Lec 15: Malware

CS492E: Introduction to Software Security

Sang Kil Cha

Malware = Malicious Software

Malware, also known as malicious code and malicious software, refers to a program that is inserted into a system, usually covertly, with the intent of compromising the confidentiality, integrity, or availability of the victim’s data, applications, or operating system or otherwise annoying or disrupting the victim.

Quoted from Guide to Malware Incident Prevention and Handling, NIST Tech Report 2005

Terminology

- Virus
- Worm
- Trojan
- Rootkit
- Spyware
- Bots
- Backdoor
- Adware
- Ransomware
- Etc.

Virus

The term is invented by ***Fred Cohen*** in 1984

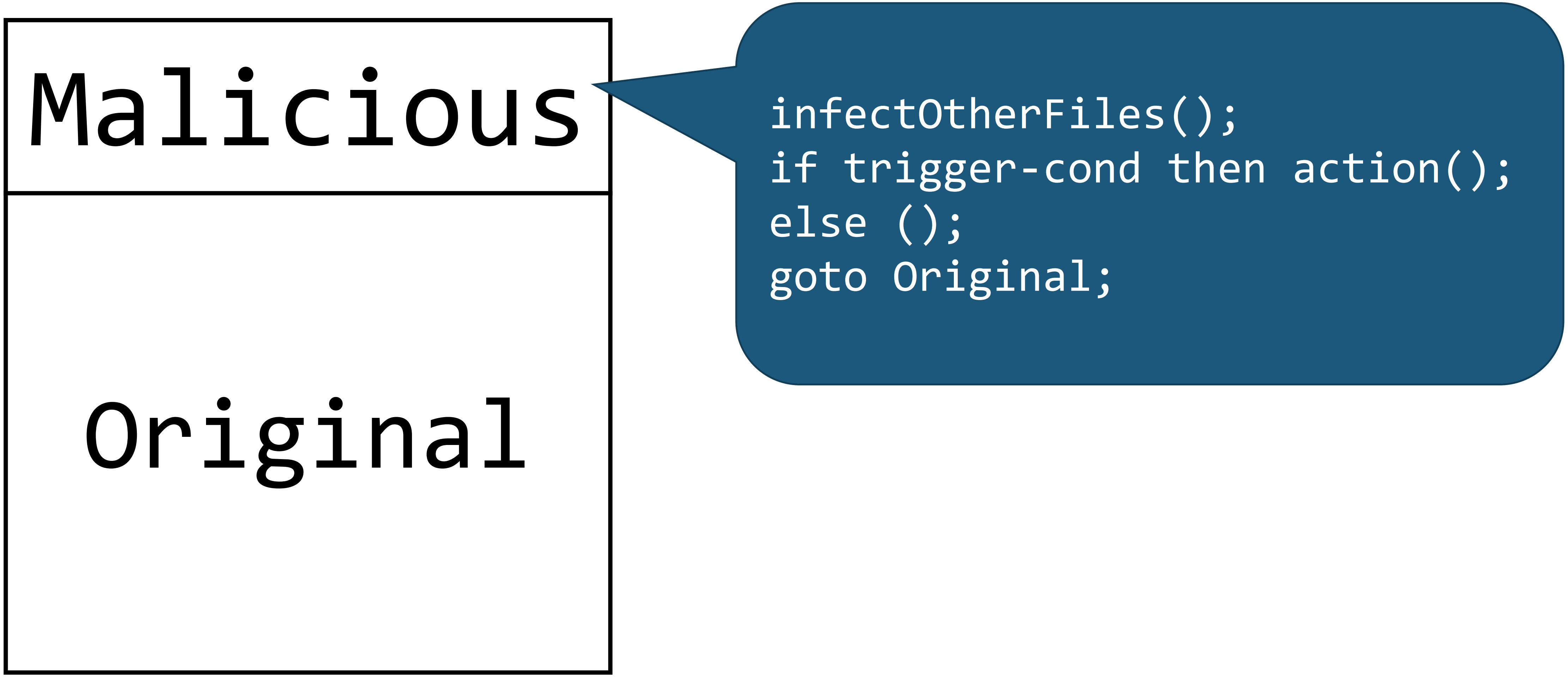
Computer Viruses: Theories and Experiments,
Computers and Security, Vol. 6, 1984

Virus

A program that can ***infect other programs*** by modifying them to include a, possibly evolved, version of itself

Computer Viruses: Theories and Experiments,
Computers and Security, Vol. 6, 1984

Virus Structure



Malicious

Original

```
infectOtherFiles();
if trigger-cond then action();
else ();
goto Original;
```

Worm

A computer worm is a standalone malware computer program that replicates itself in order to spread to other computers. Often, it ***uses a computer network to spread itself***, relying on security failures on the target computer to access it. Unlike a computer virus, it does not need to attach itself to an existing program.

- Wikipedia

Morris Worm

Exploited a ***buffer overflow*** vulnerability in `fingerd`

```
int main(int argc, char* argv[])
{
    char line[512];
    /* omitted … */
    gets(line); /* Buffer Overflow! */
    /* omitted … */
}
```

This single line allowed the Morris Worm to infect 10% of the Internet computers in 1988

Nov. 2, 1988

The first computer worm (called Morris Worm) was born.

Robert Tappan Morris

Creator of the worm
Cornell graduate
Tenured professor at MIT now

Image from http://www.nndb.com/people/466/000027385/

Worm Propagation Model

$$\frac{dI(t)}{dt} = \beta I(t) S(t)$$

Where

- $I(t)$ is a number of individuals infected as of time t
- $S(t)$ is a number of susceptible individuals at time t
- β is the contact rate (pairwise rate of infection)
- N is the size of the population, i.e., $N = I(t) + S(t)$

Worm Propagation Model (cont’d)

