# Secure the data – a priority in your business?

Gheorghe Dobrea
Xeduco ( Intelprof )
www.xeduco.net

# Teaching / Consulting  for IT Security

Last 12 months:

- Bucharest
- Lausanne
- Tokyo
- Phnom Penh
- Washington DC
- New Delhi
- Dubai etc…

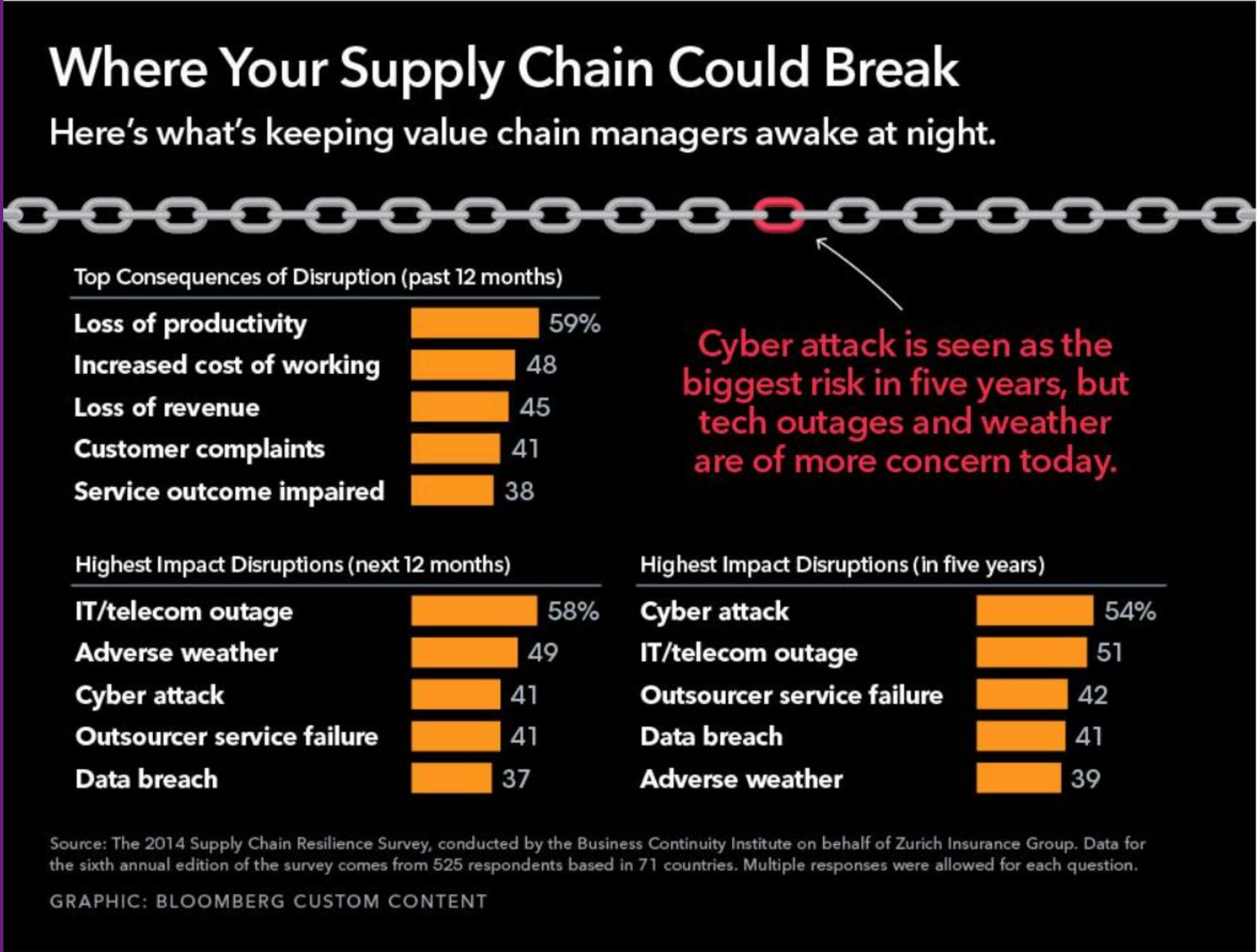
Xeduco

# Assume breach

*"There are two types of companies today, those that have been hacked and those that don't know they've been hacked."* [1]

Assumption of breach represents a maturing of defenses to meet this reality and shifts the focus from "if" to "when" an attacker gets inside an organization's network.

