



The Rise of Phishing

Dave Brunswick

Tumbleweed Communications

Anti-Phishing Working Group

The Anti-Phishing Working Group



- Industry association formed in response to the growing problem of phishing
- Founded in 2003 by Tumbleweed Communications, ISPs, Law Enforcement, and Financial Institutions
- First meeting November 2003
- Now over 250 members
- www.antiphishing.org
- Report phishing to reportphishing@antiphishing.org

Anti-Phishing Working Group
Committed to wiping out Internet scams and fraud

What is Phishing?
Phishing attacks use 'spoofed' e-mails and fraudulent websites designed to fool recipients into divulging personal financial data such as credit card numbers, account usernames and passwords, social security numbers, etc. By hijacking the trusted brands of well-known banks, online retailers and credit card companies, phishers are able to convince up to 5% of recipients to respond to them.

Mar 2004 - May 2004

Week	Cumulative Phishing Attacks	Weekly Phishing Attacks
3/26/2004	100	679
4/2/2004	443	723
4/9/2004	1081	181
4/16/2004	1363	136
4/23/2004	1641	279
4/30/2004	1972	278
5/7/2004	2151	231
5/14/2004	2419	279
5/21/2004	2740	268
5/28/2004	3050	321
6/4/2004	3319	310
6/11/2004	3681	369

APWG Members

- Over 400 members
- Over 250 companies
- 8 of the top 10 US banks
- 4 of the top 5 US ISPs
- Over 100 technology vendors
- Law enforcement from Australia, Canada, UK, USA

APWG Working Groups

- Best Practices
- Education
- Future Threat Models
- Phishing Repository
- Sizing the Problem
- Solution Evaluation/Trial
- Law Enforcement

APWG SPONSORS:

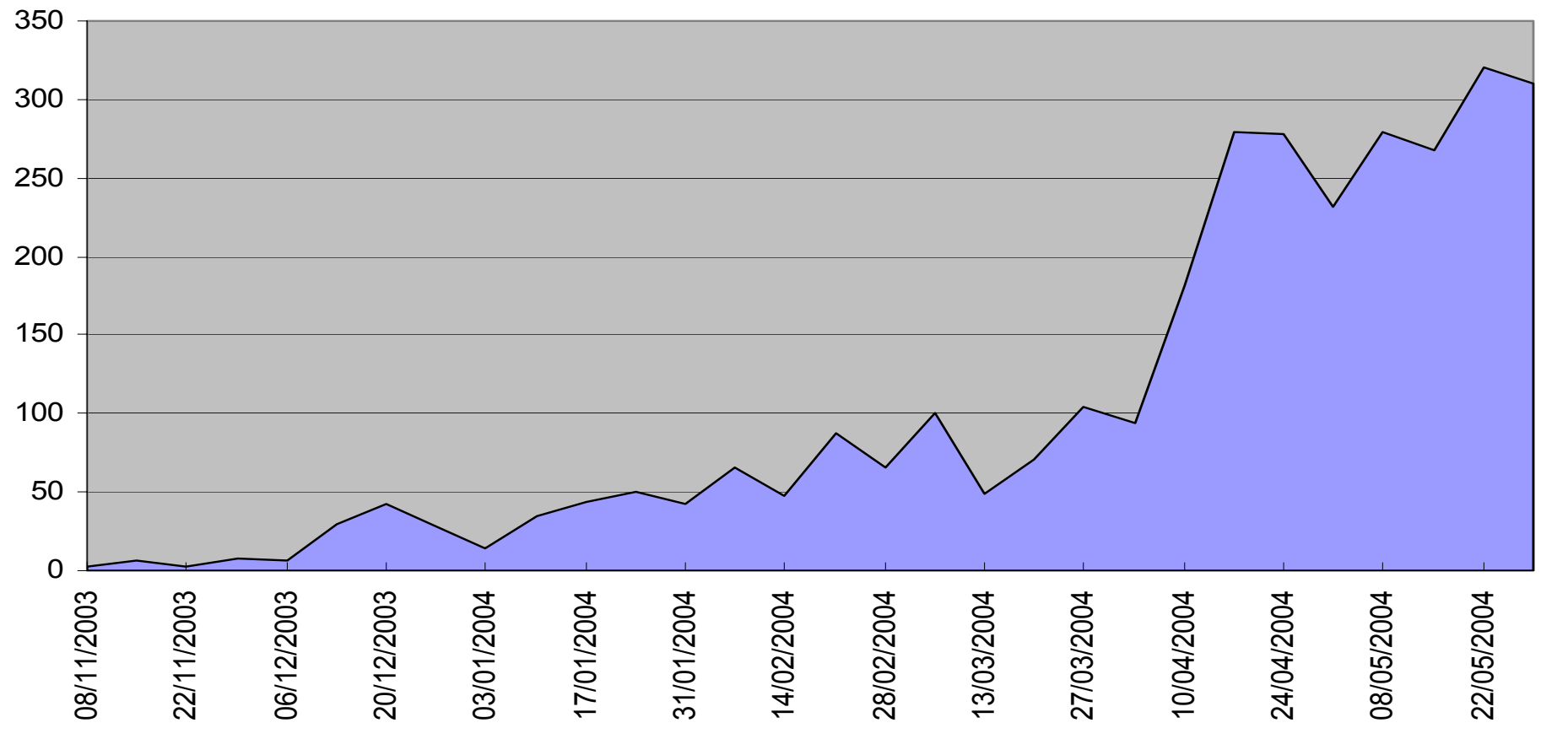
- Microsoft
- NameProtect

Phishing attacks use 'spoofed' e-mails and fraudulent websites designed to fool recipients into divulging personal financial data such as credit card numbers, account usernames and passwords, social security numbers, etc.