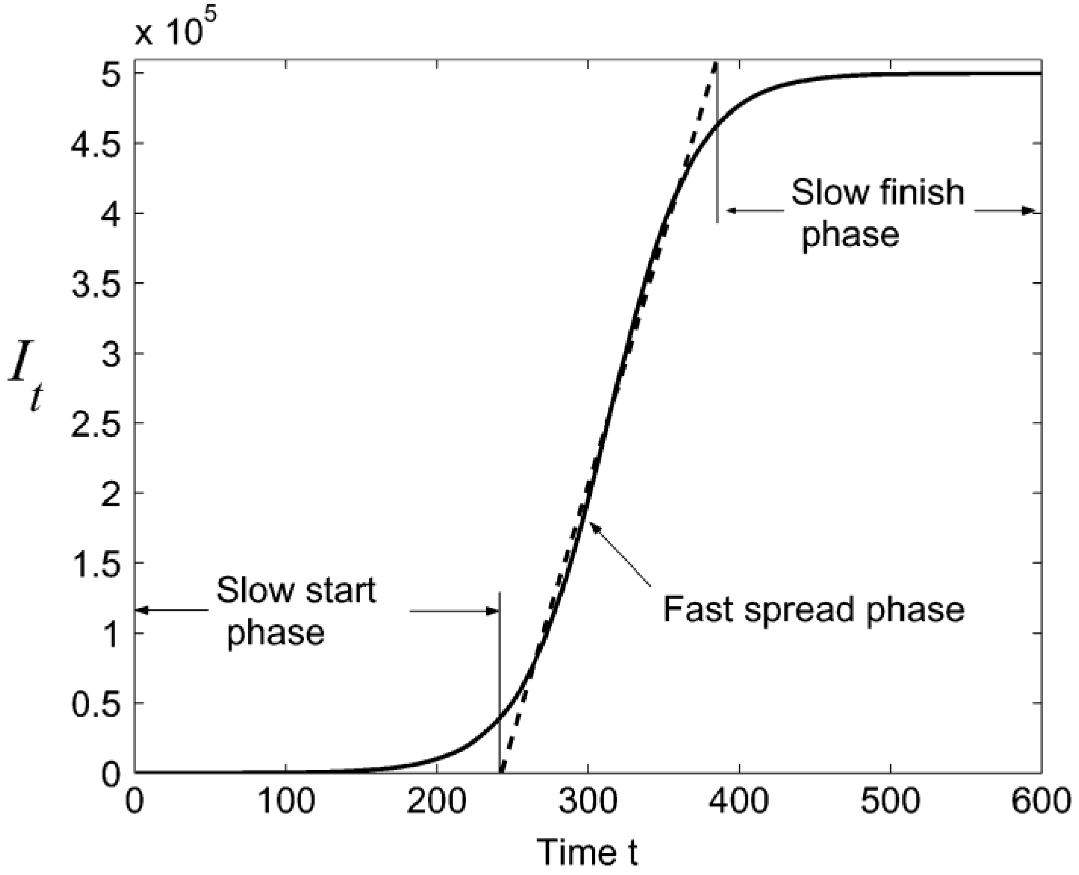


Image taken from The Monitoring and Early Detection of Internet Worms, ***IEEE/ACM Transactions on Networking, 2005***

Trojan (Trojan Horse)

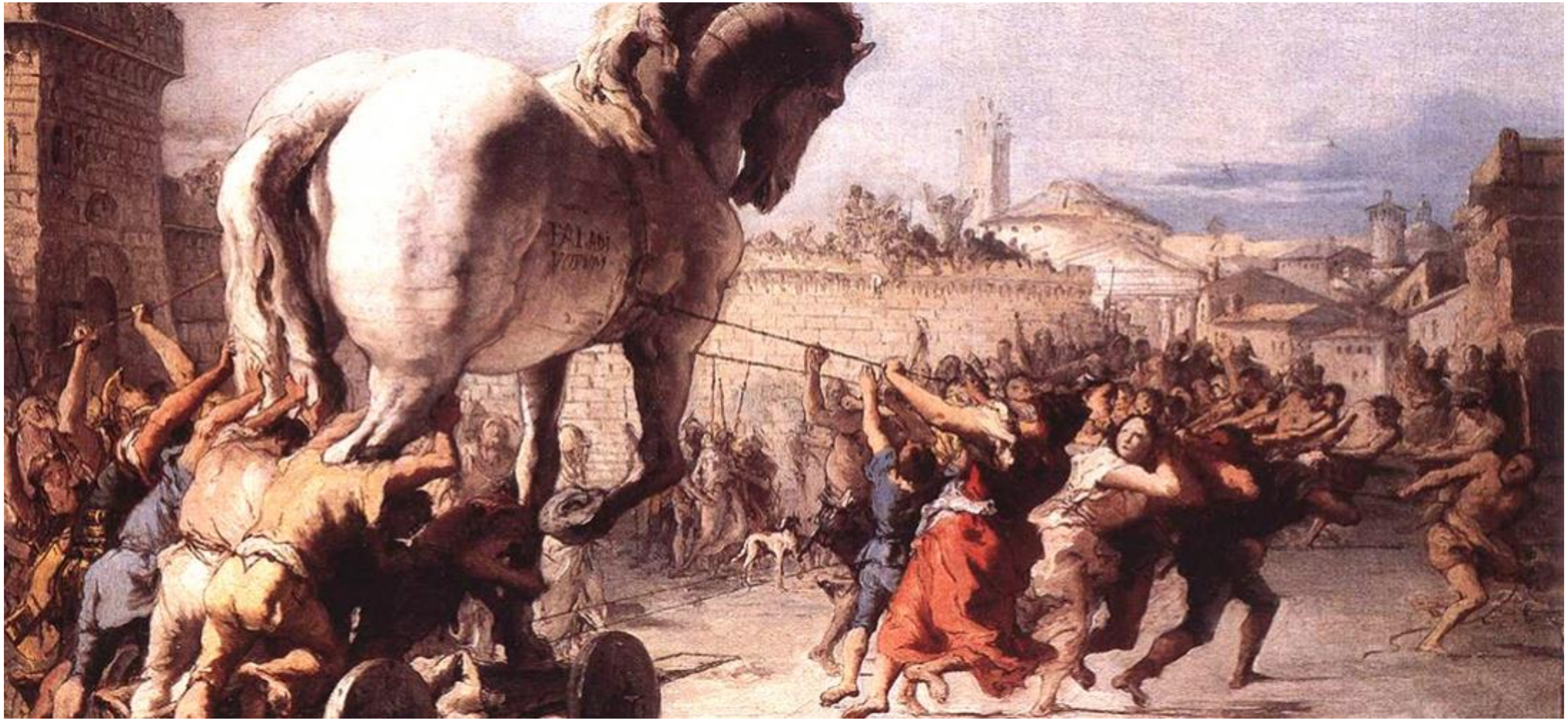


Image from http://www.slate.fr/story/114325/sarkozy-juges-mise-examen-cheval-troie

Trojan (Trojan Horse)

A computer program that appears to have a useful function, but also has a hidden and potentially malicious function that evades security mechanisms, sometimes by exploiting legitimate authorizations of a system entity that invokes it.

- Computer Security - Principles and Practice, Stallings

How Trojans Spread?

- Social engineering
  - E-mail, social network, phishing, etc.

