COSC 301
Network Management and Security

Lecture 14: Electronic Mail

Today's Focus

Electronic Mail

-- How does it work?
-- How to manage it?
-- How to ensure security & privacy?

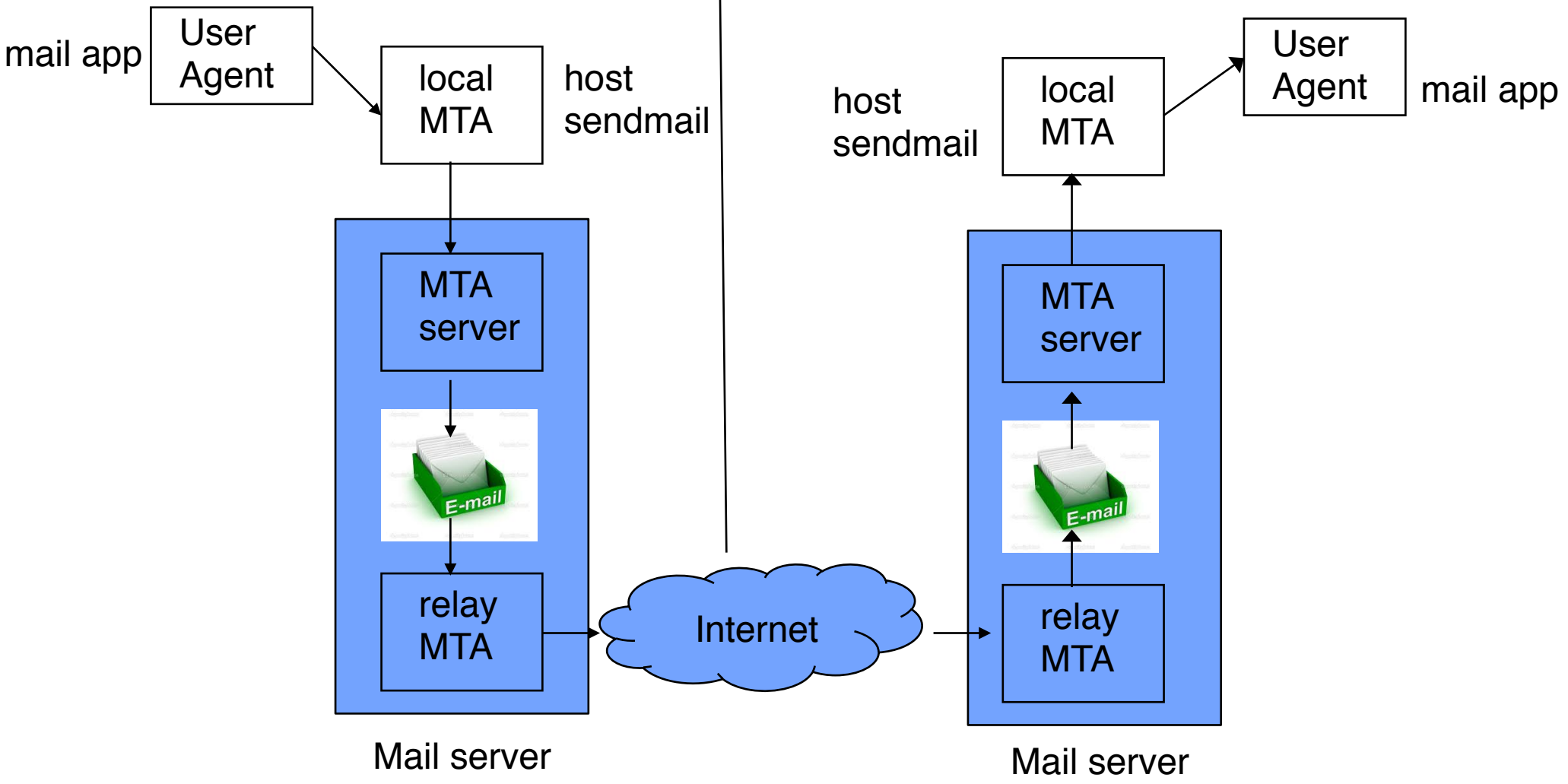
What is an email?

