

# Tracing an Email

## Priscilla Oppenheimer

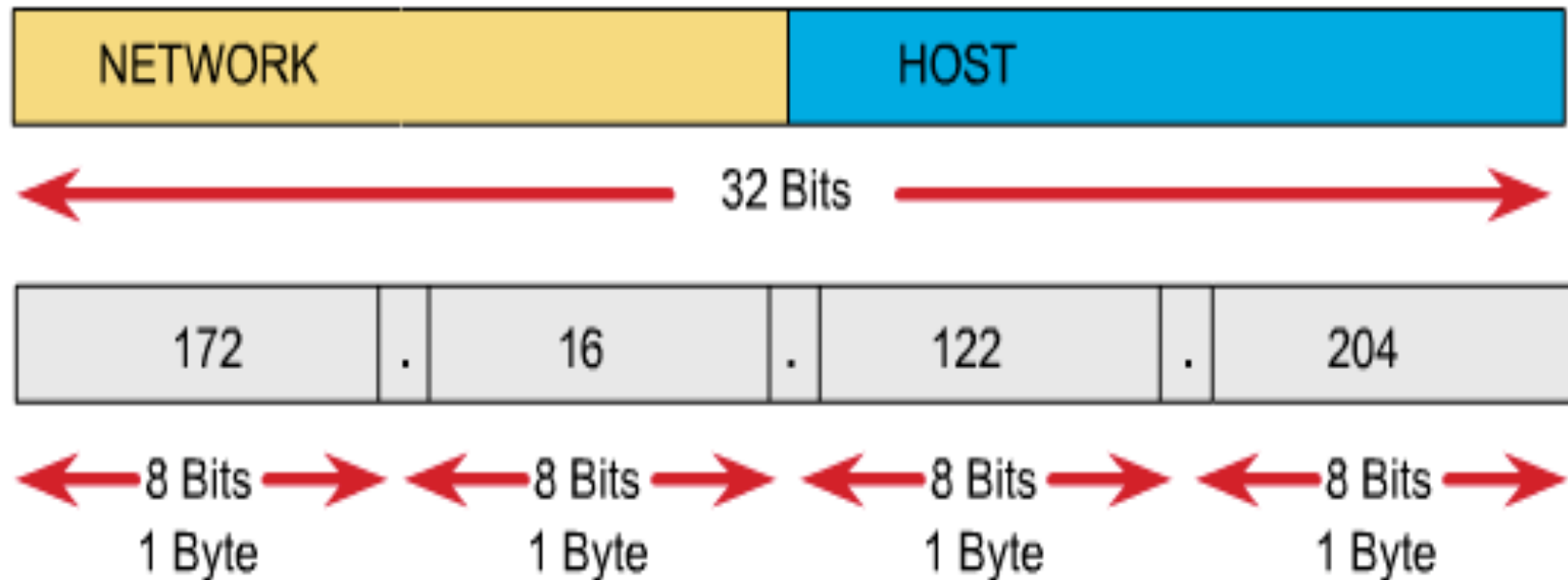
# Objectives

- Learn about phishing
- Learn about Internet Protocol (IP) addresses
- Learn about Domain Name System (DNS) names
- Learn how to determine if an email really came from the person or organization it appears to come from

# Phishing

- The act of sending an email falsely claiming to be a legitimate enterprise in an attempt to scam the recipient into surrendering private information such as a credit card number, bank account number, or PIN.

# IP Addressing



- Each interface on a network is assigned a 32-bit IP address
- The address has a prefix and suffix
  - Network and host ID

# IP Addresses

- Examples
  - 66.241.68.18
  - 140.211.107.34
  - 192.168.0.1
- Finding your own address
  - ipconfig/all on Windows
  - ifconfig on Unix

# IP Classful Addressing

<b>Class</b>	<b>First Few Bits</b>	<b>First Byte</b>	<b>Prefix Length</b>	<b>Intent</b>
A	0	1-126*	8	Very large networks
B	10	128-191	16	Large networks
C	110	192-223	24	Small networks
D	1110	224-239	NA	IP multicast
E	1111	240-255	NA	Experimental

\*Addresses starting with 127 are reserved for IP traffic local to a host.

# Address Assignment

- Managed by the Internet Assigned Numbers Authority ([IANA](#))
- Users are assigned IP addresses by Internet Service Providers (ISPs)
- ISPs obtain allocations of IP addresses from their appropriate Regional Internet Registry (RIR)

# Regional Internet Registries (RIR)

- [APNIC \(Asia Pacific Network Information Centre\)](#)
- [AfriNIC \(African Network Information Center\)](#)
- [ARIN \(American Registry for Internet Numbers\)](#)  
– North America
- [LACNIC \(Regional Latin-American and Caribbean IP Address Registry\)](#) – Latin America and parts of the Caribbean
- [RIPE NCC \(Réseaux IP Européens\)](#) – Europe, parts of the Middle East and Asia

# Private Addresses

## RFC 1918 Private IP Addressing

10.0.0.0 - 10.255.255.255

172.16.0.0 - 172.31.255.255

192.168.0.0 - 192.168.255.255

## Microsoft Automatic Private IP Addressing

169.254.0.1 - 169.254.255.254

# Your Own Address



The screenshot shows a web browser window with the title "IP Chicken - What is my IP? Find Your IP Address!". The address bar contains "http://www.ipchicken.com/". The browser's toolbar includes navigation buttons (back, forward, refresh, stop) and a search engine icon. Below the browser window, the website's header features a cartoon chicken logo and the text "IP CHICKEN Served fresh daily.™". A yellow navigation bar contains links for "CURRENT IP", "SECURITY PORT SCAN", and "HELP".

