# The Spam/Anti-Spam Battlefield

SANS Institute Masters
Presentation by T. Brian Granier

# Objectives

- What is the definition of SPAM?
- What are the motivations for SPAMming?
- What tools can I use for SPAM detection and defense?
- How can I responsibly send mass emails?

# What is the definition of SPAM?

- Often, more than just a term for email
  - Modern advertising
  - Bluejacking
- A universally agreed upon definition is difficult
- **MY** definition: SPAM is any marketing, deceptive or abusive use of email that the recipient does not wish to receive

# What are the motivations for SPAMming?

- Know your enemy
  - Understanding motivations can help us defend against them
- The biggest motivator for SPAM is money
- There are other motivators than just money

# How do SPAMmers make money?

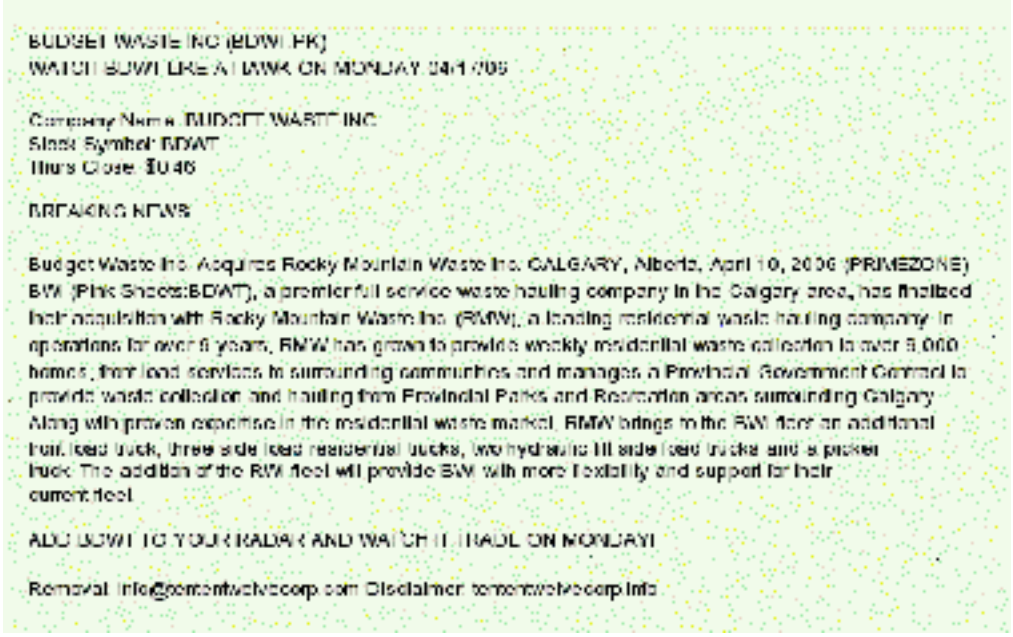
- Direct marketing and sales
- Stock market games – pump and dump
- Multi-level marketing schemes
- Nigeria scam
- Phishing
- Advertising revenue
- Validating and reselling email lists

# Direct Marketing and Sales

- Often perceived as the highest revenue generator for SPAMmers
- In reality, it is rare a SPAMmer is advertising a product they actually sell
- They may be advertising on behalf of the real manufacturer who paid them for the advertising

# Stock Market Games
# AKA Pump and Dump

- Unsolicited stock advertisements should never be acted upon!



BUDGET WASTE INC (BDWI:PK)
WATCH BDWI BREAK BMK ON MONDAY 04/17/06

Company Name: BUDGET WASTE INC
Stock Symbol: BDWI
Thurs Close: $0.46

BREAKING NEWS

Budget Waste Inc. Acquires Rocky Mountain Waste Inc. CALGARY, Alberta, April 10, 2006 (PRIMEZONE) BW (Pink Sheets:BDWI), a premier full service waste hauling company in the Calgary area, has finalized their acquisition with Rocky Mountain Waste Inc. (RMW), a leading residential waste hauling company in operations for over 6 years. RMW has grown to provide weekly residential waste collection to over 5,000 homes, front load services to surrounding communities and manages a Provincial Government Contract to provide waste collection and hauling from Provincial Parks and Recreation areas surrounding Calgary. Along with proven expertise in the residential waste market, RMW brings to the BW fleet an additional front load truck, three side load residential trucks, two hydraulic tilt side load trucks and a picker truck. The addition of the RW fleet will provide BW with more flexibility and support for their current fleet.

