



Phishing – Read Behind The Lines

Veljko Pejović

veljko@cs.ucsb.edu

What is Phishing?



- *"Phishing attacks use both social engineering and technical subterfuge to steal consumers' personal identity data and financial account credentials"*

Anti-phishing Working Group

What is Phishing?



- Social engineering aspect:
 - Sending “spoofed” e-mails
 - Building confidence between a phisher and a victim
- Technical aspect:
 - Spyware
 - Pharming - DNS poisoning

Key Characteristics



- Upsetting or exciting statements – must react immediately
- Ask for information such as username, passwords, credit card numbers, social security numbers, etc.
- Emails are typically NOT personalized
- “Masked” links

Phishing Example

Subj: **Your Bank of Oklahoma Account could be Suspended**
Date: 10/31/2005 9:17:23 PM W. Europe Standard Time
From: department@bankofoklahoma.com
To: rsutton603@aol.com
Sent from the Internet ([Details](#))



Security Alert

Please note that Your Bank of Oklahoma Account could be suspended. If there is a problem with your information, please use the following link to update your Account:

<http://secure.bankofoklahoma.com/cgi-bin/dll87443/update/default.asp>

Bank of Oklahoma Security Department
Thank you.

Please Note: Bank of Oklahoma always contacts its costumers about account expiration. That is how we show our *quality* and *respect* to our clients. However your information are 100% safe in our 128-ssl dabatase.

Actually links to
<http://212.45.13.185/bank/index.php>

Phishing Example



Dear SouthTrust customer,

We recently reviewed your account, and we suspect an unauthorized ATM and/or PIN- based point of sale transaction on your account. Protecting your account is our primary concern. Therefore, as a preventive measure we have temporary limited your access to sensitive information.

SouthTrust Bank features. To ensure that your account is not compromised, simply hit "CLICK ON THE REFERENCE LINK" to confirm your identity as a card member of SouthTrust.

[Login to your SouthTrust Online Banking with your SouthTrust username and password.](#)

[Confirm your identity as a card member of SouthTrust.](#)

[View your transaction history and report suspicious activity or any unauthorized change.](#)

<https://southtrustonlinebanking.com/retail/>

If you are not enrolled for SouthTrust Online Banking get started today! Complete the steps below and take advantage of our online services today!

[Select your account: Personal Accounts, Business Accounts, Credit Card Premiere Line or Credit Line Only.](#)

It's that easy. If you still need assistance, just click the "Help" button within Internet Banking, or [contact us](#). We're here to help you 24 hours a day, 7 days a week.

*Please do not reply to this message. Mail sent to this address cannot be answered.

*For assistance, log to your SouthTrust Bank Account and chose the "Help" link in the top right corner.

Thomas D. B. Graff, Member FDIC



Another false link!

Copyright 2005, SouthTrust. All Rights Reserved

Wachovia Bank, N.A. d/b/a SouthTrust Bank, Member FDIC

Once you get caught...

Welcome to Citi - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Forward Stop Home Search Favorites Media

Address https://web.da-us.citibank.com/signin/citifi/scripts/email_verify.jsp

citi | **verify**
your e-mail address

Please verify your e-mail

False Citi-Bank URL!

ATM/Debit Card (CIN) / Card #

Expiration Date /

PIN

Your information is transmitted using 128bit SSL encryption.

Consequences



- Customers:
 - Financial consequences – stolen financial information
 - Trust and effective communication can suffer
- Service providers (banks, retailers...)
 - Diminishes value of a brand
 - Customer loss
 - Could affect stakeholders

Spear Phishing



- Targeted at a specific company, government agency, organization, or group
- Phisher gets an e-mail address of an administrator/colleague
- Spoofed e-mail asks employees to log on to a corporate network
- A key-logger application records passwords
- Phisher can access corporate information

Phishing Techniques



- Phishing through compromised web servers
 - Find vulnerable servers
 - Gain access to the server
 - Pre-built phishing web sites are up
 - Mass emailing tools are downloaded and used to advertise the fake web site via spam email
 - Web traffic begins to arrive at the phishing web site and potential victims access the malicious content

