CNCERT/CC

Phishing:

New Internet Financial Fraud Trend

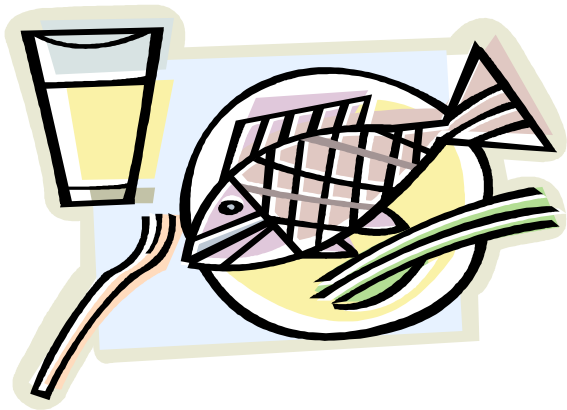
by Yuejin Du

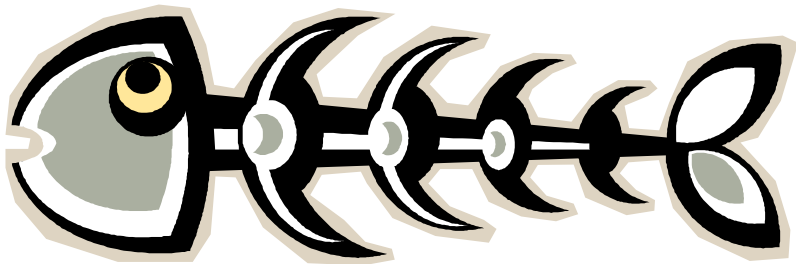
CNCERT/CC

Feb. 24th. 2005 APRICOT

www.cert.org.cn

Attendee Investigation





Contents

- Overview of Phishing
- Trends: Phishing is becoming one of the most popular Internet incidents
- Technique Issues: from both sides
- Anti-Phishing Activities of CNCERT/CC

Overview of Phishing

What is Phishing?

Phishing attacks use 'spoofed' e-mails and fake websites designed to bamboozle recipients into revealing confidential information with economic value such as credit card numbers, account usernames and passwords, social security numbers, etc.

Basic components of Phishing attack

- ‘fish’: (Identity , then money of) you—customer of Internet Bank or e-commerce
- ‘bait’: spam & story
- ‘fishhook’: fake website or Phishing Site /Trojan /Spyware
- ‘fisher’: somebody hidden somewhere

Sample of Spoofed Email

Dear US Bank Customer,

Recently there have been a large number of identity theft attempts targeting US Bank Customers.
In order to safeguard your account, we require that you confirm your banking details.

This process is mandatory, and if not completed within the nearest time your account or credit card may be subject to temporary suspension.

