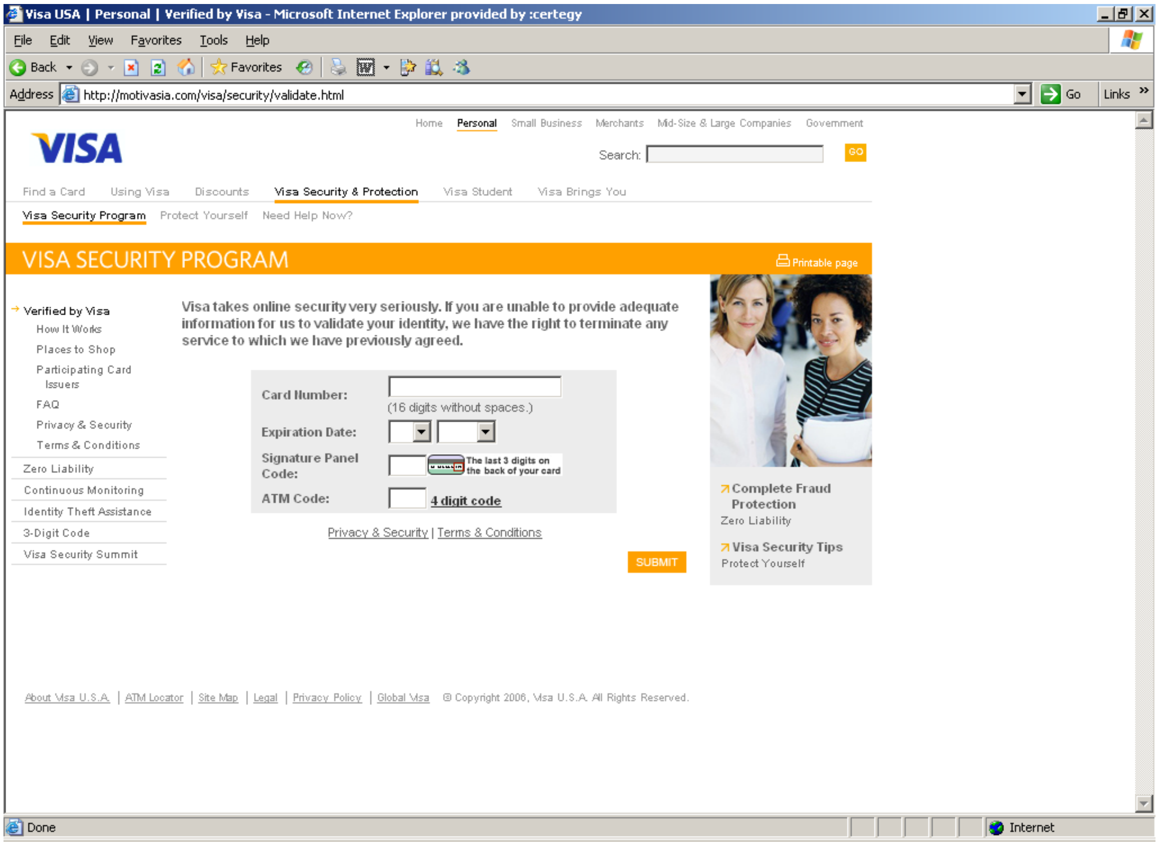
Email Address:

City:

State:

Zip Code: (5 or 9 digits)

(After the personal information has been entered the next screen, pictured below, populates asking for your card information)


Visa USA | Personal | Verified by Visa - Microsoft Internet Explorer provided by :certegy
File Edit View Favorites Tools Help
Back Favorites
Address http://motivasia.com/visa/security/validate.html
Go Links
Home Personal Small Business Merchants Mid-Size & Large Companies Government
VISA
Search: GO
Find a Card Using Visa Discounts Visa Security & Protection Visa Student Visa Brings You
Visa Security Program Protect Yourself Need Help Now?
VISA SECURITY PROGRAM
Printable page
Verified by Visa
How It Works
Places to Shop
Participating Card Issuers
FAQ
Privacy & Security
Terms & Conditions
Zero Liability
Continuous Monitoring
Identity Theft Assistance
3-Digit Code
Visa Security Summit
Complete Fraud Protection
Zero Liability
Visa Security Tips
Protect Yourself
Done
Internet

Visa takes online security very seriously. If you are unable to provide adequate information for us to validate your identity, we have the right to terminate any service to which we have previously agreed.

