Vishing (and “SMiShing”) Countermeasures

Fraud Investigation & Education
FIS

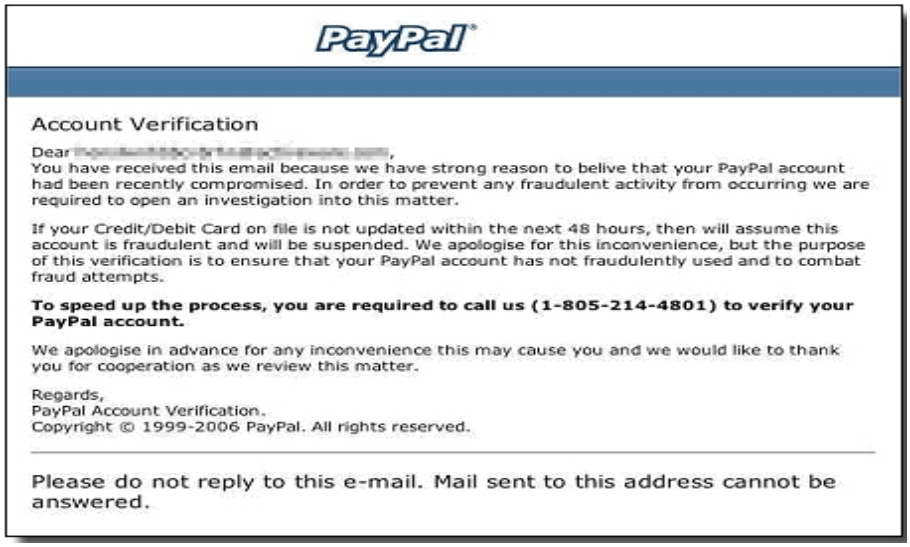
Never Compromise.

Vishing…What is it?

Vishing also called (Voice Phishing) is the voice counterpart to the phishing scheme. Instead of being directed by an email to a website, the user is asked to make a telephone call. The call triggers a voice response system that asks for the user's personal identifiable information to include: Plastic card number, Expiration date, CVV2/CVC2, and/or PIN number. To date, there have been two methods of this technique that have been identified.

The first method is via "Email blast".
The email blast has the exact same concept of phishing email that includes false statements intended to create the impression that there is an immediate threat or risk to the financial account of the person who receives the email. Instead of Weblink, there is a number provided that instructs the person to call and provide their personal identifiable information.

Example of a vishing email:



PayPal

Account Verification

Dear [redacted],
You have received this email because we have strong reason to belive that your PayPal account had been recently compromised. In order to prevent any fraudulent activity from occurring we are required to open an investigation into this matter.

If your Credit/Debit Card on file is not updated within the next 48 hours, then will assume this account is fraudulent and will be suspended. We apologise for this inconvenience, but the purpose of this verification is to ensure that your PayPal account has not fraudulently used and to combat fraud attempts.

To speed up the process, you are required to call us (1-805-214-4801) to verify your PayPal account.

We apologise in advance for any inconvenience this may cause you and we would like to thank you for cooperation as we review this matter.

Regards,
PayPal Account Verification.
Copyright © 1999-2006 PayPal. All rights reserved.

Please do not reply to this e-mail. Mail sent to this address cannot be answered.

The second method has been identified as "Cold-Call Vishing".
With this method, the fraudsters use both a war dialer program with a VoIP (Voice over Internet Protocol) technology to cover a specific area code(s). The war dialer is a program that relentlessly dials a large set of phone numbers (cell or landlines) in hopes of finding anything interesting such as voice mail boxes, private branch exchanges (PBX) or even computer modems (dial-up). VoIP is a technology that allows anyone to make a call using a broadband internet connection instead of a regular phone line. VoIP enables the fraudsters to mask or conceal their actual phone number and use a false one to avoid detection. In some cases, the fraudsters have used numbers from local merchants and financial institutions in an effort to gain the trust of the victim.

Example of a War Dialer program:

SMiShing

Smishing is a spin-off version of Vishing. In this instance the victim receives a text message via their cell phone with the implications that there is a threat to their account and request a callback to a number provided in the message. The social engineering tactics used are the same as in the phishing and vishing attacks; the only difference is the delivery method.

Below is an example of a smishing text.
"**(Financial Institution Name) Alert: You're card starting with XXXX has been deactivated. Please contact us at XXX-XXX-XXXX to reactivate your card**".

Responding to an Attack

Following are tips and recommendations when it comes to responding to a vishing/Smishing 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 phone number used in the attack – Request and verify the victims number that was contacted during the attack.
- Determine what method was the call/message received? Was it a Cell or land line? Was it a voice mail or text message?
- All details of the phone conversation or recorded message – Include the call-out number captured by caller ID or the source of the text message. Also, what type of social engineering method was used? For example: "Your account has been blocked" or "Your account is past due", or more recently "Your account has been breached".
- 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?
- Identify the callback number used in the attack.
- Research the callback number and the phone carrier – Fone Finder is a website that helps locate the service provider of the first 7 digits of the area code and phone number used. Their website is as follows: http://www.fonefinder.net/

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 a pattern has been identified.
- Explain what Vishing is and what actions can be done when a call or text message is received.
- Place an article or posting on your website with news of the vishing attempts to inform customers what's occurring in your area.
- Educational materials about phone fraud can be found at http://www.ftc.gov/bcp/edu/pubs/consumer/telemarketing/tel19.shtm.
- "Who's Calling?-Recognize and Report Phone Fraud" PDF available for print and distribution. http://www.ftc.gov/bcp/edu/pubs/consumer/telemarketing/tel19.pdf.

Reporting the Attack

Once all the information about the attack has been obtained you'll want to report it as soon as possible to contain it. Listed below are some steps and procedures in place to help you report the incident.

- Report the incident to local law enforcement – You will need to file a formal report with your local law enforcement agency about the attack.
- Contact the phone carrier's fraud department to get the callback number used in the attack shut down. Usually the phone carriers require a police report file in order to proceed so it's important to have the police report on file.
- Report the incident to the FTC, Federal Trade Commission at http://www.ftc.gov/ or call 1-877-FTC-Help.
- File a report with the Internet Crime Complaint Center at http://www.ic3.gov/default.aspx

FIS Fraud Management

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

Contact Us: 1-800-282-7629