How to Avoid Losing Your Money and Identity to Phishing

Tom Chen
tchen@engr.smu.edu
Outline

• What is Phishing?
• Examples
• Risks and threats
• Defenses
What is Phishing?

- A social engineering attack:
  - E-mail message (spam) appears from financial institution prompting user to a fake Website (eg, to verify your account)
  - Victim is tricked into submitting personal info. (account number, password) at fake Website
  - Fake Website steals confidential personal info. or downloads malicious code
Victims

- Consumers
- Financial organizations
  - Banks: Citibank, Wells Fargo, US Bank, NatWest, Barclays, Lloyds Bank,...
  - Credit card companies: VISA,...
  - Retailers: eBay, PayPal, Amazon,...
  - ISPs: AOL, MSN, Yahoo, Earthlink,...
Statistics

• $1.2 billion damages to US financial organizations so far

• In US, 57 million consumers have received phishing e-mail
  - 1.8 million consumers believe tricked (3% rate)

• Phishing sites are hosted mostly in US (32%), China (12%), Korea (11%), Japan (3%), others
December 2004 Statistics

- 1,707 active phishing Websites detected
- 24% monthly increase in phishing Websites
- Phishing Website is online for 5.9 days on average
- 55 brands hijacked
Nigeria 419 Scam

- Early example of spam used for online fraud
  - 419 is named after Nigerian criminal code
- Spam e-mail describes large funds or similar in Nigeria or other African nation (endless variations)
- User is asked for advance fee or similar to receive funds or goods
Nigeria 419 Scam

- Complications may require more advance fees until victim quits
  - Nothing is ever received

- Nigerian government is believed to running the scam, making $ billions from worldwide
  - A surprising number of people still fall victim to this scam monthly
Example 1: e-mail from Washington Mutual reports failed logins to online account and asks for confirmation of account info

---

Security Center Advisory!

Dear [Email Address],

We recently have determined that different computers have logged onto your Online Banking account, and multiple password failures were present before the logons.

We now need you to re-confirm your account information to us. If this is not completed by **December 5, 2004**, we will be forced to suspend your account indefinitely, as it may have been used for fraudulent purposes.

We thank you for your cooperation in this manner.

[Click here to verify your account]

Thank you for your prompt attention to this matter. Please understand that this is a security measure meant to help protect you and your account.

We apologize for any inconvenience.

If you choose to ignore our request, you leave us no choice but to temporarily suspend your account.

Thank you for using WAMU! The WAMU Team
Security Center Advisory!

Dear [Your Name],

We recently have determined that different computers have logged onto your Online Banking account, and multiple password failures were present before the logons.

We now need you to re-confirm your account information to us. If this is not completed by December 5, 2004, we will be forced to suspend your account indefinitely, as it may have been used for fraudulent purposes.

We thank you for your cooperation in this manner.

Click here to verify your account

Thank you for your prompt attention to this matter. Please understand that this is a security measure meant to help protect you and your account.

We apologize for any inconvenience.

If you choose to ignore our request, you leave us no choice but to temporarily suspend your account.

Thank you for using WAMU! The WAMU Team
Clues on Website: long, strange URL “http://218.62.80.234/openwebmail/wamusk/....”

IE shows rendering errors
After user logs in, the website asks for ATM/Visa check card info.

Finally, user is redirected to the real "wamu.com" site.
Example 2: e-mail asks for confirmation of eBay account or account will be suspended

From: eBay <eBay@eBay.com>
Subject: Account Violate The User Policy Second Notice
Date: December 1, 2004 5:25:40 AM CST
To: ipfix-arch-volunteers@net.doit.wisc.edu

Dear valued customer

We regret to inform you that your eBay account could be suspended if you don't re-update your account information. To resolve this problems please click here and re-enter your account information. If your problems could not be resolved your account will be suspended for a period of 24 hours, after this period your account will be terminated.

For the User Agreement, Section 9, we may immediately issue a warning, temporarily suspend, indefinitely suspend or terminate your membership and refuse to provide our services to you if we believe that your actions may cause financial loss or legal liability for you, our users or us. We may also take these actions if we are unable to verify or authenticate any information you provide to us.

Due to the suspension of this account, please be advised you are prohibited from using eBay in any way. This includes the registering of a new account. Please note that this suspension does not relieve you of your agreed-upon obligation to pay any fees you may owe to eBay.

Regards, Safeharbor Department eBay, Inc
The eBay team.
This is an automatic message. Please do not reply.
From: eBay <eBay@eBay.com>
Subject: Account Violate The User Policy Second Notice
Date: December 1, 2004 5:25:40 AM CST
To: ipfix-arch-volunteers@netid.wisc.edu

Dear valued customer,

We regret to inform you that your eBay account could be suspended if you don’t re-update your account information. To resolve this problems please click here and re-enter your account information. If your problems could not be resolved your account will be suspended for a period of 24 hours, after this period your account will be terminated.