- A formatted file in ASCII code
- Consists of
  - Envelope
  - Header
  - Body

Components in Email Architecture

- User Agent (UA)
  - For users to compose, send, and browse emails
  - mutt, pine, Mail, ThunderBird
- Mail Transport Agent (MTA)
  - Emails are handed to it for delivery
  - sendmail, exim
- Mail Access Agent (MAA)
  - Retrieve message from mailbox
  - Using POP3, IMAP

Email Architecture



Email Protocols

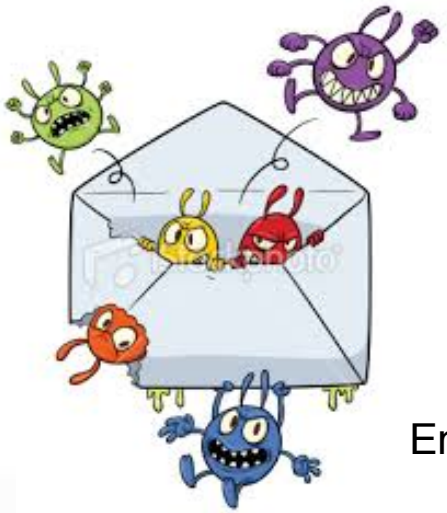
- SMTP (Simple Mail Transfer Protocol)
  - Email delivery protocol between two MTAs
  - Used twice: between the sender and the sender's mail server and between the two mail servers
- Mail fetching protocols
  - Between the receiver and its mail server
  - Post Office Protocol (POP): simple but limited in functionality
  - Internet Mail Access Protocol (IMAP): more features, more powerful and more complex.
    - Can check the e-mail header prior to downloading
    - Can search the contents for a specific string prior to downloading
    - Can partially download email

SMTP example

- S: 220 smtp.example.com ESMTP Postfix
- C: HELO relay.example.org
- S: 250 Hello relay.example.org, I am glad to meet you
- C: MAIL FROM:<bob@example.org>
- S: 250 Ok
- C: RCPT TO:<alice@example.com>
- S: 250 Ok
- C: RCPT TO:<theboss@example.com>
- S: 250 Ok
- C: DATA
- S: 354 End data with <CR><LF>.<CR><LF>
- C: From: "Bob Example" <bob@example.org>
- C: To: Alice Example <alice@example.com>
- C: Cc: theboss@example.com
- C: Date: Tue, 15 January 2008 16:02:43 -0500
- C: Subject: Test message
- C:
- C: Hello Alice.
- C: This is a test message with 5 header fields and 4 lines in the message body.
- C: Your friend,
- C: Bob
- C: .
- S: 250 Ok: queued as 12345
- C: QUIT
- S: 221 Bye
- {The server closes the connection}

