

---

# What Email can tell you?

## Examiner's perspective

Kitisak Jirawannakool

Information Security Specialist

Electronic Government Agency (Public Organization)



# Agenda

- ❖ Understand about email system
- ❖ Email Threats
- ❖ Investigation
  - ❖ Manual
  - ❖ Automated (Online)



# Contact me

---

Name : Kitisak Jirawannakool

Facebook : <http://www.facebook.com/kitisak.note>

Email : [kitisak.jirawannakool@ega.or.th](mailto:kitisak.jirawannakool@ega.or.th)  
[jkitisak@gmail.com](mailto:jkitisak@gmail.com)

Weblog : <http://foh9.blogspot.com>

Twitter : @kitisak

# #whoami

- ❖ Information Security Specialist at EGA
- ❖ OWASP Thailand Chapter Leader
- ❖ Certification and Award
  - ❖ COMTIA Security+
  - ❖ Asia Pacific Information Security Leader Achievements 2011 (ISLA) by (ISC)2
- ❖ Membership
  - ❖ APWG, ShadowServer, OWASP, MSCP, CSAThailand Chapter, MedSec



Of course, I am an anonymous cyclist, not hacker !!!!

# About EGA

- ❖ Electronics Government Agency (Public Organization)
- ❖ First established in 1997 as Government Information Technology Services (GITS)
- ❖ ~ 200 staffs
- ❖ Mainly focus on providing IT infrastructure to the Government of Thailand
- ❖ Vision
  - ❖ Enabling Complete and Secure E-Government

# Our Services (Examples)

- ❖ Government Information Network (GIN)
- ❖ Government Cloud Services (G-Cloud)
- ❖ Government Computer Emergency and Readiness Team (G-CERT)
- ❖ MailgoThai service
- ❖ Government App Center (GAC)
- ❖ Government Big/Open Data ([data.go.th](http://data.go.th))
- ❖ National Data Center
- ❖ More details : <http://www.ega.or.th>





Government Computer  
Emergency and Readiness  
Team (G-CERT)

Risk Assessment

Incident Monitoring

Information Analysis

Response Team

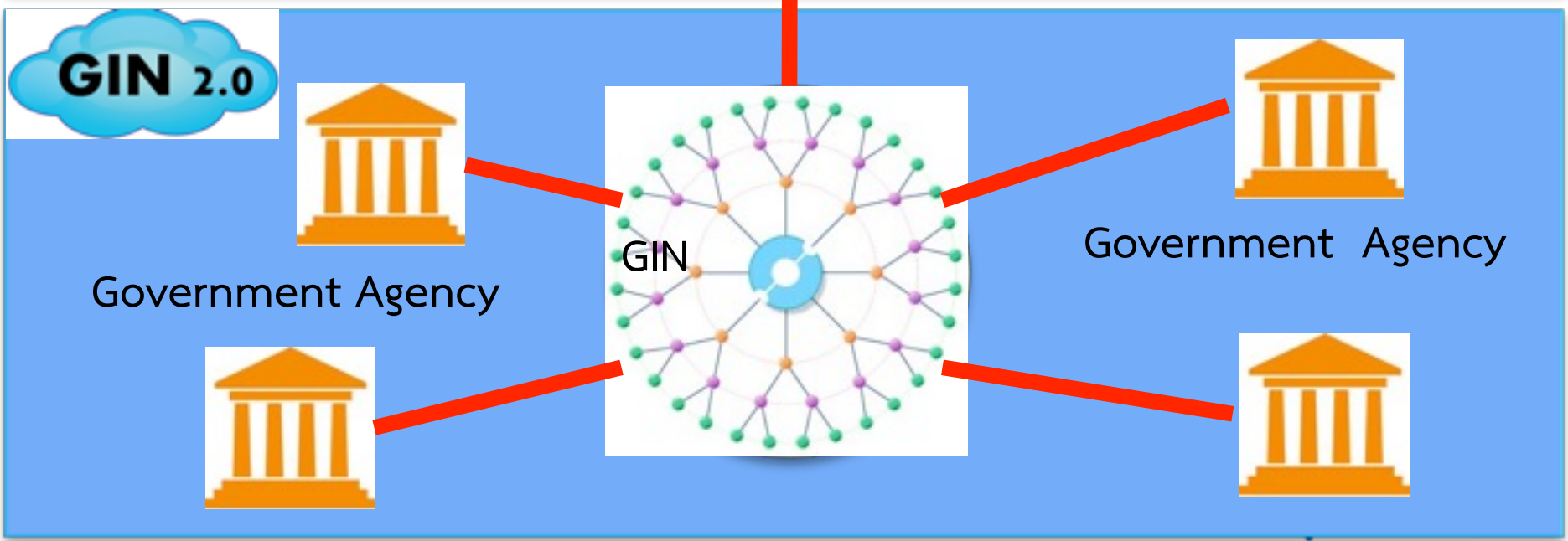
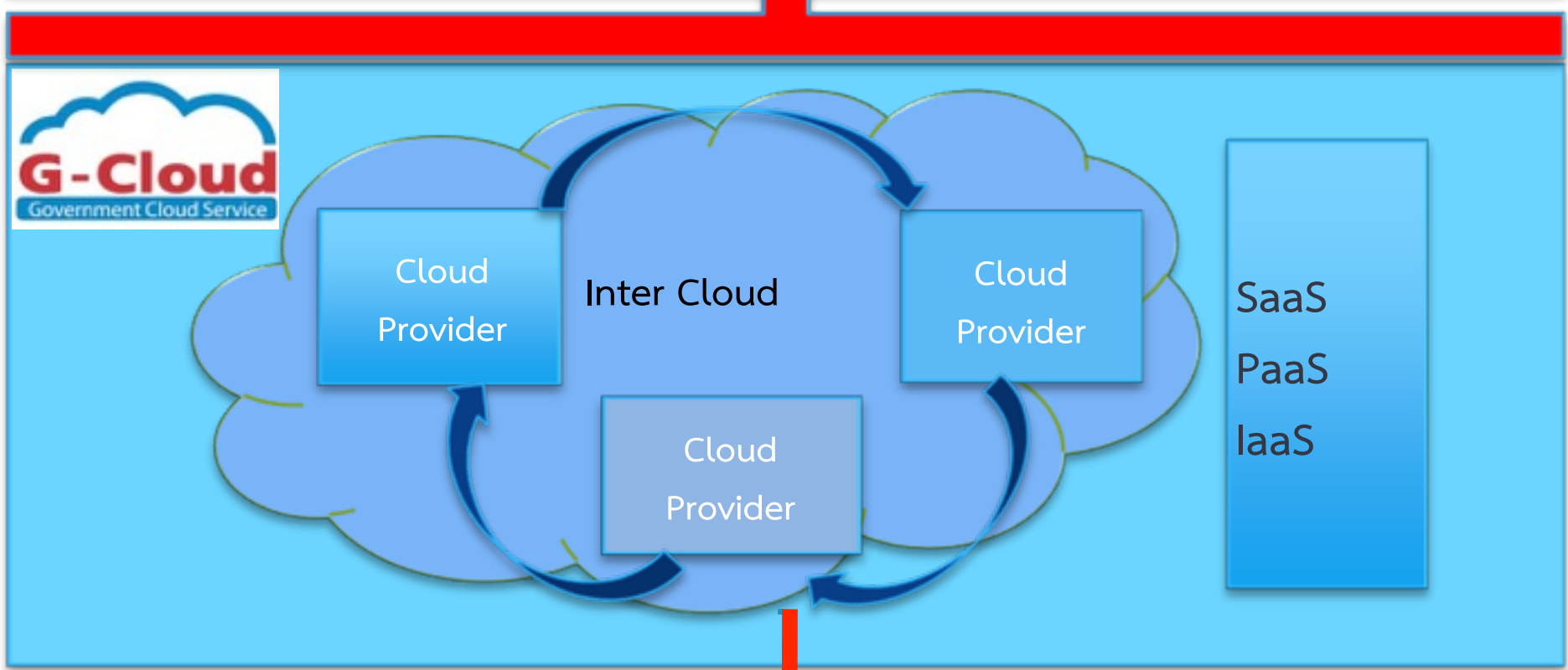
Awareness Raising