## Current IP Address

**66.241.68.18**

[Add to Favorites](#)

<b><u>Remote Control Desktop</u></b> Remote Control Any PC Online. Perfect Help Desk or IT Solution. <small>Ads by Goooooocle</small>	<b><u>Looking for a Static IP?</u></b> Run your server from Cable or DSL! Host your own Web, FTP, VPN, DVR <small>Advertise on this site</small>
---	--

## Advanced

- Name Address: OpenDoor17.ashlandfiber.net
- Remote Port: 51457
- Browser: Mozilla/5.0 (Macintosh; U; PPC Mac OS X Mach-O; en-US; rv:1.8.0.3) Gecko/20060426 Firefox/1.5.0.3

# Address Geographic Location

IP Address Locator - Enter an IP address to find its location - Lookup Country Region City et

http://www.geobytes.com/lpLocator.htm?GetLocation

Latest Headlines | Yahoo | News | GroupStudy | Cisco Docs | SOU-SIS | Novell WebAccess | Blackboard | SOU Forums

**GEOBYTES**


[ Home ] [ Contact Us ] [ Support ] [ Forum ]  
[ Free Services ] [ Merchandise ] [ IP Address Locat

The following results were generated using **GeoSelect** version II.

Address to locate:

Country Code	US	Country	United States
Region Code	USOR	Region	Oregon
City Code	USORMEDF	City	Medford
CityId	10514	Certainty	97
Latitude	42.3017	Longitude	-122.8380
Capital City	Washington, DC	TimeZone	-08:00
Nationality Singular	American	Population	278058881
Nationality Plural	Americans	Is proxy	false
CIA Map Reference	North America	Currency	US Dollar
MapBytes Remaining	Free	Currency Code	USD

Search WHOIS data at: [RIPE](#) [ARIN](#) [APNIC](#) [LACNIC](#)

Flag 


[Click here](#) to find out why our data can differ from the WHOIS data.  
[Click here](#) for a description of each of the above fields.

### Distance to Nearby Cities

km, mi, City, Region, Country

0 0	Medford, OR, US
5 3	Phoenix, OR, US
16 10	Central Point, OR, US
19 11	Talent, OR, US
24 15	Jacksonville, OR, US
24 15	Eagle Point, OR, US
27 16	Ashland, OR, US
29 18	Gold Hill, OR, US
32 20	White City, OR, US
36 22	Shady Cove, OR, US
41 25	Rogue River, OR, US
41 25	Murphy, OR, US
42 26	Williams, OR, US
43 26	Butte Falls, OR, US
49 30	Trail, OR, US
49 30	Klamath River, CA, US
52 32	Selad Valley, CA, US

Check out Geobytes other products including:  
[GeoSelect](#), [GeoNetMap](#), [GeoReport](#),  
[GeoPhrase](#), [GeoLyzer](#), [GeoRemote](#),  
[GeoDirection](#), [MapBytes](#)



Copyright 2005 | [Richard Oppenheimer](#)

# Researching IP Address with Whois

```
ibook-g4$ whois 66.241.68.18
OrgName:      Ashland Fiber Network
OrgID:        COFA
Address:      90 N Mountain Ave / 20 E Main
City:         Ashland
StateProv:    OR
PostalCode:   97520
Country:      US
ReferralServer: rwhois://rwhois.ashlandfiber.net:4321
NetRange:     66.241.64.0 - 66.241.95.255
CIDR:         66.241.64.0/19
NetName:      ASHLANDFN-1
NetHandle:    NET-66-241-64-0-1
Parent:       NET-66-0-0-0-0
NetType:      Direct Allocation
NameServer:   NS0.ASHLANDFIBER.NET
NameServer:   NS1.ASHLANDFIBER.NET
OrgTechPhone: +1-541-552-2222
OrgTechEmail: systems@ashlandfiber.net
# ARIN WHOIS database, last updated 2006-05-19 19:10
# Enter ? for additional hints on searching ARIN's WHOIS database.
```

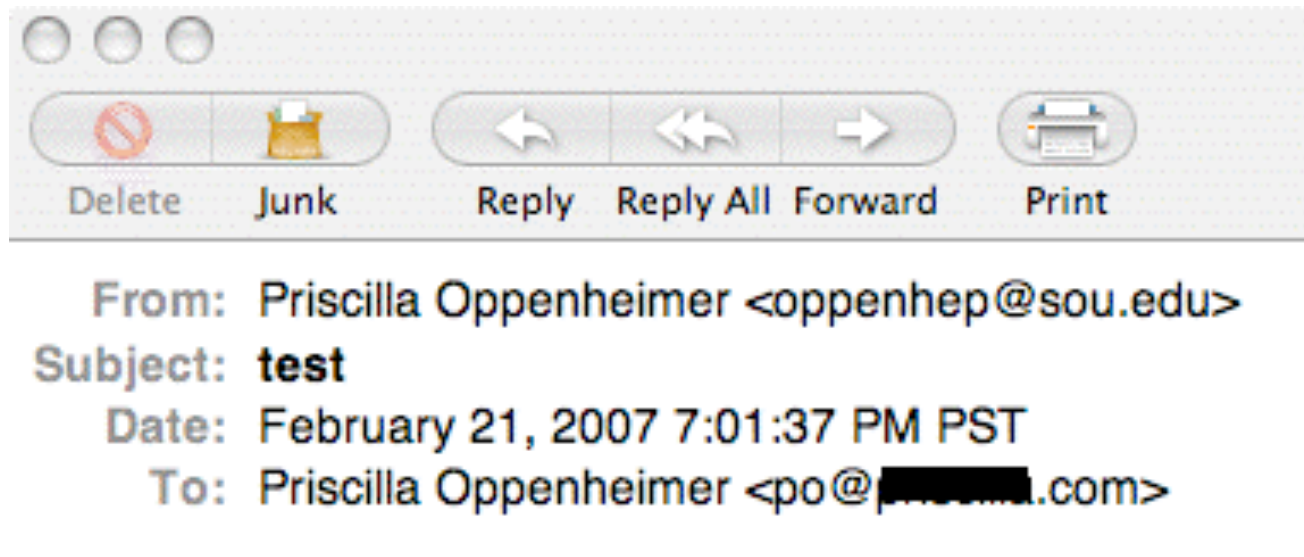
# Domain Name System

- Names map to IP addresses
- Examples
  - [www.sou.edu](http://www.sou.edu) = 140.211.107.34
  - [www.priscilla.com](http://www.priscilla.com) = 66.241.68.22
- The Domain Name System (DNS) is a set of servers that together know all the names used on the Internet
- More about this later...