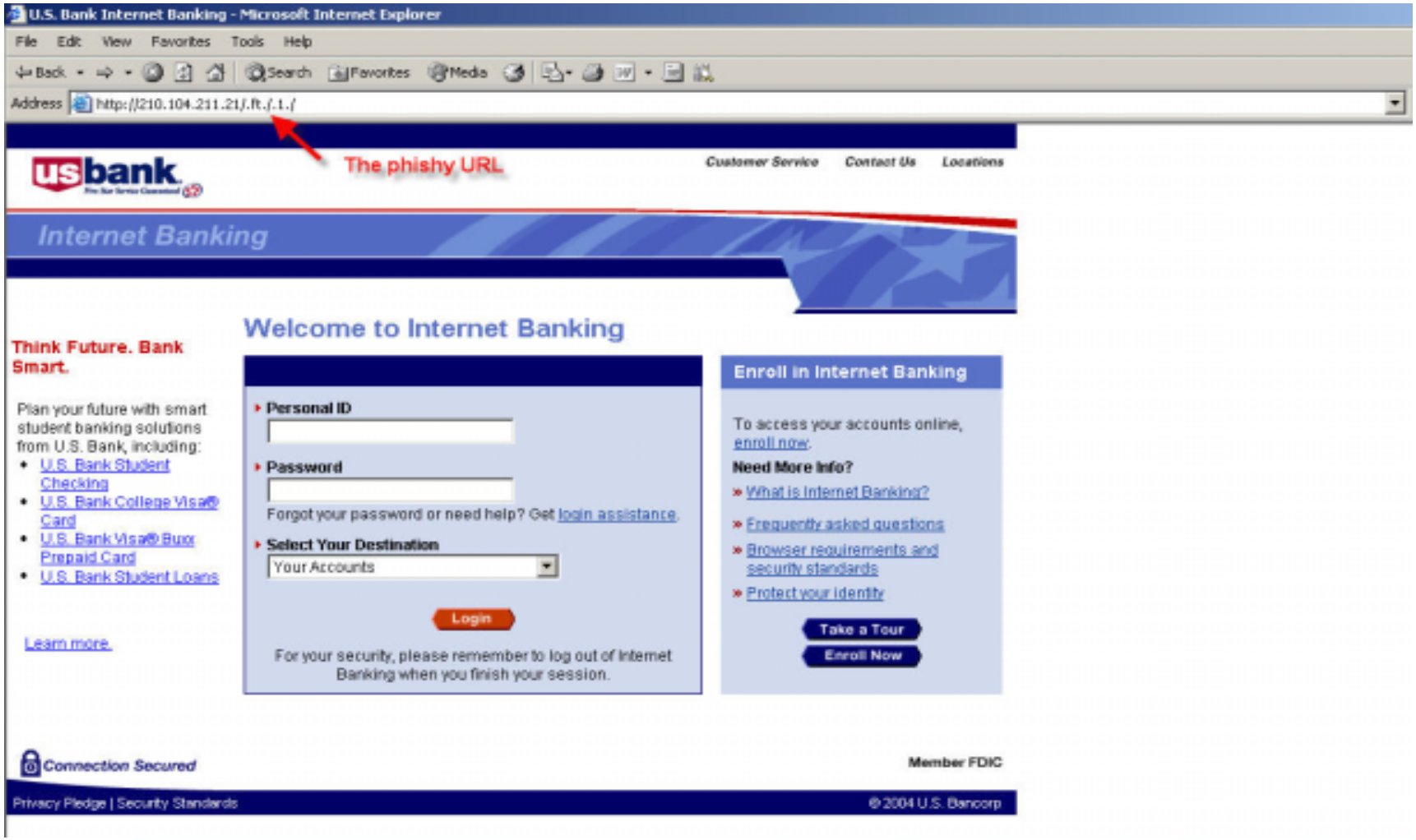
To securely confirm your US Bank Account details please follow the link:

https://www.usbank.com/internetBanking/RequestRouter?requestCmdId=upt

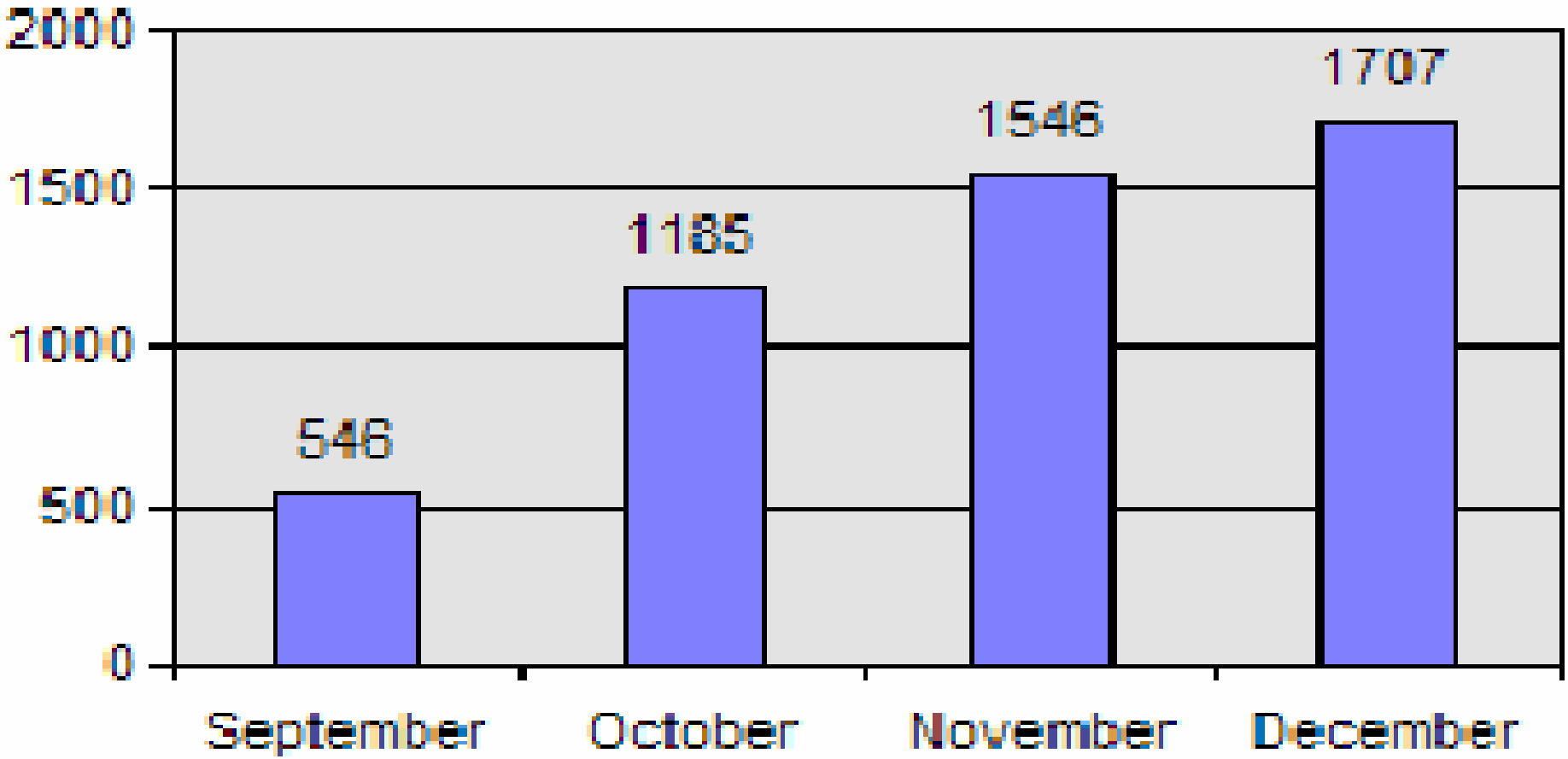
Note: You may have to report this message as "Not Junk Mail" if update link does not work.

Thank you for your prompt attention to this matter and thank you for using US Bank.

Fake Web Site — Phishing Site



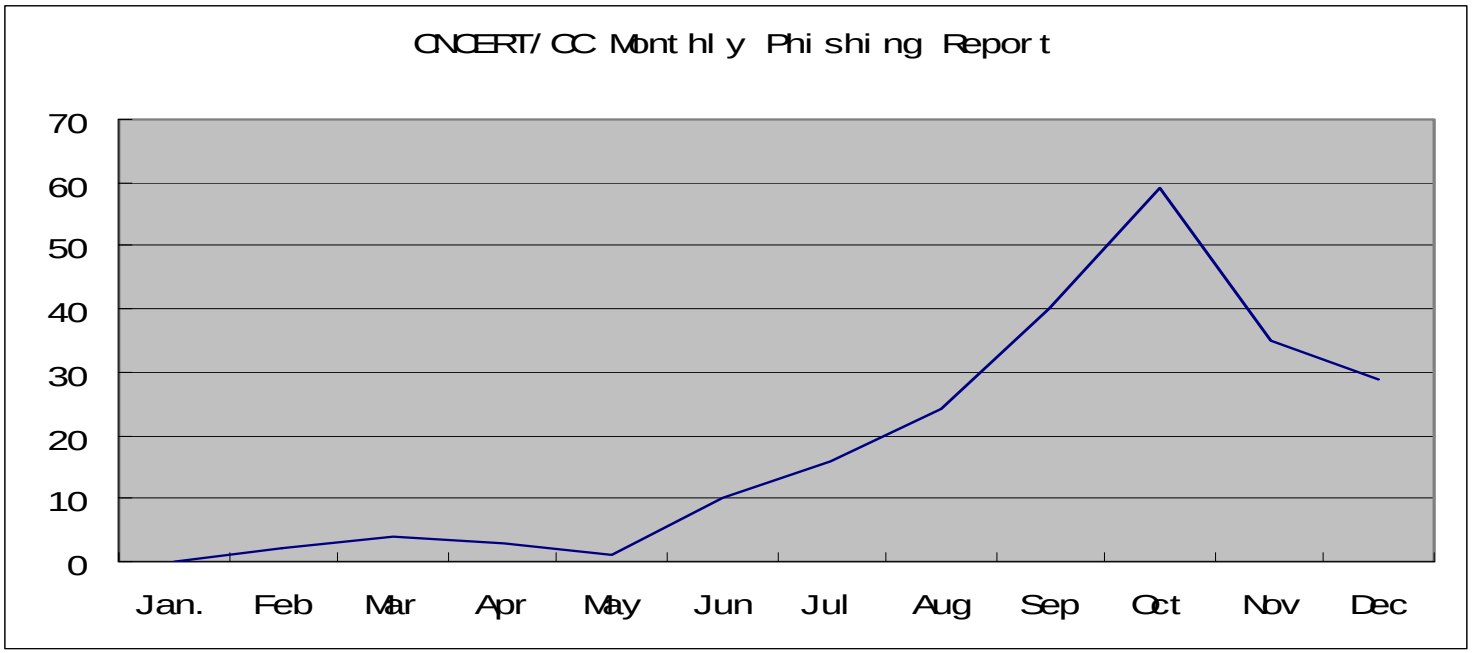
Active Reported Phishing Sites by Month September-December 2004