Services



**M@il.Go.th**  
ระบบจดหมายอิเล็กทรอนิกส์  
เพื่อการสื่อสารในภาครัฐ

Other Government's services

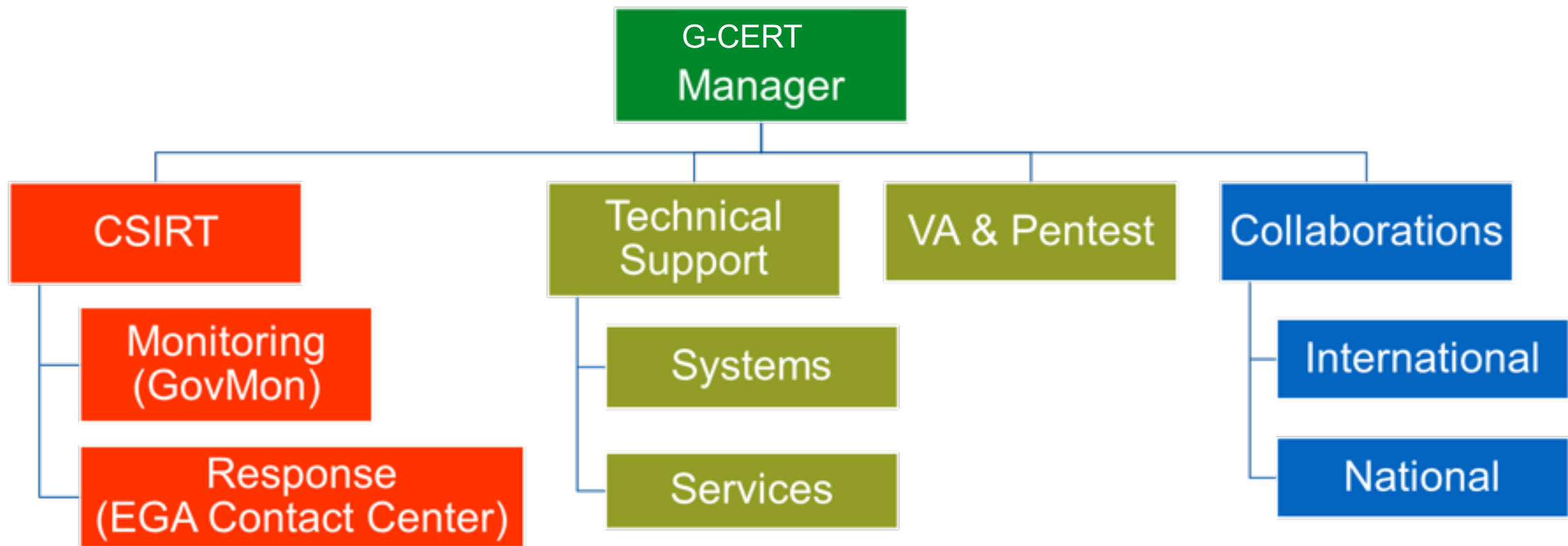


EGA Contact Center  
24x7 Helpdesk and Contact Center





# G-CERT 's Roadmap



Education (Training and Awareness Raising)

Policy and Standard

Media Relations (PR and Contents producer)

Start in 2014

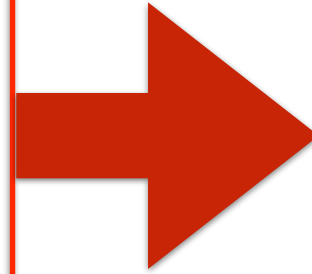
Start in 2015

Start in 2016



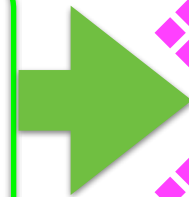
# G-CERT 's constituencies

- ❖ EGA Internal
- ❖ EGA 's customers
  - ❖ G-Cloud
  - ❖ GIN
  - ❖ other services



- ❖ Notify
- ❖ Advisory
- ❖ On-call/site Consulting

- ❖ Critical Infrastructures
- ❖ Government



- ❖ Notify
- ❖ Advisory

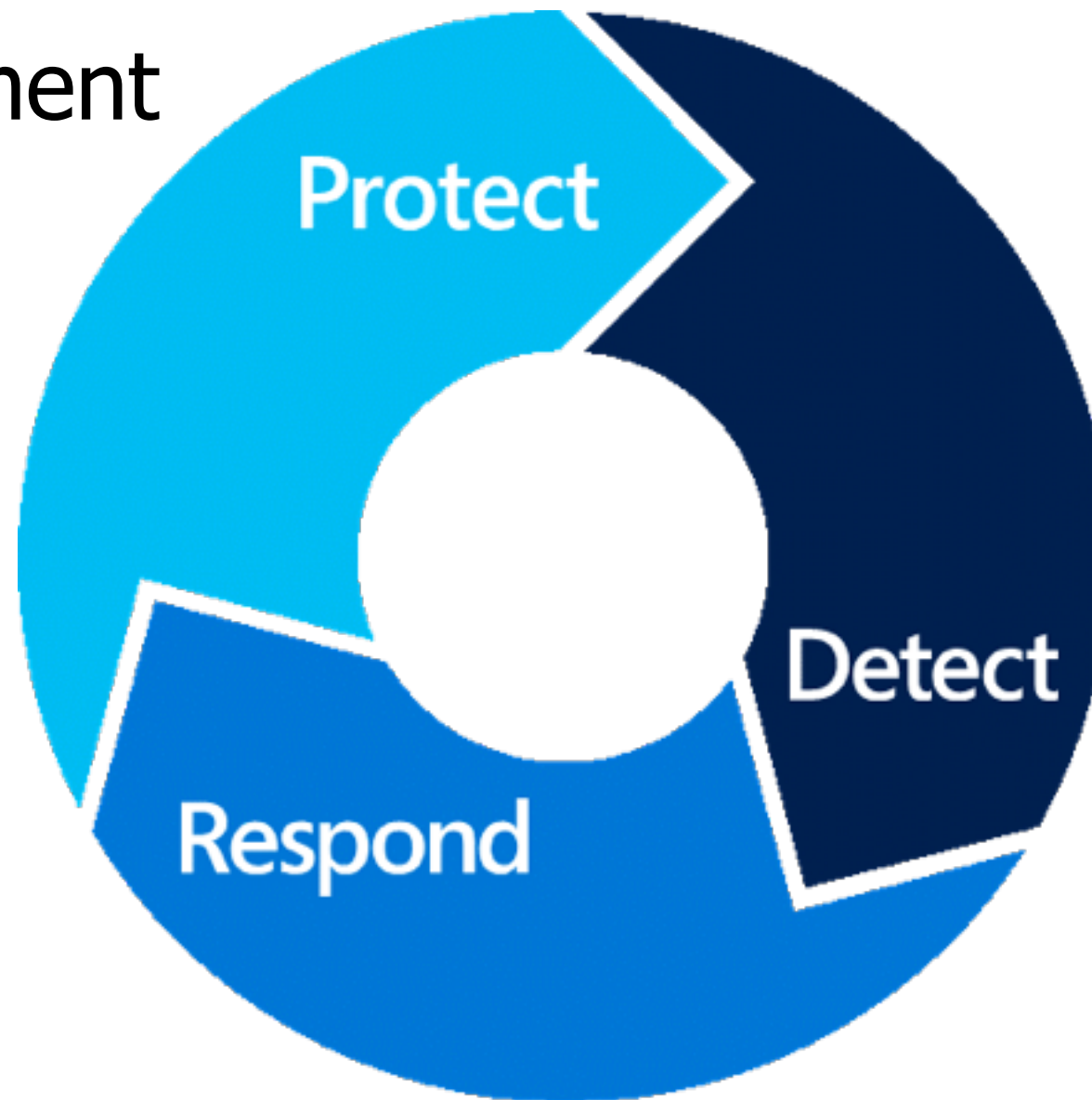
# Our Concept

- ❖ Public - help the government
- ❖ Private - by working with vendors
- ❖ Partnership - collaborate with other CERT and other IT communities



# G-CERT 's services

- ❖ Risk Management
- ❖ Securely Design
- ❖ Vulnerability Management



- ❖ Threats monitoring
- ❖ Security Operation

- ❖ Incident Response/Handling
- ❖ Security Consulting
- ❖ Security Training, Workshop and Drills





# Free IT Security Educations for Gov.

- ❖ Training courses
- ❖ Incident Drills
- ❖ Conferences





# Topics

Email System Basics

Email Crimes

Email Header

Automate Email Investigation

# Topics

Email System Basics

Email Crimes

Email Header

Automate Email Investigation

# Email Terminology

- ❖ IMAP/IMAPs
- ❖ SMTP
- ❖ HTTP/HTTPS
- ❖ POP3/POP3s
- ❖ CC
- ❖ BCC
- ❖ Attachment
- ❖ Email Client
- ❖ Email Server
- ❖ Encoding