# Email Schemes

- Scammers
- Spammers
- Phishers
- And other scum

# Basic Email Header



---

This is a test.

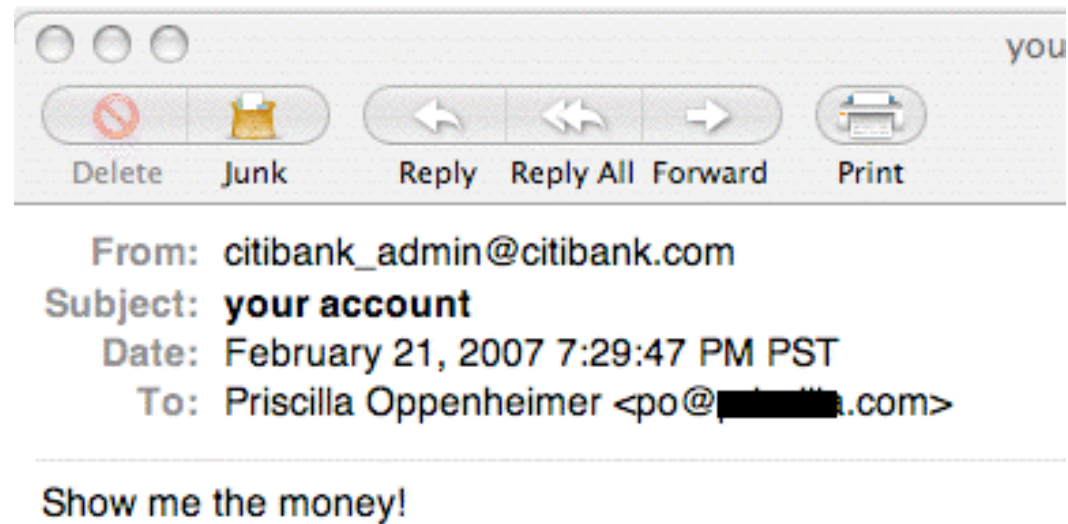
# Email Header Info

- Header info can be faked
  - From
  - Reply to
  - Return-path
  - Subject
  - Date
- Don't believe it!

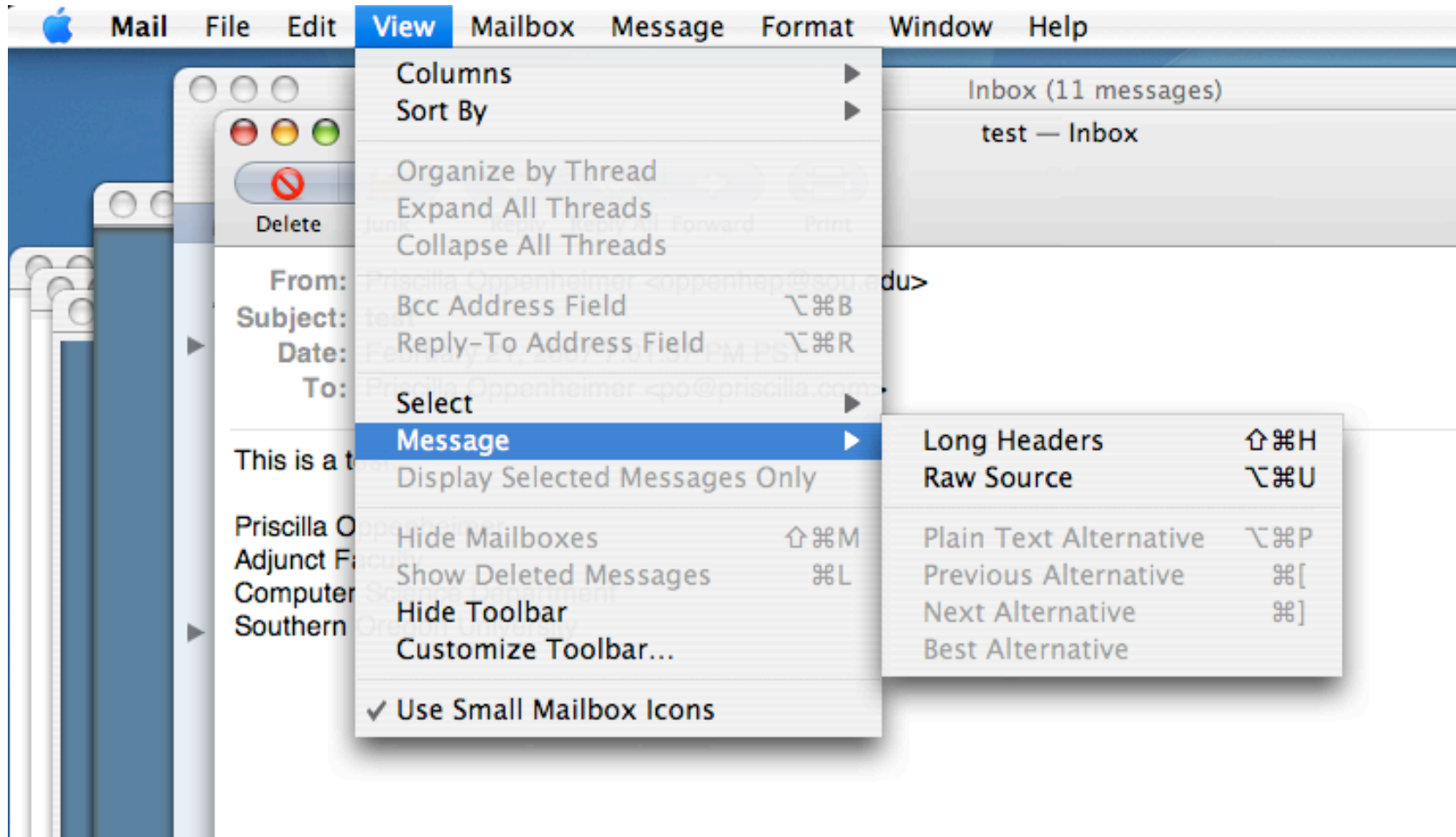
# Faking Is Easy!

```
host18$ telnet mail.target.com 25
Trying 192.168.68.22...
Connected to mail.target.com.
220 mail.target.com ESMTPostfix
HELO citibank.citibank.com
250 mail.target.com
MAIL FROM:citibank_admin@citibank.com
250 Ok
RCPT TO:po@target.com
250 Ok
DATA
354 End data with <CR><LF>.<CR><LF>
FROM:citibank_admin@citibank.com
SUBJECT:your account
TO:po@target.com
Show me the money!
.
250 Ok: queued as F23192DE9DE2
quit
221 Bye
Connection closed by foreign host.
host18$
```