Data comes from APWG

Phishing Reports CNCERT/CC received

- During the year of 2004, CNCERT/CC had received 223 Phishing reports from over 33 worldwide financial and security organization.

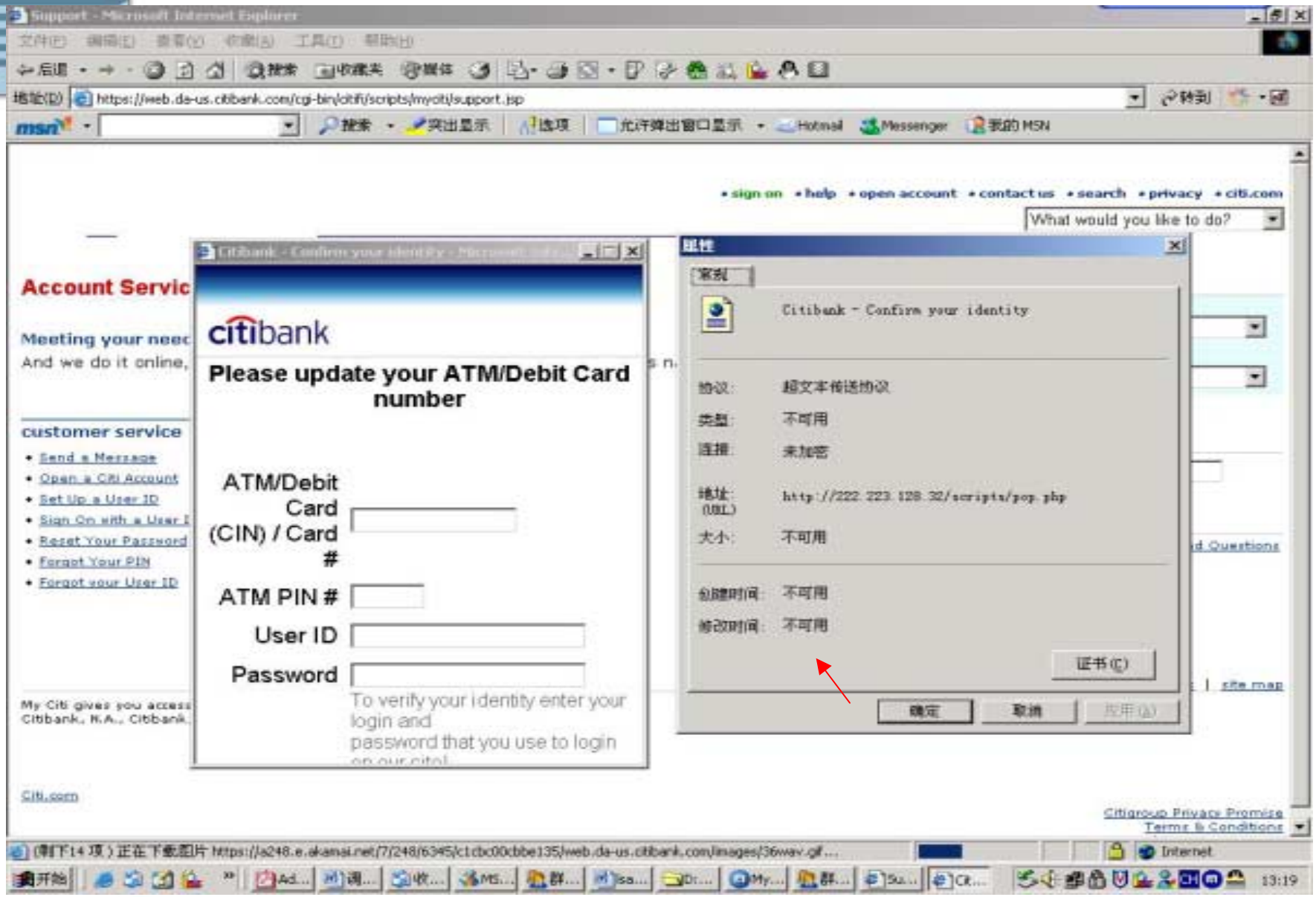


Tech. Issues: Phishing & Anti-Phishing