ADD BDWI TO YOUR RADAR AND WATCH IT TRADE ON MONDAY!

Removal: info@contentwolvecorp.com Disclaimer: contentwolvecorp.info

# Multi-level Marketing and Make Money Fast Schemes

- MLM or MMF emails will often promise to make you rich fast
- The real money maker is in the fees you pay to sign up
- Often the "product" being sold is fake, undisclosed or improperly priced
- As a general rule, avoid MLM and MMF programs, especially when unsolicited

# Nigeria SCAM
# AKA 419 Fraud

- MANY variations
- Goal is to get target to give startup money to get process started

Dear John Smith,

UPON THE INSTRUCTIONS

Based on the instructions of Her Majesty Queen of England, who directed most fund of money or assets of those that died in the last London Bomb blast should be realized to their families.

I am writing to you for a next of kin beneficiary of our customer who died in the bomb blast as well, he is Jack Smith beneficiary of A/C Number 00414610410 coded Account amount to $3.5 million. Inform us if you are related to this client, to enable us arrange and bring the money to you in your country.

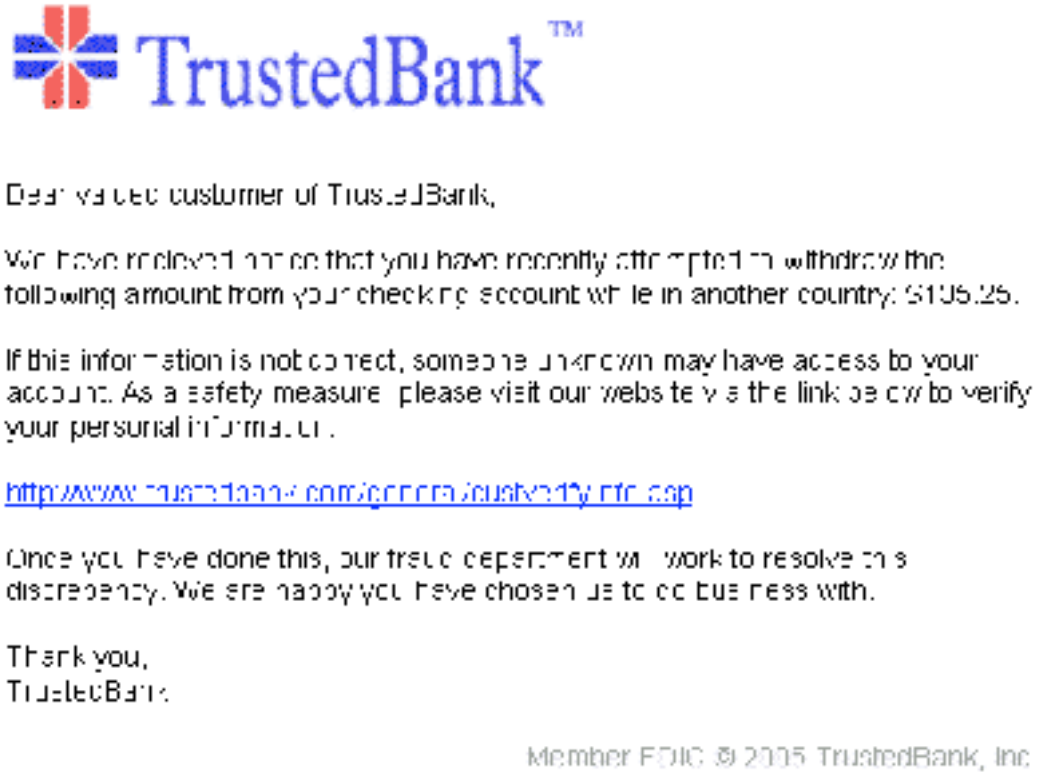
With Regards.