Email Security and Privacy

Email Spams



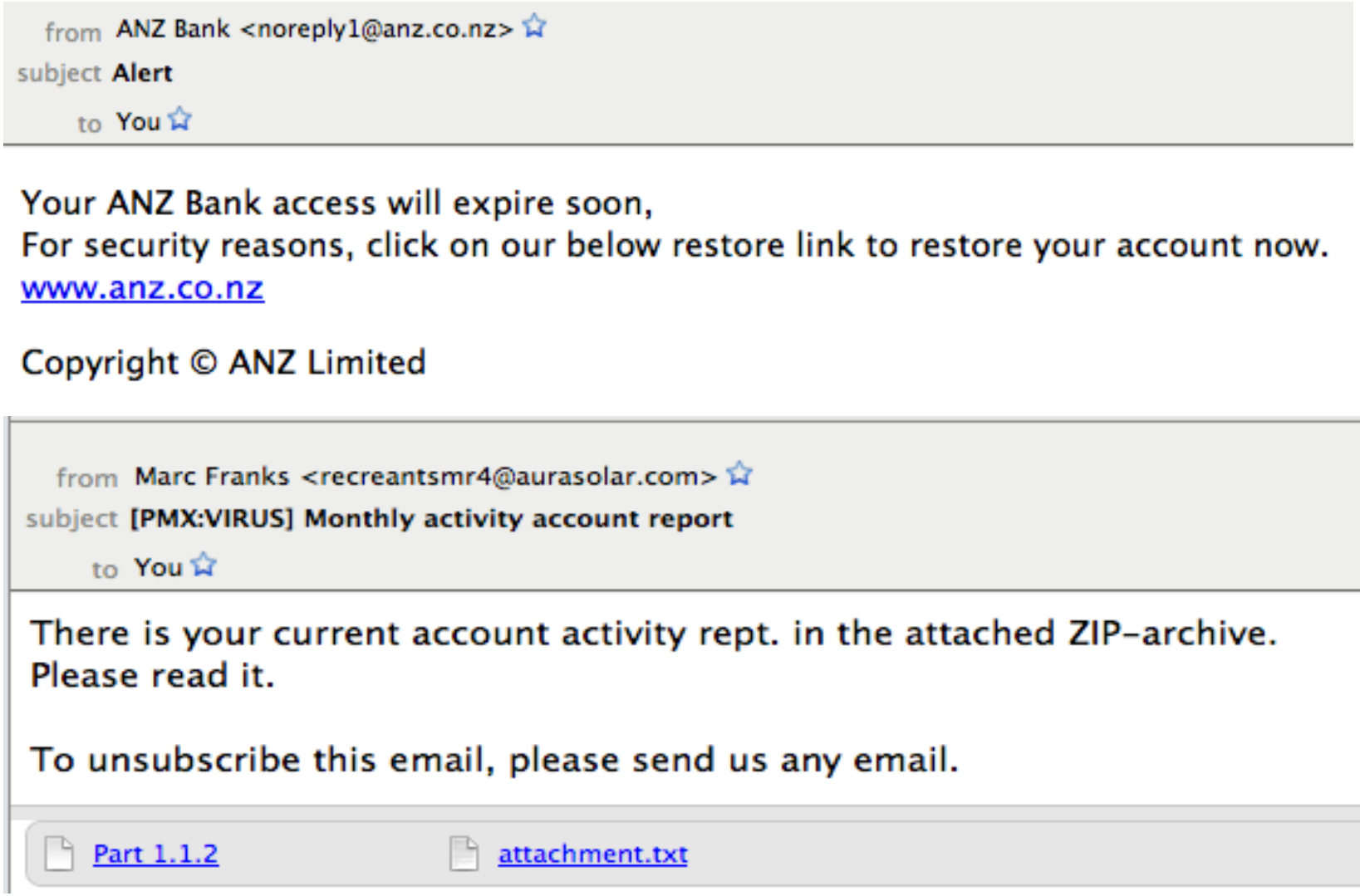
Email Virus

Attacks or threats

Email Spams (1)

- Also called **junk emails**
  - Anonymity: address and identity of the sender are concealed
  - Mass Mailing: sent to large groups of people
  - Unsolicited: not requested by the recipients
- Email spams grow steadily.
  - ~ 200 billion spam messages sent per day [2010]
  - > 97% of all emails sent over Internet are unwanted
- The negatives
  - Use up mailbox space
  - Click links in spam email may send users to phishing websites or sites that host malware.
  - May contain malware such as scripts or executable file attachments
  - Deception and fraud

Email Spams (2)



from ANZ Bank <noreply1@anz.co.nz>
subject **Alert**
to You

Your ANZ Bank access will expire soon,
For security reasons, click on our below restore link to restore your account now.
www.anz.co.nz

Copyright © ANZ Limited

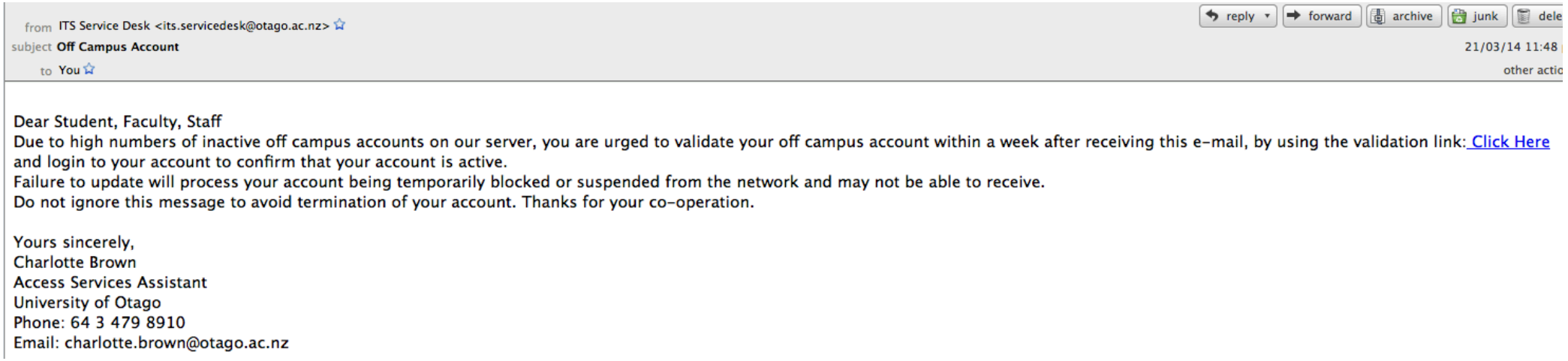
from Marc Franks <recreantsmr4@aurasolar.com>
subject **[PMX:VIRUS] Monthly activity account report**
to You

There is your current account activity rept. in the attached ZIP-archive.
Please read it.