- Drive-by download

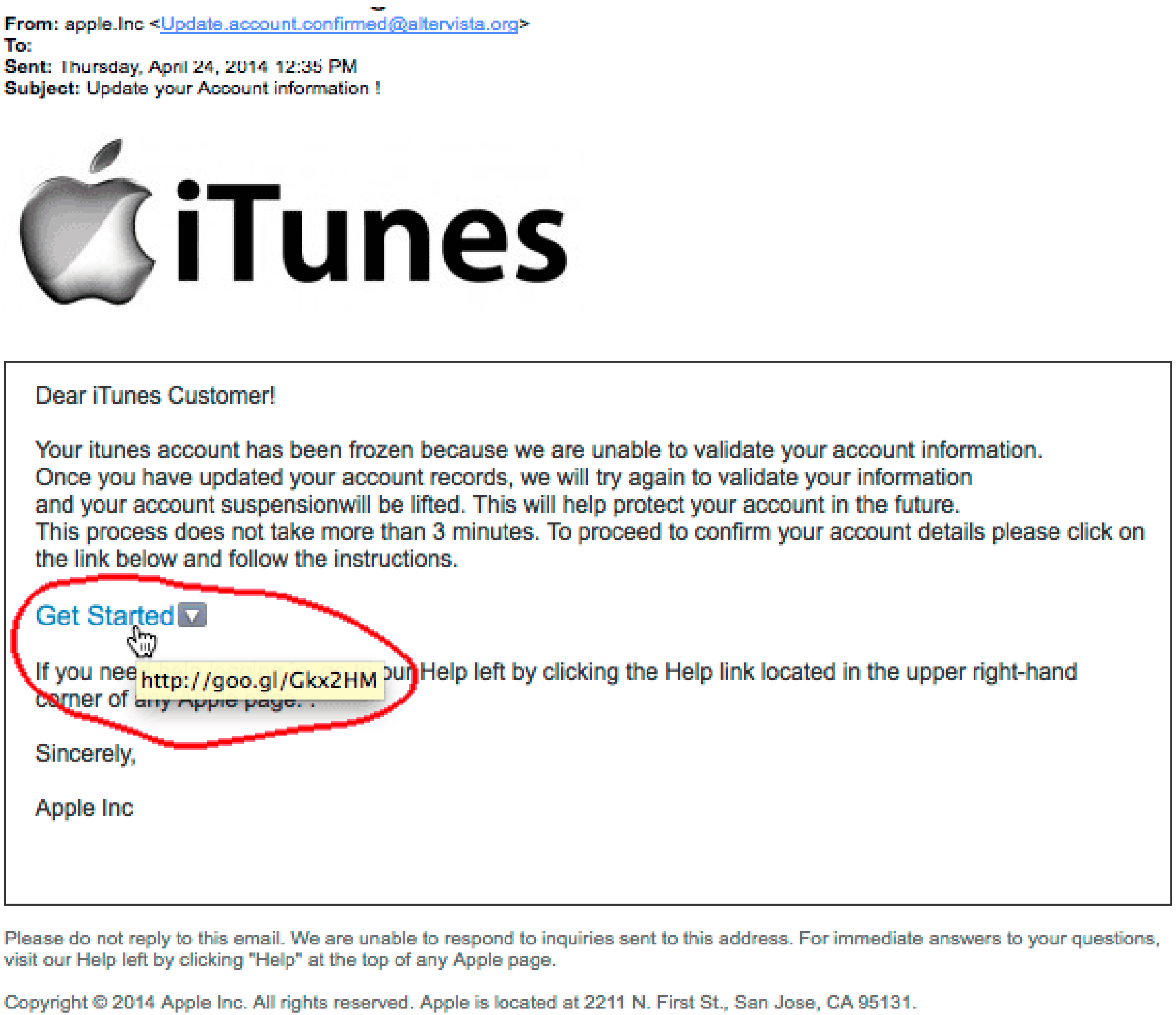
Spam E-Mail

- Advertisements (including money mule jobs)
- Trojan horse can be attached

Phishing

- Disguising as a trustworthy entity, and obtain private info

- Fishing ~ Phishing
  - Both use a bait to catch a victim ☺



From: apple.Inc <Update.account.confirmed@altervista.org>
To:
Sent: Thursday, April 24, 2014 12:35 PM
Subject: Update your Account information !

Dear iTunes Customer!

Your itunes account has been frozen because we are unable to validate your account information.
Once you have updated your account records, we will try again to validate your information
and your account suspensionwill be lifted. This will help protect your account in the future.
This process does not take more than 3 minutes. To proceed to confirm your account details please click on the link below and follow the instructions.

Get Started ▾

If you nee http://goo.gl/Gkx2HM our Help left by clicking the Help link located in the upper right-hand corner of any Apple page. .

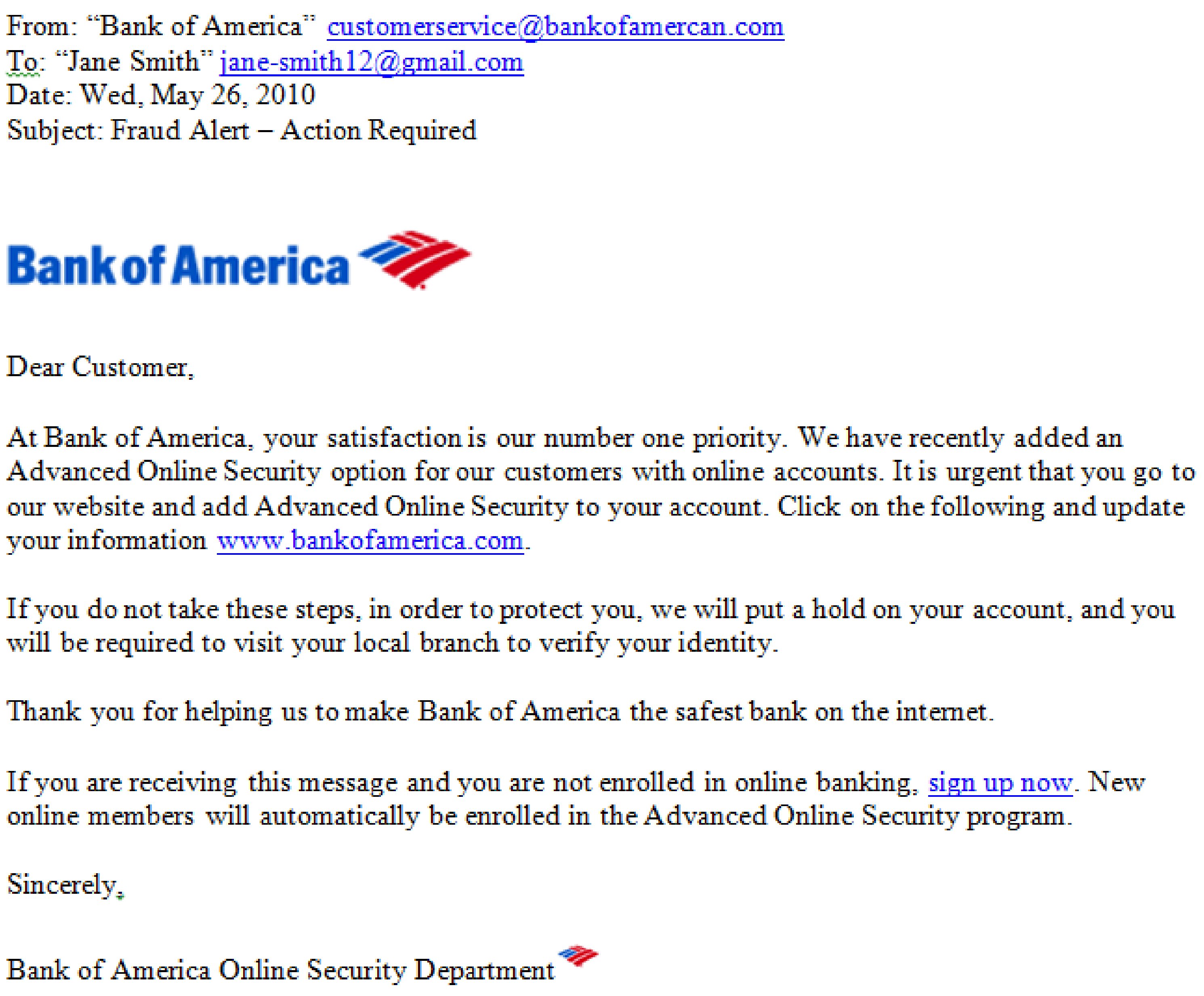
Sincerely,

Apple Inc

Please do not reply to this email. We are unable to respond to inquiries sent to this address. For immediate answers to your questions, visit our Help left by clicking "Help" at the top of any Apple page.