For the User Agreement, Section 9, we may immediately issue a warning, temporarily suspend, indefinitely suspend or terminate your membership and refuse to provide our services to you if we believe that your actions may cause financial loss or legal liability for you, our users or us. We may also take these actions if we are unable to verify or authenticate any information you provide to us.

Due to the suspension of this account, please be advised you are prohibited from using eBay in any way. This includes the registering of a new account. Please note that this suspension does not relieve you of your agreed-upon obligation to pay any fees you may owe to eBay.

Regards, Safeharbor Department eBay, Inc
The eBay team.
This is an automatic message. Please do not reply.

Link calls “cgi3.ebay.com.wws2.us/update/aw-cgi/eBayISAPI.dll/index.html” intentionally similar to real eBay URL
Clues: fake Website looks real except not exact URL

IE shows rendering errors
Example 3: realistic e-mail from Amazon asking to verify account

Dear Amazon user,

During our regular update and verification of the accounts, we couldn’t verify your account information. Either your information has changed or it is incomplete.

Please update and verify your information below.

Sign in using our secure server

Sincerely,
Amazon Security Department

---

**Updating Subscriptions and Communication Preferences**

You can access your New for You subscriptions, Special Occasion Reminders, Available to order notifications, and other communication preferences directly through [Your Account].

When logging in, remember to enter the e-mail address and password currently associated with your account. If you do not have a customer account, we’ll ask you to create one first. Simply enter your e-mail address, indicate that you are a new customer, and click the Sign in using our secure server button. On the next page, we’ll ask you to enter your name and select a password.

---

**Forgot Your Password?**

We cannot tell you your current password, but we can certainly help you acquire a new one by sending a personalized link to your e-mail address. This way, you can securely change your password to whatever you want. If you visit us from a computer you have not used before, we will ask for complete verification of your account information before proceeding with the password change. [Reset your password now].

---

**Changing Your 1-Click Settings**

Your 1-Click settings allow you to ship all of your 1-Click orders efficiently in the way you decide is best. You are always welcome to change the credit card account, shipping address, and shipment method associated with your 1-Click settings. Any changes you make, however, will affect only future 1-Click orders. If you want to change the particulars of an order you’ve already placed, visit [Your Account].

Please note: It is currently not possible to change the billing address associated with your 1-Click settings.

Want to access or change your 1-Click settings now? [Log in to Your Account].
Dear Amazon user,

During our regular update and verification of the account, we couldn't verify your account information. Either your information has changed or it is incomplete.

Please update and verify your information below.

Sign in using our secure server

Sincerely,
Amazon Security Department
Looks realistic but "http", not "https"
Next page looks real too, asking for credit card info

Finally user is redirected to real Amazon site
Example 4: generic, plain email asks to verify Citibank account info.

From: support@citibank.com
To: 
Subject: Verify your E-mail with Citibank
Date: Wed, 31 Mar 2004 10:12:49 -0800
X-Server-Info: E17A4654-9A97-42C4-AB6D-5EE56B8E577
X-Message-Info: E17A4654-9A97-42C4-AB6D-5EE56B8E577
X-MMS-Spam-Confidence: E17A4654-9A97-42C4-AB6D-5EE56B8E577
X-MMS-Content-Rating: E17A4654-9A97-42C4-AB6D-5EE56B8E577
X-MMS-Spam-Filter-ID: E17A4654-9A97-42C4-AB6D-5EE56B8E577
X-W3S-ID: E17A4654-9A97-42C4-AB6D-5EE56B8E577

Dear Citibank Member,

This email was sent by the Citibank server to verify your E-mail address. You must complete this process by clicking on the link below and entering in the small window your Citibank ATM/Debit Card number and PIN that you use on ATM.

This is done for your protection - because some of our members no longer have access to their email addresses and we must verify it.

To verify your E-mail address and access your bank account, click on the link below:
https://web.da-us.citibank.com/signin/citif/scripts/email_verify.jsp

-----------------------------------------------------

Thank you for using Citibank

-----------------------------------------------------
Link to “https://web.da-us.citibank.com/signin/citifi/scripts/email_verify.jsp” actually goes to IP address 69.65.202.82 (registered to ThePlanet Internet Services)

From: support@citibank.com
To:  
Subject: Verify your E-mail with Citibank  
Date: Wed, 31 Mar 2004 10:12:49 -0000  
X-Server-Unit: B17A4654-9A97-42C4-AB6D-5EEB56B8E577  
X-Mime-Info: B17A4654-9A97-42C4-AB6D-5EEB56B8E577  
X-MMS-Confidence: B17A4654-9A97-42C4-AB6D-5EEB56B8E577  
X-MMS-Content-Rating: B17A4654-9A97-42C4-AB6D-5EEB56B8E577  
X-MMS-Filter-ID: B17A4654-9A97-42C4-AB6D-5EEB56B8E577  
X-MMS-ID: B17A4654-9A97-42C4-AB6D-5EEB56B8E577  

Dear Citibank Member,

This email was sent by the Citibank server to verify your E-mail address. You must complete this process by clicking on the link below and entering in the small window your Citibank ATM/Debit Card number and PIN that you use on ATM.