Your responds:-Inform us your Mobile Tel, Fax number, Office Tel, for easy reach. On behalf of our Bank and the Government of Great Britain, We are so sorry for the lost of your relation. Confirm the Receipts of this message by reply mail

Example taken from: http://www.hoax-slayer.com/london-nigerian.html

# Phishing

- Trick people into giving up account information
- Often look legitimate



TrustedBank™

Dear valued customer of TrustedBank,

We have received notice that you have recently attempted to withdraw the following amount from your checking account while in another country: $135.25.

If this information is not correct, someone unknown may have access to your account. As a safety measure, please visit our website via the link below to verify your personal information.

http://www.trustedbank.com/general/custverify.htm

Once you have done this, our fraud department will work to resolve this discrepancy. We are happy you have chosen us to do business with.

Thank you,
TrustedBank

Member FDIC © 2005 TrustedBank, Inc

Example taken from Wikipedia.org

# Advertising Revenue

- SPAMmer may directly advertise a product on behalf of a client
- SPAMmer may have a relationship to get paid for every view of a specific banner ad
  - Embedded HTML rendered by email clients make this easy

# Validating and Reselling Email Lists

- The sell and resell of SPAM lists is a significant revenue source for SPAMmers
- "Validated" emails are even more valuable
  - Mail does not bounce
  - Target clicks an unsubscribe link
  - Specific crafted embedded html is accessed

# Besides money, what else motivates SPAMmers?

- Deploying Malware
- Steganography
- Reconnaissance
- Competitor Sabotage
- Humor, Chain Letters and Hoaxes

# Deploying Malware

- Many viruses spread by way of spam like methods
- Consider that anti-spam method can also help protect against new and emerging email born malware
- Typically spread by way of using client side address lists

# Steganography

- Steganography – a means of hiding data in a carrier medium
- The goal is to hide the data and the fact the data is being transmitted
- SPAM makes an EXCELLENT carrier
- http://www.spammimic.com
  - Provides a way to encode and decode data in a "SPAM" email

# Reconnaissance

- Can be used to enumerate valid email addresses to the target company
- Since it is SPAM, it is highly likely to be ignored
- If email addresses have a correlation to valid user accounts, the SPAMmer now has a list of usernames to crack against

# Competitor Sabotage

- An unscrupulous business owner may send SPAM in order to defame the character of the competitor
- Requires using spoofing techniques
- Content will often be designed to be offensive in nature
  - Links to porn from a childcare organization

# Humor, Chain Letters and Hoaxes

- The "SPAMmer" is often someone you know
- This class of SPAM is the most difficult to automatically filter
- Best defense is to train your family, friends and co-worker against gullibly sending chain letters and hoaxes
  - http://www.snopes.com

# What tools can I use for SPAM detection and defense?

- Filtering
- Avoid getting listed
- Do not become part of the problem
- Be aware of reality

# Desktop Filtering

- Offers the most control to end users
- Ideal solution for home users
- Typically cost $20 - $40
- Depends upon some end user awareness
- A few examples: Spam Shield, Spam Bully, InBoxer, Qurb, … the list is endless

# Email Server Filtering

- Run on the mail server itself
- Can become a huge performance issue
- Typically coupled with anti-virus
- Decreasing in popularity in favor of gateway solutions

# Gateway Filtering

- Ideal for large environments
- May be done in-house or a third party service
- Offers a range of control to the end users depending upon the product
- Scaleable
- Takes advantage of more filtering techniques

# Filtering Techniques

- Hashing/Checksums
  - Performing a mathematical computation against an email or portion of the email to identify and filter based upon quantity of matching email sent
- Open Relay Checks
  - Checking if the source mail server permits relays
- RBL Checks
  - Checking if the source mail server is listed on a Real-time Blackhole List such as SPEWS or Spam Cop

# More Filtering Techniques

- Bayesian Filtering
  - Statistical calculation of probability the message is spam with user input
- Heuristics
  - Combining a variety of detection techniques to recognize patterns when taken together that indicate probability of spam
- Signature Matching
  - Simple filter that looks for specific keywords