To unsubscribe this email, please send us any email.

Part 1.1.2 attachment.txt

Email Spams (3)

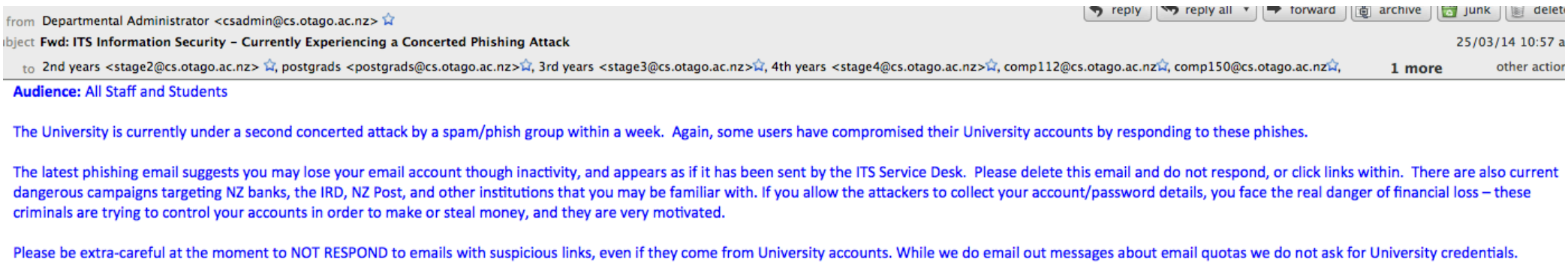


from ITS Service Desk <its.servicedesk@otago.ac.nz>
subject **Off Campus Account**
to You

reply | forward | archive | junk | dele
21/03/14 11:48
other actio

Dear Student, Faculty, Staff
Due to high numbers of inactive off campus accounts on our server, you are urged to validate your off campus account within a week after receiving this e-mail, by using the validation link: Click Here
and login to your account to confirm that your account is active.
Failure to update will process your account being temporarily blocked or suspended from the network and may not be able to receive.
Do not ignore this message to avoid termination of your account. Thanks for your co-operation.

Yours sincerely,
Charlotte Brown
Access Services Assistant
University of Otago
Phone: 64 3 479 8910
Email: charlotte.brown@otago.ac.nz



from Departmental Administrator <csadmin@cs.otago.ac.nz>
ubject **Fwd: ITS Information Security – Currently Experiencing a Concerted Phishing Attack**
to 2nd years <stage2@cs.otago.ac.nz>, postgrads <postgrads@cs.otago.ac.nz>, 3rd years <stage3@cs.otago.ac.nz>, 4th years <stage4@cs.otago.ac.nz>, comp112@cs.otago.ac.nz, comp150@cs.otago.ac.nz, **1 more**

reply | reply all | forward | archive | junk | delet
25/03/14 10:57 a
other actior

Audience: All Staff and Students

The University is currently under a second concerted attack by a spam/phish group within a week. Again, some users have compromised their University accounts by responding to these phishes.

The latest phishing email suggests you may lose your email account though inactivity, and appears as if it has been sent by the ITS Service Desk. Please delete this email and do not respond, or click links within. There are also current dangerous campaigns targeting NZ banks, the IRD, NZ Post, and other institutions that you may be familiar with. If you allow the attackers to collect your account/password details, you face the real danger of financial loss – these criminals are trying to control your accounts in order to make or steal money, and they are very motivated.

Please be extra-careful at the moment to NOT RESPOND to emails with suspicious links, even if they come from University accounts. While we do email out messages about email quotas we do not ask for University credentials.