- **First known attacks on AOL accounts in 1996**
- **Sporadic attacks up until 2003, mainly AOL, eBay and PayPal**
- **Major growth from mid-2003 until present day**
 - » Focus on English language – U.S.A, Australia and U.K.
- **2004 – first non-English language attacks on Swiss Banks**
- **Increasing sophistication of attacks**

The Growth of Phishing

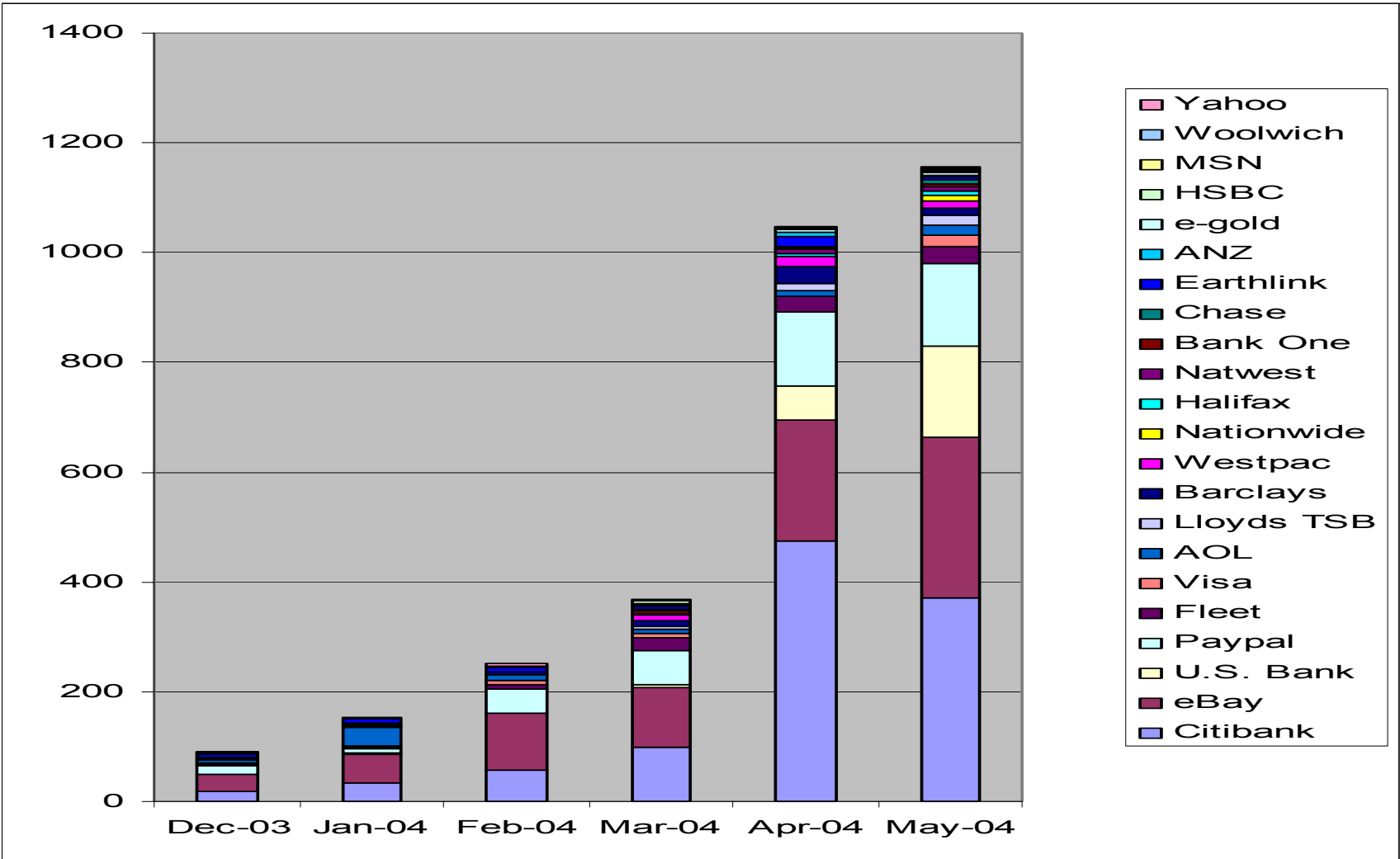
Unique Phishing Attacks (to end May 2004)