Copyright © 2014 Apple Inc. All rights reserved. Apple is located at 2211 N. First St., San Jose, CA 95131.

Image from http://macgroup.org/blog/wp-content/uploads/2014/05/phishing_email_link.png



From: “Bank of America” customerservice@bankofamercan.com
To: “Jane Smith” jane-smith12@gmail.com
Date: Wed, May 26, 2010
Subject: Fraud Alert – Action Required

Bank of America

Dear Customer,

At Bank of America, your satisfaction is our number one priority. We have recently added an Advanced Online Security option for our customers with online accounts. It is urgent that you go to our website and add Advanced Online Security to your account. Click on the following and update your information www.bankofamerica.com.

If you do not take these steps, in order to protect you, we will put a hold on your account, and you will be required to visit your local branch to verify your identity.

Thank you for helping us to make Bank of America the safest bank on the internet.

If you are receiving this message and you are not enrolled in online banking, sign up now. New online members will automatically be enrolled in the Advanced Online Security program.

Sincerely,

Bank of America Online Security Department

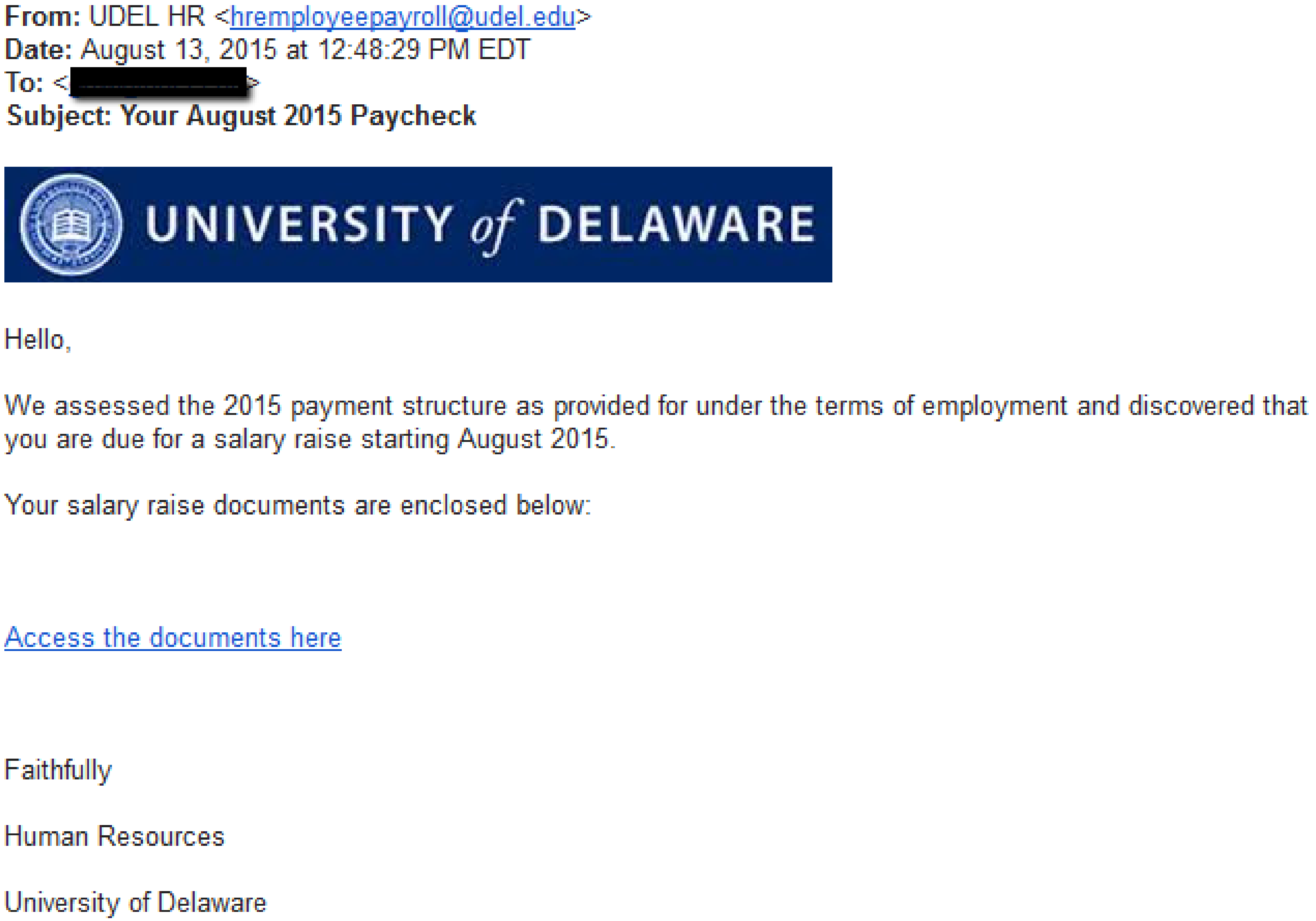
Image from http://media.gcflearnfree.org/content/5730dca54ca9130e085655b0_05_09_2016/mock_fraud_letter_3_resized.png

Spear Phishing

Phishing attempts directed at specific individuals.

- Wikipedia

Image from http://www.gtscoalition.com/wp-content/uploads/2013/10/LeapFrog-Phishing.jpg



From: UDEL HR <hremployeepayroll@udel.edu>
Date: August 13, 2015 at 12:48:29 PM EDT
To: <[redacted]>
Subject: Your August 2015 Paycheck

UNIVERSITY of DELAWARE

Hello,

We assessed the 2015 payment structure as provided for under the terms of employment and discovered that you are due for a salary raise starting August 2015.