This is done for your protection - because some of our members no longer have access to their e-mail addresses and we must verify it.

To verify your E-mail address and access your bank account, click on the link below:
https://web.da-us.citibank.com/signin/citifi/scripts/email_verify.jsp

------------------------------------------------------------------

Thank you for using Citibank.
------------------------------------------------------------------
Convincing address bar shows “https://web.da-us.citibank.com/signin/citifi/scripts/email_verify.jsp”

But real address bar is actually covered by a fake address bar graphic using Javascript and frames
Clue: “https://web.da-us.citibank.com/signin/citifi/scripts/email_verify.jsp” should be secure HTTP

But browser does not show padlock icon at bottom
Another clue: going to another URL (Yahoo) still shows top frame that says “Welcome to Citi”
Example 5: email from SunTrust Bank promotes fee waiver but feature must be activated at Website

From: SunTrust <support@suntrust.com>
Subject: Internet Banking with Bill Pay Fees Waived
Date: November 30, 2004 8:50:30 AM CST
To: Tchen <tchen@engr.smu.edu>

Dear SunTrust Bank Customer,

SunTrust Internet Banking with Bill Pay has become even better. We are waiving monthly fees for SunTrust Internet Banking with Bill Pay and SunTrust PC Banking with Bill Pay for all our clients.

As an additional security measure, you need to activate this new feature by signing on to Internet Banking. Please verify your preferred email address and the information that SunTrust uses to confirm your identity.

In the Update Internet Banking service area you can also view the accounts you currently have tied to your Internet Banking service, to view whether Bill Pay is enabled on a particular account, and to request other accounts to be added to your Internet Banking service.

To do so, simply sign on to Internet Banking.

SunTrust Internet Banking
Dear SunTrust Bank Customer,

SunTrust Internet Banking with Bill Pay has become even better. We are waiving monthly fees for SunTrust Internet Banking with Bill Pay and SunTrust PC Banking with Bill Pay for all our clients.

As an additional security measure, you need to activate this new feature by signing on to Internet Banking. Please verify your preferred email address and the information that SunTrust uses to confirm your identity.

In the Update Internet Banking service area you can also view the accounts you currently have tied to your Internet Banking service, to view whether Bill Pay is enabled on a particular account, and to request other accounts to be added to your Internet Banking service.

To do so, simply sign on to Internet Banking.

SunTrust Internet Banking
Convincingly forged IE address bar shows “https://internetbanking.suntrust.com”

Properties page show real URL is “http://196.40.75.39/s/login.html”
After user logs in, Website asks for ATM/Visa check card info

IE status bar does not show secure HTTP session
Final “log-out” page...

Finally user is redirected to real “suntrust.com” site
Example 6: e-mail from MSN looks normal asking for verification of account...

Dear MSN Customer,

During one of our regular automatical verification procedures we’ve encountered a technical problem caused by the fact that we could not verify the information that you provided during registration.

We urgently ask you to submit your information so that we could fully verify your identity, otherwise an access to MSN services for your account will be deactivated until you pass verification process.

To submit your information please use our secure online application - apply here.

Thank you for using our services, MSN Payment Processing Department.

Reproduction any of the above information is strictly prohibited.

Copyright © 2005 Microsoft Network. © All rights reserved.
In HTML editor, text is actually an HTML table with letters in separate cells - to avoid spam filters.

The cell-per-symbol table, visible in an HTML editor.
Phish page opens in front of real MSN page, looking very similar

Phish page has no address bar to reveal actual URL, which is “www.msnassistance.com”
Next page asks for personal info...
Next page asks for credit card info...

Credit/Debit Card Information

Card Type: Visa

Financial Institution Name:

Full Name on Card:

Card number:

Expiration date: MM/YYYY

CVV code:

PIN-code:

VERIFY
Final log-out page...