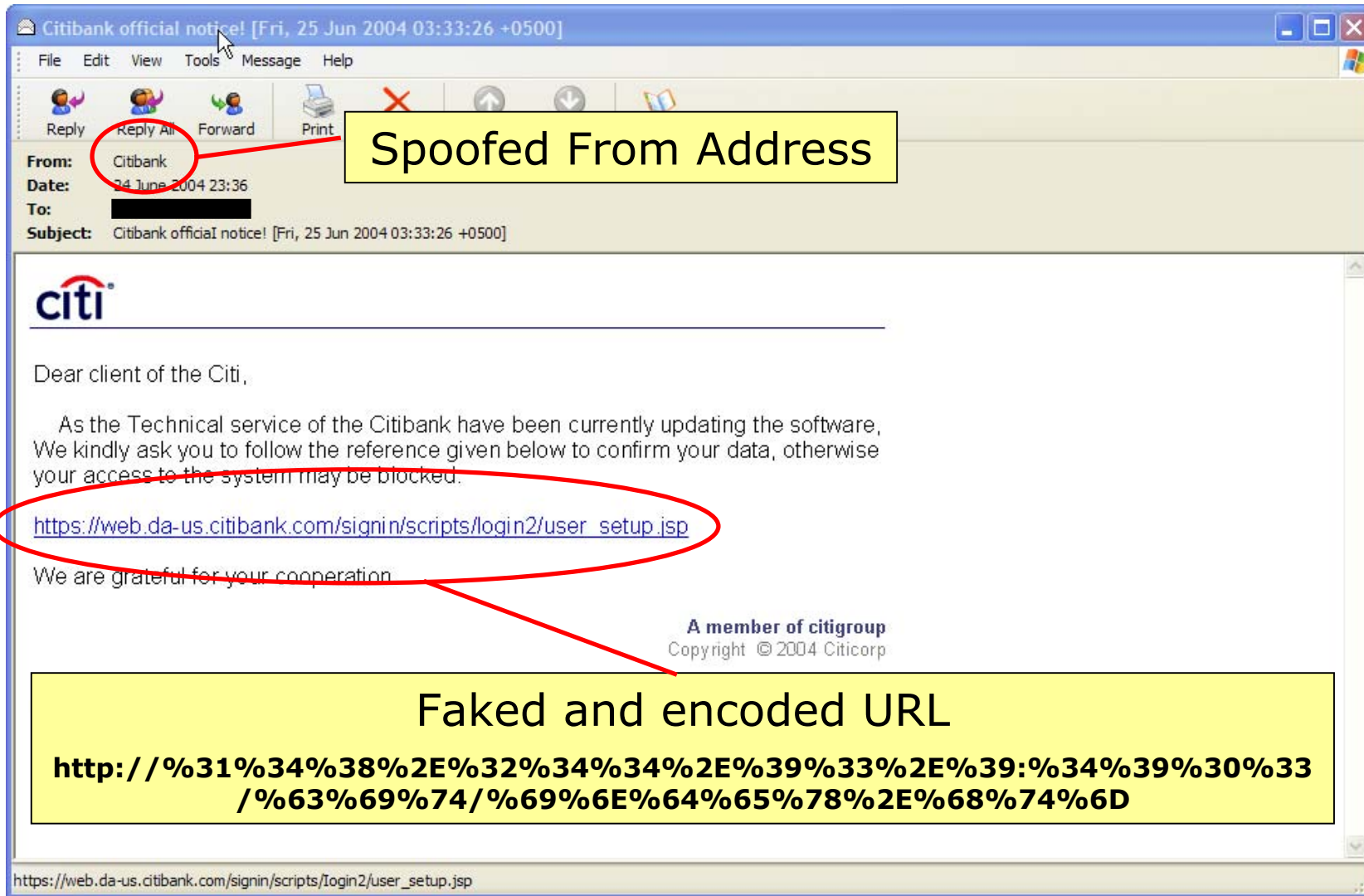


Phishing Targets (May)

	May-04	Apr-04	Mar-04	Feb-04	Jan-04	Dec-03
Citibank	370	475	98	58	34	17
eBay	293	221	110	104	51	33
U.S. Bank	167	62	4	0	2	0
Paypal	149	135	63	42	10	16
Fleet	33	28	23	9	2	1
Visa	21	0	7	8	2	4
AOL	17	9	10	10	35	4
Lloyds TSB	17	15	4	0	1	1
Barclays	15	31	11	6	1	1
Westpac	12	17	10	0	3	1
Nationwide	10	0	0	0	0	0
Halifax	9	6	1	0	1	0
Natwest	7	6	2	0	0	1
Bank One	6	4	5	0	0	1
Chase	6	3	2	0	0	0
Earthlink	6	18	5	8	9	6
ANZ	4	7	4	0	0	3
e-gold	3	5	2	2	0	2
HSBC	3	3	4	0	1	0
MSN	3	0	0	0	0	0
Woolwich	3	0	0	0	0	0
Yahoo	3	2	3	4	2	0

Phishing Targets (to May 2004)





Citibank official notice! [Fri, 25 Jun 2004 03:33:26 +0500]

File Edit View Tools Message Help


Reply Reply All Forward Print

From: Citibank

Date: 24 June 2004 23:36

To: [REDACTED]

Subject: Citibank official notice! [Fri, 25 Jun 2004 03:33:26 +0500]



Dear client of the Citi,

As the Technical service of the Citibank have been currently updating the software, We kindly ask you to follow the reference given below to confirm your data, otherwise your access to the system may be blocked.

https://web.da-us.citibank.com/signin/scripts/login2/user_setup.jsp

We are grateful for your cooperation.