- Method 1 (of ‘fisher’): using alike url & similar webpages
  - ablc.com vs ab1c.com
  - abc.com vs abc.com.cn
- Rule 1 (of ‘fish’): Confirm the correct URL of the real target you wanna access

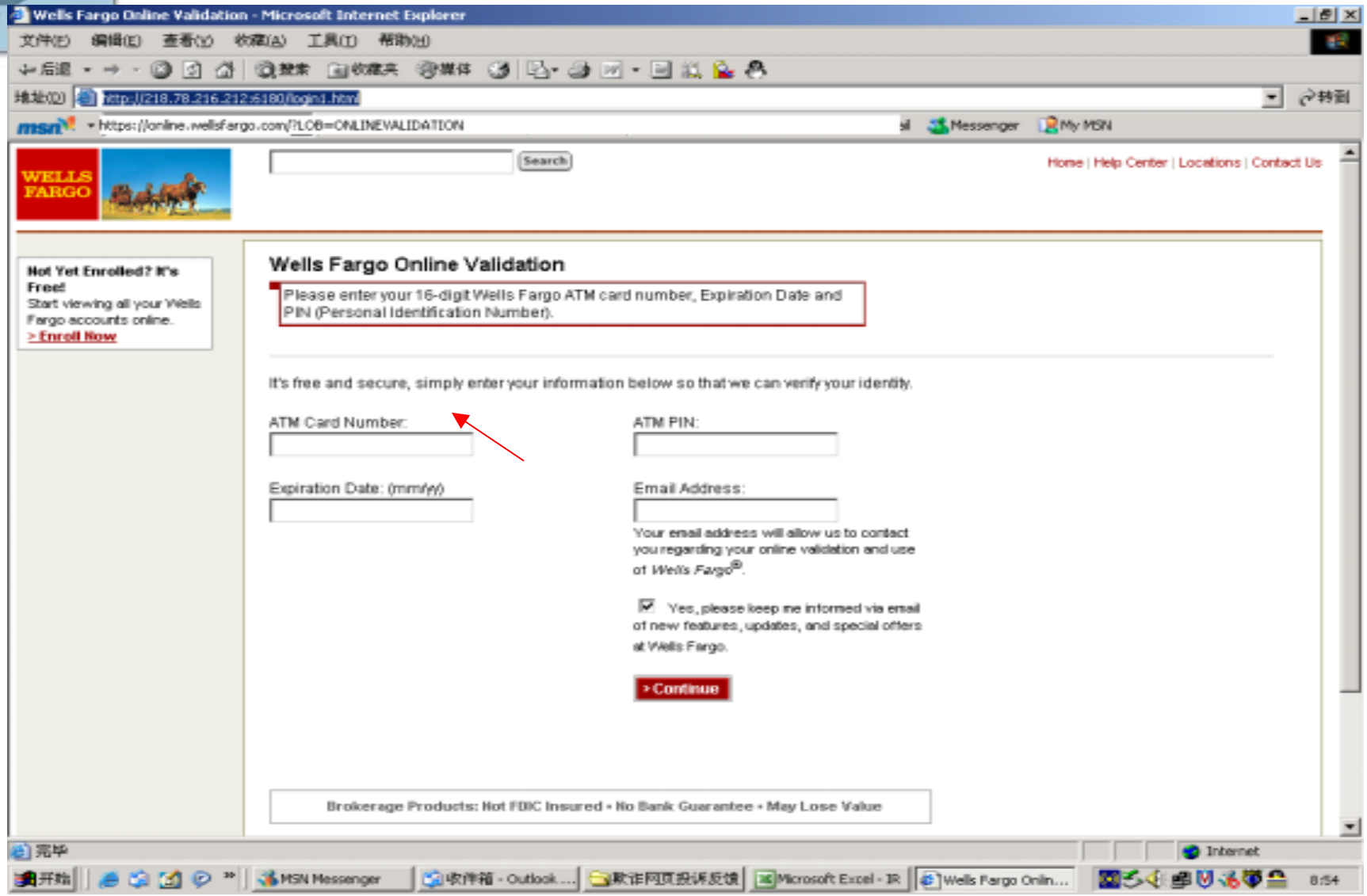
Tech. Issues (cont.)