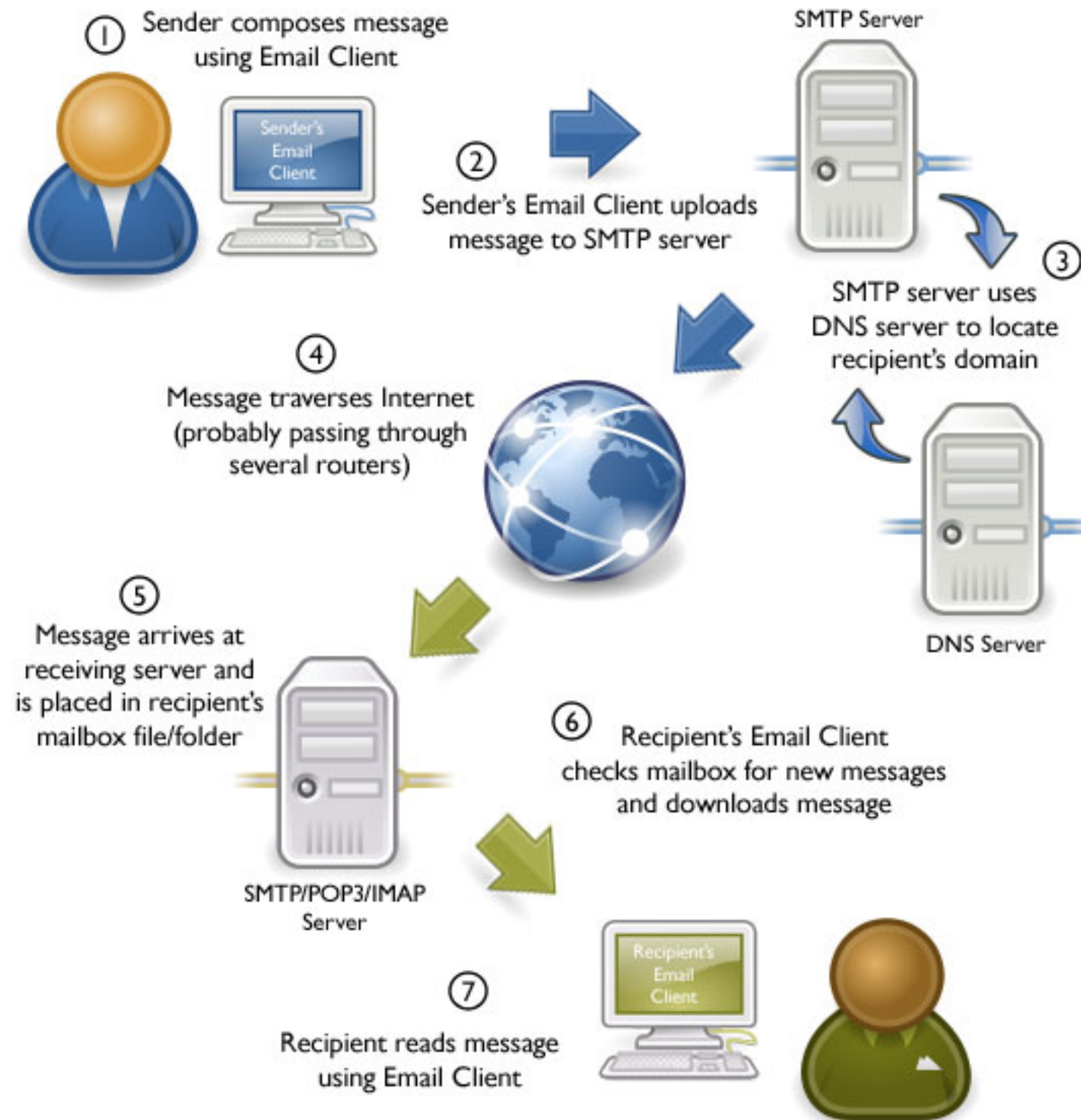


# Email Components

---

- ❖ Header
- ❖ Contents
- ❖ Sending and Delivering mechanisms
  - ❖ Email client
  - ❖ Webmail
- ❖ Mail Server and Gateway
- ❖ Protocols
  - ❖ SMTP
  - ❖ POP/IMAP(s)

# Email System



©2010 OnlyMyEmail Inc. (www.OnlyMyEmail.com) with many thanks to the Gnome project (www.gnome.org) for the images

# Email Clients

- ❖ Application that allows you to send, receive and organise emails
- ❖ Functions
  - ❖ Retrieve messages from a mailbox
  - ❖ Display the headers of all the messages in mailbox
  - ❖ Allow you to select a message header and read the body of the email message



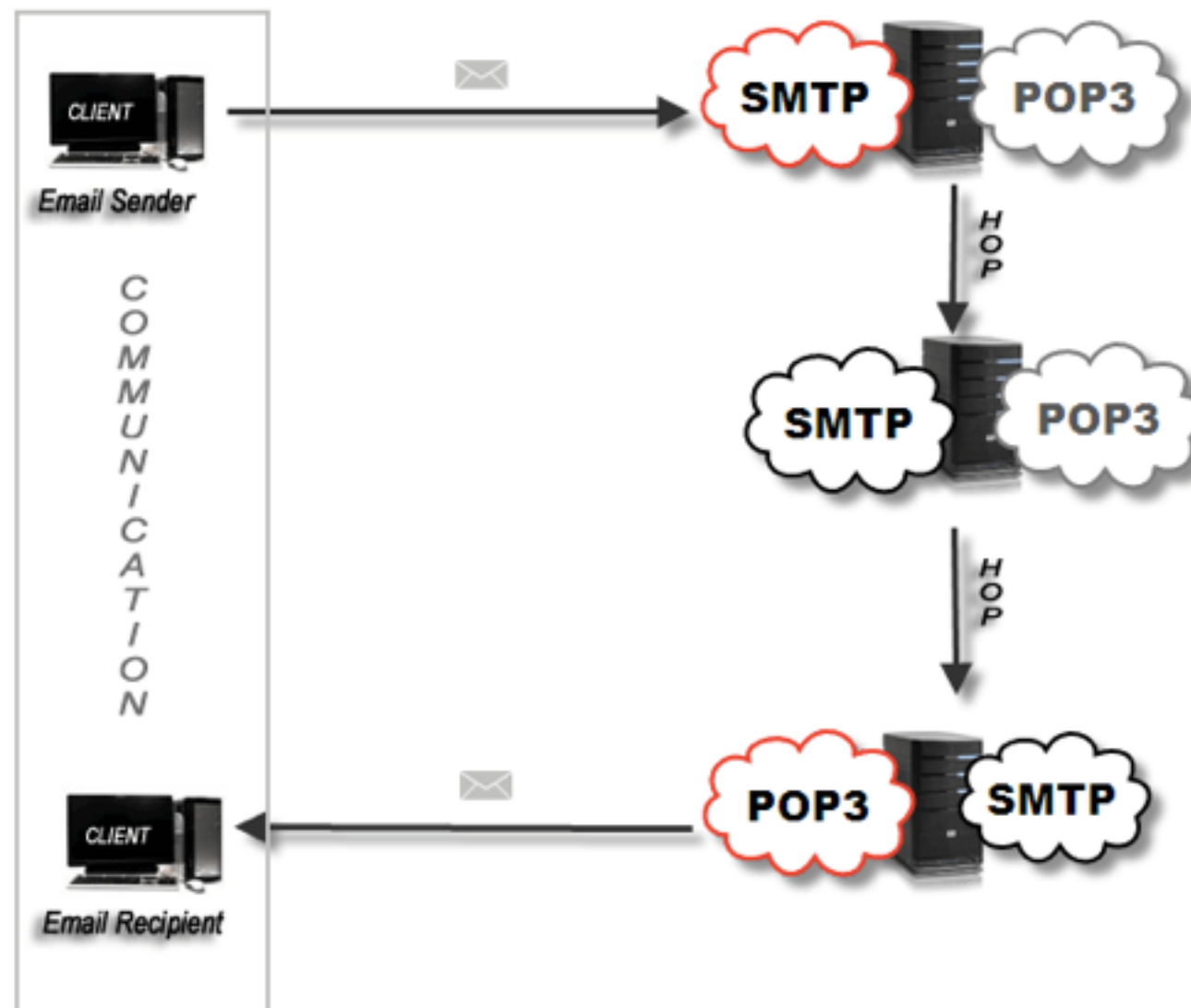
# Email Server

- ❖ A computer within the network that works as a virtual post office
- ❖ Types
  - ❖ Outgoing
    - ❖ SMTP
  - ❖ Incoming
    - ❖ IMAP
    - ❖ POP3