# Fake



# Turn on "Long Headers"



# Reading Long Header Info

- Check path by looking at “received” list
- Read it upside down (originator is at the bottom of the list)
- Uses the passive voice, so can be confusing

# Long Header Example

- Return-Path: <example@aol.com>
- Received: from mailx.target.com ([unix socket]) by mailx.target.com (Cyrus v2.2.12-OS X 10.4.0) with LMTPA; Sun, 21 May 2006 09:28:29 -0700X-Sieve: CMU Sieve 2.2
- Received: from imo-m23.mail.aol.com (imo-m23.mx.aol.com [64.12.137.4]) by mailx.target.com (Postfix) with ESMTP id 0CB7A547326for <example@example.com>; Sun, 21 May 2006 09:28:25 -0700 (PDT)
- Received: from example@aol.com by imo-m23.mx.aol.com (mail\_out\_v38\_r7.5.) id f.15.54bf1f19 (58808);Sun, 21 May 2006 12:28:18 -0400 (EDT)
- From: example@aol.com
- Message-ID: <15.54bf1f19.31a1ef21@aol.com>
- Date: Sun, 21 May 2006 12:28:17 EDT
- Subject: Killer or Coder?? See if you know...
- To: example@example.com
- MIME-Version: 1.0
- Content-Type: multipart/alternative;boundary="part1\_15.54bf1f19.31a1ef21\_boundary"
- X-Mailer: Thunderbird - Mac OS X sub 310
- X-Spam-Flag: NO

# Email Sequence

- Return-Path: <example@aol.com>
- Received: from mailx.target.com ([unix socket]) by mailx.target.com (Cyrus v2.2.12-OS X 10.4.0) with LMTPA; Sun, 21 May 2006 09:28:29 -0700X-Sieve: CMU Sieve 2.2
- Received: from imo-m23.mail.aol.com (imo-m23.mx.aol.com [64.12.137.4]) by mailx.target.com (Postfix) with ESMTTP id 0CB7A547326for <example@example.com>; Sun, 21 May 2006 09:28:25 -0700 (PDT)
- Received: from example@aol.com by imo-m23.mx.aol.com (mail\_out\_v38\_r7.5.) id f.15.54bf1f19 (58808);Sun, 21 May 2006 12:28:18 -0400 (EDT)
- From: example@aol.com
- Message-ID: <15.54bf1f19.31a1ef21@aol.com>
- Date: Sun, 21 May 2006 12:28:17 EDT
- Subject: Killer or Coder?? See if you know...
- To: example@example.com
- MIME-Version: 1.0
- Content-Type: multipart/alternative;boundary="part1\_15.54bf1f19.31a1ef21\_boundary"
- X-Mailer: Thunderbird - Mac OS X sub 310
- X-Spam-Flag: NO

# Email Sequence

- Return-Path: <example@aol.com>
- Received: from mailx.target.com ([unix socket]) by mailx.target.com (Cyrus v2.2.12-OS X 10.4.0) with LMTPA; Sun, 21 May 2006 09:28:29 -0700X-Sieve: CMU Sieve 2.2
- Received: from imo-m23.mail.aol.com (imo-m23.mx.aol.com [64.12.137.4]) by mailx.target.com (Postfix) with ESMTTP id 0CB7A547326for <example@example.com>; Sun, 21 May 2006 09:28:25 -0700 (PDT)
- Received: from <sup>1</sup>example@aol.com by <sup>2</sup>imo-m23.mx.aol.com (mail\_out\_v38\_r7.5.) id f.15.54bf1f19 (58808);Sun, 21 May 2006 12:28:18 -0400 (EDT)
- From: example@aol.com
- Message-ID: <15.54bf1f19.31a1ef21@aol.com>
- Date: Sun, 21 May 2006 12:28:17 EDT
- Subject: Killer or Coder?? See if you know...
- To: example@example.com
- MIME-Version: 1.0
- Content-Type: multipart/alternative;boundary="part1\_15.54bf1f19.31a1ef21\_boundary"
- X-Mailer: Thunderbird - Mac OS X sub 310
- X-Spam-Flag: NO

# Email Sequence

- Return-Path: <example@aol.com>
- Received: from mailx.target.com ([unix socket]) by mailx.target.com (Cyrus v2.2.12-OS X 10.4.0) with LMTPA; Sun, 21 May 2006 09:28:29 -0700X-Sieve: CMU Sieve 2.2
- Received: from imo-m23.mail.aol.com (imo-m23.mx.aol.com [64.12.137.4]) by mailx.target.com (Postfix) with ESMTTP id 0CB7A547326for <example@example.com>; Sun, 21 May 2006 09:28:25 -0700 (PDT)
- Received: from example@aol.com by imo-m23.mx.aol.com (mail\_out\_v38\_r7.5.) id f.15.54bf1f19 (58808);Sun, 21 May 2006 12:28:18 -0400 (EDT)
- From: example@aol.com
- Message-ID: <15.54bf1f19.31a1ef21@aol.com>
- Date: Sun, 21 May 2006 12:28:17 EDT
- Subject: Killer or Coder?? See if you know...
- To: example@example.com
- MIME-Version: 1.0
- Content-Type: multipart/alternative;boundary="part1\_15.54bf1f19.31a1ef21\_boundary"
- X-Mailer: Thunderbird - Mac OS X sub 310
- X-Spam-Flag: NO