[1] http://bits.blogs.nytimes.com/2013/04/22/the-year-in-hacking-by-the-numbers



# Where Your Supply Chain Could Break

## Here's what's keeping value chain managers awake at night.

Top Consequences of Disruption (past 12 months)

| | |
|---|---|
| Loss of productivity | 59% |
| Increased cost of working | 48 |
| Loss of revenue | 45 |
| Customer complaints | 41 |
| Service outcome impaired | 38 |

Cyber attack is seen as the biggest risk in five years, but tech outages and weather are of more concern today.

Highest Impact Disruptions (next 12 months)

| | |
|---|---|
| IT/telecom outage | 58% |
| Adverse weather | 49 |
| Cyber attack | 41 |
| Outsourcer service failure | 41 |
| Data breach | 37 |

Highest Impact Disruptions (in five years)

| | |
|---|---|
| Cyber attack | 54% |
| IT/telecom outage | 51 |
| Outsourcer service failure | 42 |
| Data breach | 41 |
| Adverse weather | 39 |

Source: The 2014 Supply Chain Resilience Survey, conducted by the Business Continuity Institute on behalf of Zurich Insurance Group. Data for the sixth annual edition of the survey comes from 525 respondents based in 71 countries. Multiple responses were allowed for each question.

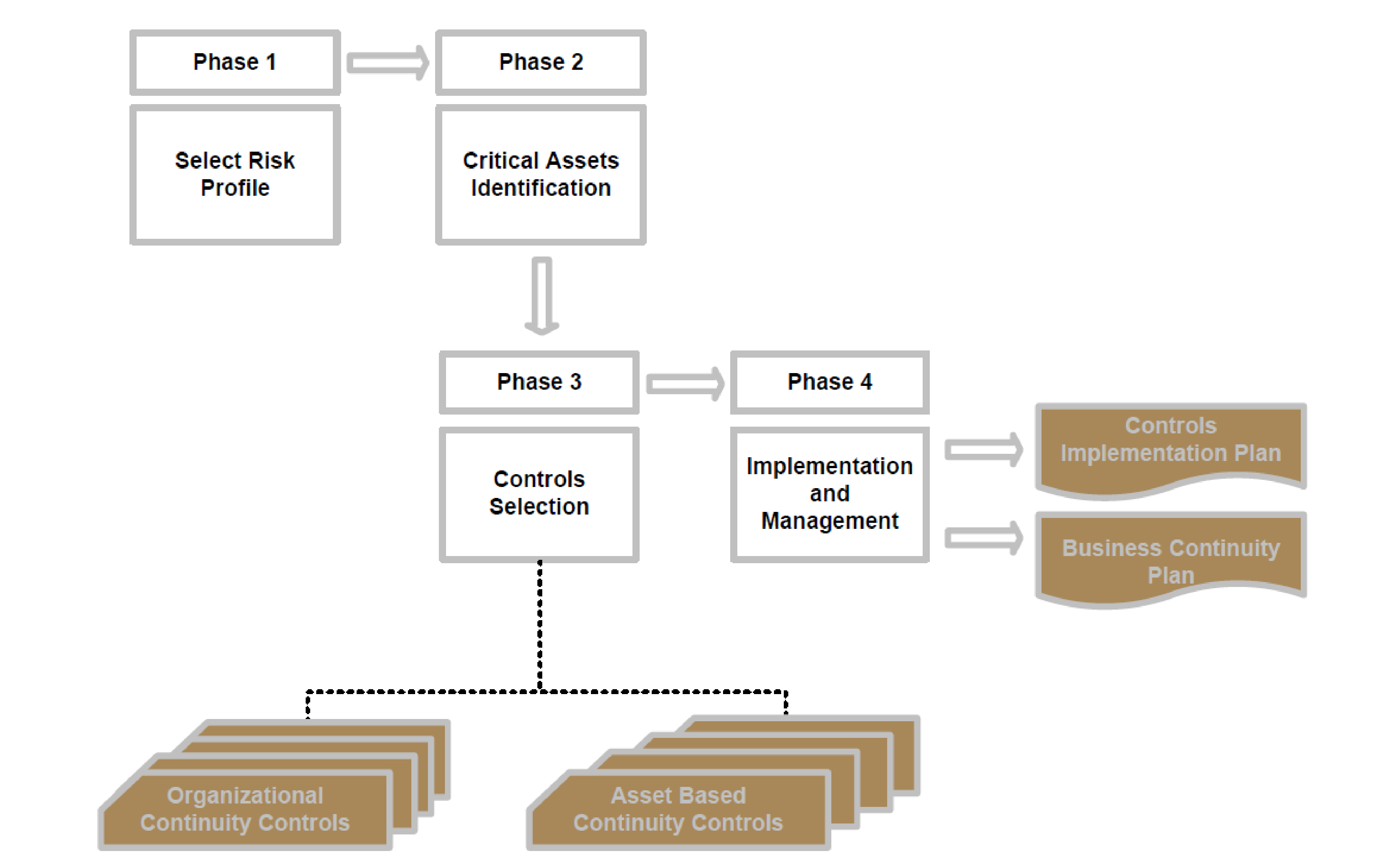
GRAPHIC: BLOOMBERG CUSTOM CONTENT

# Emerging Threat Landscape

- Cyber Physical Systems
- Mobile Computing
- Cloud Computing
- Trust Infrastructure
- Big Data
- Internet of Things/ interconnected devices/ smart environments