# Even More Filtering Techniques

- Black Listing
  - Identifying a specific source address, domain or IP from which all mail should be blocked
- White Listing
  - Identifying a specific source address, domain or IP from which all mail should be permitted
- The list goes on…

# Deploy Traditional Anti-Virus Techniques

- Recall that malware often spreads through spam like techniques
- Anti-Virus and Anti-Spam filtering often work hand in hand
- The same education about email handling for anti-virus should include discussions about handling spam

# Deploy Anti-Spyware Applications

- Spyware applications may contain address harvesting hooks
- Many training overlaps exist with avoiding spam as avoiding spyware
- Many tools commercial and free exist
  - Ad-Aware
  - Spybot Search & Destroy
  - Microsoft AntiSpyware (beta)

# Avoid the temptation to "unsubscribe"

- Unsubscribing may actually be the worst thing to do
- Remember that some spammers sell "validated" mail lists. Unsubscription requests is a form of validation
- Unsubscription should ONLY be considered from well known and reputable companies – Judgement call

# Use a "Spamsink" Account

- Create a throw away email account just for the purpose of providing to questionable sources
  - Hotmail
  - Gmail
- Consider setting up a new account every time you must provide an email address. This helps track the origin of getting on any spam list

# Avoid Putting Emails in Public Places

- Company websites
  - Re-format addresses:
    sample @ domain . com
  - Substitute ASCII codes:
    sample@domain.com
  - Use web forms
  - Display the email address as a graphic
- Public discussion forums and groups
  - Avoid using your primary email account

# Cookie Management

- Cookies can be used by spammers to harvest email addresses
- Configure browser handling of cookies
  - IE: Tools -> Internet Options -> Privacy -> Adjust slider
  - Firefox: Tools -> Options -> Privacy -> Cookies
- Consider third party softwares that will manage access and storage of cookies
  - Cookiewall, Cookie Monster, Cookie Jar etc…

# Protect Your Network

- Secure your wireless networks
  - First conviction against CAN-SPAM act involved a spammer who was wardriving to send SPAM
- One of the many reasons attackers seek to infect a system is to have a launching point for SPAM. Yet another reason for complete and thorough security protections and detections.

# Properly Configure Mail Servers

- Do not permit your mail server to relay
- Require authentication to send mail
- Keep an eye on SPF records that appear to be gaining in popularity
  - RFC 4408
  - http://www.openspf.org/

# Avoid Curiosity and Gullibility

- If it sounds too good to be true, it is probably not true
- If it sounds official, but comes from an unexpected source, it probably is not
- Be disciplined about not clicking on links or opening documents without full awareness and caution
  - Use VMWare or some other sandbox method if you just must open it

# Only Permit SMTP from Authorized Mail Servers

- Many viruses spread from local smtp engines on infected machines
- Spyware or other malware may send regular SPAM as well
- Only mail servers should legitimately need SMTP access to the Internet
- By allowing SMTP (25/TCP) to the Internet from ONLY authorized mail servers, you are practicing proper defense in depth

# Do Not Proliferate Chain Mail and Hoax Mail

- Microsoft is not tracking this email and will not give you money for forwarding it on
- You will not die a horrible death if you don't forward in ten minutes or less
- Instructions to "clean" a virus from your system by deleting a specific file or running a specific program are probably not in your best interest
- www.snopes.com – Invaluable hoax dictionary

# No Viewing Email in HTML

- Helps you identify phishing quickly
- Avoids problems with techniques that equate to account validation
  - Single pixel attached images
- Also helps in many other ways to avoid exploits that depend upon html rendering
- For Microsoft Outlook
  - Outlook 2002 SP1 or later: Add registry key HKEY_CURRENT_USER\Software\Microsoft\Office\10.0\Outlook\Options\Mail DWORD of READASPLAIN Value of 1
  - Outlook 2003: Tools > Options > Preferences > E-mail options and check the option to read all mail as plain text