# Email Sequence

- Return-Path: <example@aol.com>
- Received: from mailx.target.com ([unix socket]) by 4 mailx.target.com (Cyrus v2.2.12-OS X 10.4.0) with LMTPA; Sun, 21 May 2006 09:28:29 -0700X-Sieve: CMU Sieve 2.2
- Received: from imo-m23.mail.aol.com (imo-m23.mx.aol.com [64.12.137.4]) by 3 mailx.target.com (Postfix) with ESMTTP id 0CB7A547326for <example@example.com>; Sun, 21 May 2006 09:28:25 -0700 (PDT)
- Received: from 1 example@aol.com by 2 imo-m23.mx.aol.com (mail\_out\_v38\_r7.5.) id f.15.54bf1f19 (58808);Sun, 21 May 2006 12:28:18 -0400 (EDT)
- From: example@aol.com
- Message-ID: <15.54bf1f19.31a1ef21@aol.com>
- Date: Sun, 21 May 2006 12:28:17 EDT
- Subject: Killer or Coder?? See if you know...
- To: example@example.com
- MIME-Version: 1.0
- Content-Type: multipart/alternative;boundary="part1\_15.54bf1f19.31a1ef21\_boundary"
- X-Mailer: Thunderbird - Mac OS X sub 310
- X-Spam-Flag: NO

# Checking ARIN

A screenshot of a web browser displaying the ARIN (American Registry for Internet Numbers) home page. The browser's address bar shows the URL <http://www.arin.net/index.shtml>. The page features a blue header with the ARIN logo and a mission statement: "Applying the principles of stewardship, ARIN, a nonprofit corporation, allocates Internet Protocol resources; develops consensus-based policies; and facilitates the advancement of the Internet through information and educational outreach." Below the header, the main content area is titled "American Registry for Internet Numbers" and is organized into several sections: "Announcements" (with an RSS 2.0 feed icon), "Registration Services" (including links for Request and manage number resources, Guidelines, Templates, and Routing Registry), "Policies" (including links for Policy proposals, Internet Resource Policy Evaluation Process, and Number Resource Policy Manual), "International Community" (including links for Information about other RIRs, Internet community organizations, and Number Resource Organization (NRO)), and "Billing" (including links for Service fee information, Fee Schedule, and Make Payment / Update). On the right side, there is a "Search WHOIS" box with the IP address "64.12.137.4" entered and a "Need WHOIS help?" link. At the bottom right, there are links for "Network Abuse", "Contact Us", and "Suggestions".

American Registry for Internet Numbers (ARIN) – Home Page

<http://www.arin.net/index.shtml>

Yahoo GroupStudy Cisco Docs SOU-SIS Novell WebAccess Blackboard Merriam-Webster TCP/IP Guide Data Communicat

**ARIN**  
American Registry for Internet Numbers

Applying the principles of stewardship, ARIN, a nonprofit corporation, allocates Internet Protocol resources; develops consensus-based policies; and facilitates the advancement of the Internet through information and educational outreach.

## American Registry for Internet Numbers

**Announcements**

RSS 2.0

Wed, 14 Feb 2007  
**Maintenance Work on Saturday, 17 February 2007**

Wed, 31 Jan 2007  
**Maintenance Release of RSA Posted**

Wed, 31 Jan 2007  
**Postel Network Operator's Scholarship**

Tue, 23 Jan 2007  
**Deadline for Policy**

**Registration Services**

- Request and manage number resources; Guidelines; Templates; Routing Registry
- ★ [Templates](#)
- ★ [Guidelines](#)

**Policies**

- Policy proposals, manual, and archives
- ★ [Internet Resource Policy Evaluation Process](#)
- ★ [Number Resource Policy Manual](#)

**International Community**

- Information about other RIRs, Internet community organizations; Number Resource Organization (NRO)

**Billing**

- Service fee information and online payment forms
- ★ [Fee Schedule](#)
- ★ [Make Payment / Update](#)

64.12.137.4

[Search WHOIS](#)

[Need WHOIS help?](#)

★ [Network Abuse](#)

★ [Contact Us](#)

★ [Suggestions](#)

# ARIN Whois Result

The screenshot shows a web browser window titled "ARIN: WHOIS Database Search". The address bar contains "http://ws.arin.net/whois". Below the address bar is a navigation menu with links to "Yahoo", "GroupStudy", "Cisco Docs", "SOU-SIS", "Novell WebAccess", "Blackboard", and "Merriam-Webster". A blue banner contains the text "ARIN WHOIS Database Search". Below this banner is a "Relevant Links" section with links to "ARIN Home Page", "ARIN Site Map", and "Training: Querying ARIN's WHOIS". A search box contains the text "Search ARIN WHOIS for: 64.12.137.4" and a "Submit Query" button. The search results are displayed in a text-based format:

```
OrgName: America Online, Inc.
OrgID: AMERIC-158
Address: 10600 Infantry Ridge Road
City: Manassas
StateProv: VA
PostalCode: 20109
Country: US

NetRange: 64.12.0.0 - 64.12.255.255
CIDR: 64.12.0.0/16
NetName: AOL-MTC
NetHandle: NET-64-12-0-0-1
Parent: NET-64-0-0-0-0
NetType: Direct Assignment
NameServer: DNS-01.NS.AOL.COM
NameServer: DNS-02.NS.AOL.COM
Comment:
RegDate: 1999-12-13
Updated: 1999-12-16

RTechHandle: AOL-NOC-ARIN
RTechName: America Online, Inc.
RTechPhone: +1-703-265-4670
RTechEmail: domains@aol.net

# ARIN WHOIS database, last updated 2007-02-21 19:10
# Enter ? for additional hints on searching ARIN's WHOIS database.
```