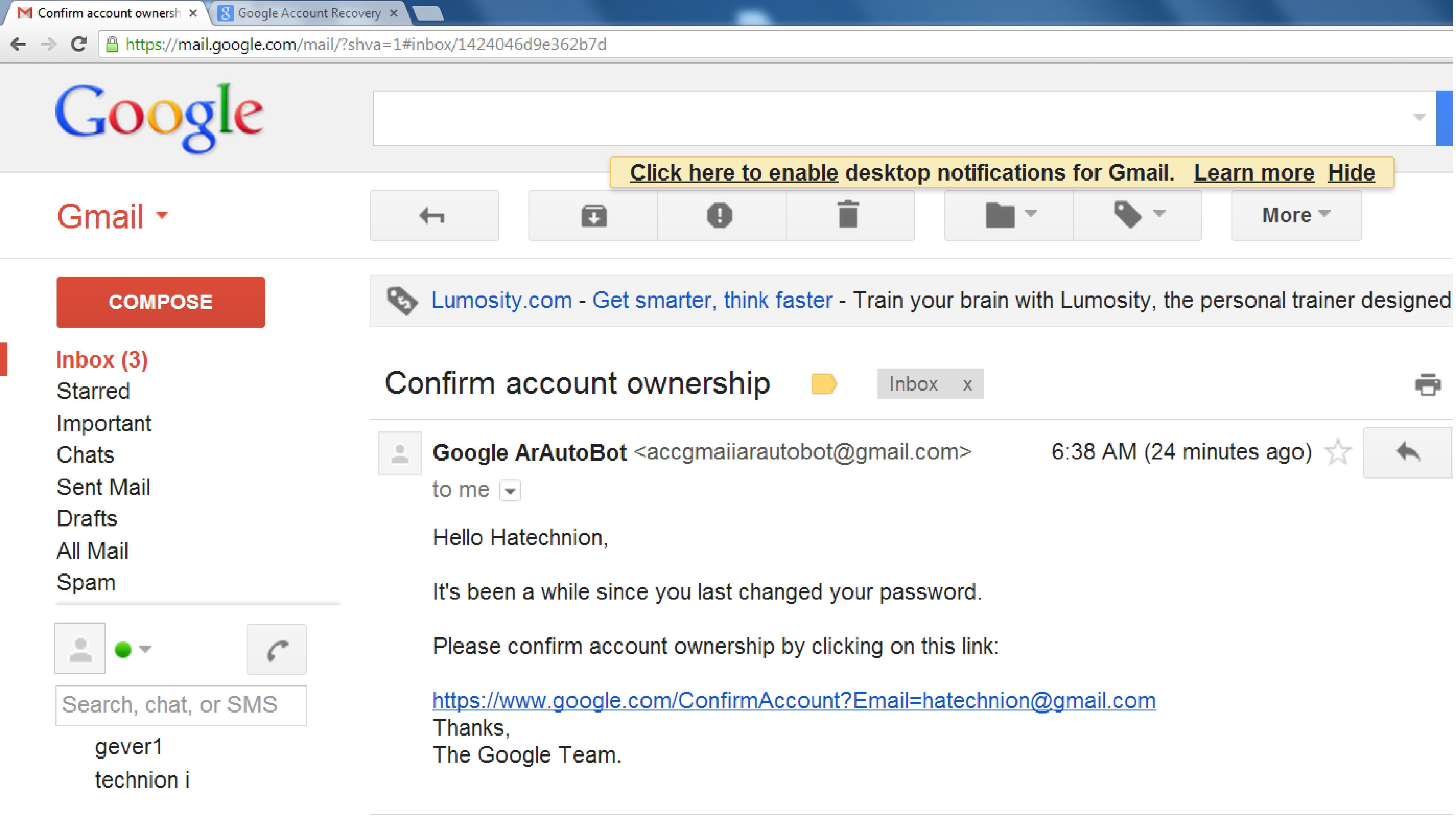
Your salary raise documents are enclosed below:

Access the documents here

Faithfully

Human Resources

University of Delaware


Confirm account ownersh
Google Account Recovery
https://mail.google.com/mail/?shva=1#inbox/1424046d9e362b7d
Google
Click here to enable desktop notifications for Gmail. Learn more Hide
Gmail
More
COMPOSE
Lumosity.com - Get smarter, think faster - Train your brain with Lumosity, the personal trainer designed
Inbox (3)
Starred
Important
Chats
Sent Mail
Drafts
All Mail
Spam
Search, chat, or SMS
gever1
technion i

Confirm account ownership Inbox x

Google ArAutoBot <accgmaiiarautobot@gmail.com> 6:38 AM (24 minutes ago)

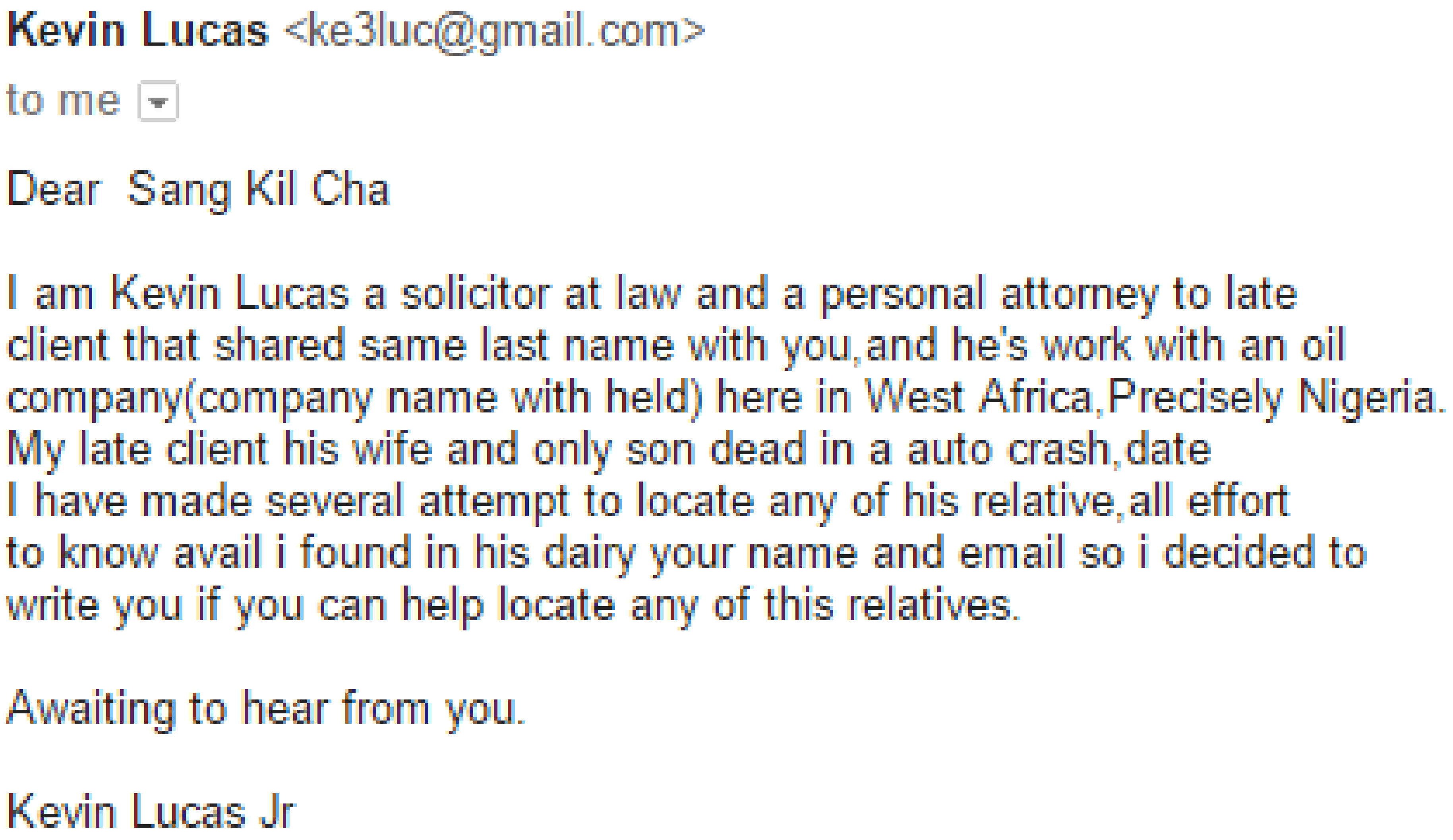
to me

Hello Hatechnion,

It's been a while since you last changed your password.