- Method 2: Real website but fake pop-up windows
- Rule 2: Watch out pop-up windows
- Tip: some banks announced that they never use pop-up windows in their websites


Support - Microsoft Internet Explorer
https://web.da-us.citibank.com/cgi-bin/citifi/scripts/myciti/support.jsp
sign on
help
open account
contact us
search
privacy
citi.com
What would you like to do?
Account Servic
Meeting your need
And we do it online.
customer service
Send a Message
Open a Citi Account
Set Up a User ID
Reset Your Password
Forgot Your PIN
Forgot your User ID
citibank
Please update your ATM/Debit Card number
ATM/Debit Card (CIN) / Card #
ATM PIN #
User ID
Password
To verify your identity enter your login and password that you use to login
Citibank - Confirm your identity
协议: 超文本传送协议
类型: 不可用
连接: 未加密
地址 (URL): http://222.223.128.32/scripts/pop.php
大小: 不可用
创建时间: 不可用
修改时间: 不可用
证书(C)
确定
取消
site map
Citi.com
Citigroup Privacy Promise
Terms & Conditions
Internet

Tech. Issue (cont.)

- Method 3: Try to hide the real URL information in your browser
- Rule 4: Check that information
- Tip: usually this is not difficult to find out


Wells Fargo Online Validation - Microsoft Internet Explorer
https://online.wellsfargo.com/?LOB=ONLINEVALIDATION
Messenger
My MSN
WELLS FARGO
Search
Home | Help Center | Locations | Contact Us
Not Yet Enrolled? It's Free!
Start viewing all your Wells Fargo accounts online.
> Enroll Now
Wells Fargo Online Validation
Please enter your 16-digit Wells Fargo ATM card number, Expiration Date and PIN (Personal Identification Number).
It's free and secure, simply enter your information below so that we can verify your identity.
ATM Card Number:
ATM PIN:
Expiration Date: (mm/yy)
Email Address:
Your email address will allow us to contact you regarding your online validation and use of Wells Fargo®.
Yes, please keep me informed via email of new features, updates, and special offers at Wells Fargo.
> Continue
Brokerage Products: Not FDIC Insured • No Bank Guarantee • May Lose Value
完毕
Internet
MSN Messenger
Microsoft Excel - IR
Wells Fargo Onlin...
8:54

Tech. Issue (cont.)

- Method 4: use IE vulnerabilities to make the browser ‘lie’ to you
- Rule 4: Update your system on time ; or try to check the source code of a web page
- Tip: this might be difficult for some Internet users

Tech. Issue (cont.)