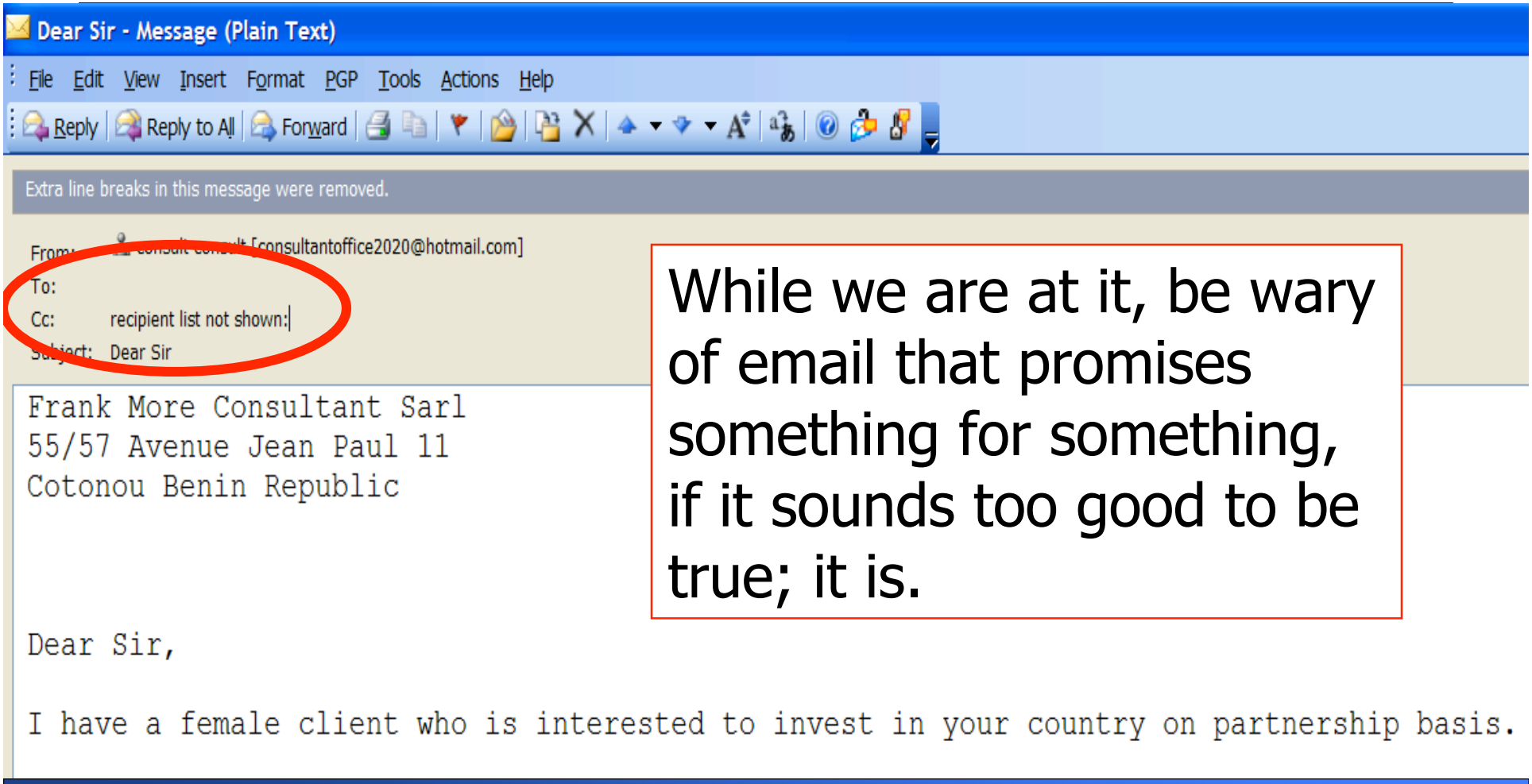
# Other Outlook Settings

- Tools > Options > Security > Zone: Restricted sites
  - Use Zone Settings to ensure that all scripting and controls are disabled by default.
- Tools > Options > Mail Format
  - Compose in this message format: Plain Text
  - Deselect "Use Microsoft Word to edit e-mail messages"
  - Deselect "Use Microsoft Word to read Rich Test e-mail messages"
  - Internet Format > Convert to plain text format