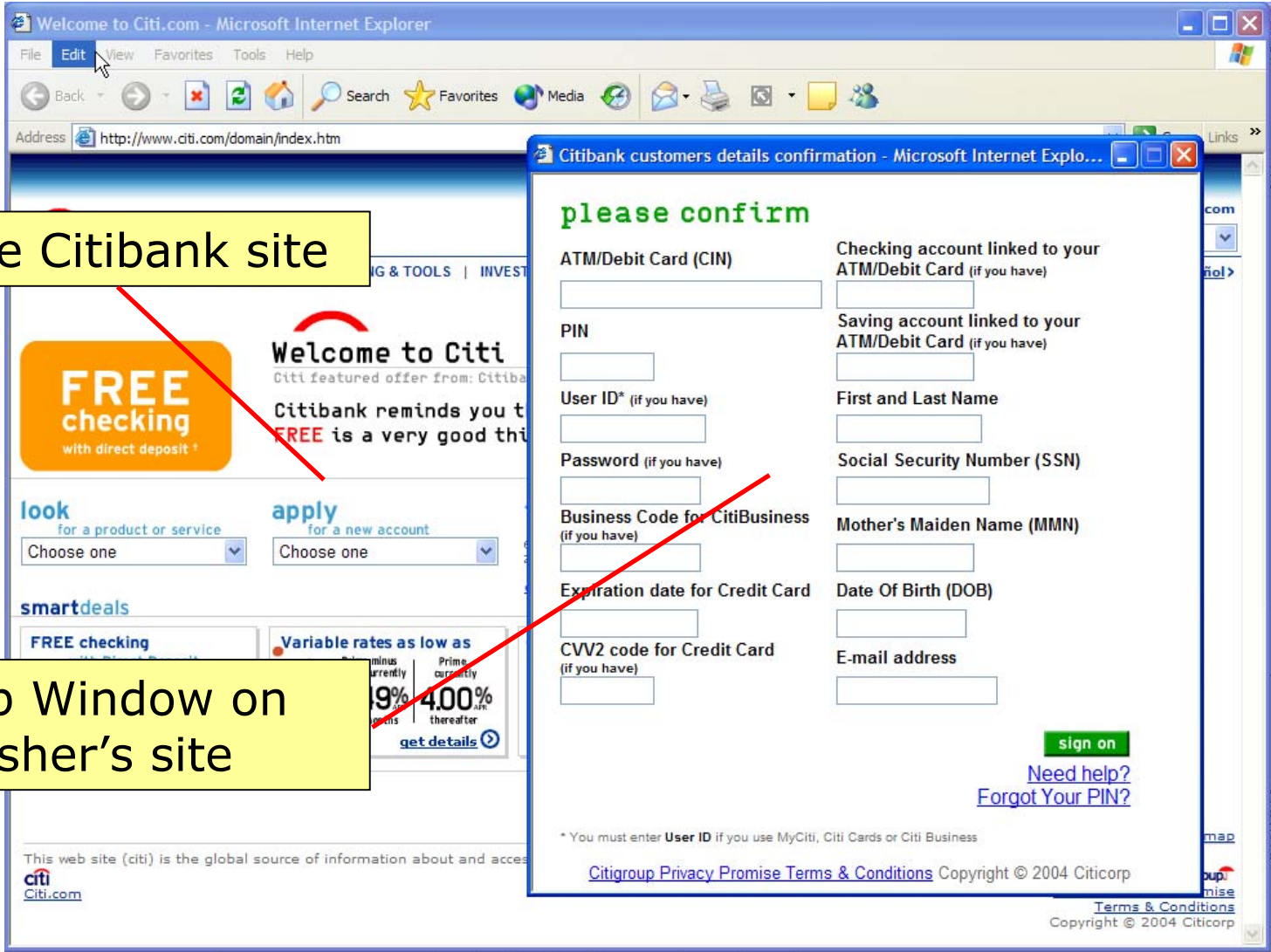
A member of citigroup
Copyright © 2004 Citicorp

Faked and encoded URL

http://%31%34%38%2E%32%34%34%2E%39%33%2E%39:%34%39%30%33/%63%69%74/%69%6E%64%65%78%2E%68%74%6D

https://web.da-us.citibank.com/signin/scripts/login2/user_setup.jsp

Typical Website

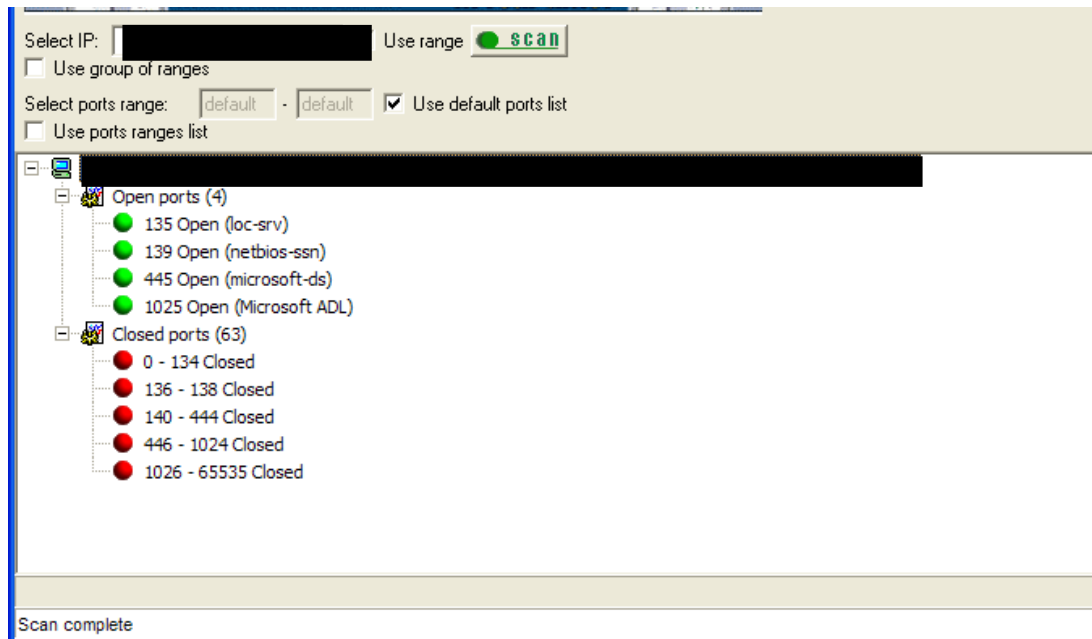


Genuine Citibank site

Popup Window on Phisher's site

- **Email sources**

- » Majority relayed through compromised adsl/cable connected Windows machines
- » 95% of FROM: addresses spoofed

