Phishing to Steal Your PC, Money, and Identity

Tom Chen
SMU
tchen@ engr.smu.edu
Outline

- What is Phishing?
- Threats
- Defenses (Research?)
What is Phishing?

- A social engineering attack:
  - Email message (type of spam) appears from financial institution asking to verify your account or transaction
  - Victim submits account info. 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,...
Example 1: email from Washington Mutual reports failed logins to online account and asks for confirmation of account info

Security Center Advisory!

Dear [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
Link to IP address 218.68.80.234 (in China)

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 WAMUI! The WAMU Team
Clues: Website shows long, strange URL “http://218.62.80.234/openwebmail/wamusk/...”

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

Finally user is redirected to real “wamu.com” site
Example 2: text message claims problem with Earthlink payment... User fills in form and emails to “invoice-apply@earthling.net”

No fake Website used in this case
Example 3: email 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](https://www.ebay.com/reupdate) 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@net.dit.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.
Clues: fake Website looks real except not exact URL

IE shows rendering errors
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-Uid: B17A4654-8A97-42C4-AB6D-5EBE56B8E577
X-Message-Info: B17A4654-8A97-42C4-AB6D-5EBE56B8E577
X-MMS-Spam-Confidence: B17A4654-8A97-42C4-AB6D-5EBE56B8E577
X-MMS-Content-Rating: B17A4654-8A97-42C4-AB6D-5EBE56B8E577
X-MMS-Spam-Filter-ID: B17A4654-8A97-42C4-AB6D-5EBE56B8E577
X-WSS-ID: B17A4654-8A97-42C4-AB6D-5EBE56B8E577

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 -0800

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/citifi/scripts/email_verify.jsp

Thank you for using Citibank.
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
Clue: going to another URL (Yahoo) still shows top frame that says “Welcome to Citi”
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
Clues: forged IE address bar shows “https://internetbanking.suntrust.com”

Properties page shows 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
Statistics

• $1.2 billion damages to US financial organizations so far

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

• Phishing sites are hosted mostly in US (29%), China (16%), Korea (9%), Russia (8%), others
October 2004 Statistics

- 6,597 new unique phishing messages and 1,142 active phishing Web sites detected
- 25% monthly increase in phishing Websites
- Phishing Website is online for 6.4 days on average
- 44 brands hijacked (banks, credit card companies, retailers,...)
Motivations

- Easy profits:
  - Phishing emails (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 Web sites (and move later)
  - Even low success rate (3% or perhaps higher) can be very profitable
Motivations (cont)

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

- Identity theft
  - Stolen bank accounts and passwords/PINs
  - Stolen social security numbers, addresses
  - Stolen credit card numbers
- Download spyware to victim PC to eavesdrop
- Infect victim with virus
Defenses

• User education and awareness
• Commercial products and services
  - Spamtraps
  - Managed email 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 type URLs in browser, stay with known Websites, do not open attachments, check for known scams
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 “l”, 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
Spamtraps

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

• Phishing continues social engineering in modern vectors (email + Web)
  - Will keep increasing as long as it works

• Current defenses are educational and technological
  - Defenses are trying to keep up with attacks, not keep ahead