Card Number: (16 digits without spaces.)

Expiration Date:

Signature Panel Code: The last 3 digits on the back of your card

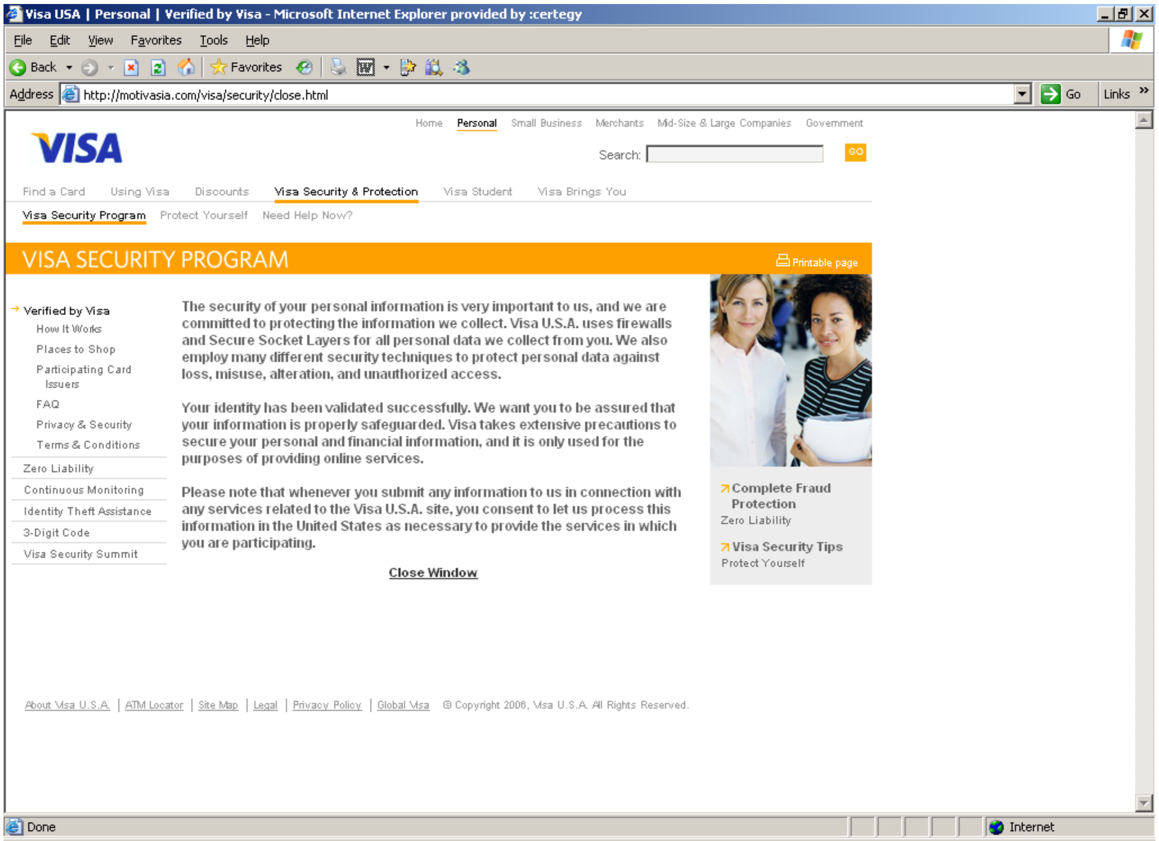
ATM Code: 4 digit code

Privacy & Security | Terms & Conditions

SUBMIT

About Visa U.S.A. | ATM Locator | Site Map | Legal | Privacy Policy | Global Visa © Copyright 2006, Visa U.S.A. All Rights Reserved.

