Corporate Account Take Over

WALPOLE CO-OPERATIVE BANK

Agenda

- □ What is Corporate Account Take Over
- □ How does it work?
- □ Types of Cyber-Threats and Countermeasures
- □ Current Trends
- □ Security Approach
- □ Tools/Resources/References
- □ Questions

What is Corporate Account Take Over?

WALPOLE
CO-OPERATIVE
BANK

1. Form of Corporate Identity Theft
2. Business' online credentials are stolen by malware
3. Criminal Entities initiate fraudulent banking activity
4. The Corporate customers' credentials are compromised
5. Money is transferred via wire or ACH transactions
6. Little or no ability to recover the losses

Who is Affected?

1. Potential Targets Include:
   a. Municipalities, school districts, large non-profit organizations
   b. Corporate businesses
   c. Any customers that perform electronic transfers
2. Losses range from tens of thousands to millions of Dollars
3. These thefts have affected both large and small banks

How does it work?

WALPOLE
CO-OPERATIVE
BANK

1. Criminals target victims by scams
2. Victim unknowingly installs software by clicking on a link or visiting an infected web site
3. Fraudsters begin monitoring the accounts
4. Victim logs on to their Online Banking system
5. Fraudsters Collect Login Credentials
6. Fraudsters wait for the right time and then depending on the controls in place – they login after hours or, in the case where a token is used, they went until the code is entered and then hijack the session and return a message indicating Online Banking is temporarily unavailable

Types of Cyber-Threats and Countermeasures

WALPOLE
CO-OPERATIVE
BANK

1. The threats to businesses today are many and varied. Malware can find its way onto computers in any number of ways.
   a. Drive-by downloading
   b. Email-phishing
   c. Social Engineering
   d. Hacking/Exploiting weaknesses
   e. Virus and Worm infections

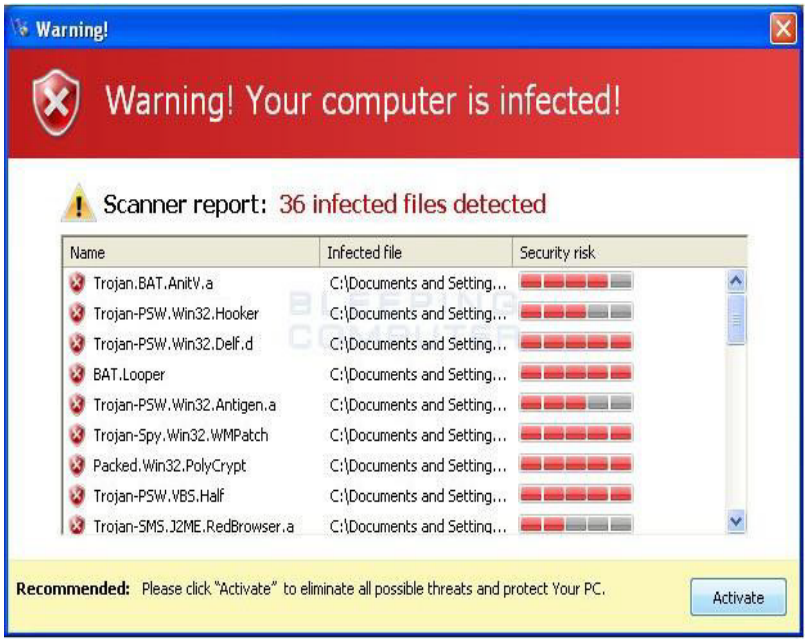
2. Many SMBs (the majority of your customer base) do not have the resources or expertise to protect their computer systems from the majority of these attacks.

Malware

Short for *malicious software,* is software designed to infiltrate a computer system without the owner’s informed consent

Malware includes computer viruses, worms, Trojan horses, spyware shonest adware, crime ware, most rootkits, Remote Access Trojans), rogue software, scareware and unwanted software

- Viruses: A computer program that can copy itself and infect a computer
- Spyware: A type of malware that is installed on computers that collects little bits of information at a time about users without t knowledge
- Rogue Software/Scareware: Form of malware that deceives or misleads users into paying for the fake or simulated removal of malware.



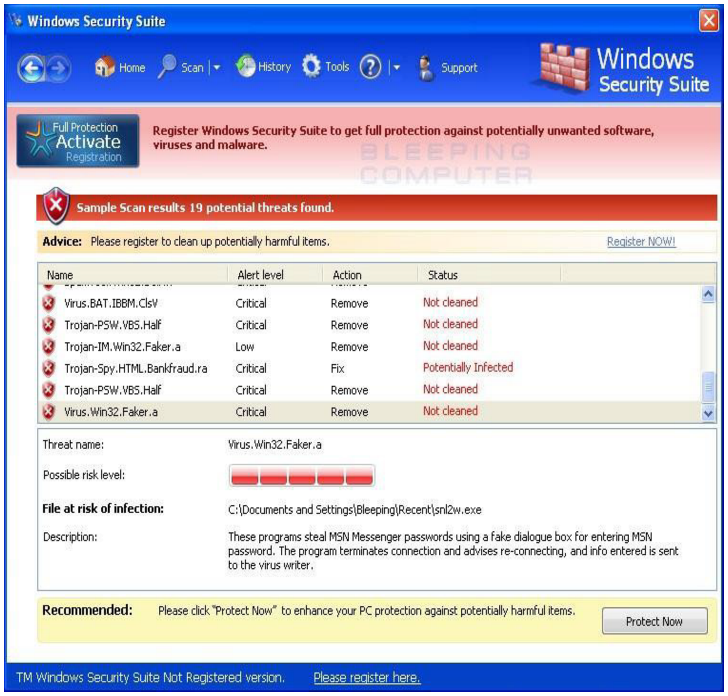
Warning!

Warning! Your computer is infected!

Scanner report: 36 infected files detected

Name	Infected file	Security risk
Trojan.BAT.AnitV.a	C:\Documents and Setting...	🟥🟥🟥🟥⬜
Trojan-PSW.Win32.Hooker	C:\Documents and Setting...	🟥🟥🟥⬜⬜
Trojan-PSW.Win32.Delf.d	C:\Documents and Setting...	🟥🟥🟥🟥🟥
BAT.Looper	C:\Documents and Setting...	🟥🟥🟥🟥🟥
Trojan-PSW.Win32.Antigen.a	C:\Documents and Setting...	🟥🟥🟥⬜⬜
Trojan-Spy.Win32.WMPatch	C:\Documents and Setting...	🟥🟥🟥🟥🟥
Packed.Win32.PolyCrypt	C:\Documents and Setting...	🟥🟥🟥🟥🟥
Trojan-PSW.VBS.Half	C:\Documents and Setting...	🟥🟥🟥🟥🟥
Trojan-SMS.J2ME.RedBrowser.a	C:\Documents and Setting...	🟥🟥⬜⬜⬜

Recommended: Please click “Activate” to eliminate all possible threats and protect Your PC.