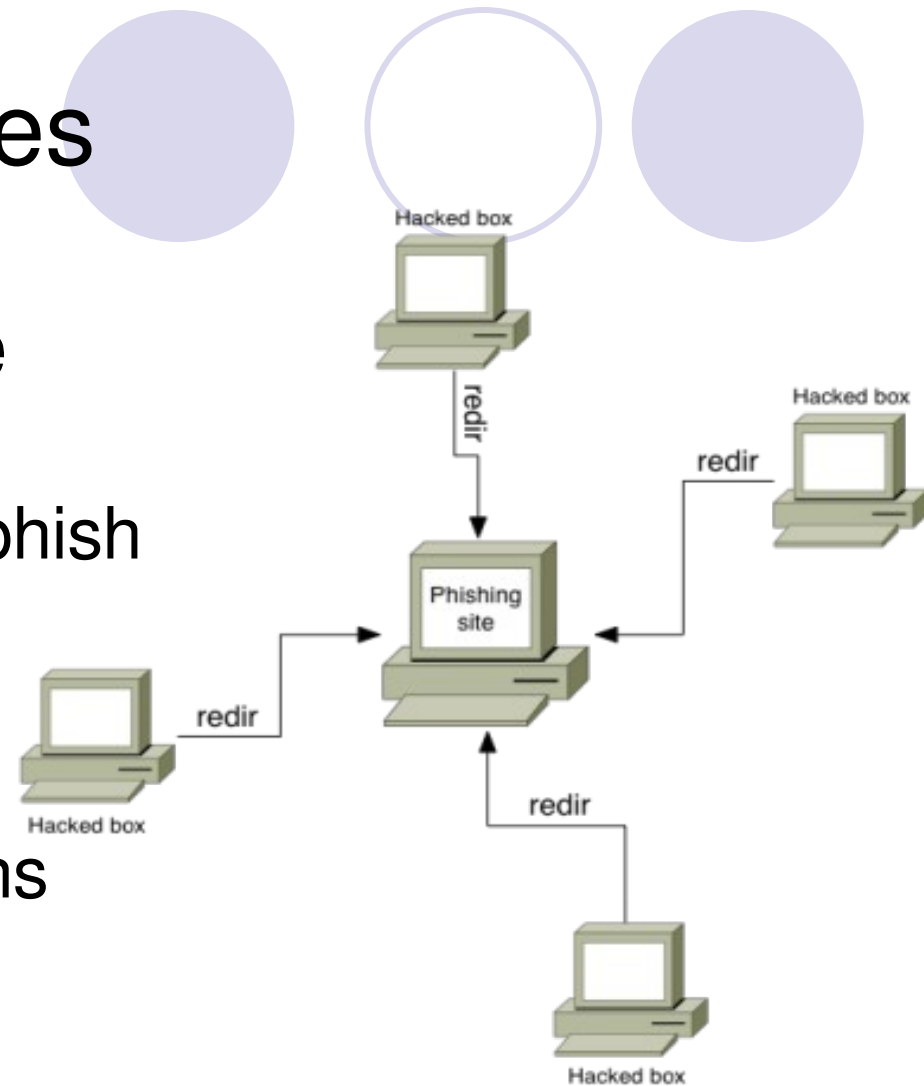
Phishing Techniques



- Phishing through port redirection
 - Find vulnerable servers
 - Install software that will forward port 80 traffic to a remote server
 - Make sure that it is running even after a reboot,
 - Try not to get detected
 - Web traffic begins to arrive at the phishing web site and potential victims access the malicious content

Phishing Techniques

- Combined technique
 - If a remote host is lost other will continue to phish
 - If the central phishing site is lost, compromise another and update redirections
 - Faster configuration setup, concurrent adjustments can be made



Phishing Techniques



- Additional approaches
 - Register similar sounding DNS domains and setting up fake web sites, e.g. www.paypa1.com
www.welsfargo.com
 - Configure the fake phishing web site to record any input data that the user submits silently log them and then forward the user to the real web site
 - Attempt to exploit weaknesses in the user's web browser to mask the true nature of the message content

Phishing Techniques

- Transfer of funds
 - International transfers are monitored, find an intermediate person to send the money
 - “Hello! We finding Europe persons, who can Send/Receive bank wires from our sellings, from our European clients. To not pay TAXES from international transfers in Russia. We offer 10% percent from amount u receive and pay all fees, for sending funds back. Amount from 1000 euro per day. All this activity are legal in Europe, Thank you, FINANCIE LTD.”

Pharming



- Typing URL e.g. www.newegg.com
Translates to IP address 216.52.208.185
- DNS – a dictionary with pairs URL - IP
- What happens if somebody hacks DNS?
 - Instead of 216.52.208.185 ,
www.newegg.com might take us to
192.168.10.103
 - Usually, a false web page is there



Pharming

- How hard is it to perform DNS poisoning?
 - Local DNS cache
 - Local DNS
 - Wireless routers

Statistics for August 2006, APWG

- *Number of unique phishing reports received in August: **26150***
- *Number of unique phishing sites received in August: **10091***
- *Number of brands hijacked by phishing campaigns in Aug: **148***
- *Number of brands comprising the top 80% of phishing campaigns in August: **17***
- *Country hosting the most phishing websites: **United States***
- *Contain some form of target name in URL: **48 %***
- *No hostname just IP address: **36 %***
- *Percentage of sites not using port 80: **5.9 %***
- *Average time online for site: **4.5 days***
- *Longest time online for site: **31 days***

Phishing Prevention



- Public Education:
 - Do not believe anyone addressing you as a 'Dear Customer' 'Dear business partner', etc.
 - Do not respond to an e-mail requesting username, password, bank account number, etc.
 - Do not click on the link provided in an e-mail message
 - Report phishing or spoofed e-mails

Phishing Prevention



- Necessary software infrastructure:
 - Website authentication
 - Certificate
 - E-mail authentication
 - Digital signature
 - Anti-virus software



References

- Anti-Phishing Working Group
<http://www.antiphishing.org>
- The HoneyNet Project & Research Alliance: Behind the Scenes of Phishing Attacks
<http://www.honeynet.org>
- Phishing, M. E. Kabay, Norwich University
- Let's Go Phishing, MOREnet, University of Missouri
- You've Been Hacked, J. King, Bakersfield College



Thank You!

Phishing – Read Behind The Lines

Veljko Pejović
veljko@cs.ucsb.edu