# Another Email Example

- Return-Path: example@illustration.com
- Received: from mailx.target.com ([unix socket]) by mailx.target.com (Cyrus v2.2.12-OS X 10.4.0) with LMTPA; Wed, 17 May 2006 22:57:14 -0700X-Sieve: CMU Sieve 2.2
- Received: from mail.illustration.com (mail.illustration.com [65.116.147.195]) by mailx.target.com (Postfix) with ESMTP id A866E4E8701for <example@example.com>; Wed, 17 May 2006 22:57:13 -0700 (PDT)
- Received: from homepkha40dpju (adsl-70-231-238-174.dsl.snfc21.sbcglobal.net [70.231.238.174]) (AUTH: LOGIN example, SSL: TLSv1/SSLv3,128bits,RC4-MD5) by mail.illustration.com with esmtp; Wed, 17 May 2006 22:57:12 -0700 id 0002E02B.446C0CB8.0000DA9E
- From: example@illustration.com
- To: example@example.com
- Subject: RE: Pictures
- Date: Wed, 17 May 2006 23:13:07 -0700
- Message-ID: JNELIMECMEOKKFFEKHBCAEJMCNAA.example@illustration.com
- MIME-Version: 1.0Content-Type: text/plain;charset="us-ascii"Content-Transfer-Encoding: 7bitX-Priority: 3 (Normal)
- In-Reply-To: 5832859D-BFB7-4ADA-A295-0BDE9739354E@example.com
- Importance: Normal

# Another Email Example

- Return-Path: example@illustration.com
- Received: from mailx.target.com ([unix socket]) by mailx.target.com (Cyrus v2.2.12-OS X 10.4.0) with LMTPA; Wed, 17 May 2006 22:57:14 -0700X-Sieve: CMU Sieve 2.2
- Received: from mail.illustration.com (mail.illustration.com [65.116.147.195]) by mailx.target.com (Postfix) with ESMTP id A866E4E8701for <example@example.com>; Wed, 17 May 2006 22:57:13 -0700 (PDT)
- Received: from homepkha40dpju (adsl-70-231-238-174.dsl.snfc21.sbcglobal.net [70.231.238.174]) (AUTH: LOGIN example, SSL: TLSv1/SSLv3,128bits,RC4-MD5) by mail.illustration.com with esmtp; Wed, 17 May 2006 22:57:12 -0700 id 0002E02B.446C0CB8.0000DA9E
- From: example@illustration.com
- To: example@example.com
- Subject: RE: Pictures
- Date: Wed, 17 May 2006 23:13:07 -0700
- Message-ID: JNELIMECMEOKKFFEKHBCAEJMCNAA.example@illustration.com
- MIME-Version: 1.0Content-Type: text/plain;charset="us-ascii"Content-Transfer-Encoding: 7bitX-Priority: 3 (Normal)
- In-Reply-To: 5832859D-BFB7-4ADA-A295-0BDE9739354E@example.com
- Importance: Normal

# Another Email Example

- Return-Path: example@illustration.com
- Received: from mailx.target.com ([unix socket]) by mailx.target.com (Cyrus v2.2.12-OS X 10.4.0) with LMTPA; Wed, 17 May 2006 22:57:14 -0700X-Sieve: CMU Sieve 2.2
- Received: from mail.illustration.com (mail.illustration.com [65.116.147.195]) by mailx.target.com (Postfix) with ESMTP id A866E4E8701for <example@example.com>; Wed, 17 May 2006 22:57:13 -0700 (PDT)
- Received: from homepkha40dpju (adsl-70-231-238-174.dsl.snfc21.sbcglobal.net [70.231.238.174]) (AUTH: LOGIN example, SSL: TLSv1/SSLv3,128bits,RC4-MD5) by mail.illustration.com with esmtp; Wed, 17 May 2006 22:57:12 -0700 id 0002E02B.446C0CB8.0000DA9E
- From: example@illustration.com
- To: example@example.com
- Subject: RE: Pictures
- Date: Wed, 17 May 2006 23:13:07 -0700
- Message-ID: JNELIMECMEOKKFFEKHBCAEJMCNAA.example@illustration.com
- MIME-Version: 1.0Content-Type: text/plain;charset="us-ascii"Content-Transfer-Encoding: 7bitX-Priority: 3 (Normal)
- In-Reply-To: 5832859D-BFB7-4ADA-A295-0BDE9739354E@example.com
- Importance: Normal