Please confirm account ownership by clicking on this link:

https://www.google.com/ConfirmAccount?Email=hatechnion@gmail.com
Thanks,
The Google Team.



Kevin Lucas <ke3luc@gmail.com>

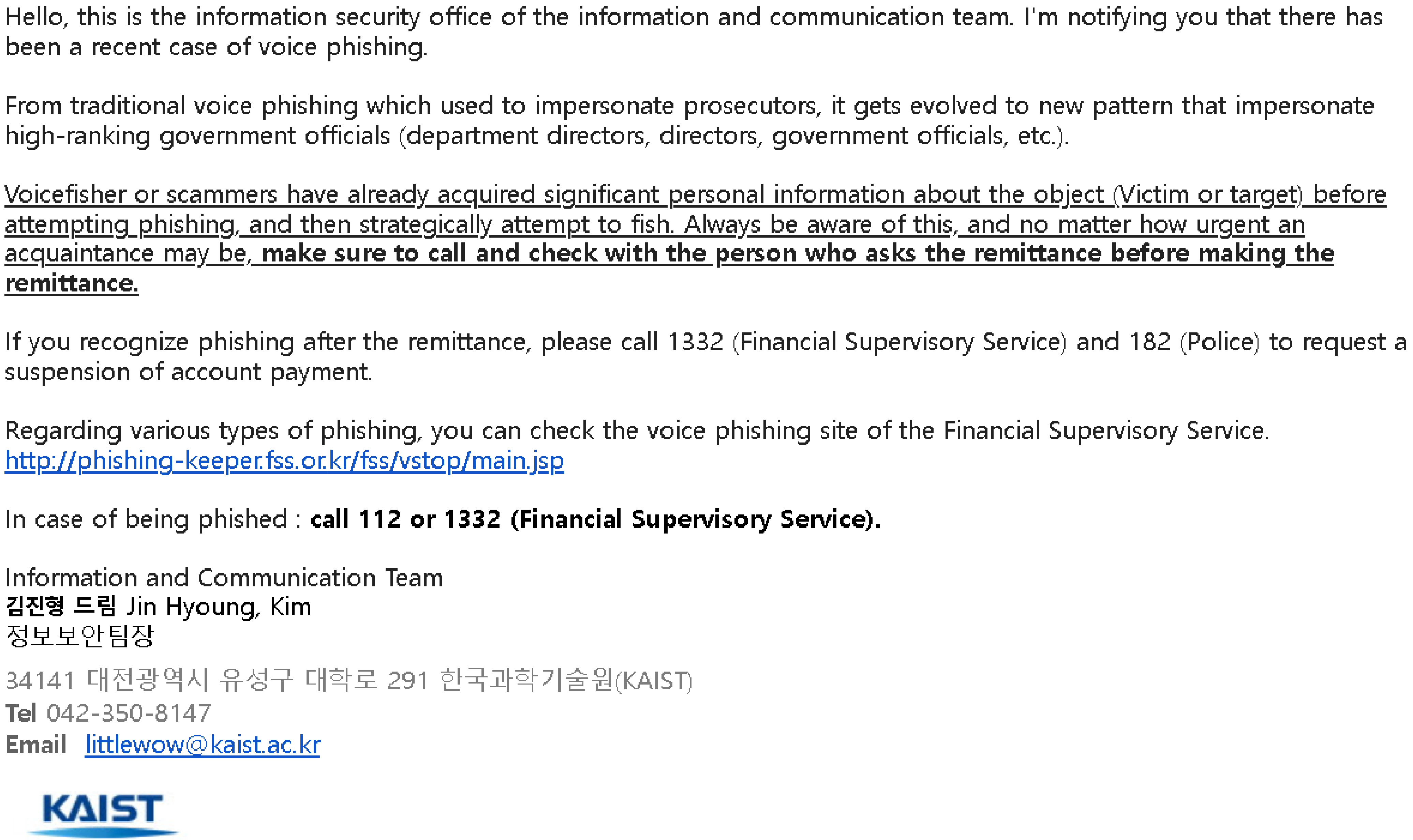
to me

Dear Sang Kil Cha

I am Kevin Lucas a solicitor at law and a personal attorney to late
client that shared same last name with you,and he's work with an oil
company(company name with held) here in West Africa,Precisely Nigeria.
My late client his wife and only son dead in a auto crash,date
I have made several attempt to locate any of his relative,all effort
to know avail i found in his dairy your name and email so i decided to
write you if you can help locate any of this relatives.

Awaiting to hear from you.

Kevin Lucas Jr



Hello, this is the information security office of the information and communication team. I'm notifying you that there has been a recent case of voice phishing.

From traditional voice phishing which used to impersonate prosecutors, it gets evolved to new pattern that impersonate high-ranking government officials (department directors, directors, government officials, etc.).

Voicefisher or scammers have already acquired significant personal information about the object (Victim or target) before attempting phishing, and then strategically attempt to fish. Always be aware of this, and no matter how urgent an acquaintance may be, **make sure to call and check with the person who asks the remittance before making the remittance.**

If you recognize phishing after the remittance, please call 1332 (Financial Supervisory Service) and 182 (Police) to request a suspension of account payment.

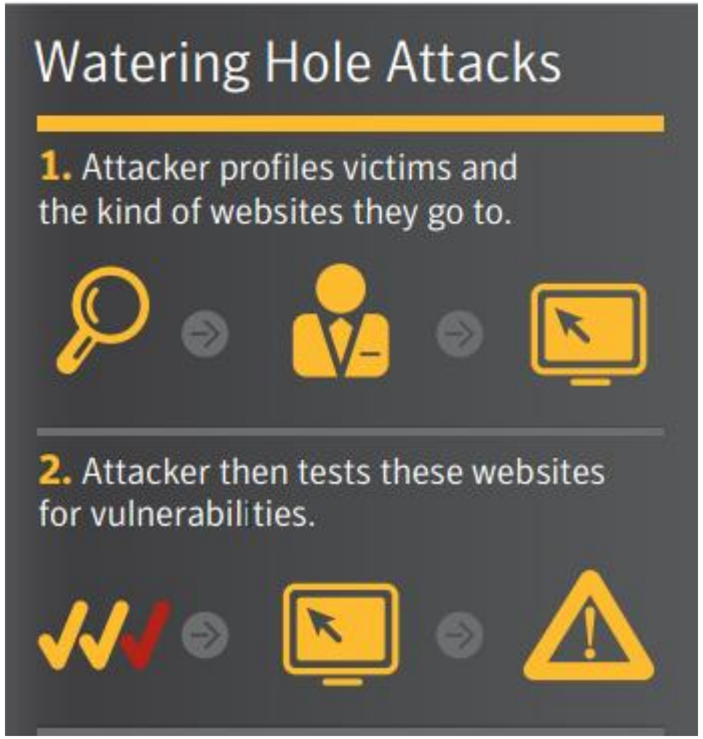
Regarding various types of phishing, you can check the voice phishing site of the Financial Supervisory Service.
http://phishing-keeper.fss.or.kr/fss/vstop/main.jsp