# SMTP

- ❖ Simple Mail Transfer Protocol
- ❖ Default port is 25/TCP





# 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}
```

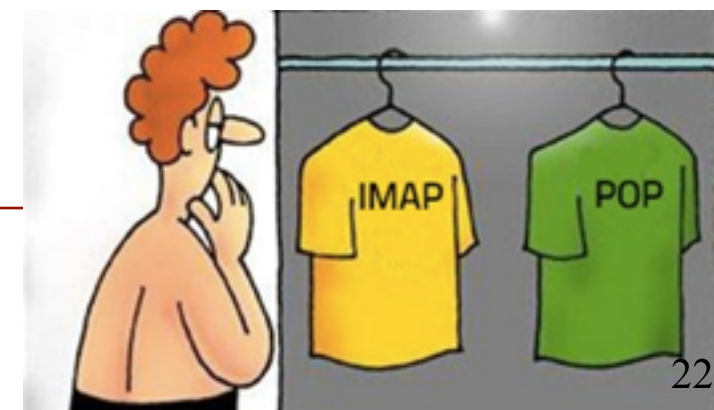
# POP3 & IMAP servers

## POP3 - Post Office Protocol

- ❖ You can use only one computer to check your email (no other devices)
- ❖ Your mails are stored on the computer that you use
- ❖ Sent mail is stored locally on your PC, not on a mail server
- ❖ Port 110/TCP

## IMAP - Internet Messaging Access Protocol

- ❖ You can use multiple computers and devices to check your email
- ❖ Your mails are stored on the server
- ❖ Sent mail stays on the server so you can see it from any device
- ❖ Port 143/TCP





# Email Message

## Header

**From:** sexybeast@gmail.com  
**To:** rcarey@gmail.com  
**CC:** everyoneincreation@gmail.com  
**Subject:** URGENT BUSINESS MATTER!!!

### **Good afternoon, Mr. Carey:**

I am writing to you today to introduce myself. I am an ad specialty sales rep hear in your area. I have worked with other businesses in the community and feel I can be of service to you as well.

BTW: I have been in the business for 25 years. Please contact me if you have any upcoming events or promotions.

Regards,  
John Jones, account exec  
ABC Sales

## Body

## Signature

# Topics

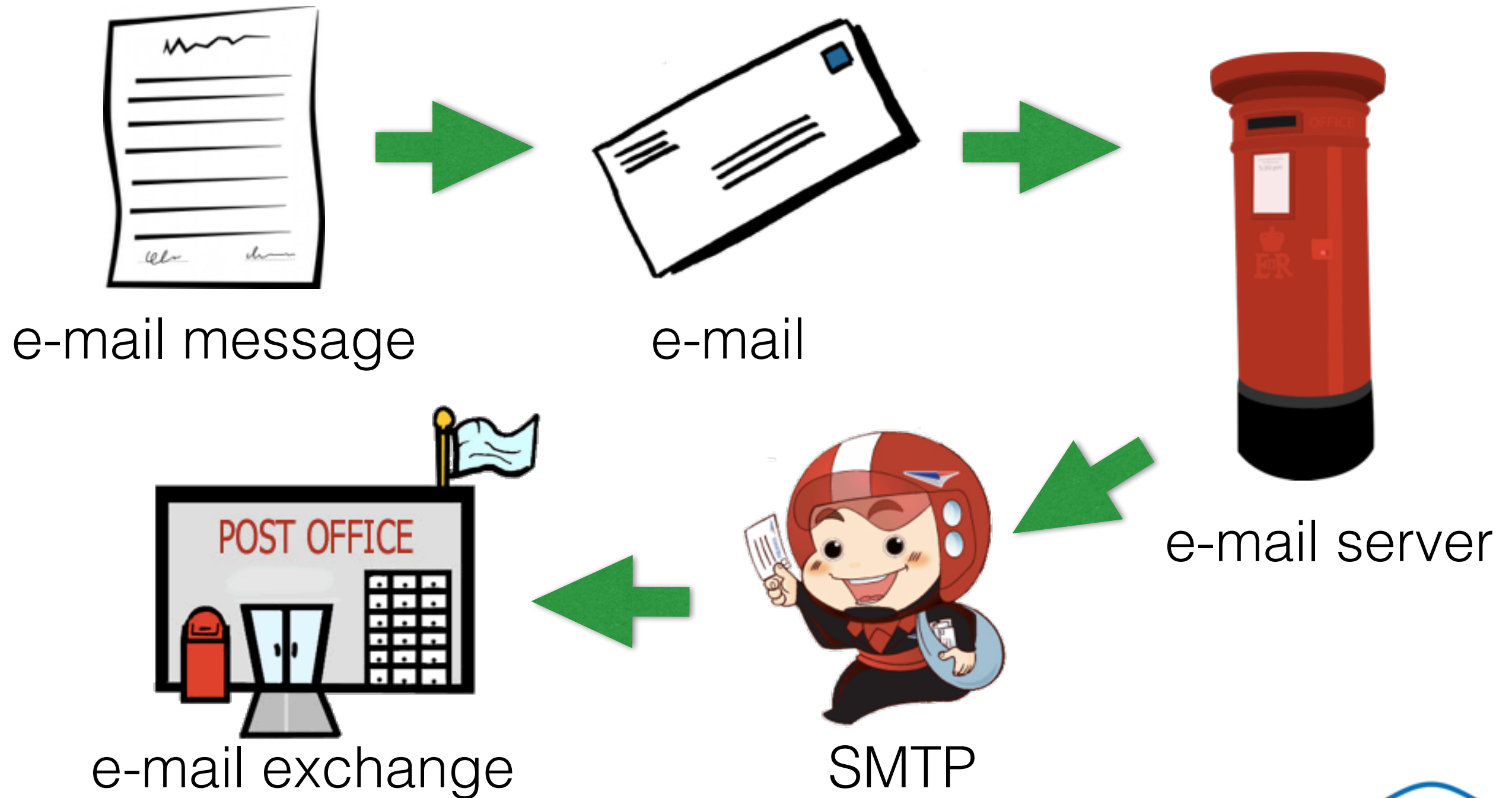
Email System Basics

Email Crimes

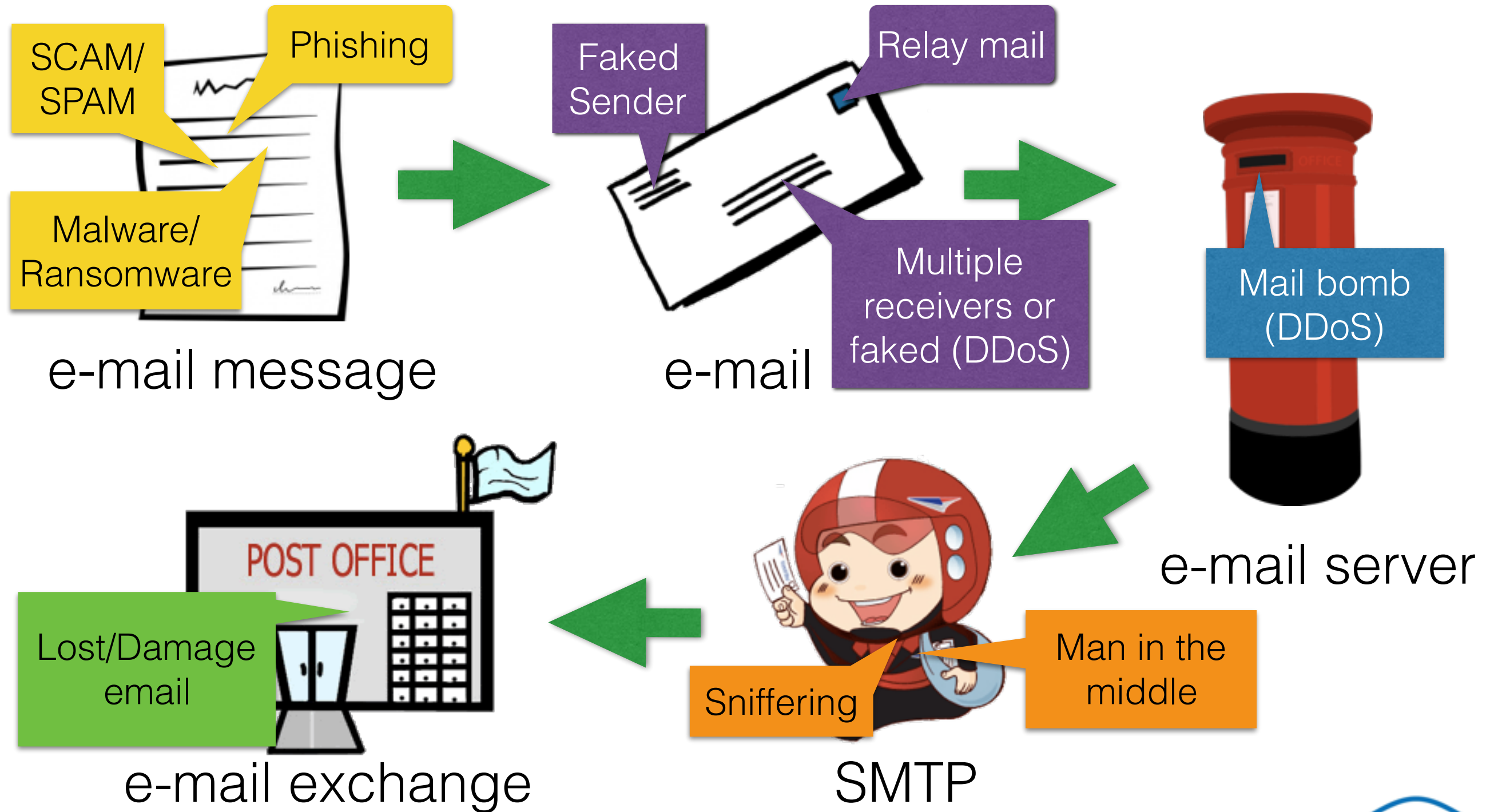
Email Header

Automate Email Investigation

# Mail Ecosystem



# Email Attacks - Overview



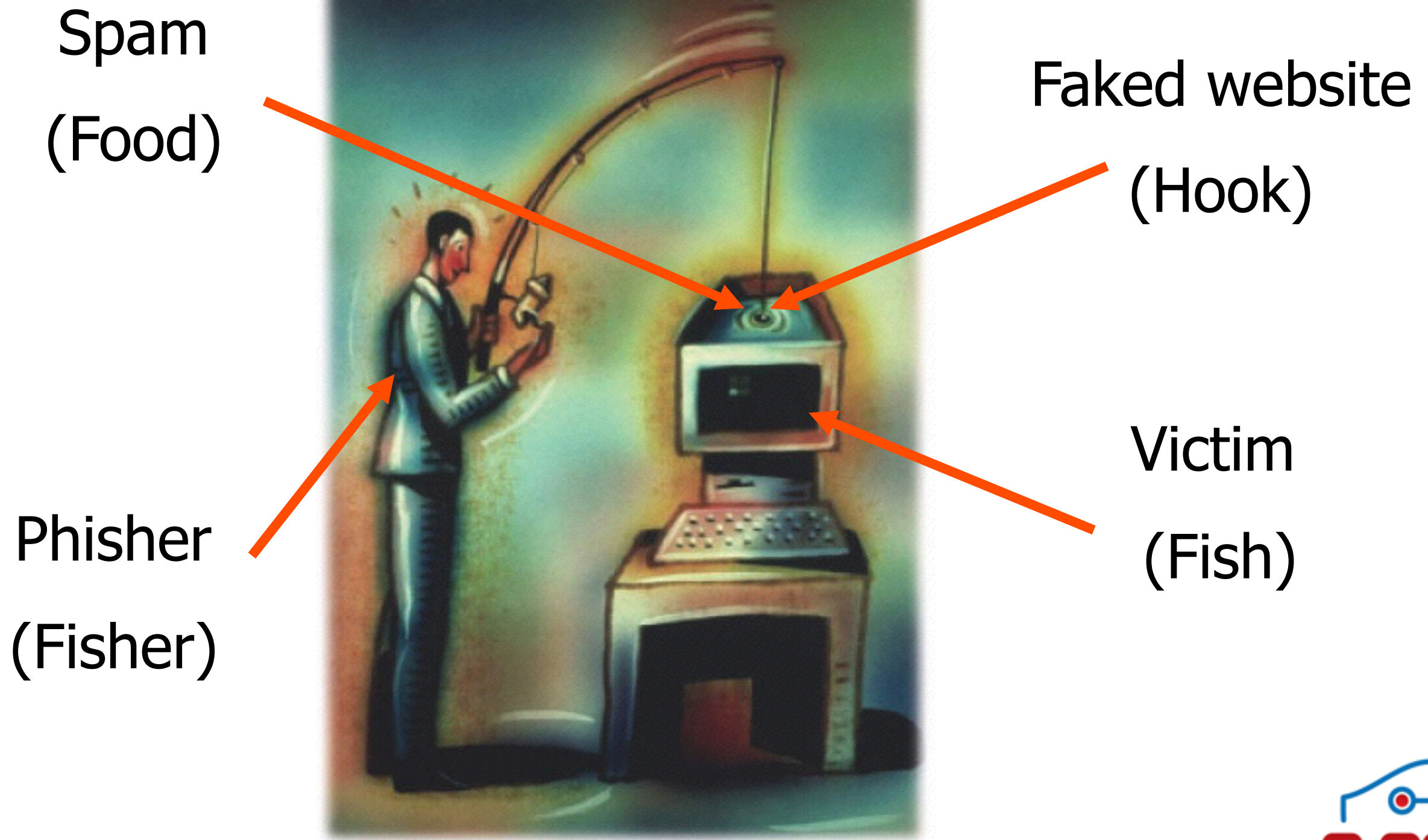
# SPAM/SCAM

- ❖ Spam is a kind of thing that is useless, and sometimes people spam for fun, but annoy others.
- ❖ Scam is a kind of thing where you steal some thing, or a rip off, or some thing. Lie for your own greed. or giving some one for some thing of theirs when you aren't even going to give your something.





# Phishing



# Types of phishing

- ❖ Consumer-focused phishing
  - ❖ Widely spread (will show examples later)
- ❖ Spear phishing
  - ❖ Pick a few targets and try to phish



# Spear phishing email

- ❖ Targeted phishing attack
  - ❖ Contains contextual content instead of random messages
- ❖ Harder to detect, since spearphishing emails look more genuine
- ❖ Victims are asked to
  - ❖ Download malicious attachments
  - ❖ Reply with sensitive information
  - ❖ Click on URLs
  - ❖ ...

# Anatomy of phishing email (1)

From: Internal Revenue Service [irs-service@IRS.GOV] Sent: Tue 2/3/2009 3:55 PM  
To:  
Cc:  
Subject: Official Notification

After the last annual calculations of your fiscal are eligible to receive a tax refund of \$92.50. Please submit the tax refund request and allow us 3-6 days in order to process it. A refund can be delayed for a variety of reasons. For example submitting invalid records or applying after the deadline.

To access the form for your tax refund, please click here :