Email Spoofing/Phishing

- Spoofing is the creation of email messages with a forged sender address
  - Simple to do because the core protocol do no authentication
- Phishing is the attempt to acquire sensitive information such as usernames, passwords, and credit card details by masquerading as a trustworthy entity
  - Typically carried out by email spoofing
- Tips to identify spoofing and phishing email
  - Are the URLs legitimate?
  - Incorrect grammar/spelling
  - Suspicious attachments
  - Request for personal information
  - Urgent/Too good to be true
  - IP Reputation

Manual detection of spams

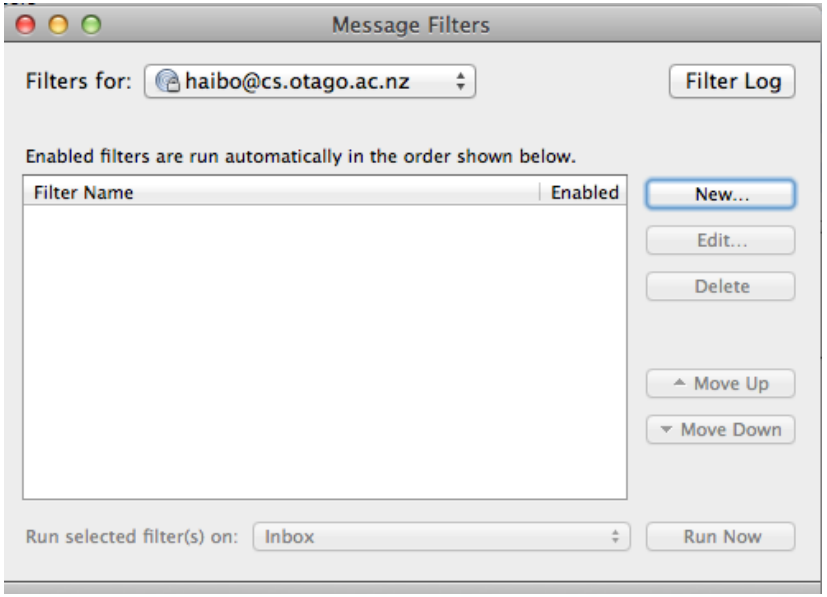
- Return-Path: <mdp@dataclick.com.ar>
- Delivered-To: hzy@cs.otago.ac.nz
- Received: from mailhost.staff.otago.ac.nz (its-mail-p11.registry.otago.ac.nz [10.67.0.110])
- by chasm.otago.ac.nz (Postfix) with ESMTPS id 710893583BDE
- for <hzy@cs.otago.ac.nz>; Wed, 5 Apr 2017 19:20:17 +1200 (NZST)
- X-CrossPremisesHeadersFilteredBySendConnector:
- its-mail-p11.registry.otago.ac.nz
- Received: from mailhub7.otago.ac.nz (10.31.30.64) by
- mailhost.staff.otago.ac.nz (10.67.0.112) with Microsoft SMTP Server id
- 15.0.1178.4; Wed, 5 Apr 2017 19:20:17 +1200
- Received: from server9054prueba.fangio.net ([190.106.132.71])
- by mailhub7.otago.ac.nz (8.13.8/8.13.8) with ESMTP id v357KFXx011478
- for <hzy@cs.otago.ac.nz>; Wed, 5 Apr 2017 19:20:16 +1200
- Message-ID: <201704050720.v357KFXx011478@mailhub7.otago.ac.nz>
- Received: from [192.168.1.100] (unknown [41.82.73.209])
- (Authenticated sender: mdp@dataclick.com.ar)
- by server9054prueba.fangio.net (Postfix) with ESMTPA id E755F62CDB;
- Wed, 5 Apr 2017 04:18:40 -0300 (ART)
- Content-Type: multipart/alternative; boundary="==========0755280919=="
- MIME-Version: 1.0
- Subject: Its me Ruth
- To: Recipients <mdp@dataclick.com.ar>
- From: <mdp@dataclick.com.ar>
- Date: Wed, 5 Apr 2017 08:19:46 +0100
- Reply-To: <ruthmawerer@gmail.com>
- X-PMX-Version: 5.6.0.2009776, Antispam-Engine: 2.7.2.376379, Antispam-Data: 2017.4.5.70920
- X-PerlMx-Spam: Gauge=XXXXIIIIII, Probability=46%,