# Learn to Read SMTP Headers

- Helps to identify true source of SPAM
- Headers are essential when reporting to abuse contacts
- Learn more at:
  http://www.stopspam.org/email/headers.html

# Be Wary of Email W/O Recipient List (i.e. To: or CC:)

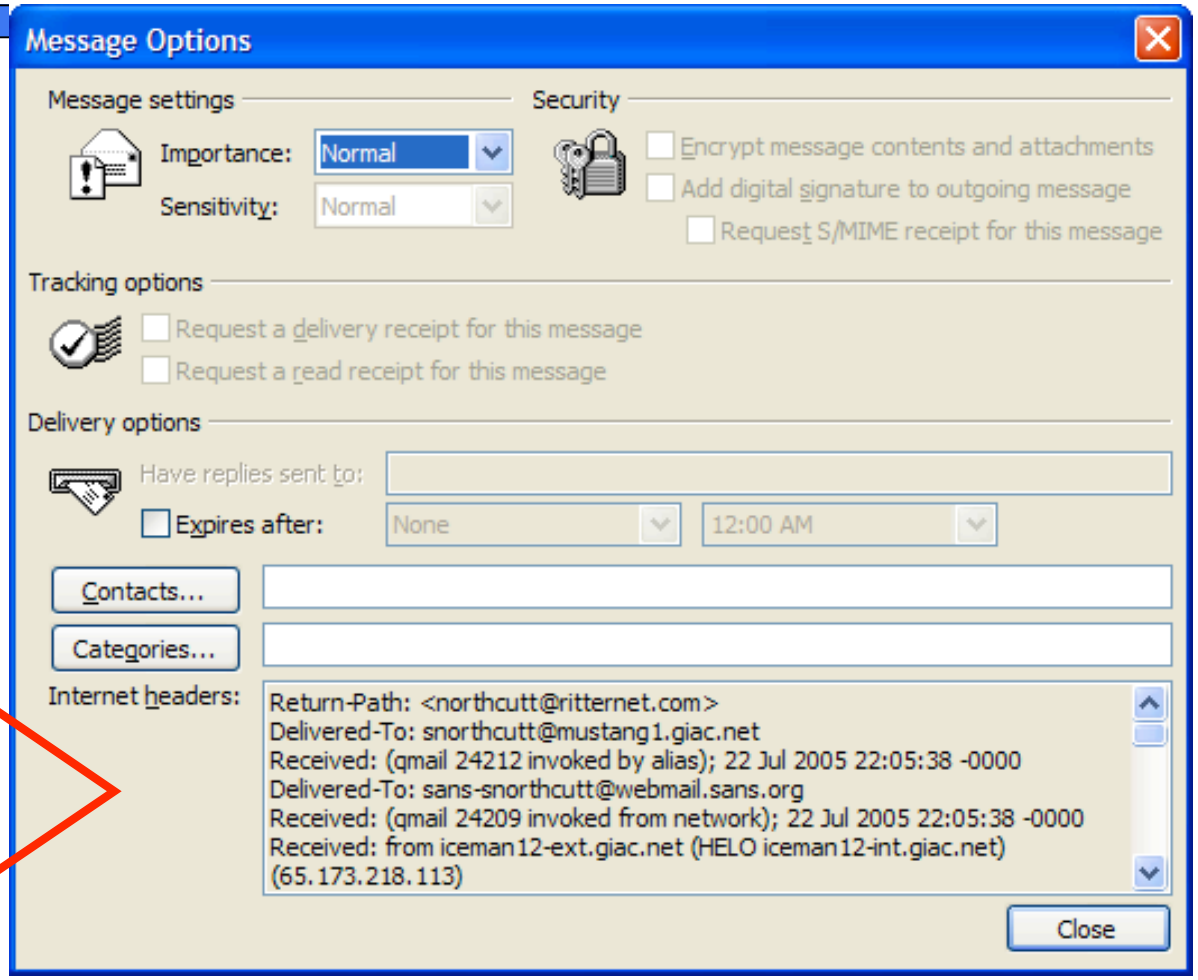



While we are at it, be wary of email that promises something for something, if it sounds too good to be true; it is.