Windows Security Suite

Register Windows Security Suite to get full protection against potentially unwanted software, viruses and malware.

Sample Scan results 19 potential threats found.

Advice: Please register to clean up potentially harmful items. Register NOW!

Name	Alert level	Action	Status
Virus.BAT.IBBM.ClsV	Critical	Remove	Not cleaned
Trojan-PSW.VBS.Half	Critical	Remove	Not cleaned
Trojan-IM.Win32.Faker.a	Low	Remove	Not cleaned
Trojan-Spy.HTML.Bankfraud.ra	Critical	Fix	Potentially Infected
Trojan-PSW.VBS.Half	Critical	Remove	Not cleaned
Virus.Win32.Faker.a	Critical	Remove	Not cleaned

Threat name: Virus.Win32.Faker.a

Possible risk level: 🟥🟥🟥🟥🟥

File at risk of infection: C:\Documents and Settings\Bleeping\Recent\snl2w.exe

Description: These programs steal MSN Messenger passwords using a fake dialogue box for entering MSN password. The program terminates connection and advises re-connecting, and info entered is sent to the virus writer.

Recommended: Please click “Protect Now” to enhance your PC protection against potentially harmful items.

TM Windows Security Suite Not Registered version. Please register here.

E-mail

WALPOLE CO-OPERATIVE BANK

- Some experts feel e-mail is the biggest security threat of all
- The fastest, most-effective method of spreading malicious code to the largest number of users
- Also a large source of wasted technology resources
- Examples of corporate e-mail waste:
  - Electronic Greeting Cards
  - Chain Letters
  - Jokes and graphics
  - Spam and junk e-mail

Hoaxes

- Hoaxes attempt to trick or defraud users
- A hoax could be malicious, instructing users to delete a file necessary to the operating system by claiming it is a virus
- It could also be a scam that convinces users to send money or personal information
- Phishing attacks fall into the category

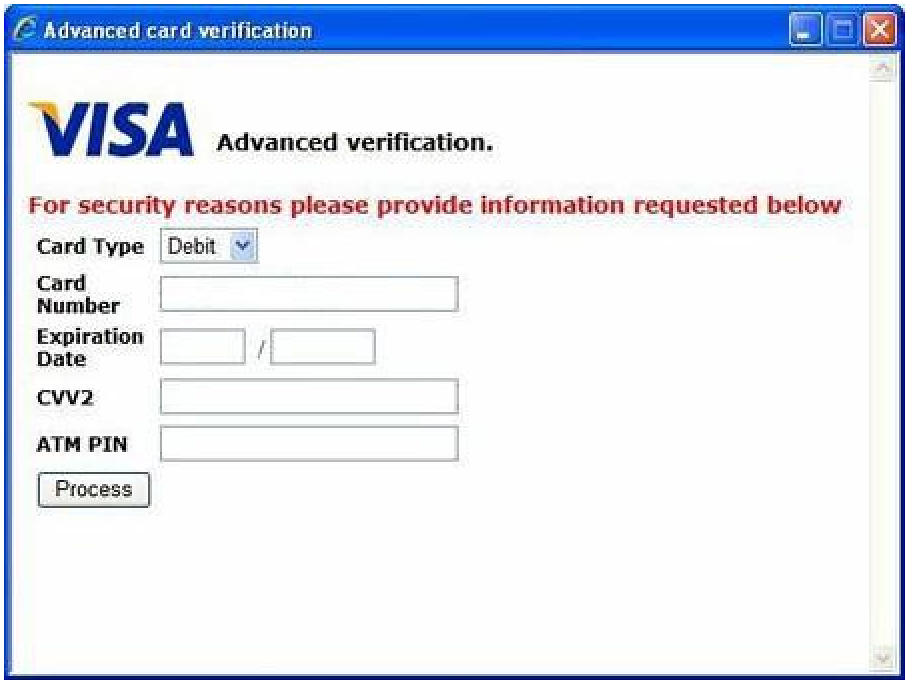
Phishing

WALPOLE CO-OPERATIVE BANK

Criminally fraudulent process of attempting to acquire sensitive information(usernames, passwords, credit card information by, masquerading as a trustworthy entity in an electronic communication

Commonly used means :

- Social Web sites
- Auction sites
- Online payment processors
- IT administrators