Source: ENISA ETL Report 2014

# The Four Phases of Business Continuity Model Approach



Phase 1

Select Risk Profile

Phase 2

Critical Assets Identification

Phase 3

Controls Selection

Phase 4

Implementation and Management

Controls Implementation Plan

Business Continuity Plan

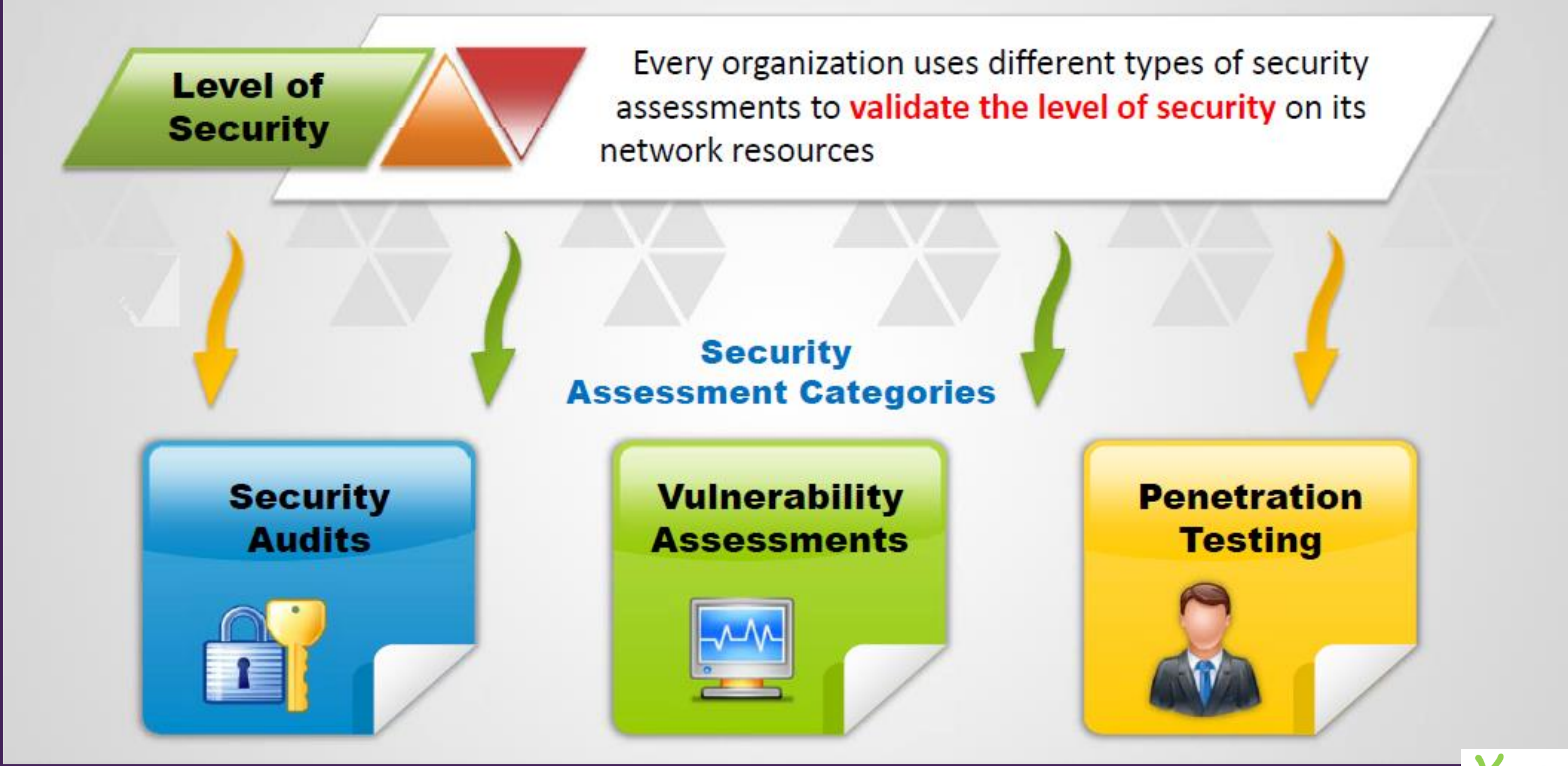