<http://cimaonline.ca/form/Internal/Revenue/Service/index.html>

Regards,  
Internal Revenue Service.

© Copyright 2009, Internal Revenue Service U.S.A.

Phishing emails are often sent from addresses that look official.

Clicking on this link would take you to a fraudulent website with a form to enter your personal information.

Notice that the URL does not direct you to an official IRS website.

# Anatomy of phishing email (2)

**From:** University of Memphis Webmail Management [webmaster@memphis.edu]  
**Sent:** Thursday, October 30, 2008 3:52 PM  
**Subject:** VERIFY YOUR EMAIL ACCOUNT

Attention: Outlook Web User,

This message is to all University of Memphis Webmail Users.

We are currently upgrading our data base and webmail network ce  
All inactive email accounts will be deleted, as we intend to increas  
create more space for registration of new users (Staff and Student

To prevent your account from being deleted, we kindly request that you confirm your account information for  
update, by providing the information below:  
Username :  
Password :

Warning!!! Failure to do this will render your email

Thanks for your understanding  
Warning Code: VX2G99AAJ  
University of Memphis Webmail Management

In this example, references to the University are used to try to trick you into responding.

But, you can be sure this email is fake because the University will never request your username and password.



# How to Help Protect Yourself

**1** Don't trust links in an email.

**DANGER!** <http://www.amazon.com/update>

**2** Never give out personal information upon email request.

**DANGER!** Name:

Credit Card:

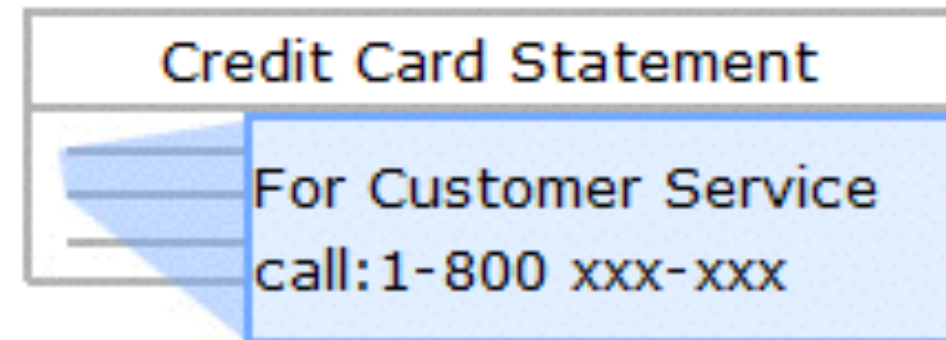
**3** Look carefully at the web address.



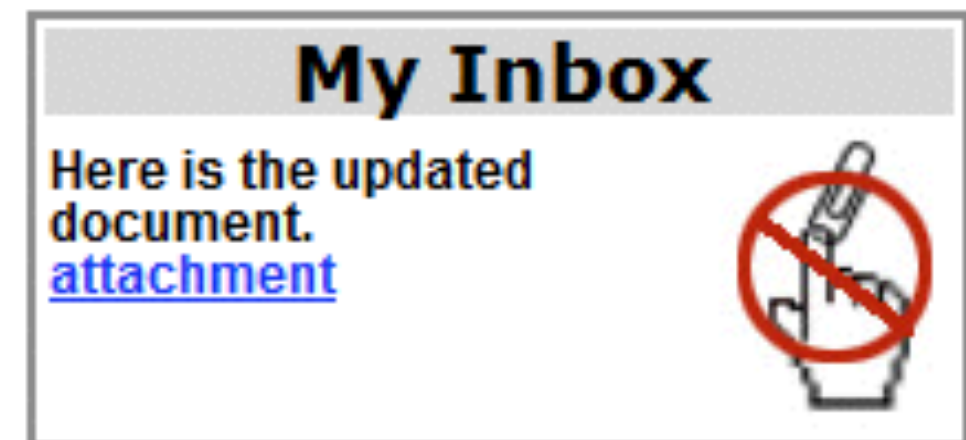
**4** Type in the real website address into a web browser.



**5** Don't call company phone numbers in emails or instant messages. Check a reliable source such as a phone book or credit card statement.

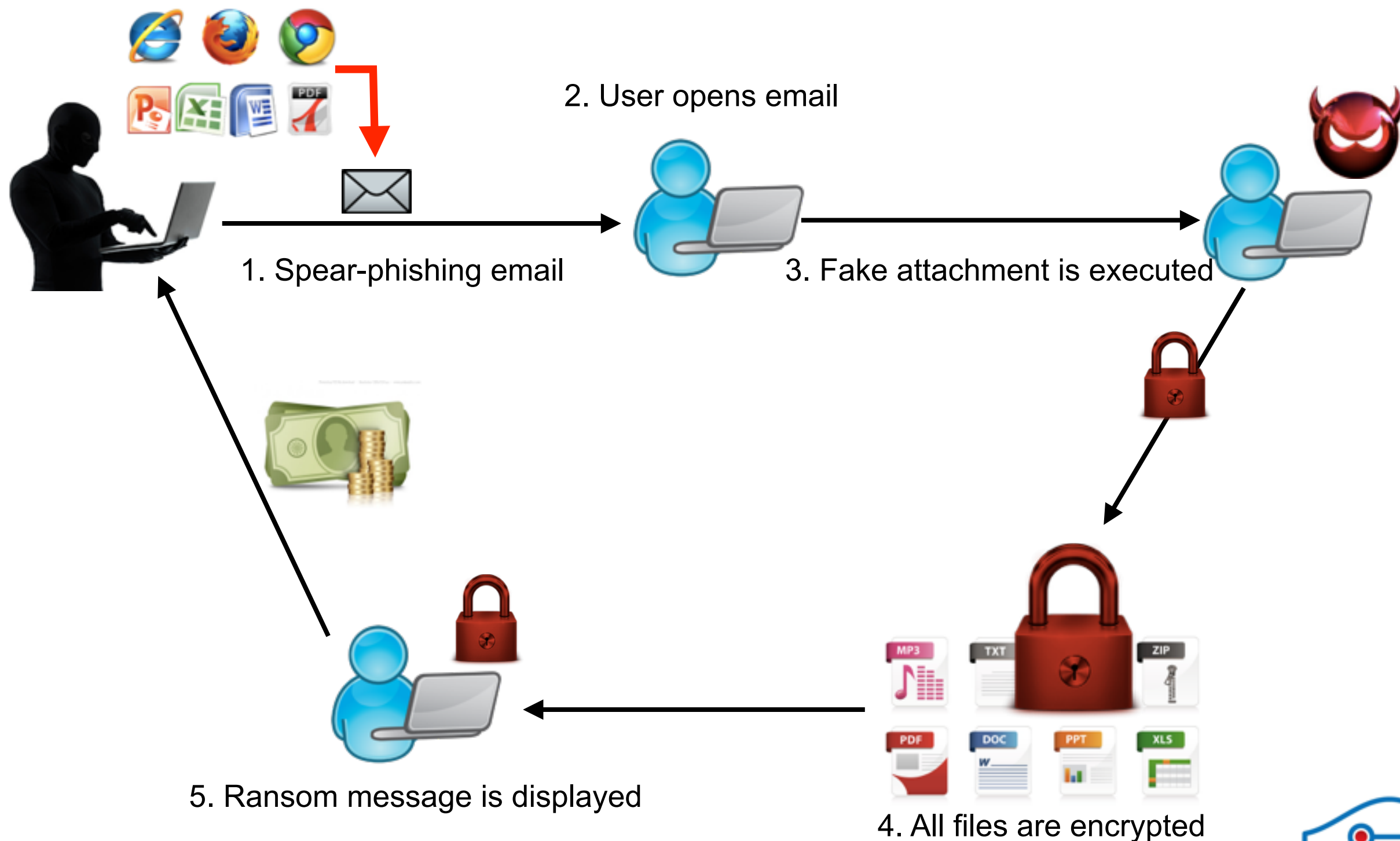


**6** Don't open unexpected email attachments or instant message download links.



Reference : <http://education.apwg.org/>

# Spear Phishing + Ransomware



# Email Spoofing

- ❖ **Forgery of an email header** that the message appears to have originated from someone or somewhere other than the actual source
- ❖ Spammers and perpetrators of phishing change the email header fields
  - ❖ From
  - ❖ Return-Path
  - ❖ Reply-To-Fields

# Faking Sender

- ❖ Deception strategy
  - ❖ The new email which is little bit different from the original
  - ❖ For examples
    - ❖ ggtw123@gmail.com -> qqtw123@gmail.com
    - ❖ little\_bee@company.co.th -> little\_bee@c0mpany.co.th
- ❖ Spoof whole email
  - ❖ Use the mail relaying techniques
  - ❖ Account compromised



# Mail Relaying (Spoof sender)

- ❖ Use the SMTP service directly (bypass authentication)
- ❖ telnet <ip address of mail server> 25