Advanced card verification

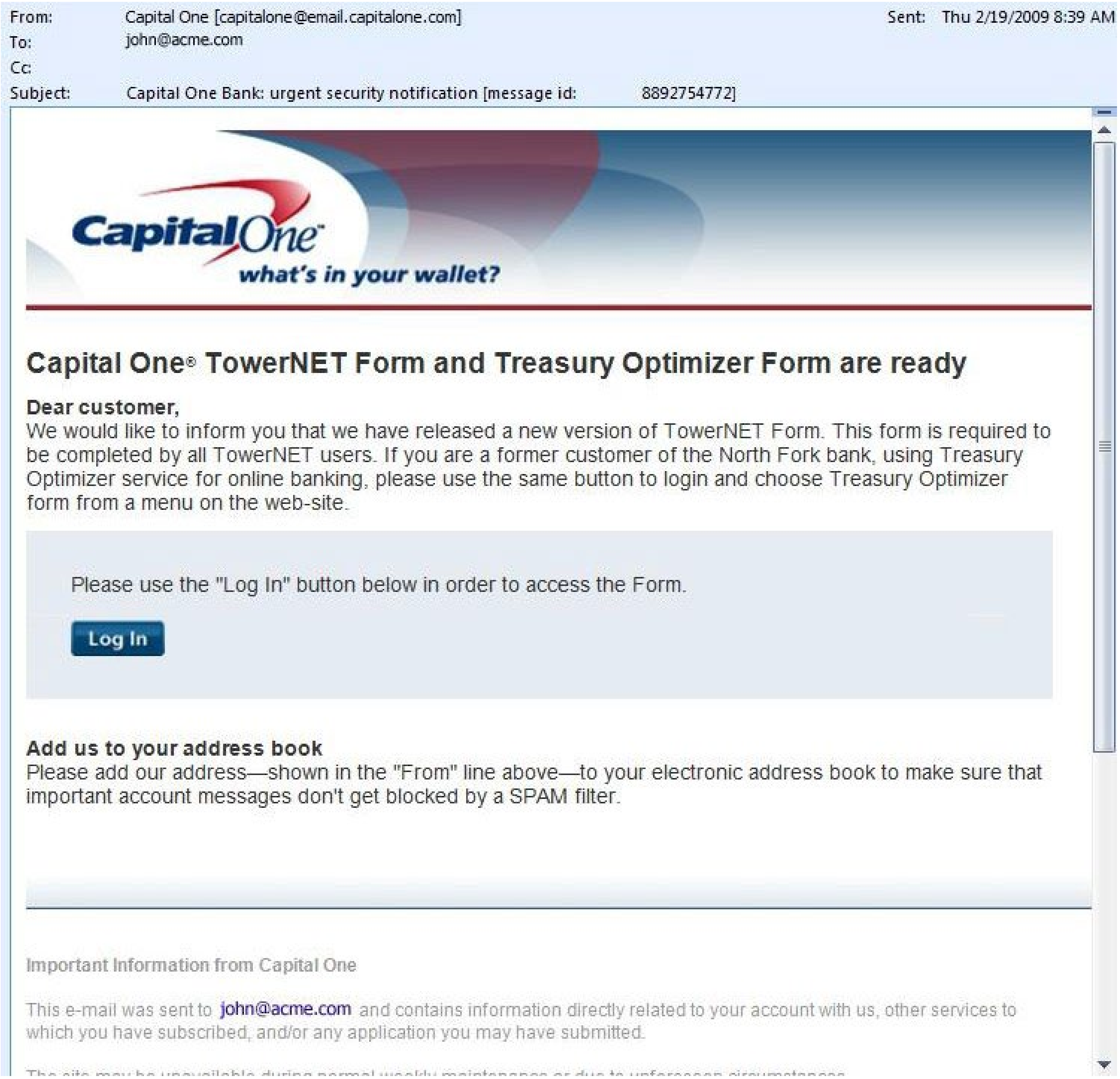
VISA Advanced verification.

For security reasons please provide information requested below

Card Type	Debit
Card Number	
Expiration Date	/
CVV2	
ATM PIN	

Process

Phishing



From: Capital One [capitalone@email.capitalone.com]
Sent: Thu 2/19/2009 8:39 AM
To: john@acme.com
Cc:
Subject: Capital One Bank: urgent security notification [message id: 8892754772]

Capital One® TowerNET Form and Treasury Optimizer Form are ready

Dear customer,
We would like to inform you that we have released a new version of TowerNET Form. This form is required to be completed by all TowerNET users. If you are a former customer of the North Fork bank, using Treasury Optimizer service for online banking, please use the same button to login and choose Treasury Optimizer form from a menu on the web-site.

Please use the "Log In" button below in order to access the Form.

Log In

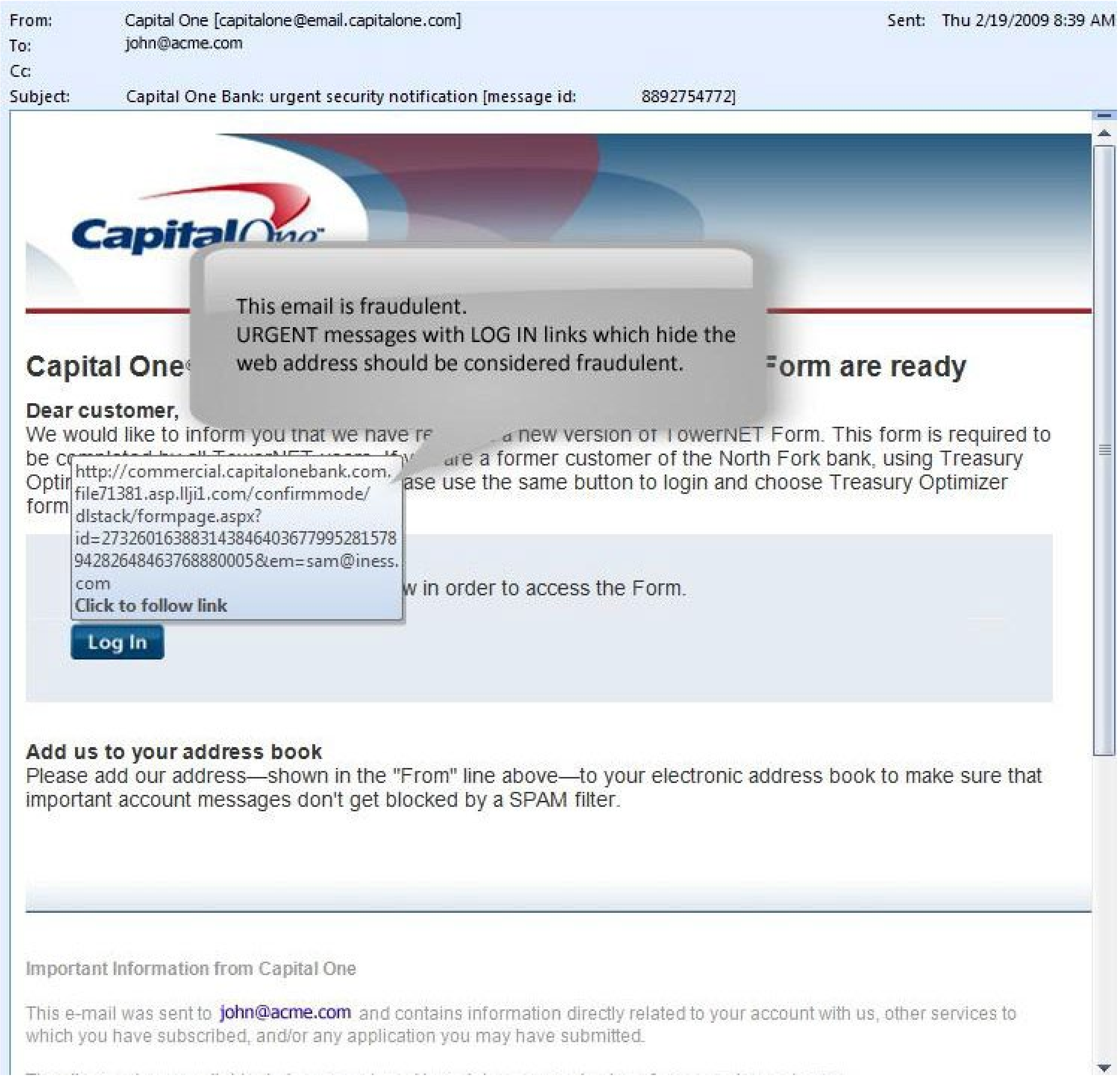
Add us to your address book
Please add our address—shown in the "From" line above—to your electronic address book to make sure that important account messages don't get blocked by a SPAM filter.