Organizational Continuity Controls

Asset Based Continuity Controls

Source: ENISA BCM Report 2014

Xeduco

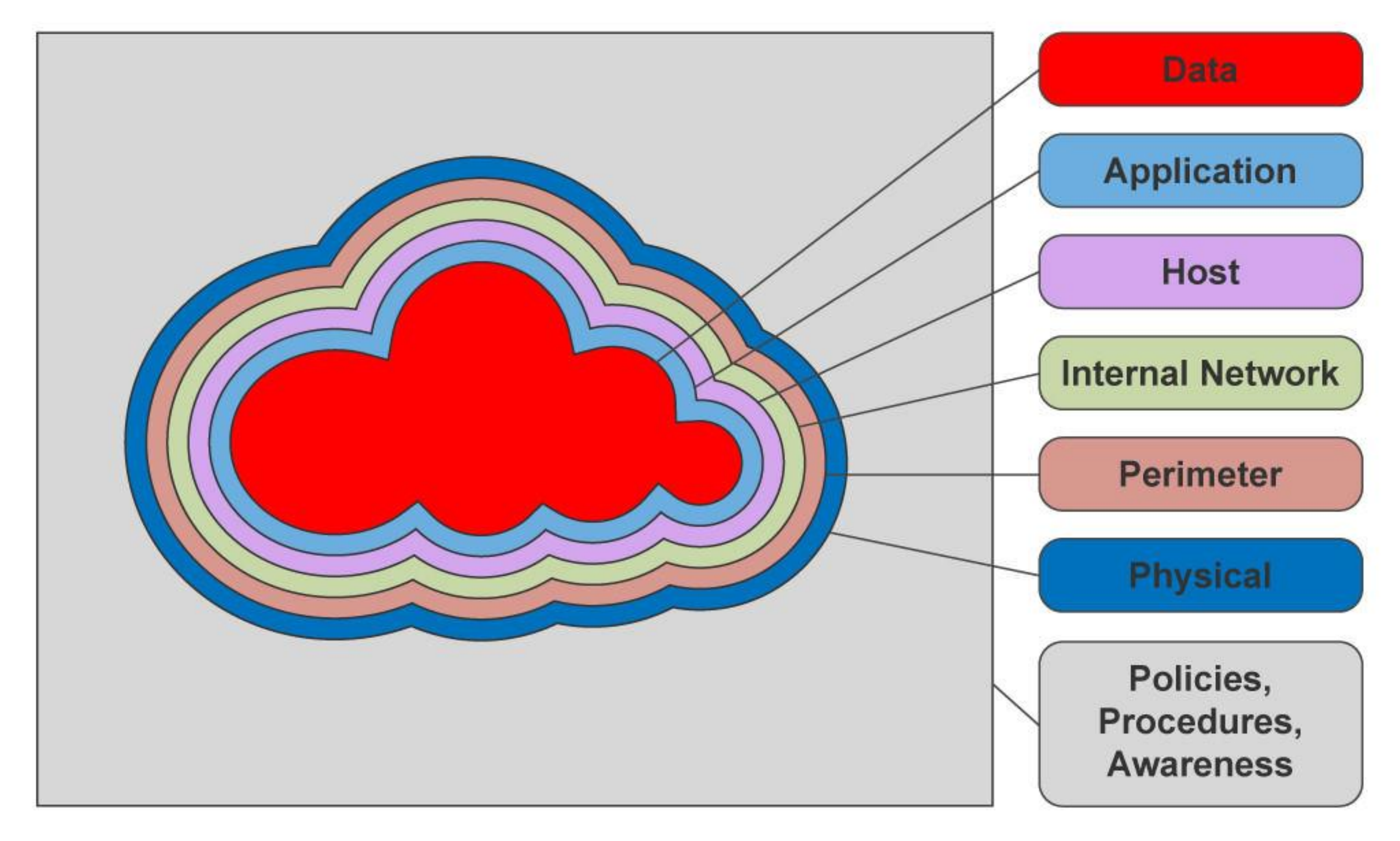
# Security Assessment Categories



Every organization uses different types of security assessments to **validate the level of security** on its network resources