```
Command Prompt
220 in07.muc1.mx.trendmicro.eu ESMTP Postfix
HELO local.domain.com
250 in07.muc1.mx.trendmicro.eu
MAIL FROM: [redacted]@[redacted]
250 2.1.0 Ok
RCPT TO: [redacted]
250 2.1.5 Ok
DATA
354 End data with <CR><LF>.<CR><LF>
"SUBJECT: [This is test]"

This is test, please ignore.
.
250 2.0.0 Ok: queued as DC9A[redacted]
QUIT
221 2.0.0 Bye

Connection to host lost.
```

# Mail bombing

- ❖ Sending large number of emails
- ❖ Focus on consuming resources
  - ❖ Capacity of mailbox
  - ❖ Bandwidth
- ❖ A kind of DDoS attack



# Sniffing and Man in the middle attack

- ❖ Target to unsecured communication
- ❖ Focus on 2 things
  - ❖ Steal information
  - ❖ Modify message



# Topics

Email System Basics

Email Crimes

Email Header

Automate Email Investigation



Received-SPF: pass (google.com: domain of chris@example.com; Tue, 12 Jul 2016 13:40:34 -0700) with ESMTTP id n2s15516221pfj-66.171.248.166 as permitted sender) client-ip=66.171.248.166  
Authentication-Results: mx.google.com: spf=pass  
chris@example.com designates 66.171.248.166 as  
smtp.mailfrom=chris@example.com  
Received: from [192.168.1.122] (192.168.1.1) by  
ESMTTP (EIMS X 3.3.9) for <joe.user@example.com>  
13:40:34 -0700  
From: Chris <chris@example.com>  
Content-Type: multipart/alternative;  
boundary="Apple-Mail=\_3EEF9FAD-3853-48CF-8509-  
are email headers



# Email Header

- ❖ The line which identify particular routing information of the message, including the sender, recipient, date and subject. Some headers are mandatory, such as the FROM, TO and DATE headers.
- ❖ How can we get email header?
  - ❖ Every emails have it
  - ❖ Depends on which application do you use
  - ❖ Need more skill to interpret

# Simple mail header

```
Return-path: <sender@senderdomain.tld>
Delivery-date: Wed, 13 Apr 2011 00:31:13 +0200
Received: from mailexchanger.recipientdomain.tld([ccc.ccc.ccc.ccc])
by mailserver.recipientdomain.tld running ExIM with esmtp
id xxxxxx-xxxxxx-xxx; Wed, 13 Apr 2011 01:39:23 +0200
Received: from mailserver.senderdomain.tld ([bbb.bbb.bbb.bbb]
helo=mailserver.senderdomain.tld)
by mailexchanger.recipientdomain.tld with esmtp id xxxxxx-xxxxxx-xx
for recipient@recipientdomain.tld; Wed, 13 Apr 2011 01:39:23 +0200
Received: from senderhostname [aaa.aaa.aaa.aaa] (helo=[senderhostname])
by mailserver.senderdomain.tld with esmtpa (Exim x.xx)
(envelope-from <sender@senderdomain.tld>) id xxxxx-xxxxxx-xxxx
for recipient@recipientdomain.tld; Tue, 12 Apr 2011 20:36:08 -0100
Message-ID: <xxxxxxxxx.xxxxxxxxxx@senderdomain.tld>
Date: Tue, 12 Apr 2011 20:36:01 -0100
X-Mailer: Mail Client
From: Sender Name <sender@senderdomain.tld>
To: Recipient Name <recipient@recipientdomain.tld>
Subject: Message Subject
```



# Header Details

- ❖ Return Path: The email address which should be used for bounces. The mail server will send a message to the specified email address if the message cannot be delivered
- ❖ Delivery-date: The data the message was delivered
- ❖ Date: The date the message was sent
- ❖ Message-ID: The ID of the message
- ❖ X-Mailer: The mail client (mail program) used to send the message
- ❖ From: The message sender in the format: "Friendly Name" <email@address.tld>
- ❖ To: The message recipient in the format: "Friendly Name" <email@address.tld>
- ❖ Subject: The message subject

# Other common header

- ❖ In-Reply-To: contains the message id of what the e-mail is being replied to. Not all e-mail servers will use this feature.
- ❖ Cc: contains any e-mail address that was sent a carbon copy of the message.
- ❖ Bcc: is any Blind Carbon Copy (BCC) e-mails that were also send the e-mail. Although not all e-mail programs display this information because of privacy concerns, there are several programs that will.
- ❖ Received: contain each of the mail servers that the e-mail has passed through to get to your Inbox.
- ❖ MIME: to know how to understand and display the e-mail in the e-mail program.
- ❖ .....

# Lines beginning with X-:

Anything beginning with X- is extra data that is not contained in any standard and is often used by the e-mail server or clients to provide additional information that can be used with the sending and delivery of an e-mail.

- ❖ X-Complaints-To: - Where to direct your complaints you have about an e-mail you received.
- ❖ X-Confirm-Reading-To: - Create an automatic response for read messages.
- ❖ X-Errors-To: The address to send an e-mail to for any errors encountered.
- ❖ X-Mailer: - Program used to send the e-mail.
- ❖ ... continue to next page



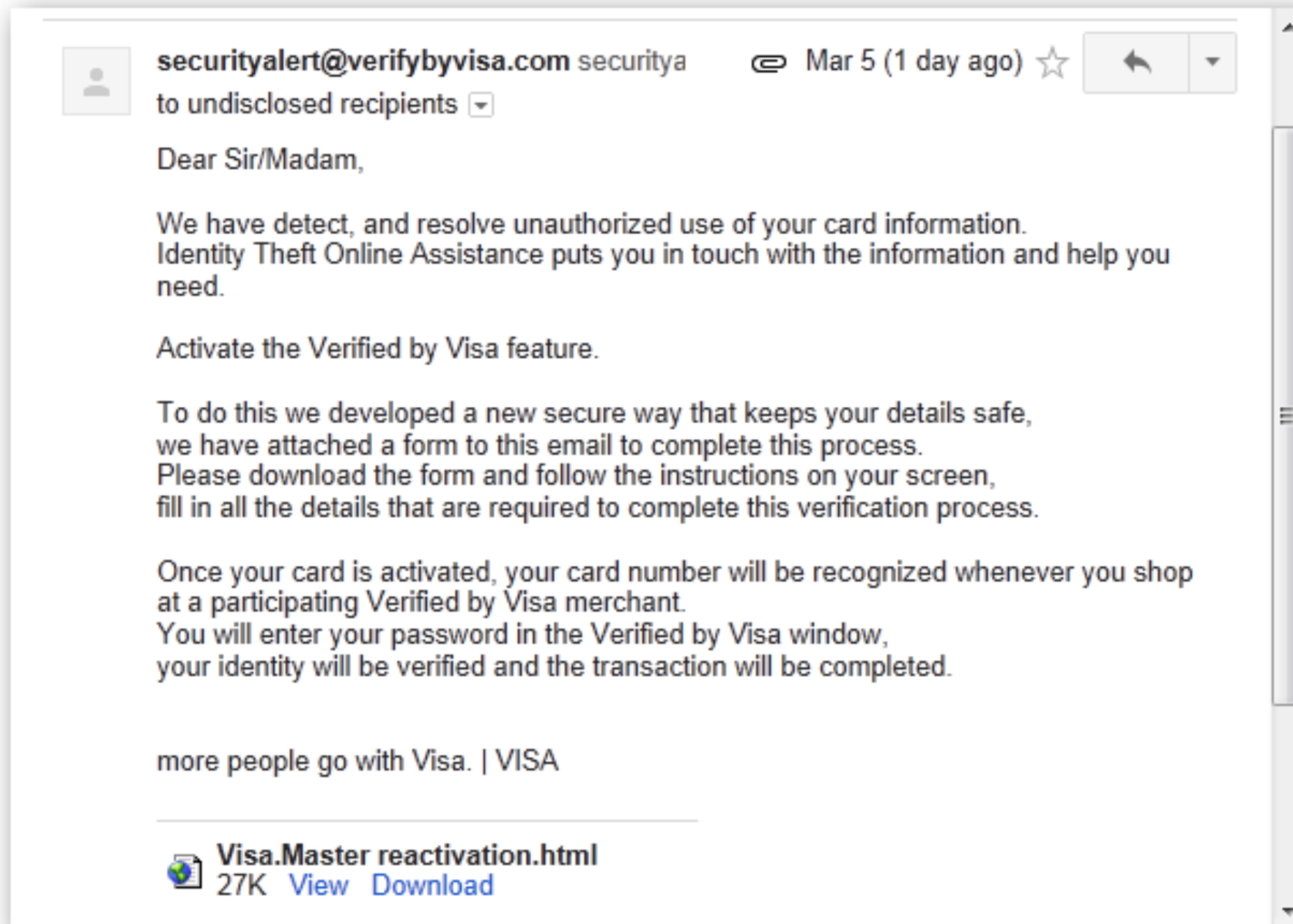
# Lines beginning with X-: (Cont'd)

- ❖ X-PMFLAGS: - Additional information used with Pegasus Mail.
- ❖ X-Priority: - Priority of e-mail being sent.
- ❖ X-Sender: - Additional information about the sender of the e-mail.
- ❖ X-Spam-zzz: - Where zzz is any number of different spam tags relating to the Spam filter on the e-mail server. Some of these include: Checker-Version, Level, Report, and Status.
- ❖ X-UIDL: - Used with e-mails distributed over POP.

# Email route