In case of being phished : **call 112 or 1332 (Financial Supervisory Service).**

Information and Communication Team
김진형 드림 Jin Hyoung, Kim
정보보안팀장

34141 대전광역시 유성구 대학로 291 한국과학기술원(KAIST)
Tel 042-350-8147
Email littlewow@kaist.ac.kr

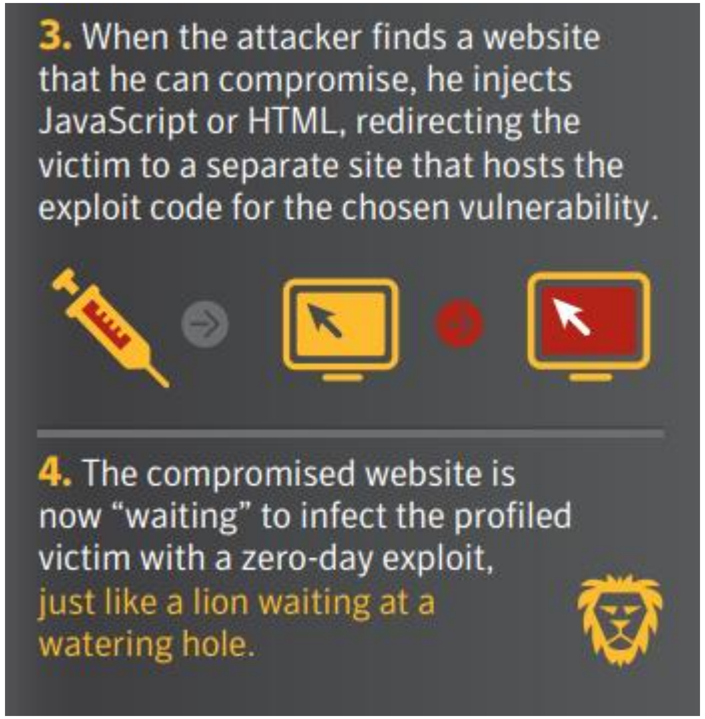
Watering Hole Attacks



Watering Hole Attacks

1. Attacker profiles victims and the kind of websites they go to.

2. Attacker then tests these websites for vulnerabilities.



3. When the attacker finds a website that he can compromise, he injects JavaScript or HTML, redirecting the victim to a separate site that hosts the exploit code for the chosen vulnerability.

4. The compromised website is now "waiting" to infect the profiled victim with a zero-day exploit, just like a lion waiting at a watering hole.

Image from https://www.symantec.com/content/en/us/about/media/pdfs/b-istr_18_watering_hole_edits.en-us.pdf

Watering Hole

Image from https://i.ytimg.com/vi/FneQ6m1QFFs/maxresdefault.jpg

Bot (Zombie)

A program activated on an infected machine that is activated to launch attacks on other machines.

Botnet is the collection of bots.

- Computer Security - Principles and Practice, Stallings

Command and Control (C&C) Server

- Use existing protocols such as IRC and HTTP
  - E.g., each bot connects to an IRC server, and join a specific channel

- Use custom protocols
  - E.g., qbot

Each bot needs to know a specific IP address (or a channel name) of the C&C server

DNS-based C&C Server

- Use a custom domain name generation algorithm
- Each bot randomly generates a series of domain names to be used
- C&C server can be reached unless the generation algorithm is revealed by a defender

P2P-based Botnets

Each bot is a command distribution server as well as a client.

- How about bots that are behind firewall?
- When a bot wants to join a botnet, it needs to know the IP of at least one node in the botnet that can take incoming connections
  - Bootstrapping
- Peer poisoning possible!
  - Having a fake node that provides fake list of IPs

Spyware

Software that collects information from a computer and transmits it to another system.

- Monitoring keystrokes (keylogger)
- Monitoring screen/camera data
- Monitoring network traffic

Rootkit

A collection of utilities that enable access to a compromised machine. A rootkit often masks its existence and other malware.

- Example
  - `ps` command does not show the rootkit process
  - `ls` command does not show malicious files

Logic Bomb

A logic bomb is a piece of code intentionally inserted into a software system that will set off a malicious function when specified conditions are met.

- Wikipedia

Sony BMG Copy Protection Rootkit

Over 22 million CDs (2005-2007) included malware

- A rootkit that hides the existence of the malware
- A logic bomb that interferes CD copying

Image from https://en.wikipedia.org/wiki/Sony_BMG#/media/File:Sony_BMG.svg

Dropper / Downloader

A program that installs other malware on a target machine.

- The malware code can be contained within the ***dropper***
- Or can be downloaded by the ***downloader***

Backdoor

Any mechanism that bypasses a normal security check; it may allow unauthorized access to functionality in a program, or onto a compromised system.

- Computer Security - Principles and Practice, Stallings

Adware

Advertising that is integrated into software. It can result in pop-up ads or redirection of a browser to a commercial site.