Important Information from Capital One

This e-mail was sent to john@acme.com and contains information directly related to your account with us, other services to which you have subscribed, and/or any application you may have submitted.

The site may be unavailable during normal weekly maintenance or due to unforeseen circumstances.

Phishing



From: Capital One [capitalone@email.capitalone.com]

Sent: Thu 2/19/2009 8:39 AM

To: john@acme.com

Cc:

Subject: Capital One Bank: urgent security notification [message id: 8892754772]

This email is fraudulent.
URGENT messages with LOG IN links which hide the web address should be considered fraudulent.

Capital One ... Form are ready

Dear customer,
We would like to inform you that we have re ... a new version of TowerNET Form. This form is required to be c ... are a former customer of the North Fork bank, using Treasury Optir ... ase use the same button to login and choose Treasury Optimizer form

http://commercial.capitalonebank.com.file71381.asp.llji1.com/confirmmode/dlstack/formpage.aspx?id=27326016388314384640367799528157894282648463768880005&em=sam@iness.com
Click to follow link

... w in order to access the Form.

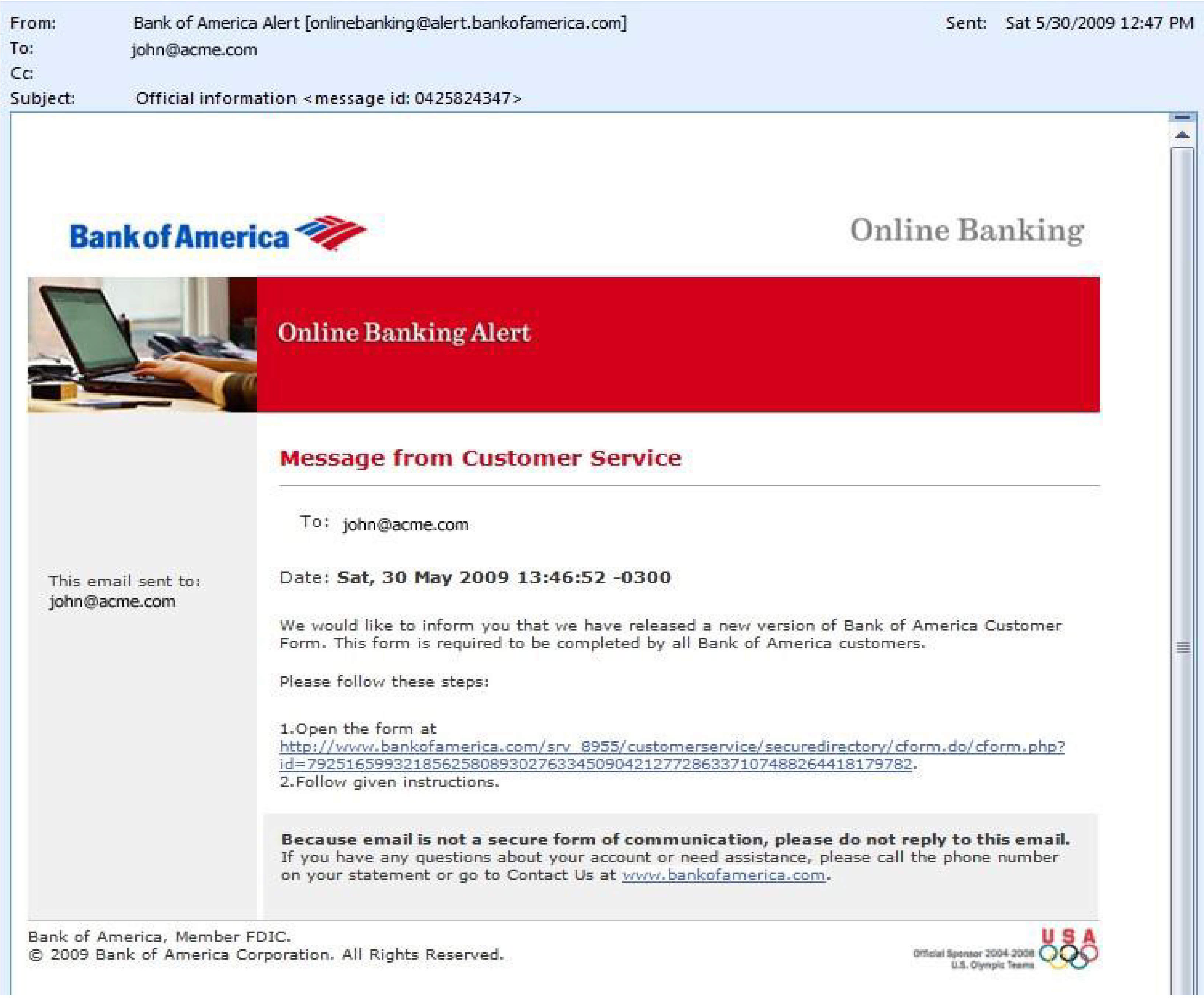
Add us to your address book
Please add our address—shown in the "From" line above—to your electronic address book to make sure that important account messages don't get blocked by a SPAM filter.

Important Information from Capital One

This e-mail was sent to john@acme.com and contains information directly related to your account with us, other services to which you have subscribed, and/or any application you may have submitted.

Phishing

WALPOLE
CO-OPERATIVE
BANK



From: Bank of America Alert [onlinebanking@alert.bankofamerica.com]

Sent: Sat 5/30/2009 12:47 PM

To: john@acme.com

Cc:

Subject: Official information <message id: 0425824347>

Bank of America

Online Banking

Online Banking Alert

This email sent to:
john@acme.com

Message from Customer Service

To: john@acme.com

Date: **Sat, 30 May 2009 13:46:52 -0300**

We would like to inform you that we have released a new version of Bank of America Customer Form. This form is required to be completed by all Bank of America customers.