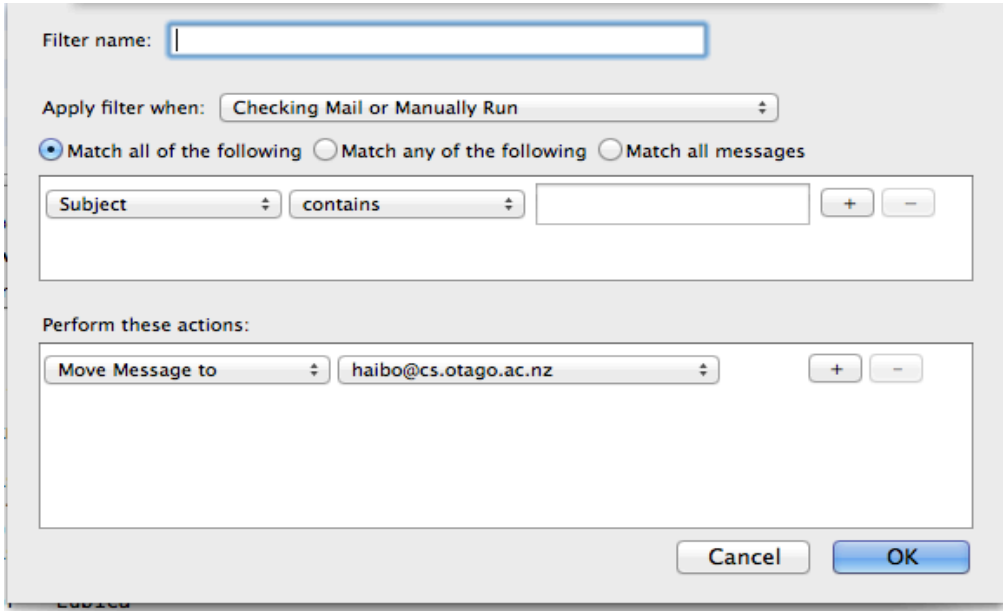
Anti-Spam Techniques (1)

- Detect spam email
  - Subject line: “I have money for you”
  - Attachments: .exe
  - Contents
  - DNSBLs: lists of domain names of known spammers
- End-user techniques
  - Report an unsolicited email: http://complaints.antispam.govt.nz
  - Do not expose your email address unless necessary
    - Spammers can collect email addresses from websites, customer lists, newsgroups, and viruses which harvest users' address books.
  - Avoid responding to spams
  - Disposable email addresses

Anti-Spam Techniques (2)

- Automated techniques
  - DNS-based blacklists
  - Pattern detection
  - Email filtering
    - Statistical content filtering
    - Checksum-based filtering
    - Rule-based filtering
    - Hybrid filtering
    - …





Email Virus

- A virus (malware program) that comes within an attached file in an email message.
  - Trojan horse
  - macro virus
  - …
- Don't trust attachments. Pay attention to the extensions of the attachments
  - Files with .EXE or .VBS extensions are always suspect
  - zip archives may contain executable codes
  - A full list of blocked extensions in Otago Email system http://www.otago.ac.nz/its/services/security/otago030398.html
- If uncertain, scan it using an anti-virus software

Email Bomb

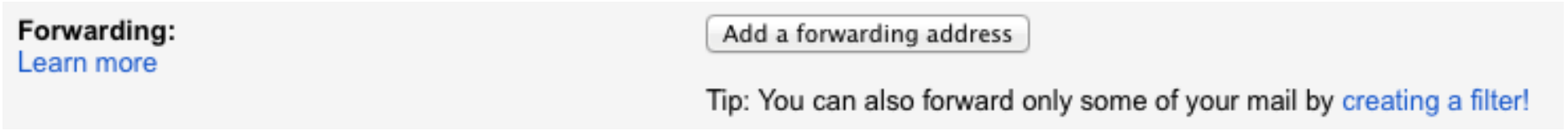
- A form of network abuse consisting of sending huge volumes of email to an address in attempt to overflow the mailbox or the server where the email address is hosted.
- Is a type of denial-of-service attack (DDoS)
- Methods of Email bombing
  - Mass mailing
    - Can be easily detected by spam filters
  - List linking
    - Mailing lists
  - Zip bombing
    - Zip files that take long time for the email server to unpack and check contents.