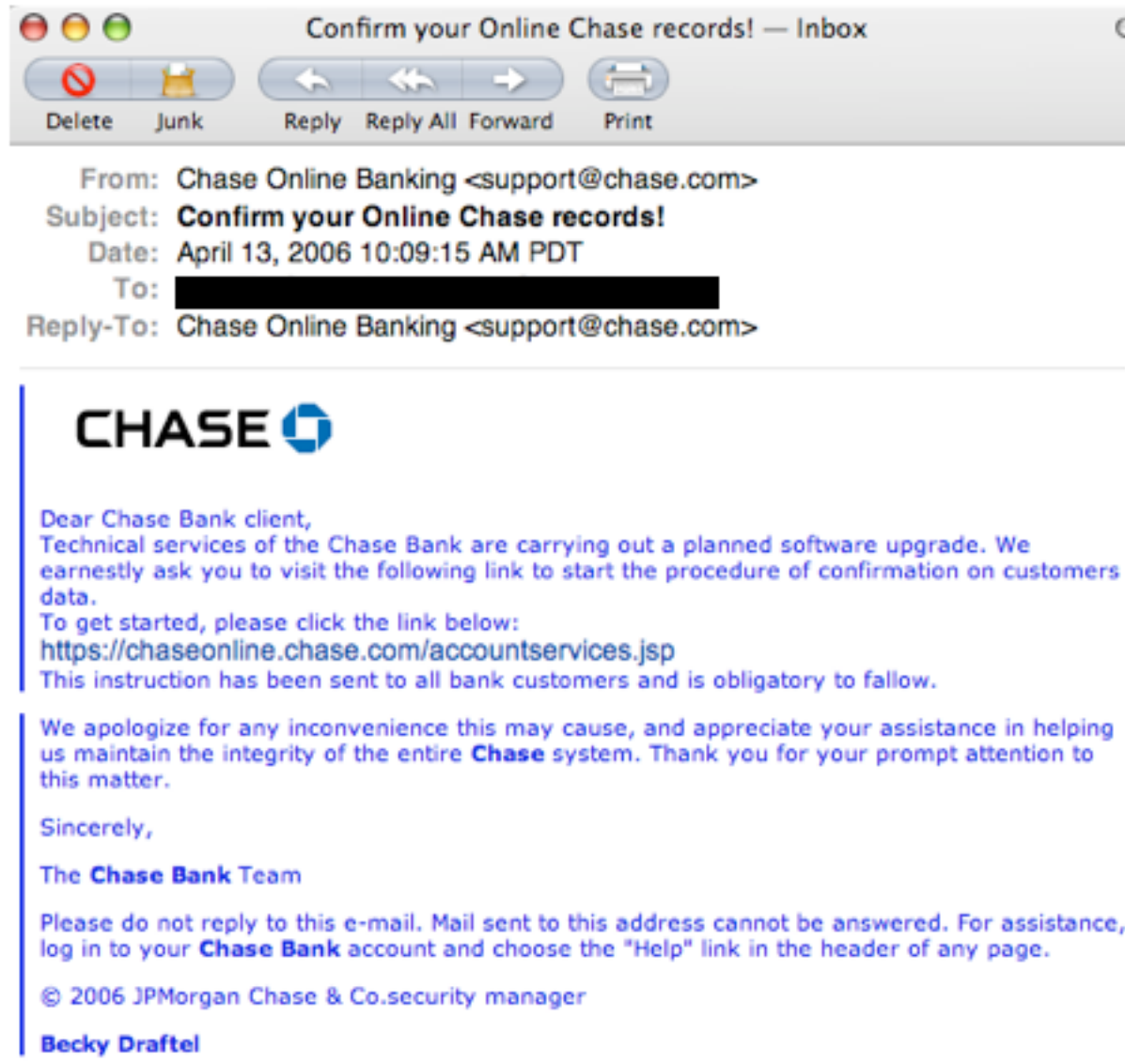
# Another Email Example

- Return-Path: example@illustration.com
- Received: from mailx.target.com ([unix socket]) by mailx.target.com (Cyrus v2.2.12-OS X 10.4.0) with LMTPA; Wed, 17 May 2006 22:57:14 -0700X-Sieve: CMU Sieve 2.2
- Received: from mail.illustration.com (mail.illustration.com [65.116.147.195])<sup>3</sup> by mailx.target.com (Postfix) with ESMTTP id A866E4E8701for <example@example.com>; Wed, 17 May 2006 22:57:13 -0700 (PDT)
- Received: from homepkha40dpju (adsl-70-231-238-174.dsl.snfc21.sbcglobal.net [70.231.238.174]) (AUTH: LOGIN example, SSL: TLSv1/SSLv3,128bits,RC4-MD5) by<sup>2</sup> mail.illustration.com with esmtp; Wed, 17 May 2006 22:57:12 -0700 id 0002E02B.446C0CB8.0000DA9E
- From: example@illustration.com
- To: example@example.com
- Subject: RE: Pictures
- Date: Wed, 17 May 2006 23:13:07 -0700
- Message-ID: JNELIMECMEOKKFFEKHBCAEJMCNAA.example@illustration.com
- MIME-Version: 1.0Content-Type: text/plain;charset="us-ascii"Content-Transfer-Encoding: 7bitX-Priority: 3 (Normal)
- In-Reply-To: 5832859D-BFB7-4ADA-A295-0BDE9739354E@example.com
- Importance: Normal

# Another Email Example

- Return-Path: example@illustration.com
- Received: from mailx.target.com ([unix socket]) by mailx.target.com (Cyrus v2.2.12-OS X 10.4.0) with LMTPA; Wed, 17 May 2006 22:57:14 -0700X-Sieve: CMU Sieve 2.2
- Received: from mail.illustration.com (mail.illustration.com [65.116.147.195]) by mailx.target.com (Postfix) with ESMTP id A866E4E8701for <example@example.com>; Wed, 17 May 2006 22:57:13 -0700 (PDT)
- Received: from homepkha40dpju (adsl-70-231-238-174.dsl.snfc21.sbcglobal.net [70.231.238.174]) (AUTH: LOGIN example, SSL: TLSv1/SSLv3,128bits,RC4-MD5) by mail.illustration.com with esmtp; Wed, 17 May 2006 22:57:12 -0700 id 0002E02B.446C0CB8.0000DA9E
- From: example@illustration.com
- To: example@example.com
- Subject: RE: Pictures
- Date: Wed, 17 May 2006 23:13:07 -0700
- Message-ID: JNELIMECMEOKKFFEKHBCAEJMCNAA.example@illustration.com
- MIME-Version: 1.0Content-Type: text/plain;charset="us-ascii"Content-Transfer-Encoding: 7bitX-Priority: 3 (Normal)
- In-Reply-To: 5832859D-BFB7-4ADA-A295-0BDE9739354E@example.com
- Importance: Normal

# Phishing Example



# Phishing Example Header

- Return-Path: <support@chase.com>
- Received: from mailx.target.com ([unix socket]) by mailx.target.com (Cyrus v2.2.12-OS X 10.4.0) with LMTPA; Thu, 13 Apr 2006 09:13:12 -0700X-Sieve: CMU Sieve 2.2
- Received: from 66.240.255.32 (unknown [66.240.255.32]) by mailx.target.com (Postfix) with SMTP id 4AAF81425D4 for <example@example.com>; Thu, 13 Apr 2006 09:13:12 -0700 (PDT)
- Received: from 235.82.160.144 by ; Thu, 13 Apr 2006 12:08:15 -0500
- Message-ID: <circuitry@aol.com>
- From: "Chase Online Banking " <support@chase.com>
- Reply-To: "Chase Online Banking " <support@chase.com>
- To: example@example.com
- Subject: Confirm your Online Chase records!
- Date: Thu, 13 Apr 2006 13:09:15 -0400
- X-Mailer: Microsoft Outlook, Build 10.0.2616MIME-Version: 1.0
- Content-Type: multipart/alternative;boundary="--241369552528522502883"X-Priority: 1X-MSMail-Priority: High