# Examine Email Headers to Detect Spoofed Email

View Options
or with Outlook 2003 in reading pane:
right click, Options

**Email Headers**



# **RCPT TO:** is Destination Mailbox
# **TO:** is Display Mailbox

**The 'Destination' and the 'Display' mailboxes do NOT match and they should.**

**MAIL FROM: sender@somehost.com**
**RCPT TO: faber@sans.org** 
**DATA**
**From: spoof@someotherhost.com**
**To: anyone@anyhost.com** 
**Subject: Test Mail**
**Date: Mon, 18 Jul 18:00:00 +0100**
**MIME-Version: 1.0**
**Content-Type: text/plain**
**Hello, world**

# Return Path and From

**The 'Return-Path' and the 'From' do NOT match and they should.**

**Return-Path: <sender@somehost.com>**
**Delivered-To: faber@mx1.sans.org**
**Received:18 Jul 2005 15:52:43 -0400 (EDT)**
**Received: from mymailserver.net**
**by mua.mymailserver.net**
**for <faber@sans.org>; Mon, 18 Jul 15:52:43 -0400 (EDT)**

**From: spoof@wellsfargo.com**
**To: anyone@anyhost.com**
**Subject: Test Mail**
**Date: Mon, 18 Jul 18:00:00 +0100**
**MIME-Version: 1.0**
**Content-Type: text/plain**

# Follow the Path

5 → Received: from mail.spamfilter.com ([**274.82.240.51**]) by mail.final.recipient with sendmail(2.9.13)

4 → Received: from mail2.dshield.org (HELO iceman12-int.giac.net) (**274.173.218.116**)
by mail.spamfilter.com with AES256-SHA encrypted SMTP
Delivered-To: giac-ombudsman@giac.org

3 → Received: from unknown (HELO iceman12-ext.giac.net) (**274.173.218.115**)
by iceman12-int.giac.net with SMTP

2 → Received: from unknown (HELO so-net.ne.jp) (**222.168.113.245**)
by iceman12-ext.giac.net with SMTP

1 → Received: from Igzd5CJv (unknown [**208.105.230.47**]) by so-net.ne.jp (Coremail) with SMTP id q7UMK4x28C9HCbpN.1 for <ombudsman@giac.org>
Subject: sweet emotion !!
From: =?shift-jis?B?i1STY4FAikeU/A==?= <sayo_nara221@ocn.ne.jp>
To: <ombudsman@giac.org>
Return-Path: sayo_nara221@ocn.ne.jp

# How can I responsibly send mass emails?

- There are sometimes legitimate reasons to send out mass mailing
- Doing so runs the risk of being called a SPAMmer
- Responsible companies will take action to avoid this classification – but what steps should you take?

# How do I populate my mailing list?

- Double opt-in
  - User provides email address
  - User confirms subscription by response email
- Do not buy mailing lists
  - You have no control over how the seller obtained the email address
- Consider using listservs
  - Listservs allow for users to directly sign-up

# How should my recipient list be maintained?

- Periodic purge
  - Require recipients to positively respond
- Protect your mailing list
  - Never share your list with a third party
- Provide a working and immediate way to unsubscribe
  - Many will refuse to use it, but it should exist

# How should I actually send the mass emails?

- Do it in house
  - Protects recipient list and internalizes all responsibility and control
- Consider rate limiting
  - Keep an eye on bandwidth
- Hide the recipients (BCC or otherwise)
  - Be very careful that a recipient will not see other recipients email addresses
- Use legitimate DNS domains matching to appropriate IPs
  - Consider SPF records

# What else should I consider?

- Consult with legal counsel
  - CAN-SPAM in the US
  - Other legal issues may apply
- Monitor blacklist sites
  - http://relays.osirusoft.com/cgi-bin/rbcheck.cgi
  - http://tqmcube.com/rblcheck.php

# SPAM/Anti-Spam Battlefield Summary

- The SPAM/Anti-SPAM battlefield is constantly changing
  - Update your weapons
- Take measures to reduce the proliferation of SPAM
- Be responsible and do not become part of the problem