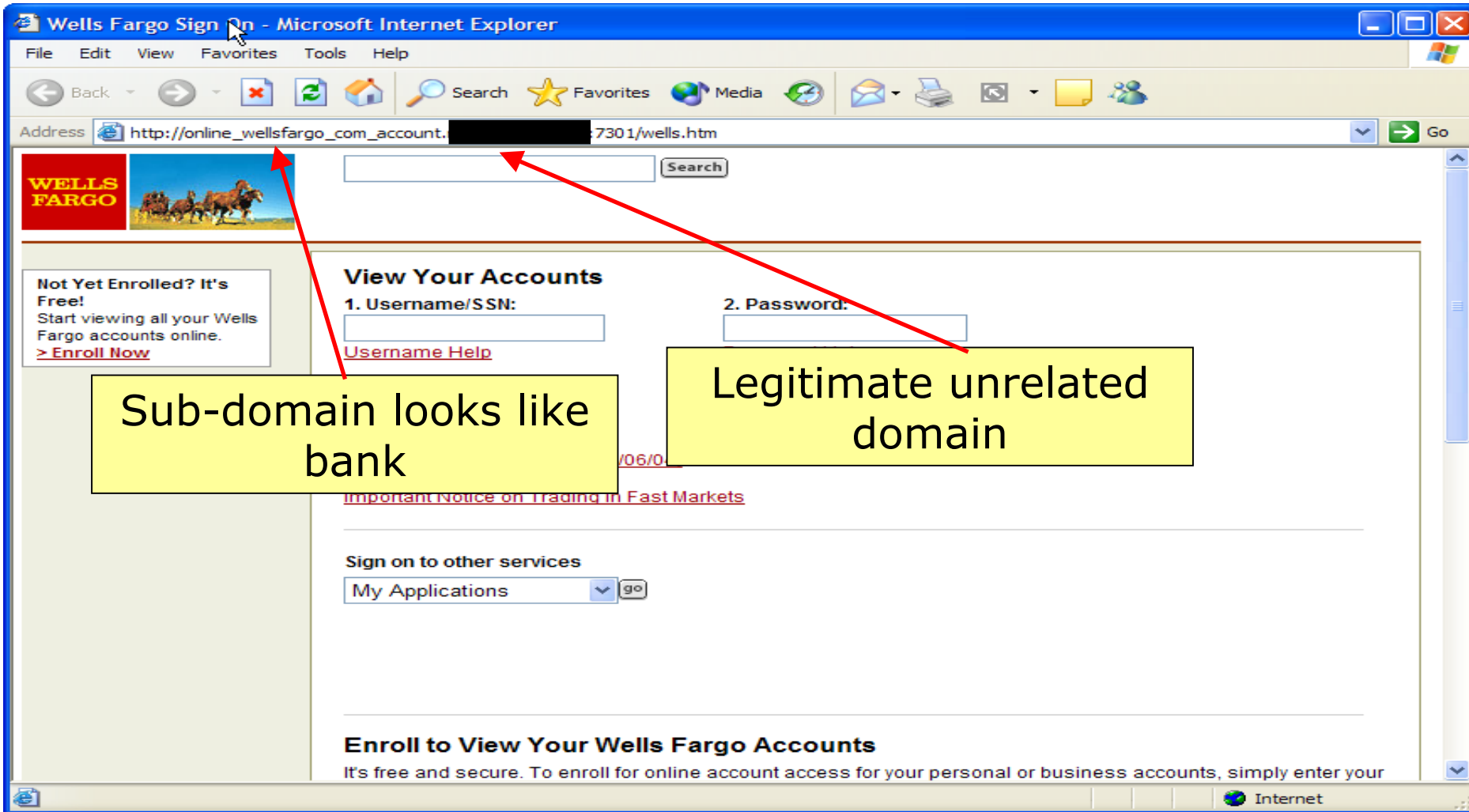


- **Websites**

- » Compromised Windows Cable/ADSL machines
 - Worms/trojans/backdoors
 - Open remote access services (VNC)
- » Subverted legitimate sites
 - Wide open/badly configured machines
 - Unpatched vulnerabilities
- » Throw away hosting