# Phishing Example Header

- Return-Path: <support@chase.com>
- Received: from mailx.target.com ([unix socket]) by mailx.target.com (Cyrus v2.2.12-OS X 10.4.0) with LMTPA; Thu, 13 Apr 2006 09:13:12 -0700X-Sieve: CMU Sieve 2.2
- Received: from 66.240.255.32 (unknown [66.240.255.32]) by mailx.target.com (Postfix) with SMTP id 4AAF81425D4 for <example@example.com>; Thu, 13 Apr 2006 09:13:12 -0700 (PDT)
- Received: from 235.82.160.144 by ; Thu, 13 Apr 2006 12:08:15 -0500
- Message-ID: <circuitry@aol.com>
- From: "Chase Online Banking " <support@chase.com>
- Reply-To: "Chase Online Banking " <support@chase.com>
- To: example@example.com
- Subject: Confirm your Online Chase records!
- Date: Thu, 13 Apr 2006 13:09:15 -0400
- X-Mailer: Microsoft Outlook, Build 10.0.2616MIME-Version: 1.0
- Content-Type: multipart/alternative;boundary="--241369552528522502883"X-Priority: 1X-MSMail-Priority: High

# Phishing Example Header

- Return-Path: <support@chase.com>
- Received: from mailx.target.com ([unix socket]) by mailx.target.com (Cyrus v2.2.12-OS X 10.4.0) with LMTPA; Thu, 13 Apr 2006 09:13:12 -0700X-Sieve: CMU Sieve 2.2
- Received: from 66.240.255.32 (unknown [66.240.255.32]) by mailx.target.com (Postfix) with SMTP id 4AAF81425D4 for <example@example.com>; Thu, 13 Apr 2006 09:13:12 -0700 (PDT)
- Received: from 235.82.160.144 by ; Thu, 13 Apr 2006 12:08:15 -0500
- Message-ID: <circuitry@aol.com>
- From: "Chase Online Banking " <support@chase.com>
- Reply-To: "Chase Online Banking " <support@chase.com>
- To: example@example.com
- Subject: Confirm your Online Chase records!
- Date: Thu, 13 Apr 2006 13:09:15 -0400
- X-Mailer: Microsoft Outlook, Build 10.0.2616MIME-Version: 1.0
- Content-Type: multipart/alternative;boundary="--241369552528522502883"X-Priority: 1X-MSMail-Priority: High

# Phishing Example Header

- Return-Path: <support@chase.com>
- Received: from mailx.target.com ([unix socket]) by mailx.target.com (Cyrus v2.2.12-OS X 10.4.0) with LMTPA; Thu, 13 Apr 2006 09:13:12 -0700X-Sieve: CMU Sieve 2.2
- Received: from 66.240.255.32 (unknown [66.240.255.32]) by mailx.target.com (Postfix) with SMTP id 4AAF81425D4 for <example@example.com>; Thu, 13 Apr 2006 09:13:12 -0700 (PDT)
- Received: from 235.82.160.144 by ; Thu, 13 Apr 2006 12:08:15 -0500
- Message-ID: <circuitry@aol.com>
- From: "Chase Online Banking " <support@chase.com>
- Reply-To: "Chase Online Banking " <support@chase.com>
- To: example@example.com
- Subject: Confirm your Online Chase records!
- Date: Thu, 13 Apr 2006 13:09:15 -0400
- X-Mailer: Microsoft Outlook, Build 10.0.2616MIME-Version: 1.0
- Content-Type: multipart/alternative;boundary="--241369552528522502883"X-Priority: 1X-MSMail-Priority: High

# Phishing Example Sneaky Methods

- Received: from 235.82.160.144
  - That's a multicast address and should never be used as a source address
- Received: from 66.240.255.32
  - According to ARIN, the number belongs to California Regional Intranet, Inc. in San Diego
    - Could be suspicious?

# Phishing Example Domain Name System (DNS) Research

- Where should chase.com really be coming from?
- **nslookup** command
- **dig** command
- whois can do names too
- [www.dnsstuff.com](http://www.dnsstuff.com)

# Phishing Example DNS Name Research

## DNS Lookup: chase.com A record

Generated by [www.DNSstuff.com](http://www.DNSstuff.com) at 17:32:57 GMT on 23 Feb 2007.

Domain	Type	Class	TTL	Answer
chase.com.	A	IN	600	<a href="http://159.53.60.105">159.53.60.105</a>
chase.com.	NS	IN	600	ns06.jpmorganchase.com.
chase.com.	NS	IN	600	ns1.jpmorganchase.com.
chase.com.	NS	IN	600	ns2.jpmorganchase.com.
chase.com.	NS	IN	600	ns05.jpmorganchase.com.
ns1.jpmorganchase.com.	A	IN	600	159.53.46.53
ns2.jpmorganchase.com.	A	IN	600	159.53.78.53
ns05.jpmorganchase.com.	A	IN	600	159.53.110.152
ns06.jpmorganchase.com.	A	IN	600	159.53.110.153

# Phishing Example

## Raw Source of Part of Message Text

- To get started, please click the link below:  
</FONT><BR></BLOCKQUOTE><BLOCKQUOTE cite=3D" " type=3D"cite"><A href=3D"http://chase.com.login-personal.com/start.html" target=3D\_blank <a><FONT color=3D#003399>https://chaseonline.chase.com/accountservices.jsp</FONT>=</A></B></FONT> <BR></BLOCKQUOTE>

# Phishing Example

## Raw Source of Part of Message Text

- To get started, please click the link below:  
</FONT><BR></BLOCKQUOTE><BLOCKQUOTE cite=3D" " type=3D"cite"><A href=3D"http://chase.com.login-personal.com/start.html" target=3D\_blank <a><FONT color=3D#003399>https://chaseonline.chase.com/accountservices.jsp</FONT>=</A></B></FONT> <BR></BLOCKQUOTE>

# Summary

- IANA assigns IP addresses
- Regional Registries assign addresses for regions
- Start with ARIN when researching
  - ARIN will tell you where to go for non-American addresses
- Turn on long headers in email
- Don't fall for silly stuff in the body of the email