(Below is the closing screen after the personal & financial information has been collected.)



http://motivasia.com/visa/security/close.html

The security of your personal information is very important to us, and we are committed to protecting the information we collect. Visa U.S.A. uses firewalls and Secure Socket Layers for all personal data we collect from you. We also employ many different security techniques to protect personal data against loss, misuse, alteration, and unauthorized access.

Your identity has been validated successfully. We want you to be assured that your information is properly safeguarded. Visa takes extensive precautions to secure your personal and financial information, and it is only used for the purposes of providing online services.

Please note that whenever you submit any information to us in connection with any services related to the Visa U.S.A. site, you consent to let us process this information in the United States as necessary to provide the services in which you are participating.

© Copyright 2006, Visa U.S.A. All Rights Reserved.

So the example shown above is one of many different types of phishing methods that are deployed by the fraudsters. You always want you be aware of several factors: (1). Where did the email originate from? (2). Verify the address in the URL bar. (3). Never provide personal or financial information if you can't verify the source.

Types of Phishing Attacks:
There have been numerous different types of phishing attacks that have been identified. Listed below are some of the more prevalent.

<u>Deceptive Phishing</u> – In this method the phisher uses common social engineering tactics to fool the victim in releasing personal/financial information. Some of the more common tactics used are: "You're account has been blocked", "Congratulations! You've been selected to participate in our Fraud Protection Services". The phisher's goal here is to have the victim act immediately when they open the email.

Malware-based Phishing – Involves running malicious software on user's pc's. Malware can be introduced as an email attachment or as a downloadable file from a website.

Key loggers & Screen loggers – Are several varieties of malware programs that track keyboard input and are able to send the information to the hacker via the internet. These programs can embed themselves into user's browsers that run automatically when the browser is started.

Session Hijacking – is an attack where user's activities are monitored until they sign in to a target account or transaction and establish their login credentials. At that point the malicious software takes over and can undertake unauthorized actions, such as transferring funds, without the user's knowledge.

System Reconfiguration Attacks – This attack modifies the settings on the user's PC for malicious purposes.

DNS-Based Phishing AKA "Pharming" – Pharming is the term given to hosts files modifications or Domain Name System (DNS)-based phishing. With a Pharming scheme, hackers tamper with the host files so that requests for website address return a bogus or fake website.

Content-Injection Phishing – Hackers replace part of the content of a legitimate site with false content designed to capture login credentials and/or account number sequence.

Man-in-the-Middle Phishing – In these attacks hackers' position themselves between the user and the legitimate website and collect the data as it's passing from one source to another.

Responding to an Attack

Hopefully, many of you should have some sort of set procedures in place to deal with a phishing attack. Unfortunately, this is one fraud scheme that will continue to evolve as we look into the future. Following are some tips and recommendations when it comes to responding to a phishing attack.

Staff Preparation:
Procedures should be in place for employees to capture and log information to report the incident. These procedures should include:

- Information on the phishing scheme used in the attack – Request and verify the victims email address contacted during the attack.
- Gather all details of the message used in the phishing attack including the imbedded link that was provided in the email. Request the phishing email from the victim. They can either forward it or send as an attachment so that all of the contents are available to you. Also, what type of social engineering method was used? For example: "Your account has been blocked" or "Your account is past due", or "We noticed some suspicious activity".
- Determine what information was solicited – You want to capture specific details. For example: were they looking for the card number? Expiration date? PIN number? Get as much information as possible.
- Determine what information did the customer provide?

The idea is to collect as much information as you can and to report your findings. (Please see "Reporting the Attack" below.)