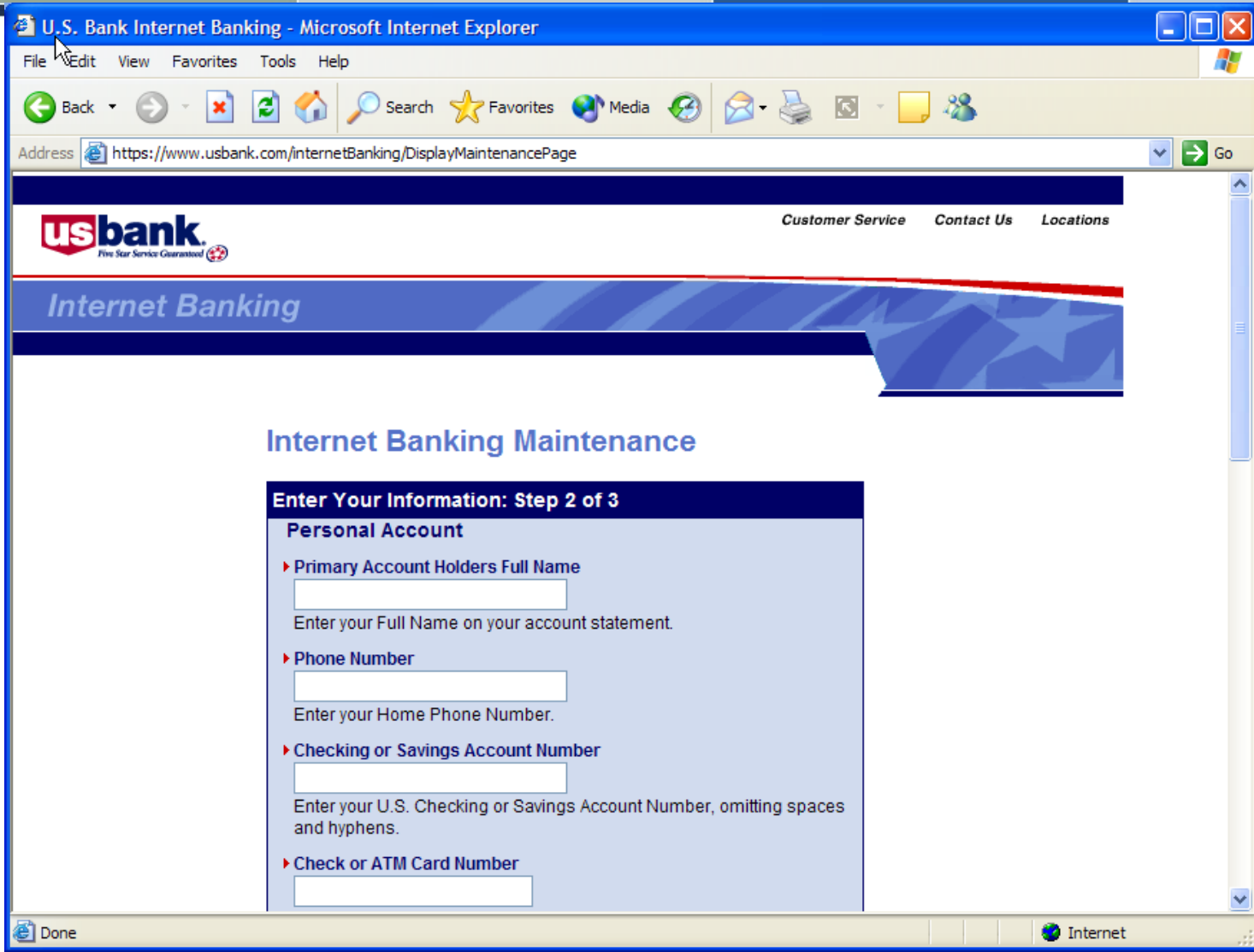
- **Email should not be traceable**
- **Web site should not be traceable**
- **Money should not be traceable**
- **User needs reason to give details:-**
 - » “your account will be deactivated...”
 - » “fraud on your account...”
 - » “win a prize...”
- **Web site should look convincing:-**
 - » Correct colours/logos
 - » Not given away by URL.....

Hiding the URL



The screenshot shows a Microsoft Internet Explorer browser window titled "Wells Fargo Sign On - Microsoft Internet Explorer". The address bar contains the URL "http://online_wellsfargo_com_account.[REDACTED]:7301/wells.htm". The page content includes a Wells Fargo logo, a search bar, and a sign-on form with fields for "1. Username/SSN:" and "2. Password:". Two yellow callout boxes with red arrows pointing to the URL and the password field contain the text "Sub-domain looks like bank" and "Legitimate unrelated domain" respectively. The browser interface includes standard menu items (File, Edit, View, Favorites, Tools, Help) and navigation buttons (Back, Forward, Stop, Refresh, Home, Search, Favorites, Media, Print, Stop, Go).

Hiding the URL



The screenshot shows a Microsoft Internet Explorer browser window with the following details:

- Title Bar:** U.S. Bank Internet Banking - Microsoft Internet Explorer
- Menu Bar:** File, Edit, View, Favorites, Tools, Help
- Address Bar:** https://www.usbank.com/internetBanking/DisplayMaintenancePage
- Page Content:**
 - usbank** logo with "Five Star Service Guaranteed" tagline.
 - Navigation links: [Customer Service](#), [Contact Us](#), [Locations](#)
 - Section header: **Internet Banking**
 - Main heading: **Internet Banking Maintenance**
 - Form section: **Enter Your Information: Step 2 of 3**
 - Personal Account**
 - Primary Account Holders Full Name**