Please follow these steps:

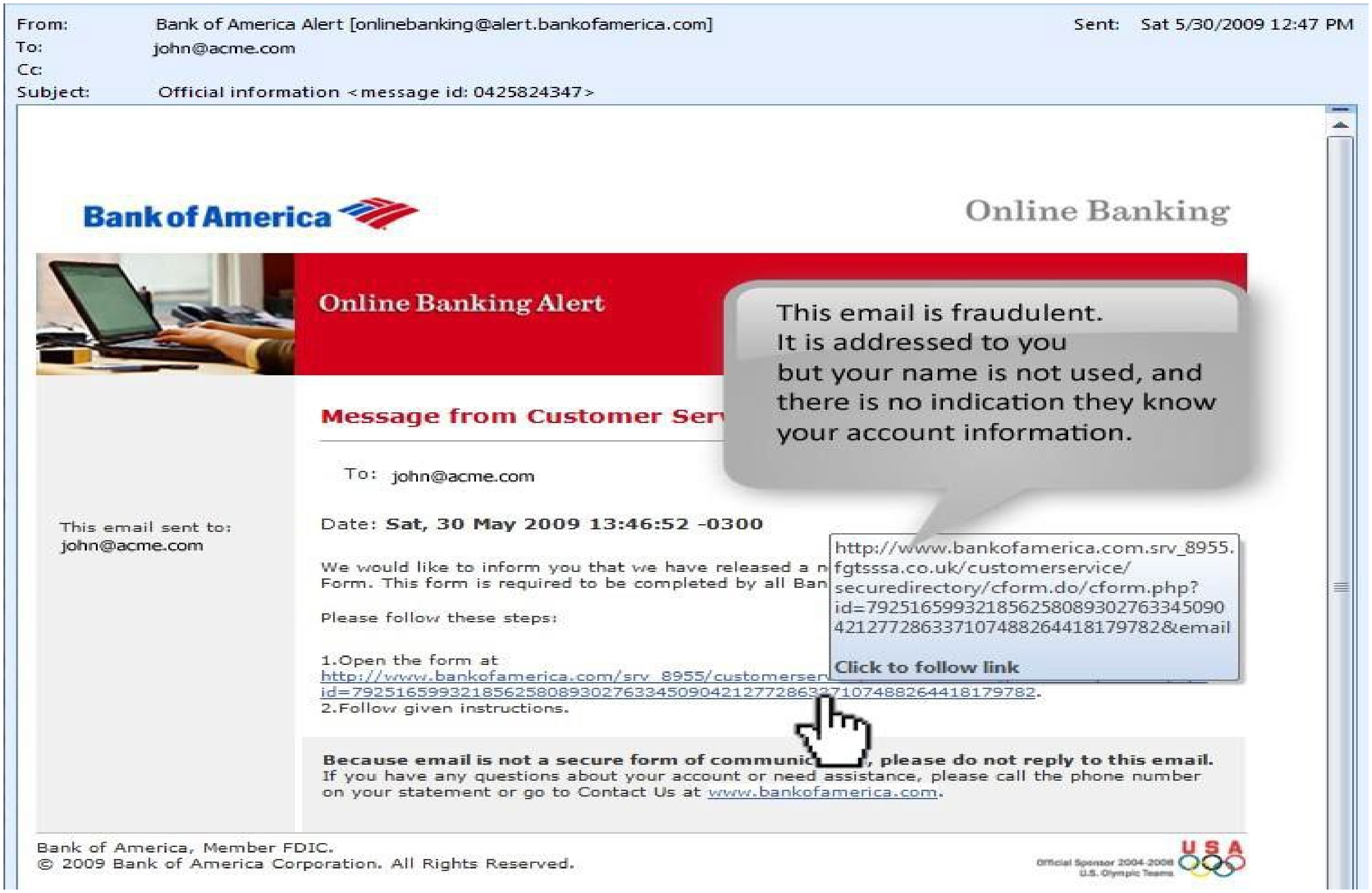
1.Open the form at
http://www.bankofamerica.com/srv_8955/customerservice/securedirectory/cform.do/cform.php?id=792516599321856258089302763345090421277286337107488264418179782.
2.Follow given instructions.

Because email is not a secure form of communication, please do not reply to this email. If you have any questions about your account or need assistance, please call the phone number on your statement or go to Contact Us at www.bankofamerica.com.

Bank of America, Member FDIC.
© 2009 Bank of America Corporation. All Rights Reserved.

USA
Official Sponsor 2004-2008
U.S. Olympic Teams

Phishing



From: Bank of America Alert [onlinebanking@alert.bankofamerica.com]
Sent: Sat 5/30/2009 12:47 PM
To: john@acme.com
Cc:
Subject: Official information <message id: 0425824347>

Message from Customer Serv

To: john@acme.com

This email sent to:
john@acme.com

Date: **Sat, 30 May 2009 13:46:52 -0300**

We would like to inform you that we have released a n
Form. This form is required to be completed by all Ban

Please follow these steps:

1.Open the form at
http://www.bankofamerica.com/srv_8955/customerserv
id=792516599321856258089302763345090421277286337107488264418179782.
2.Follow given instructions.

Because email is not a secure form of communic , please do not reply to this email.
If you have any questions about your account or need assistance, please call the phone number on your statement or go to Contact Us at www.bankofamerica.com.

Bank of America, Member FDIC.
© 2009 Bank of America Corporation. All Rights Reserved.