```
(3)Received: from
mailexchanger.recipientdomain.tld([ccc.ccc.ccc.ccc])
by mailserver.recipientdomain.tld running ExIM with esmtp
id xxxxxx-xxxxxx-xxx; Wed, 13 Apr 2011 01:39:23 +0200
(2)Received: from mailserver.senderdomain.tld ([bbb.bbb.bbb.bbb]
helo=mailserver.senderdomain.tld)
by mailexchanger.recipientdomain.tld with esmtp id xxxxxx-xxxxxx-xx
for recipient@recipientdomain.tld; Wed, 13 Apr 2011 01:39:23 +0200
(1)Received: from senderhostname [aaa.aaa.aaa.aaa]
(helo=[senderhostname])
by mailserver.senderdomain.tld with esmtpa (Exim x.xx)
(envelope-from <sender@senderdomain.tld) id xxxxx-xxxxxx-xxxx
for recipient@recipientdomain.tld; Tue, 12 Apr 2011 20:36:08 -0100
```

# Workshop#1



Delivered-To: myemail@gmail.com  
Received: by 10.60.14.3 with SMTP id l3csp12958oec;  
Mon, 5 Mar 2012 23:11:29 -0800 (PST)  
Received: by 10.236.46.164 with SMTP id r24mr7411623yhb.101.1331017888982;  
Mon, 05 Mar 2012 23:11:28 -0800 (PST)  
Return-Path: <securityalert@verifybyvisa.com>  
Received: from ms.externalemail.com (ms.externalemail.com. [XXX.XXX.XXX.XXX])  
by mx.google.com with ESMTP id t19si8451178ani.110.2012.03.05.23.11.28;  
Mon, 05 Mar 2012 23:11:28 -0800 (PST)  
Received-SPF: fail (google.com: domain of securityalert@verifybyvisa.com does not  
designate XXX.XXX.XXX.XXX as permitted sender) client-ip=XXX.XXX.XXX.XXX;  
Authentication-Results: mx.google.com; spf=hardfail (google.com: domain of  
securityalert@verifybyvisa.com does not designate XXX.XXX.XXX.XXX as permitted sender)  
smtp.mail=securityalert@verifybyvisa.com  
Received: with MailEnable Postoffice Connector; Tue, 6 Mar 2012 02:11:20 -0500  
Received: from mail.lovingtour.com ([211.166.9.218]) by ms.externalemail.com with  
MailEnable ESMTP; Tue, 6 Mar 2012 02:11:10 -0500  
Received: from User ([118.142.76.58])  
by mail.lovingtour.com  
; Mon, 5 Mar 2012 21:38:11 +0800  
Message-ID: <6DCB4366-3518-4C6C-B66A-F541F32A4C4C@mail.lovingtour.com>  
Reply-To: <securityalert@verifybyvisa.com>  
From: "securityalert@verifybyvisa.com" <securityalert@verifybyvisa.com>  
Subject: Notice  
Date: Mon, 5 Mar 2012 21:20:57 +0800  
MIME-Version: 1.0  
Content-Type: multipart/mixed;  
boundary="--=\_NextPart\_000\_0055\_01C2A9A6.1C1757C0"  
X-Priority: 3  
X-MSMail-Priority: Normal  
X-Mailer: Microsoft Outlook Express 6.00.2600.0000  
X-MimeOLE: Produced By Microsoft MimeOLE V6.00.2600.0000  
X-ME-Bayesian: 0.000000

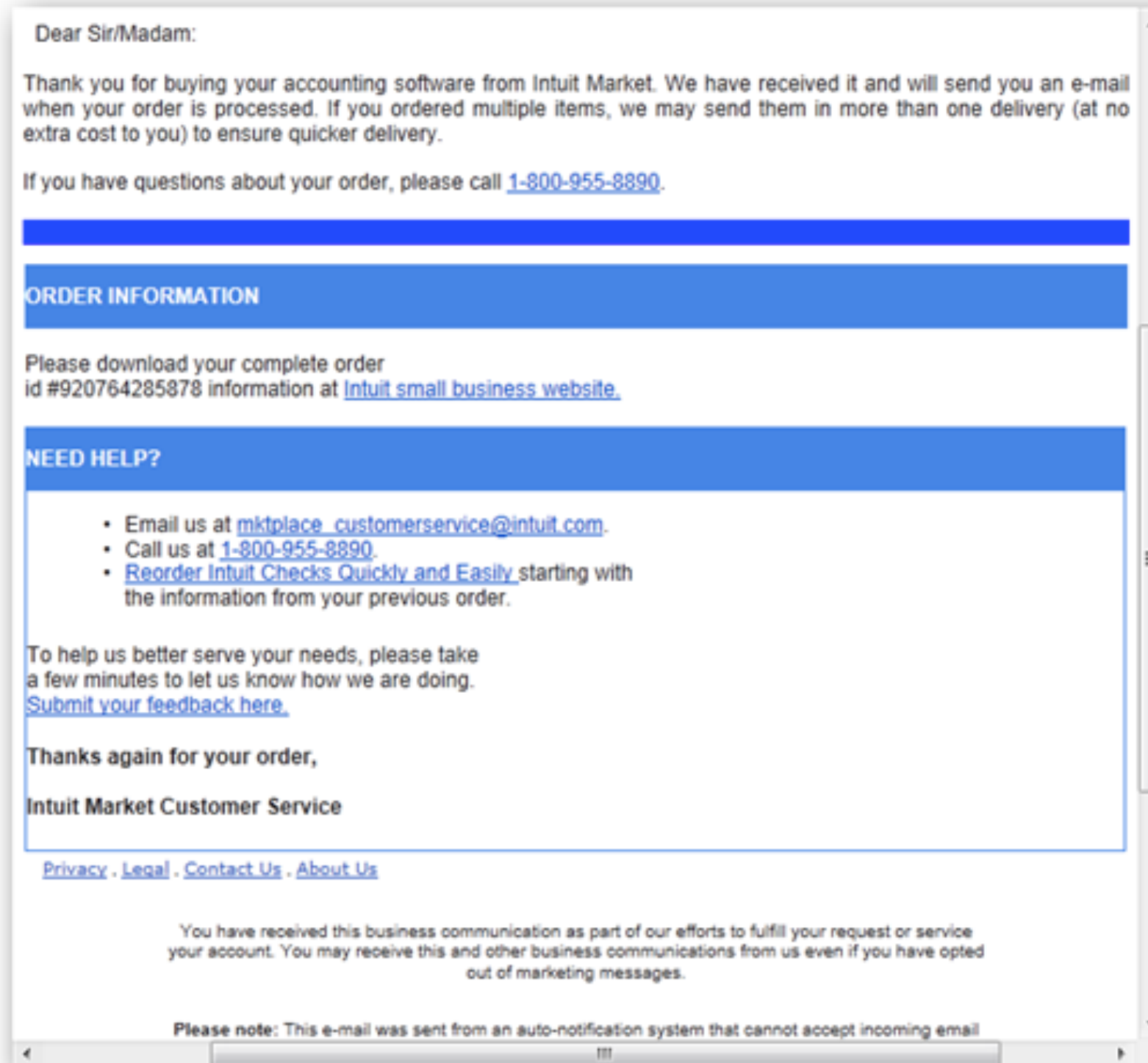
# What we know from header

```
Reply-To: <securityalert@verifybyvisa.com>  
From:  
"securityalert@verifybyvisa.com"<securityalert@verifybyvisa.com>  
Subject: Notice  
Date: Mon, 5 Mar 2012 21:20:57 +0800  
MIME-Version: 1.0  
Content-Type: multipart/mixed;  
boundary="--=_NextPart_000_0055_01C2A9A6.1C1757C0"  
X-Priority: 3  
X-MSMail-Priority: Normal  
X-Mailer: Microsoft Outlook Express 6.00.2600.0000  
X-MimeOLE: Produced By Microsoft MimeOLE V6.00.2600.0000  
X-ME-Bayesian: 0.000000
```