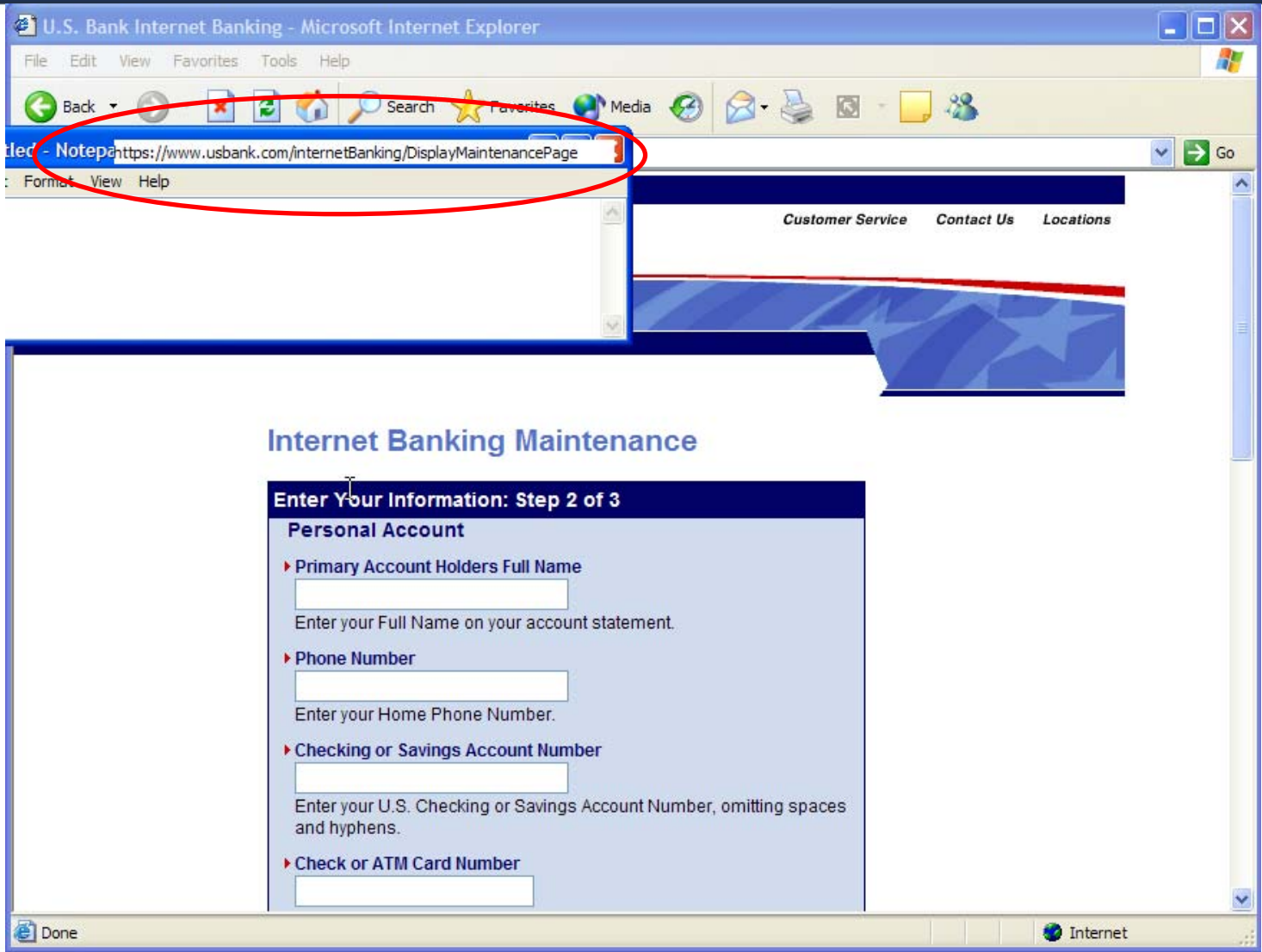
Enter your Full Name on your account statement.
 - Phone Number**

Enter your Home Phone Number.
 - Checking or Savings Account Number**

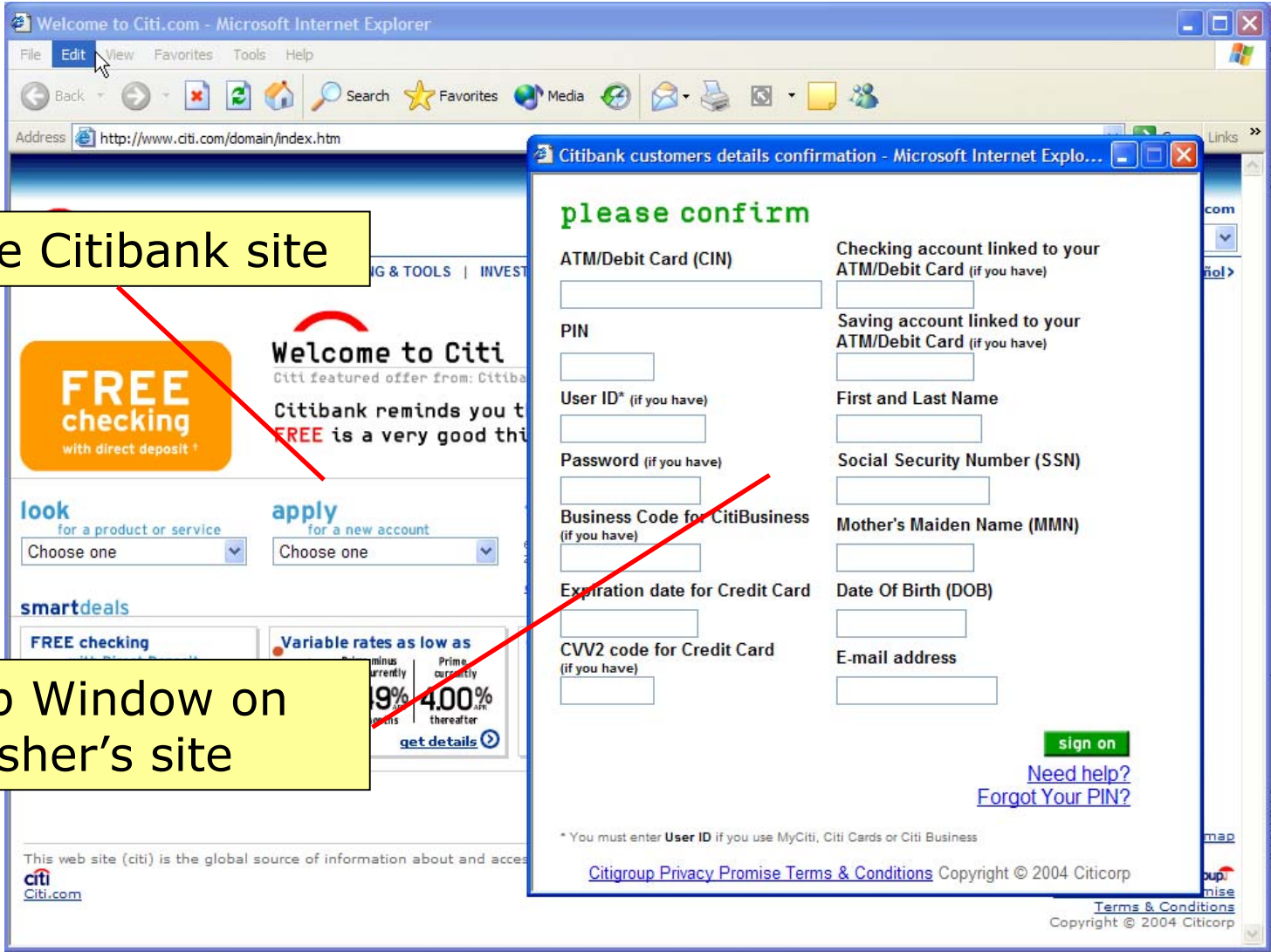
Enter your U.S. Checking or Savings Account Number, omitting spaces and hyphens.
 - Check or ATM Card Number**