Thank you

Try MSN Internet Software for FREE!

copyright 2005 Microsoft Corporation. All rights reserved. Terms of Use Advertise MSN Privacy Statement GetNetWise Anti-Spam Policy
Motivations

• Easy profits:
  - Phishing e-mails (like spam) are low cost to hit millions of people
  - Social engineering attack is low tech and easy to craft
  - Easy to register and set up phishing Websites (and move later)
  - Even low success rate (3% or perhaps higher) can be very profitable
Motivations (cont)

• Low risk
  - Phishing e-mail often sent through compromised “zombies” or open mail relays are hard to trace
  - Phishing Websites are registered with phony info and moved around frequently to different IP addresses
Risks and Threats

- **Identity theft**
  - Stolen bank accounts, passwords/PINs, social security numbers, addresses, credit card numbers

- **Websites can exploit browser vulnerabilities to download malicious code (viruses, Trojan horses, spyware) to victim PCs**
Defenses

- User education and awareness
  - Humans are weakest part of defenses
- Commercial products and services
  - Coordination groups
  - Spamtraps
  - Managed e-mail services
  - Fraud detection
  - Browser toolbars
User Awareness

• Users should look for telltale signs of phishing email
  - Lack of personalization, suspicious URLs, attachments, random or misspelled words, bad grammar, urgent tone

• Users should manually type URLs in browser, stay with known Websites, do not open attachments, check for known scams, use secure HTTPS connections
User Awareness (cont)

- But phishers have many tricks to fool even cautious users
  - HTML email can look like plain text and hide Javascript or invisible content
  - Similar URLs can be easily crafted by “1” instead of “I”, or “0” instead of “O”
  - Similar domain names can be registered
    - “mybank.com” could be confused with “mybank.com.us” or “mybank.fake.com”
User Awareness (cont)

• Many tricks (cont)
  - Host name obfuscation, eg, “http://mybank.com:login@210.10.3.5/index.htm” actually goes to IP address 210.10.3.5, not mybank.com
  - HTML allows graphics or complete pages to cover underlying pages

• Increasing user awareness will not be effective solution
Coordination Groups

- Anti-Phishing Working Group includes 706 financial institutions, online retailers, ISPs, law enforcement agencies
  - Collects voluntary submissions of phishing, analyzes examples, tracks statistics, raises public awareness

- Digital PhishNet includes Microsoft, AOL, Verisign, FBI, Secret Service
  - To coordinate info and shut down Websites
Coordination Groups (cont)

- Phish Report Network includes Microsoft, eBay, Visa, WholeSecurity
  - Collects submissions of new attacks, issue alerts to subscribers

- Trusted Electronic Communications Forum includes IBM, Fidelity, Charles Schwab, retailers, telecom companies
  - To find technological solutions, promote best practices, pursue legal action against
Spamtraps

- Spamtraps (e-mail honeypots) are computers loaded with fake e-mail accounts
  - Fake e-mail accounts are not used for legitimate purposes
  - Virtually all e-mail to spamtraps is spam
  - Spam is analyzed manually and automatically for new phishing attacks
  - Links lead to phishing Websites
Websense

- Websense Security Labs mines and analyzes over 24 million Websites daily
- Operates global honeynet (network of honeypots) to discover new attacks
- Software for client companies to automatically report suspicious Websites for analysis
- Classifies and reports threats to clients
Webwasher

- Operates honeypots to collect spam and analyze new phishing attacks
- Maintains database of known fraudulent sites
- Webwasher URL Filter blocks known fraudulent sites
- Webwasher AntiSpam filters e-mail for spam
NameProtect

- Working with MasterCard to detect phishing attacks in real time
- Continually monitors Websites, domain names, spam e-mail, to detect trademark or copyright infringement and fraudulent sites
Cyota

- FraudAction analyzes data from various probes, spamtraps, partners, to detect new phishing attacks
- Analysts create risk assessment reports for each attack
- Send alerts to client banks
MarkMonitor

- Fraud Protection service analyzes data from honeypots to identify new attacks
- Monitors chat rooms, newsgroups, domain registries
- Correlates data to identify potential threats
- Alerts clients about high risk threats to corporate brands
WebRoot Phish Net

• Phish Net encrypts personal data on PC and alerts user if PC is transmitting personal info

• WebRoot also keeps blacklist of known fraudulent sites, compares to visited Website
CoreStreet SpoofStick

- Toolbar prominently identifies real URL of visited Website
- Will not detect popups covering a legitimate site
Earthlink ScamBlocker

• Earthlink keeps list of known fraudulent sites
• Browser toolbar prevents loading known sites, redirects to Earthlink’s servers
• Depends on up-to-date list at Earthlink
GeoTrust TrustWatch

- GeoTrust rates Websites for trustworthiness and verifies by trusted third party
- Browser toolbar displays color code (green/yellow/red)
Conclusions

• Be very careful
  - New, more clever phishing scams can be expected

• Current defenses are educational and technological
  - Neither alone will be sufficient
  - Defenses are trying to keep up with attacks, not keep ahead