```
Received: from User ([118.142.76.58])  
by mail.lovingtour.com  
; Mon, 5 Mar 2012 21:38:11 +0800
```



# Workshop#2



Delivered-To: myemail@gmail.com  
Received: by 10.60.14.3 with SMTP id l3csp15619oec;  
Tue, 6 Mar 2012 04:27:20 -0800 (PST)  
Received: by 10.236.170.165 with SMTP id p25mr8672800yh1.123.1331036839870;  
Tue, 06 Mar 2012 04:27:19 -0800 (PST)  
Return-Path: <security@intuit.com>  
Received: from ms.externalemail.com (ms.externalemail.com. [XXX.XXX.XXX.XXX])  
by mx.google.com with ESMTP id o2si20048188yhn.34.2012.03.06.04.27.19;  
Tue, 06 Mar 2012 04:27:19 -0800 (PST)  
Received-SPF: fail (google.com: domain of security@intuit.com does not designate  
XXX.XXX.XXX.XXX as permitted sender) client-ip=XXX.XXX.XXX.XXX;  
Authentication-Results: mx.google.com; spf=hardfail (google.com: domain of  
security@intuit.com does not designate XXX.XXX.XXX.XXX as permitted sender)  
smtp.mail=security@intuit.com  
Received: with MailEnable Postoffice Connector; Tue, 6 Mar 2012 07:27:13 -0500  
Received: from dynamic-pool-xxx.hcm.fpt.vn ([118.68.152.212]) by ms.externalemail.com  
with MailEnable ESMTP; Tue, 6 Mar 2012 07:27:08 -0500  
Received: from apache by intuit.com with local (Exim 4.67)  
(envelope-from <security@intuit.com>)  
id GJMV8N-8BERQW-93  
for <jason@myemail.com>; Tue, 6 Mar 2012 19:27:05 +0700  
To: <jason@myemail.com>  
Subject: Your Intuit.com invoice.  
X-PHP-Script: intuit.com/sendmail.php for 118.68.152.212  
From: "INTUIT INC." <security@intuit.com>  
X-Sender: "INTUIT INC." <security@intuit.com>  
X-Mailer: PHP  
X-Priority: 1  
MIME-Version: 1.0  
Content-Type: multipart/alternative;  
boundary="——03060500702080404010506"  
Message-Id: <JXON1H-5GTPKV-0H@intuit.com>  
Date: Tue, 6 Mar 2012 19:27:05 +0700

# What we know from header

```
To: <jason@myemail.com>
Subject: Your Intuit.com invoice.
X-PHP-Script: intuit.com/sendmail.php for 118.68.152.212
From: "INTUIT INC." <security@intuit.com>
X-Sender: "INTUIT INC." <security@intuit.com>
X-Mailer: PHP
X-Priority: 1
MIME-Version: 1.0
Content-Type: multipart/alternative;
boundary="——03060500702080404010506"
Message-Id: <JXON1H-5GTPKV-0H@intuit.com>
Date: Tue, 6 Mar 2012 19:27:05 +0700
X-ME-Bayesian: 0.000000
```

```
Received: from apache by intuit.com with local (Exim 4.67)
(envelope-from <security@intuit.com>)
id GJMV8N-8BERQW-93
for <jason@myemail.com>; Tue, 6 Mar 2012 19:27:05 +0700
```

```
Received: from dynamic-pool-xxx.hcm.fpt.vn ([118.68.152.212]) by
ms.externalemail.com with MailEnable ESMTP; Tue, 6 Mar 2012 07:27:08 -0500
```

# Is this too difficult?



## Let's talk about automate tools

# Topics

Email System Basics

Email Crimes

Email Header

Automate Email Investigation



<https://toolbox.googleapps.com/apps/messageheader/analyzeheader>

The screenshot shows a web browser window with the URL <https://toolbox.googleapps.com/apps/messageheader/analyzeheader>. The page title is "Messageheader". The browser's address bar shows the URL and a star icon for bookmarks. Below the address bar is a navigation bar with the "Google Apps Toolbox" logo and a list of tools: Home, Browserinfo, Check MX, Dig, HAR Analyzer, Log Analyzer, Log analyzer for Google Drive, Messageheader, Other Tools, and Help. The main content area has a heading "Paste email header below" and a large text input field. To the right of the input field is a "Help" section with the following text: "How do I get email headers ?", "Interpreting email headers", "What can this tool tell from email headers ?", and a bulleted list: "Identifies delivery delays.", "Identify approximate source of delay.", and "Identify who may be responsible.". At the bottom of the input field, there is a red warning icon and the text "Please submit a valid SMTP header". Below the input field is a blue button labeled "Analyse the header above".

Messageheader

<https://toolbox.googleapps.com/apps/messageheader/analyzeheader>

Google Apps Toolbox

Home Browserinfo Check MX Dig HAR Analyzer Log Analyzer Log analyzer for Google Drive Messageheader Other Tools Help

Paste email header below

Help

How do I get email headers ?  
Interpreting email headers  
What can this tool tell from email headers ?

- Identifies delivery delays.
- Identify approximate source of delay.
- Identify who may be responsible.

Please submit a valid SMTP header

Analyse the header above

<b>MessageId</b>	CY4PR17MB09991128877721C1C0D60451BEE50@CY4PR17MB0999.namprd17.prod.outlook.com
<b>Created at:</b>	9/2/2016, 6:04:52 PM ( Delivered after 18 sec )
<b>From:</b>	Graham O'Sullivan <gosullivan@alienvault.com>
<b>To:</b>	"kitisak@ega.or.th" <kitisak@ega.or.th>
<b>Subject:</b>	Hello from AlienVault
<b>SPF:</b>	none
<b>DKIM:</b>	pass

#	Delay	From *		To *	Protocol	Time received
0	4 sec	mail-co1nam03on0130.outbound.protection.outlook.com	→	mx4.mail.go.th	ESMTPS	9/2/2016, 6:04:56 PM
1	10 sec	localhost	→	localhost	SMTP	9/2/2016, 6:05:06 PM
2	1 sec	[10.100.1.49]	→	pro02.zi.mail.go.th	ESMTPS	9/2/2016, 6:05:07 PM
3		pro02.zi.mail.go.th	→	mta07.zi.mail.go.th	ESMTP	9/2/2016, 6:05:07 PM
4		mta07.zi.mail.go.th	→	localhost	ESMTP	9/2/2016, 6:05:07 PM
5		localhost	→	mta07.zi.mail.go.th	ESMTP	9/2/2016, 6:05:07 PM
6		mta07.zi.mail.go.th	→	localhost	ESMTP	9/2/2016, 6:05:07 PM
7	2 sec	localhost	→	mta07.zi.mail.go.th	ESMTP	9/2/2016, 6:05:09 PM
8	1 sec	mta07.zi.mail.go.th	→	mbs05.zi.mail.go.th		9/2/2016, 6:05:10 PM

<http://www.iptrackeronline.com/email-header-analysis.php>













The screenshot shows a web browser window with two tabs: "Messageheader" and "Complete email header analysis". The address bar displays the URL [www.iptrackeronline.com/email-header-analysis.php](http://www.iptrackeronline.com/email-header-analysis.php). The browser's toolbar includes various icons and a bookmarks bar with entries like "Apps", "Hacky Shacky | Kno...", "Apple", "Training Resources", "Interesting Pages", "News", "Training Online", and "Internal System".

The website header features the logo "ipTRACKERonline.com" in large, bold, red letters, with the tagline "Geo Marketing. IP Address tools and a whole lot more" underneath. A dark blue navigation bar contains links for "Home", "IP Address Tools", "Downloads", and "Web Gadgets". Below this, there are links for "Buy API Credits" and "Email Analysis".


The main content area is titled "Email Header Analysis" with the subtitle "How to extract email headers, a brief tutorial." Below the title is a large text input box with the placeholder text "Paste email header here". At the bottom of the input box is a button labeled "Submit header for analysis".

On the left side of the page, there is a social media sharing widget. It shows a "Like" button with a count of "4.1K", a "Share" button with a count of "13K+", a "Pin it" button, a "G+1" button, a "StumbleUpon" button with a count of "114", and a "Tweet" button with a count of "86".

## Email header analysis report

All valid IP Addresses found in the header.					
Ip Address	3rd Party Info	Provider	City	Flag	Country
* 16.9.2.105	 	Hewlett-packard Company	Palo Alto		United States
2.7.2.210	 	Orange	n/a		France
185.51.104.206	 	Airspeed Communications Limited	Cork		Ireland
104.47.40.130	 	Microsoft Azure	Redmond		United States

able originating IP address

Header Analysis	
Originating Info	Email info
Originating IP address 16.9.2.105	From Graham O'Sullivan <gosulli
Originating hostname 16.9.2.105	Originating Email address gosullivan@alienvault.com
Originating Organization Hewlett-packard Company	Subject Hello from AlienVault
 Originating Country United States	Date Sent Fri, 2 Sep 2016 11:04:52 +
Originating City Palo Alto	Message ID

4.1K

Like

Share

13K+

Pin it

114

G+1

86

Tweet



# Challenges

- ❖ How can we get email header?
- ❖ What will you do if attackers delete email?
  - ❖ need your forensics skill => not include in today topics
- ❖ Interpreting is very important
  - ❖ need to learn more about new header types
  - ❖ sending from Webmail, Email client application or Scripts
- ❖ Dealing with the IP address which is got from the last Receive from
  - ❖ Whois, nslookup, and etc.
  - ❖ Google is your friend



Any questions?

[kitisak.jirawannakool@ega.or.th](mailto:kitisak.jirawannakool@ega.or.th)