Email Privacy

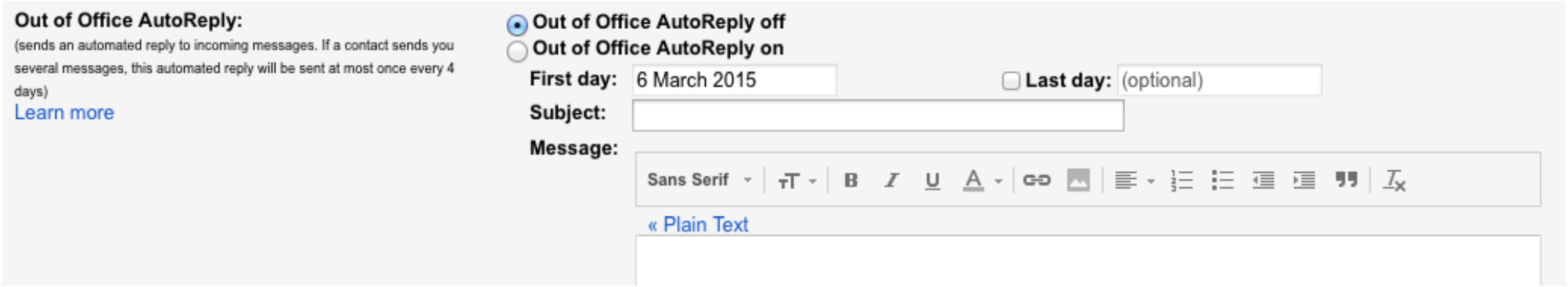
- STARTTLS: a TLS(SSL) layer on top of the SMTP connection that protects emails from being sniffed during transmission
  - encryption takes place between individual SMTP relays, not between the sender and the recipient.
- S/MIME(Secure MIME): a standard for public key encryption and signing of MIME data
  - digital signing and message encryption using certificates

MTA Configuration (1)

- Auto-forwarding
  - Automatically forward emails to another mailbox

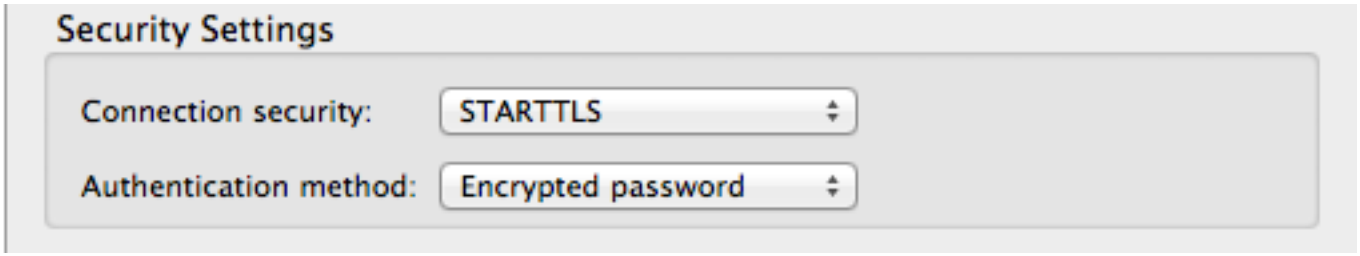


- Auto-reply
  - I am on vacation between ** and **.

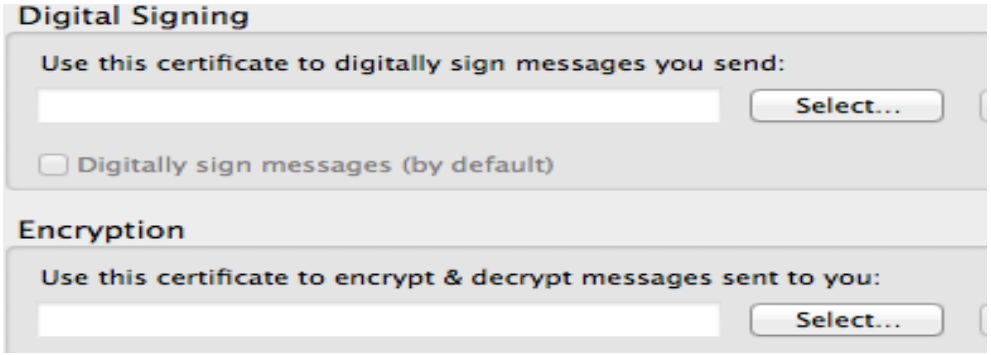


MTA Configuration (2)

- Email fetching protocol
  - POP or IMAP?
- Mailing list
- Server security setting



- Digital signature and encryption



Summary

- Email format and SMTP
- Manual SPAM checking
- Security risks of emails, like malware, DDoS