- Status Bar:** Done, Internet

Hiding the URL: Pop up name window



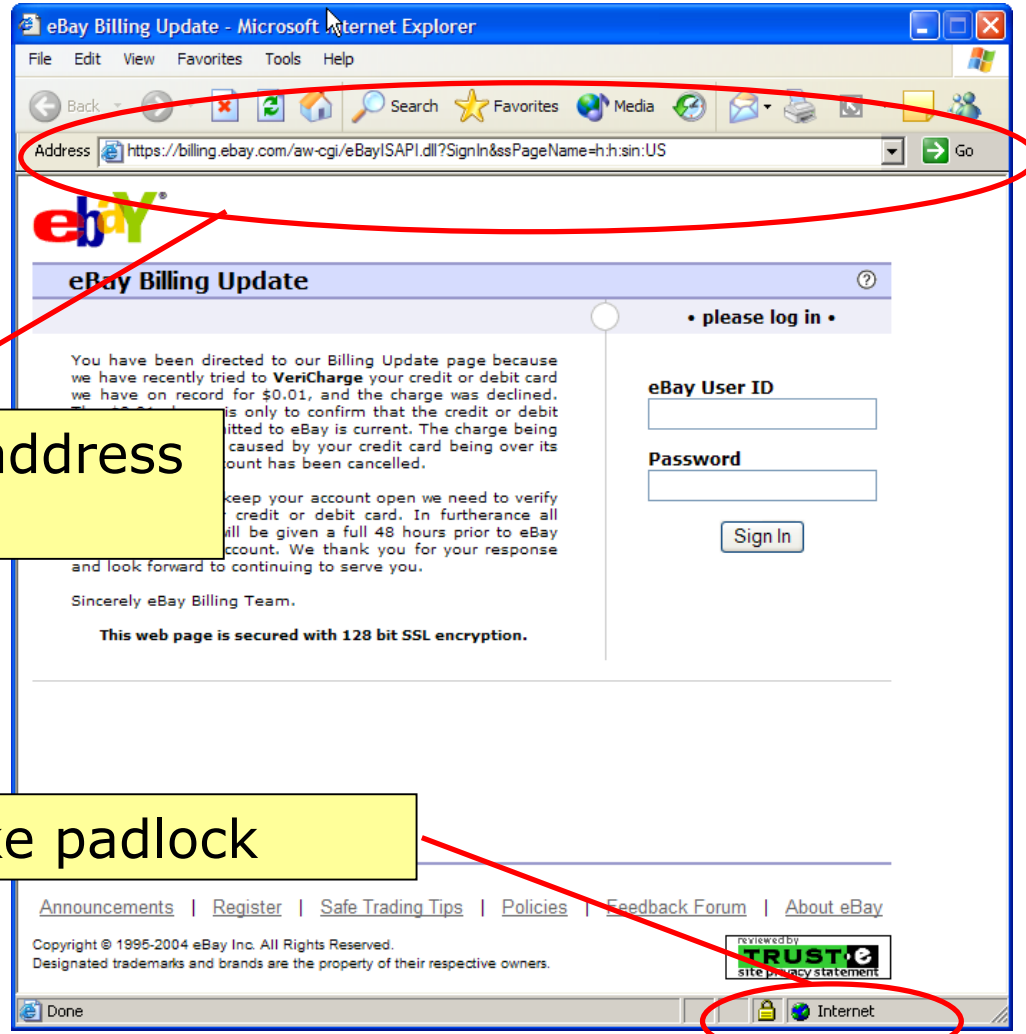
Hiding the URL: Pop up on top



Genuine Citibank site

Popup Window on Phisher's site

Hiding the URL: Fake browser parts



Fake browser address bar

Fake padlock

- **Legislation**
 - » It's already illegal!
- **Spam filters**
 - » Can catch a proportion
 - » Relies on continual updates
 - » Needs action from recipients/ISPs
- **Education**
 - » Tell people about phishing
 - » Educate people about security vulnerabilities
- **Two Factor Web Authentication**
 - » Cost of roll out
- **Email authentication**
 - » Solves the underlying problem – spoofing of FROM addresses
 - Sender-ID/Caller-ID/SPF
 - S/MIME digital signatures
 - » Will take time to roll out