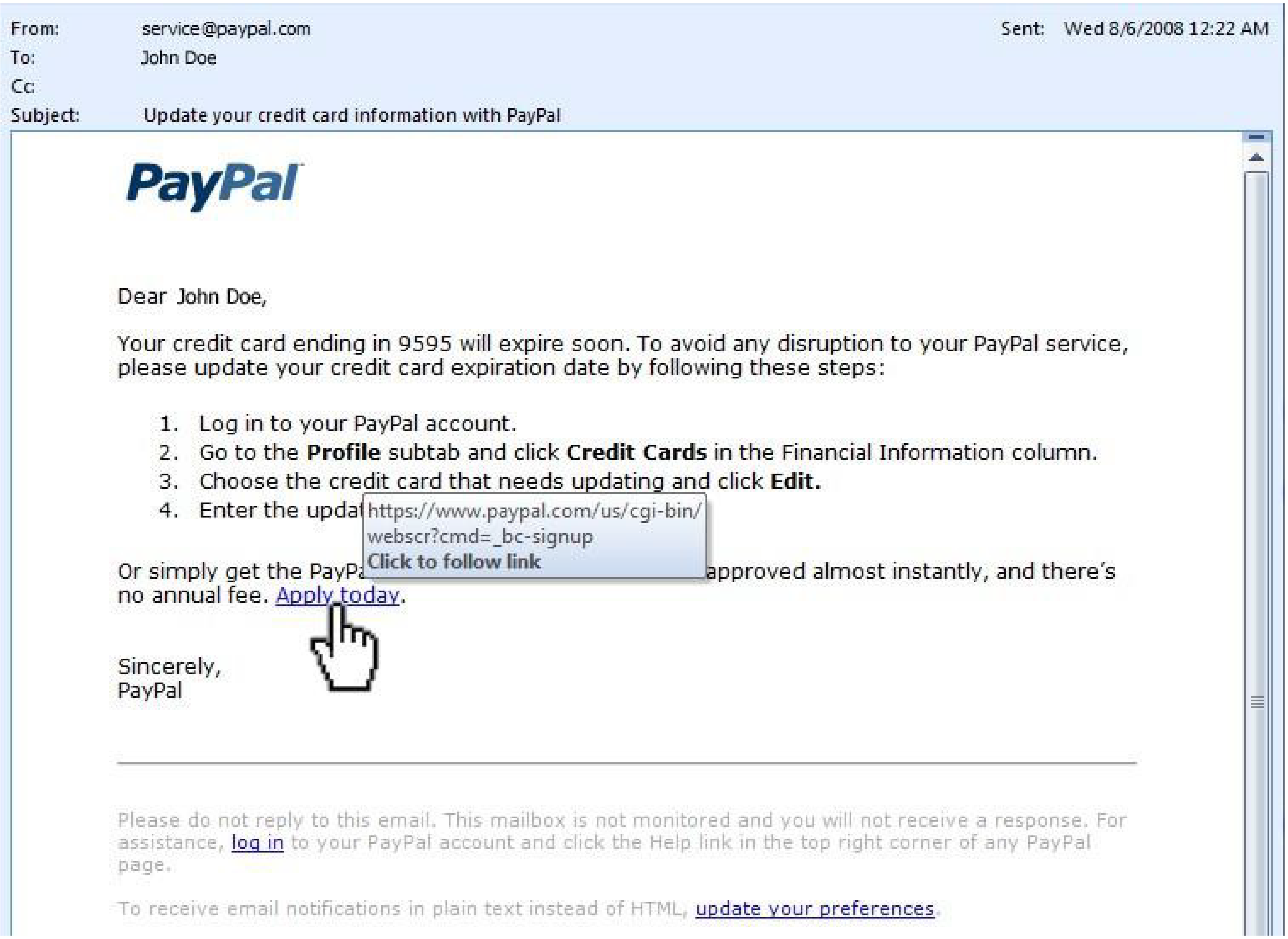
http://www.bankofamerica.com.srv_8955.fgtsssa.co.uk/customerservice/securedirectory/cform.do/cform.php?id=792516599321856258089302763345090421277286337107488264418179782&email

Click to follow link

This email is fraudulent.
It is addressed to you
but your name is not used, and
there is no indication they know
your account information.

Phishing

WALPOLE CO-OPERATIVE BANK



From: service@paypal.com

Sent: Wed 8/6/2008 12:22 AM

To: John Doe

Cc:

Subject: Update your credit card information with PayPal

Dear John Doe,

Your credit card ending in 9595 will expire soon. To avoid any disruption to your PayPal service, please update your credit card expiration date by following these steps:

1. Log in to your PayPal account.
2. Go to the **Profile** subtab and click **Credit Cards** in the Financial Information column.
3. Choose the credit card that needs updating and click **Edit.**
4. Enter the updat

https://www.paypal.com/us/cgi-bin/webscr?cmd=_bc-signup

Click to follow link

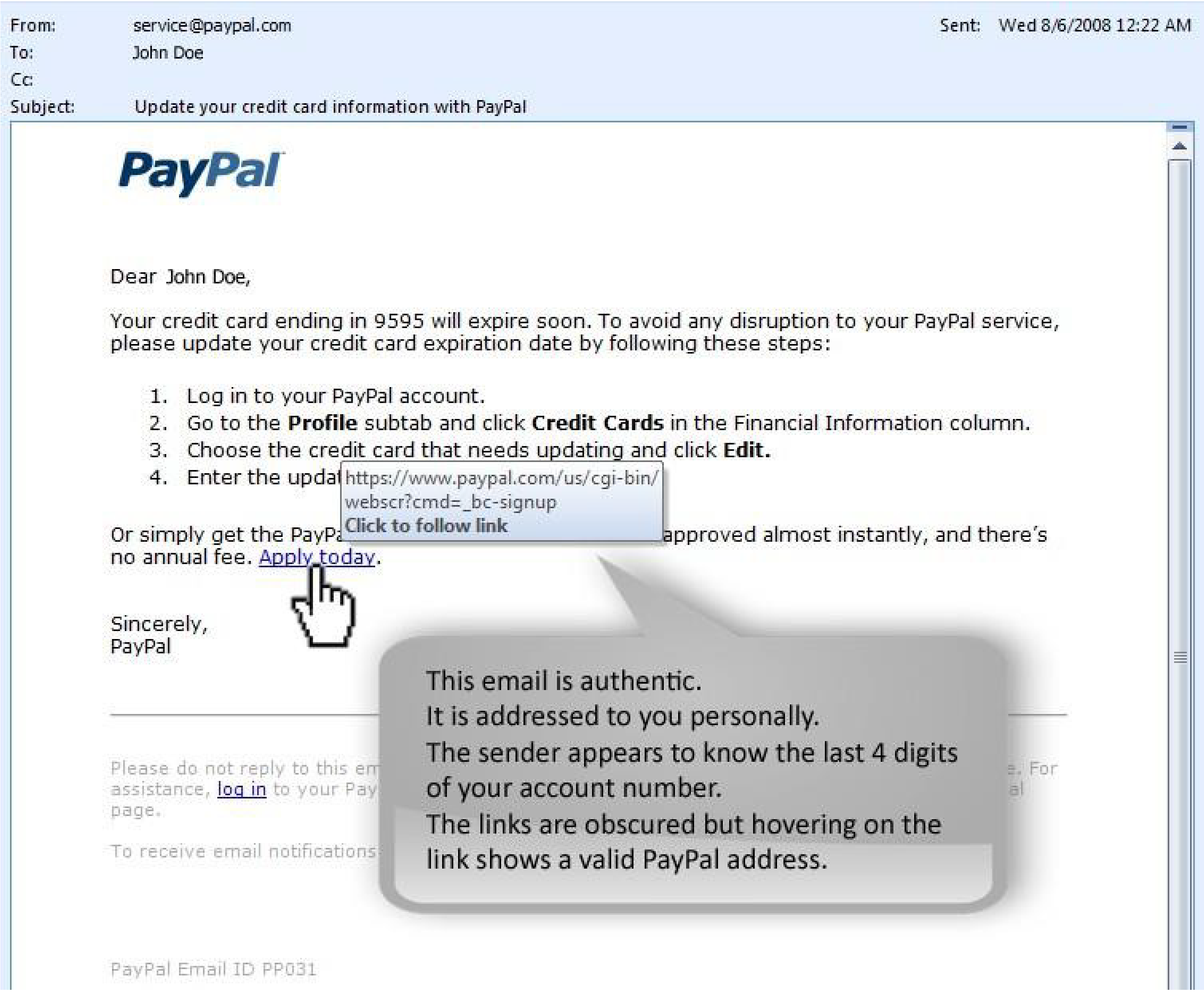
Or simply get the PayPa approved almost instantly, and there's no annual fee. Apply today.