- ‘Ultimate’ Rules?
  - Do not click the hyperlink in the uncertain emails? Inputting the URL by yourself instead of just clicking the hyperlink, is an effect rule for a lot of attack methods.
  - Do not open the email attachments;
  - ….
- ‘Ultimate’ Methods:
  - Use monitor program in your computer like a spy, steal the valuable information and then try to send it out; or just hijack DNS to make the ‘ultimate rule’ useless
  - Plenty of ways for planting the malicious program into your computer:
    - Use IE vulnerabilities to plant particular trojans into your computer: Try to redirect your access to particular website which contains malicious code , then the malicious code can use the IE vulnerablity to plan the spyware into your computer (we discovered about 1200 such websites in 2004)
    - Use other vulnerabilities to put malicious code or spyware into your computer
- Tip: Do not use Internet……?

Multi-parts should be responsible for Anti-phishing

- Bank/Financial organization: ensure that their website is uneasy to be imitated or mimic. Also, responsible to provide the security awareness education.
- LEA: catch the criminals and to make them be punished
- Vendors/Industry side: provide techniques and products for anti-phishing
- Internet User / IDC (Host owners) : protect their hosts so that they are not easy to be abused by bad guys.
- Customers (financial customers) : aware how to protect themselves from being cheated
- CSIRTs: ?

CSIRTs' responsibility on anti-phishing

- Incident handling: locate the phishing site and try to shut it down asap, so that less customers will be cheated
- Tech. support: for data analysis; malicious code analysis;
- Awareness and training: make more users aware
- Coordination:

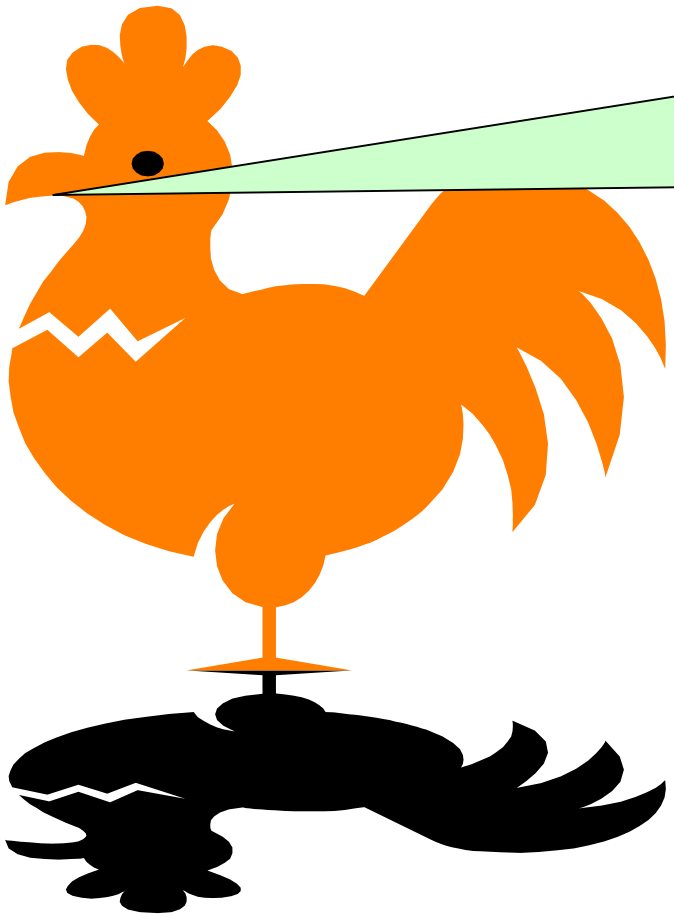
Difficulties for handling Phishing Incidents

- Host the fake websites in other countries
- Locate and communicate with the fake website host owners (they are also victims), seeking for their cooperation
- Technique barriers, e.g. visitor IP filter in one of the cases
- Related to legislation issues; anti-spam; vulnerability handling; anti malicious code; anti Botnet; etc

What CNCERT/CC is Doing

- receive report and investigate the info of the host, such as the location, owner, ISP.
- CNCERT/CC's certain branch convince the host owner to take the site down, provide the data, tech support and security consultant. (CERT is not police, and host owner is also a victim. CERT may only convince host owner to cooperate.)
- Provide awareness education and consultant to the public
- Effectiveness: reduced phishing site number and percentage in the end of the year; APWG partner;

Q & A



Happy New Rooster Year !

dyj@cert.org.cn