- Computer Security - Principles and Practice, Stallings

Benign vs. Malicious Adware

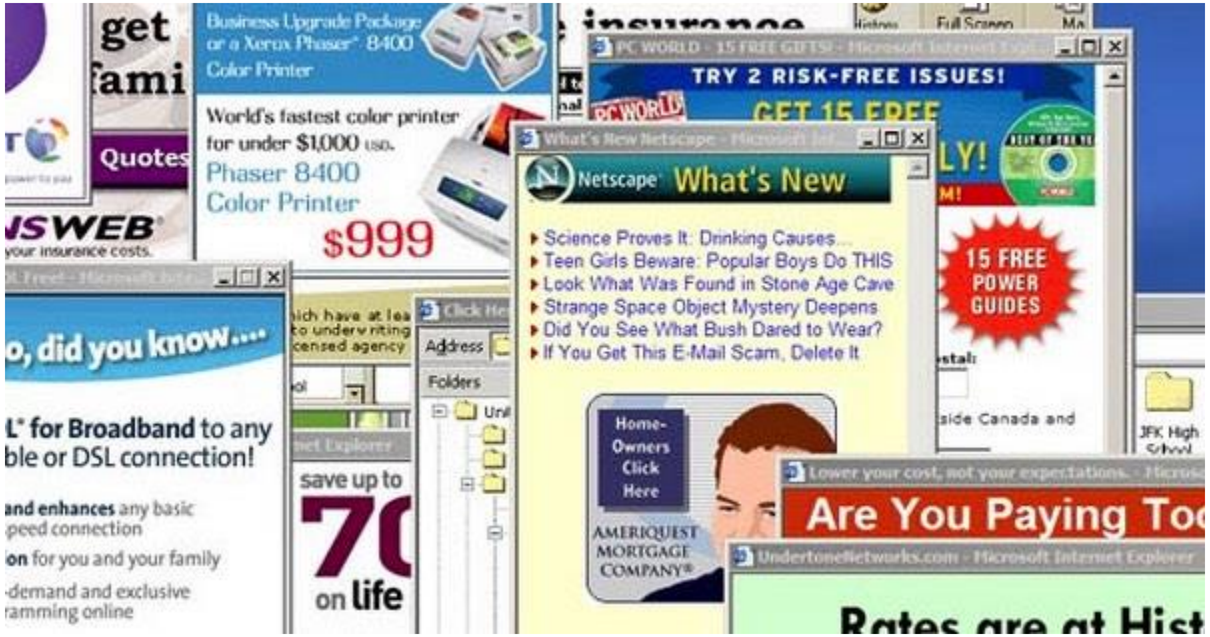

get
fami
Quotes
ISWEB
your insurance costs.
Business Upgrade Package or a Xerox Phaser® 8400 Color Printer
World's fastest color printer for under $1,000 USD.
Phaser 8400 Color Printer
$999
insurance
PC WORLD - 15 FREE GIFTS! - Microsoft Internet Expl...
TRY 2 RISK-FREE ISSUES!
PC WORLD
GET 15 FREE
LY!
15 FREE POWER GUIDES
What's New Netscape - Microsoft Int...
Netscape What's New
Science Proves It: Drinking Causes...
Teen Girls Beware: Popular Boys Do THIS
Look What Was Found in Stone Age Cave
Strange Space Object Mystery Deepens
Did You See What Bush Dared to Wear?
If You Get This E-Mail Scam, Delete It
Home-Owners Click Here
AMERIQUEST MORTGAGE COMPANY®
o, did you know....
L® for Broadband to any ble or DSL connection!
and enhances any basic peed connection
on for you and your family
demand and exclusive ramming online
save up to
70
on life
Click He
Address
Folders
Lower your cost, not your expectations. - Microso
Are You Paying Too
UndertoneNetworks.com - Microsoft Internet Explorer
Rates are at Hist
side Canada and
JFK High School

Image from https://techmonitor.ai/what-is/what-is-adware-4931901

Ransomware

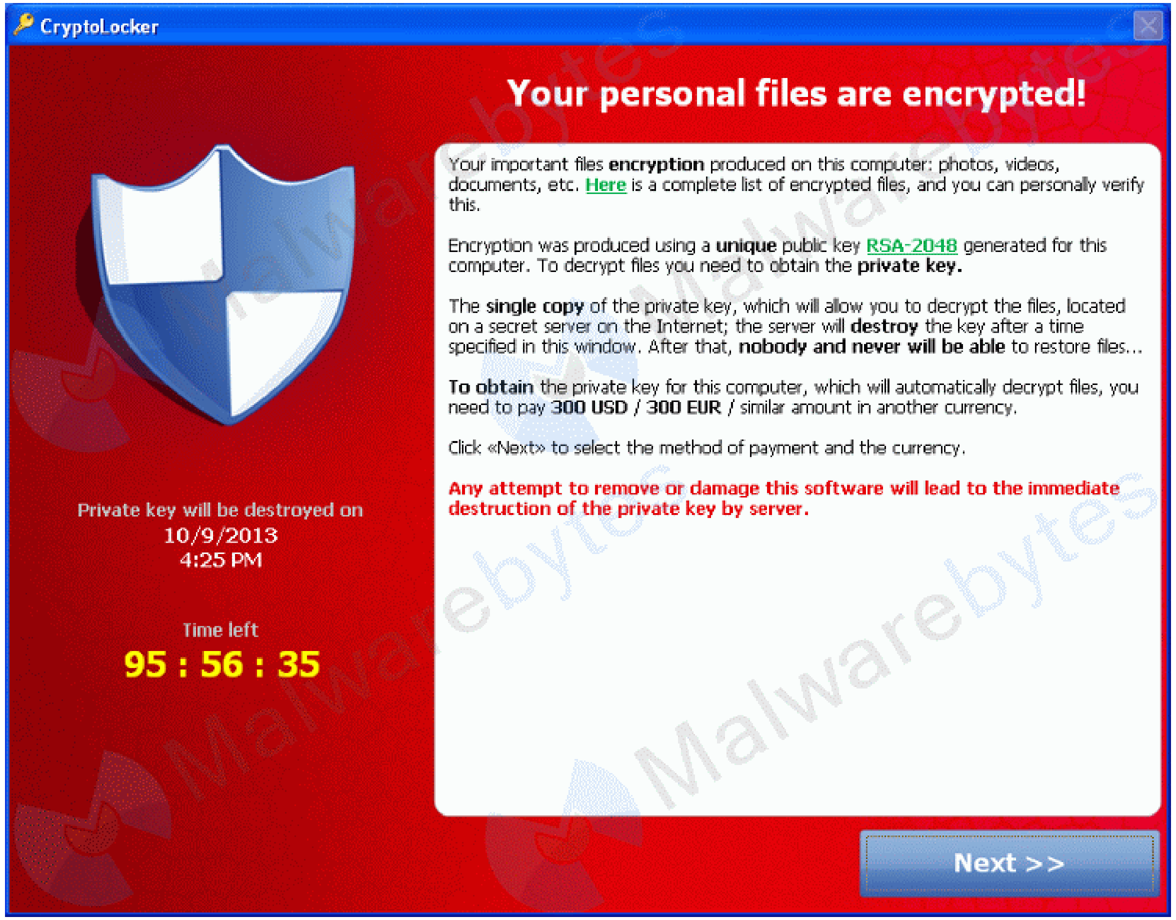
- Cryptovirus (Cryptoviral extortion attack)
  - Cryptovirology: Extortion-Based Security Threats and Countermeasures, ***Oakland 1996***

- Cryptography also has negative usage!

Cryptoviral Extortion

1. Attacker generates a key pair and places the corresponding public key in the malware
2. Malware generates a random symmetric key and encrypts the victim’s data with it
3. Malware uses the public key to encrypt the symmetric key, and “securely” delete the original symmetric key.
4. Show the victim a message with the encrypted symmetric key how to pay the ransom
5. When the payment received, the attacker deciphers the key and send to the victim

Example: CryptoLocker



Your personal files are encrypted!

Your important files **encryption** produced on this computer: photos, videos, documents, etc. Here is a complete list of encrypted files, and you can personally verify this.

Encryption was produced using a **unique** public key RSA-2048 generated for this computer. To decrypt files you need to obtain the **private key.**

The **single copy** of the private key, which will allow you to decrypt the files, located on a secret server on the Internet; the server will **destroy** the key after a time specified in this window. After that, **nobody and never will be able** to restore files...

To obtain the private key for this computer, which will automatically decrypt files, you need to pay **300 USD / 300 EUR** / similar amount in another currency.

Click «Next» to select the method of payment and the currency.

Any attempt to remove or damage this software will lead to the immediate destruction of the private key by server.

Private key will be destroyed on
10/9/2013
4:25 PM

Time left
95 : 56 : 35

Image from http://images.techhive.com/images/article/2014/01/cryptolocker-100222101-orig.png

How to Defend against Cryptovirus?

- Typical anti-malware can help
- Access control to cryptographic tools (APIs)
- Theoretical fault-tolerant model
  - How to Withstand Mobile Virus Attacks, ***PDOS 1991***

APT (Advanced Persistent Threat)

Not a new type of malware, but combination of intrusion techniques

- Advanced: advanced intrusion technologies and malware
- Persistent: progressively and stealthily attack the target until the target is compromised over an extended period

- Example: Aurora, Stuxnet

The Arms Race (or Weapons Race)

Attacker vs. Defender

Questions?