Sincerely,
PayPal

Please do not reply to this email. This mailbox is not monitored and you will not receive a response. For assistance, log in to your PayPal account and click the Help link in the top right corner of any PayPal page.

To receive email notifications in plain text instead of HTML, update your preferences.

Phishing



From: service@paypal.com Sent: Wed 8/6/2008 12:22 AM
To: John Doe
Cc:
Subject: Update your credit card information with PayPal

PayPal

Dear John Doe,

Your credit card ending in 9595 will expire soon. To avoid any disruption to your PayPal service, please update your credit card expiration date by following these steps:

1. Log in to your PayPal account.
2. Go to the **Profile** subtab and click **Credit Cards** in the Financial Information column.
3. Choose the credit card that needs updating and click **Edit.**
4. Enter the updat

https://www.paypal.com/us/cgi-bin/webscr?cmd=_bc-signup
Click to follow link

Or simply get the PayPa approved almost instantly, and there's no annual fee. Apply today.

Sincerely,
PayPal

Please do not reply to this em e. For assistance, log in to your Pay al page.

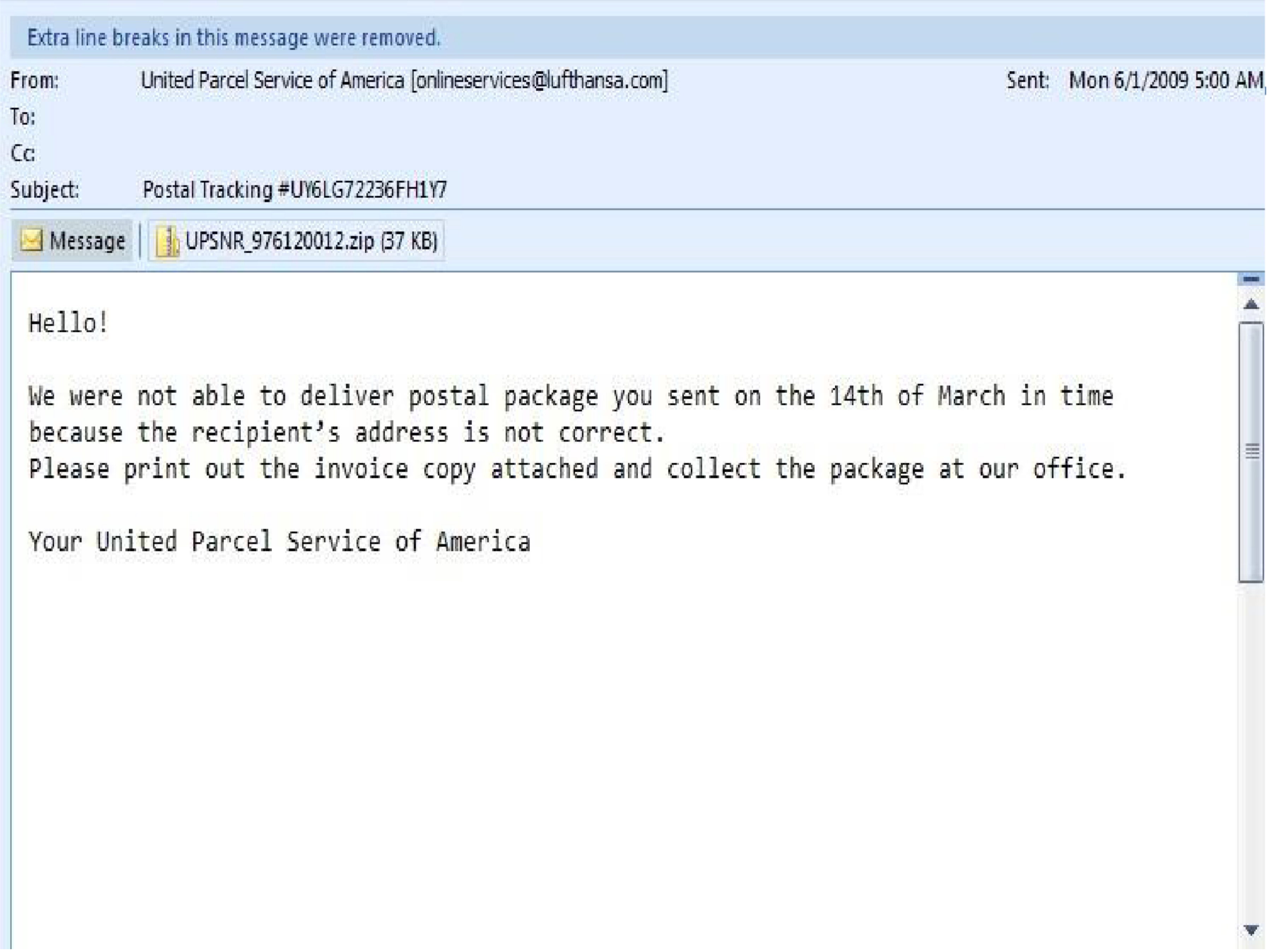
To receive email notifications

PayPal Email ID PP031

This email is authentic.
It is addressed to you personally.
The sender appears to know the last 4 digits of your account number.
The links are obscured but hovering on the link shows a valid PayPal address.