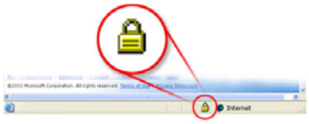
Alert Staff and Customers:

- Notify both staff and customers as soon as an attack has been identified.
- Explain what phishing is and what actions can be done when an email message is received.
- Place an article or posting on your website with news of the phishing attempts to inform customers what's occurring in your area.
- Educational materials about phishing can be found at www.antiphishing.org and www.ftc.gov.

How to avoid Phishing scams

While phishing scams continue to increase in terms of velocity and sophistication, consumers should always be aware about what type of personal information is being requested. As a general rule the consumer should never provide personal information to an organization to which they already belong to. Below is a list of recommendations compiled by the Anti-Phishing Working Group (APWG) that one can use to avoid becoming a victim of these scams.

- Be suspicious of any email with urgent requests for personal information
  - Phishers use social engineering tactics in hopes of getting the victim to respond as quickly as possible before they realize the scam. This usually includes upsetting or exciting (but false) statements in their emails to get people to react immediately.
  - They typically ask for personal information such as usernames, passwords, credit/debit account numbers, social security numbers, etc.
  - Phishing emails are usually not personalized, but sometimes can be. Valid messages from known trusted sources will usually contain some sort of personalization but we encourage calling and verifying if you are unsure.
- Don't use or click on the links that's been provided in the email, instant message, or chat to get to any web page if you feel that the message might not be authentic or especially if you don't know the sender.
  - Instead, verify with the source via by phone or by visiting their webpage directly by typing in the web address in the browser
- Avoid filling out forms or fields in email messages that ask for personal information.
- Always verify that the website is secure via the web browser when submitting personal sensitive data.
  - Phishers are now able to spoof both the "https://" (that you normally see on secure web server) AND a legitimate looking address in the URL bar. To countermeasure; type in the address of the website instead of clicking on the link provided in the email.
  - Phishers may also spoof the yellow lock that is normally seen on a secure website shown here.


©2003 Microsoft Corporation. All rights reserved. Terms of Use | Privacy Statement
Internet

The lock icon has been considered as an indicator that the website is a secure site. When you double click on the lock icon it should display the security certificate for that site. When the address information does not match between the URL bar and the security certificate, close the browser page immediately.

- If the link provided in the email has been clicked on, verify the address in the URL bar. Be aware of the site that pops up on screen.
- Consider installing a Web browser tool bar to help protect you from known fraudulent websites. These toolbars match where you are going with lists of known phishing Web sites and will alert you.
  - The newer version of Internet Explorer version 7 includes this tool bar as does Firefox version 2
  - There are several tool bars that are free to all internet users and available for download. They are: Netcraft at http://toolbar.netcraft.com/ and EarthLink ScamBlocker at http://www.earthlink.net/earthlinktoolbar
- Regularly log into your online accounts
- Make sure that your browser is up to date and security patches installed and applied.

Reporting the Attack

Once you have collected all the information about the phishing attack you should report it immediately to minimize the impact and results. Below are some recommendations to report "phishing" or "spoofed" emails to the following groups:

- reportphishing@antiphishing.org - Submit an email complaint to the link on the left. To do so, create a new email and drop the phishing email from your inbox onto this new email message. Do not forward the email if you can't help it, this approach loses information and requires more manual processing.
- File a complaint with the Internet Crime Complaint Center at www.ic3.gov. This site accepts complaints from either the person who believes they were defrauded or from a third party to the complainant.
- Submit an email complaint to the Federal Trade Commission at spam@uce.gov.
- If Visa's brand is used in the attack, report the incident and forward the email directly to Visa at Phishing@visa.com.
- Also notify the source that is being victimized by the phishing scam. Be sure to forward the email to that source.

FIS Fraud Management

"We provide peace of mind by making electronic transactions safe, simple, and secure."

Contact Us: 1-800-282-7629