Source: EC-Council

# Defence in Depth Strategy



Data

Application

Host

Internal Network

Perimeter

Physical

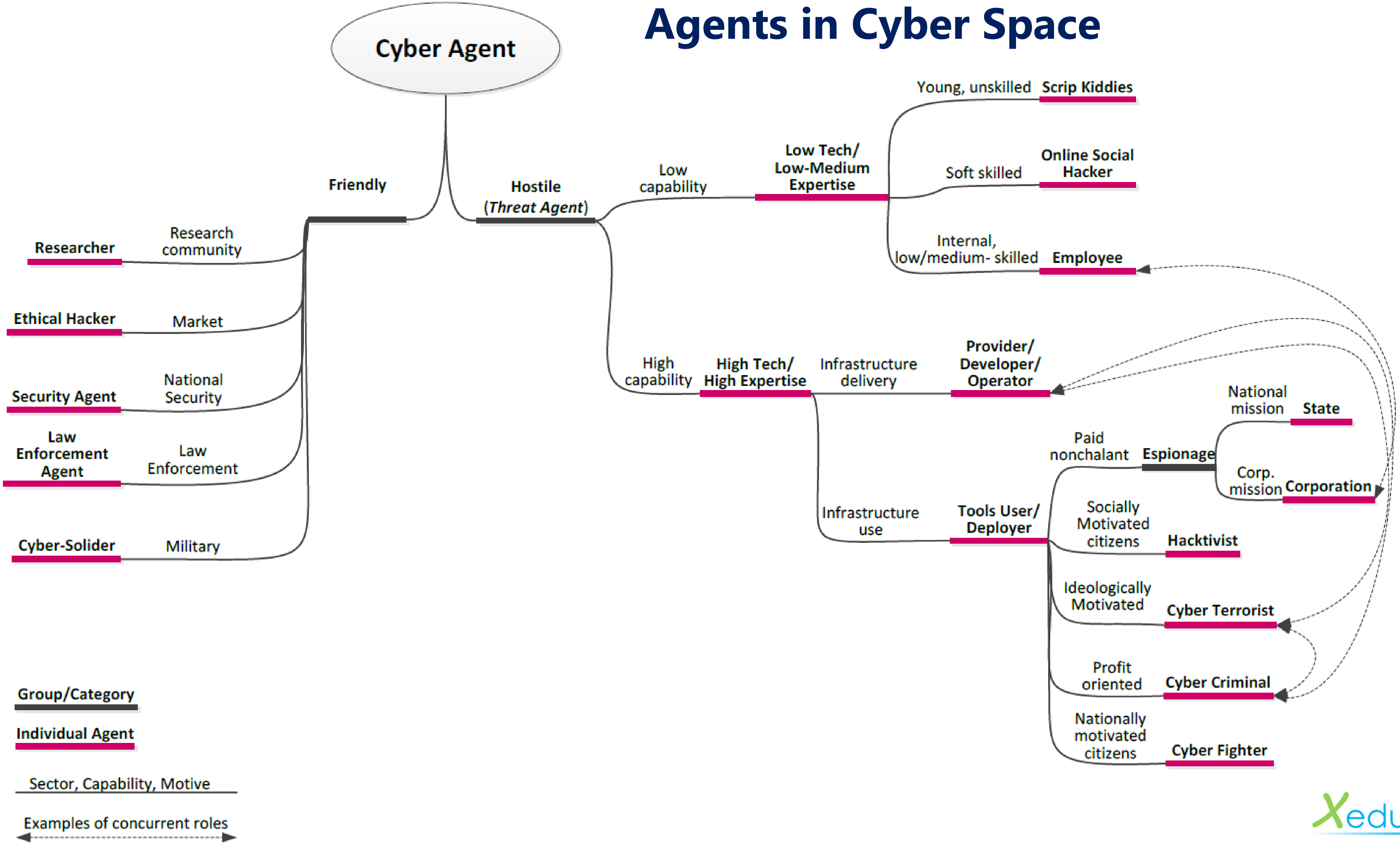
Policies, Procedures, Awareness

Source: EC-Council

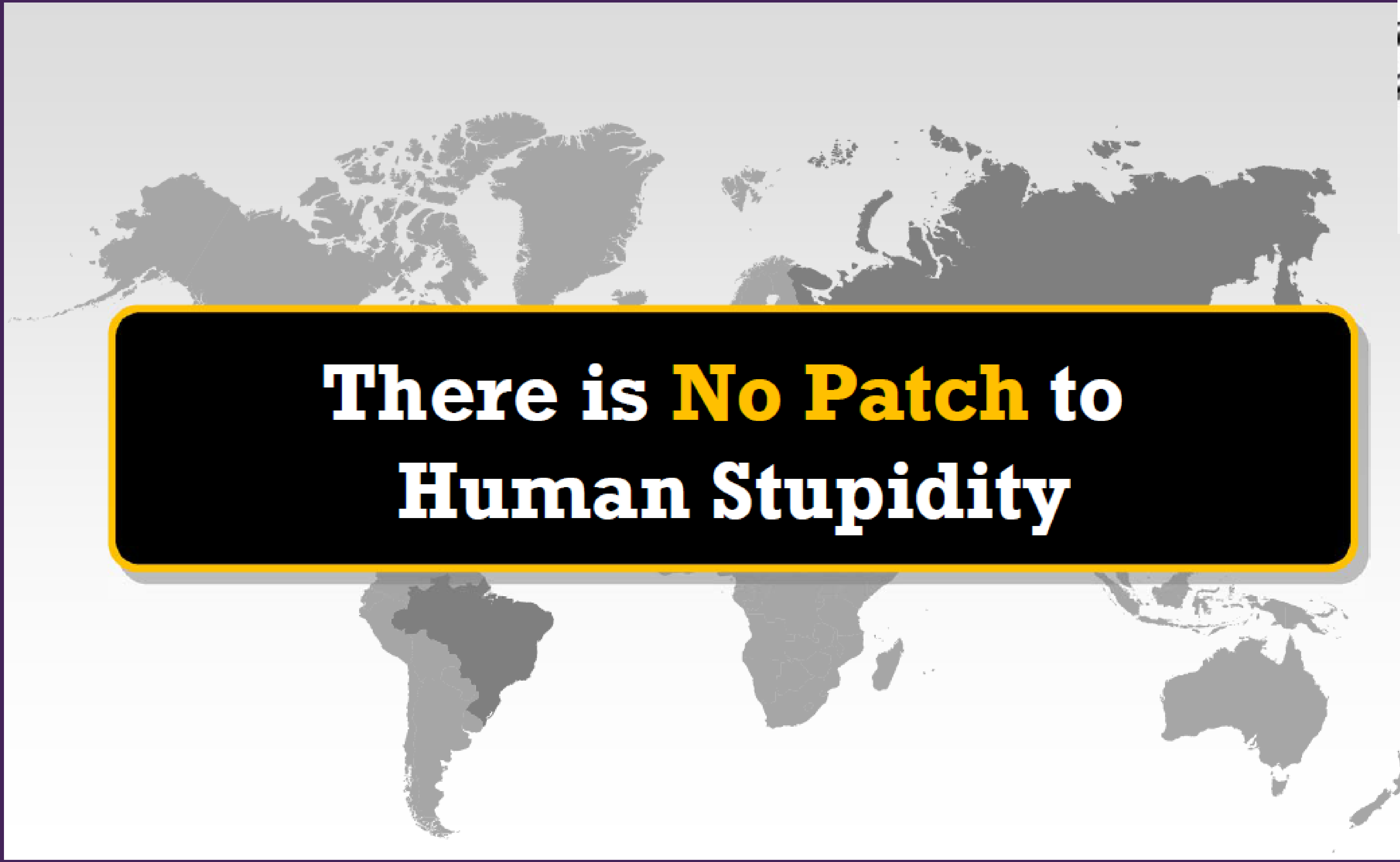
# Mandatory steps to take before you become the next victim ☺

- Make sure you encrypt computers, hard drives, databases and all the data.
- Run and test frequent backups and disaster recovery plans.
- Manage the **BYOD** (Bring Your Own Device) dilemma
- Make sure you enforce better password management policies.
- Create and manage corporate security policies around the standards such as ISO 27001 or COBIT.
- Educate employees against social engineering and phishing attacks.