Phishing

WALPOLE CO-OPERATIVE BANK



Extra line breaks in this message were removed.

From: United Parcel Service of America [onlineservices@lufthansa.com]

Sent: Mon 6/1/2009 5:00 AM

To:

Cc:

Subject: Postal Tracking #UY6LG72236FH1Y7

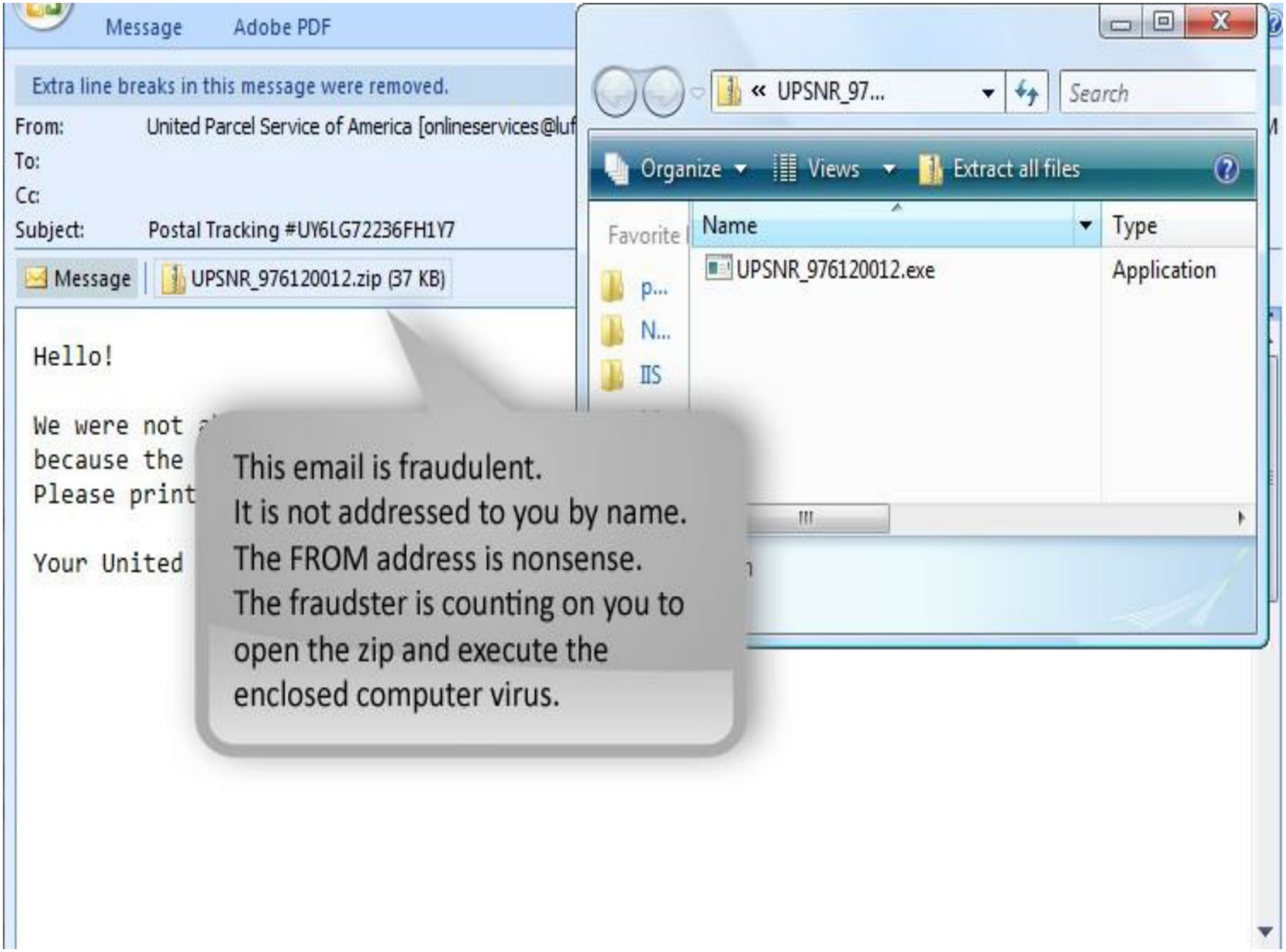
Message | UPSNR_976120012.zip (37 KB)

Hello!

We were not able to deliver postal package you sent on the 14th of March in time because the recipient's address is not correct.
Please print out the invoice copy attached and collect the package at our office.

Your United Parcel Service of America

Phishing



Extra line breaks in this message were removed.

From: United Parcel Service of America [onlineservices@luf

To:

Cc:

Subject: Postal Tracking #UY6LG72236FH1Y7

Message | UPSNR_976120012.zip (37 KB)

```
Hello!

We were not a
because the
Please print

Your United
```

Name	Type
UPSNR_976120012.exe	Application

This email is fraudulent.
It is not addressed to you by name.
The FROM address is nonsense.
The fraudster is counting on you to open the zip and execute the enclosed computer virus.

Security Approach

- Protect
  - Education is Key – Train employees
  - Install and Maintain Real Time Anti-virus/Anti-spyware/Firewall software and keep it up to date
  - Secure their computer networks
  - Limit Administrative Rights
    - Do not allow employees to install any software without receiving approval
  - Install and Maintain Spam Filters
  - Surf the Internet carefully
  - Install security updates to operating systems and all applications as they become available
  - Block Pop-Ups
  - Do not open attachments from e-mail
  - Do not use public Internet access points
  - Recommend dual control from separate devices

Security Approach

WALPOLE
CO-OPERATIVE
BANK

- Detect
  - Education is Key – Train their employees
  - Reconcile Accounts Daily
  - Be on the alert for suspicious e-mails
  - Install Anti-virus/Anti-spyware/Firewall software and keep it up to date
    - Perform a full scan at least once a month (weekly)
  - Note any changes in the performance of your computer
    - Dramatic loss of speed, computer locks up, unexpected rebooting, unusual popups, etc.

Security Approach

- Respond
  - Education is Key – Train their employees
    - Make sure that their employees know how and to whom to report suspicious activity to at the Company and the bank
  - Contact the Bank:
    - If they suspect a Fraudulent Transaction
    - If they are trying to process an Online Wire or ACH Batch & receive a maintenance page
    - If they receive an email claiming to be from the Bank and it is requesting personal/company information.