# Agents in Cyber Space

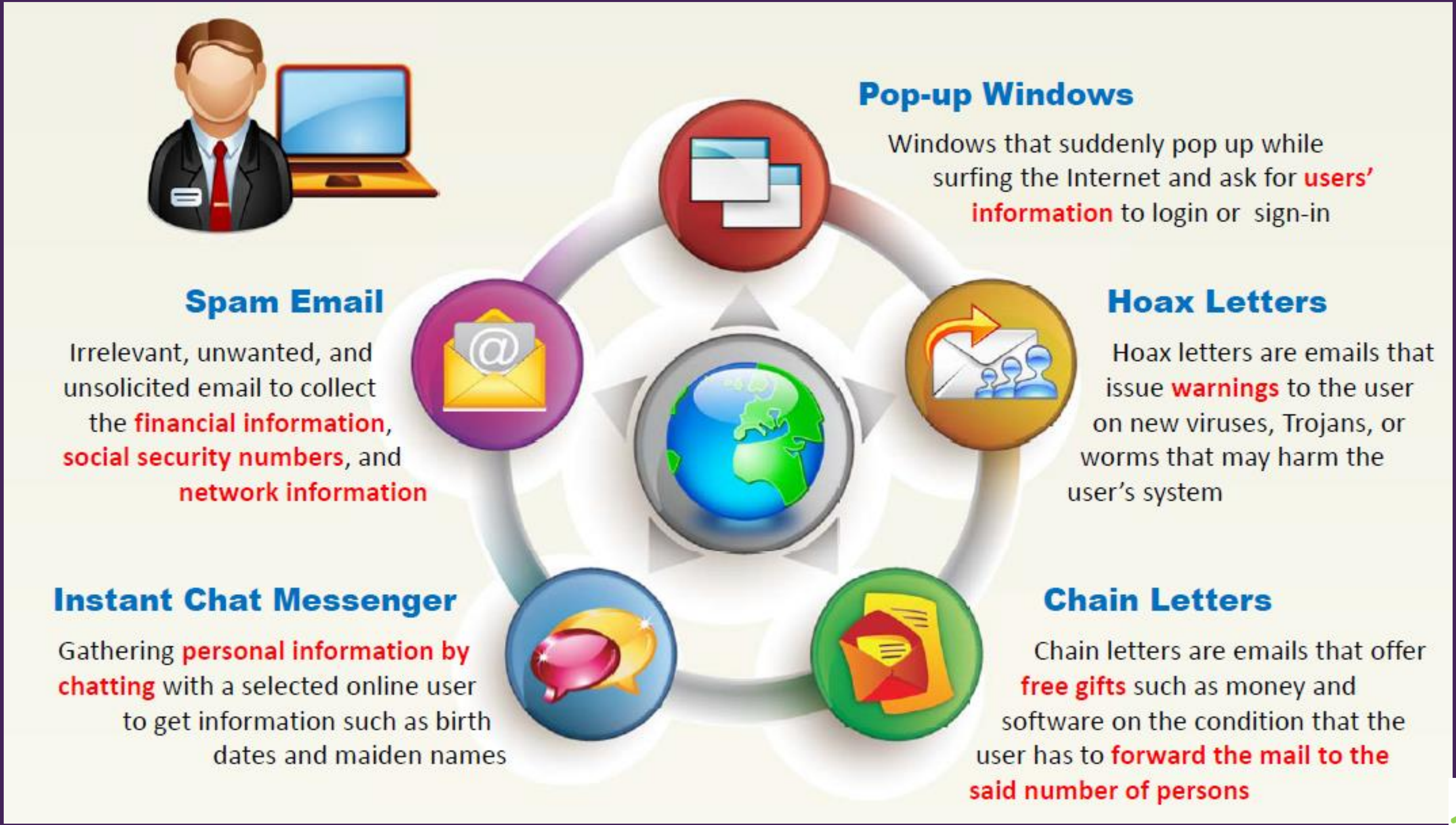


# Social Engineering Attacks:



**There is No Patch to Human Stupidity**

# Computer-based Social Engineering Attacks



### Pop-up Windows

Windows that suddenly pop up while surfing the Internet and ask for **users' information** to login or sign-in

### Spam Email

Irrelevant, unwanted, and unsolicited email to collect the **financial information**, **social security numbers**, and **network information**

### Hoax Letters

Hoax letters are emails that issue **warnings** to the user on new viruses, Trojans, or worms that may harm the user's system

### Instant Chat Messenger

Gathering **personal information by chatting** with a selected online user to get information such as birth dates and maiden names

### Chain Letters

Chain letters are emails that offer **free gifts** such as money and software on the condition that the user has to **forward the mail to the said number of persons**

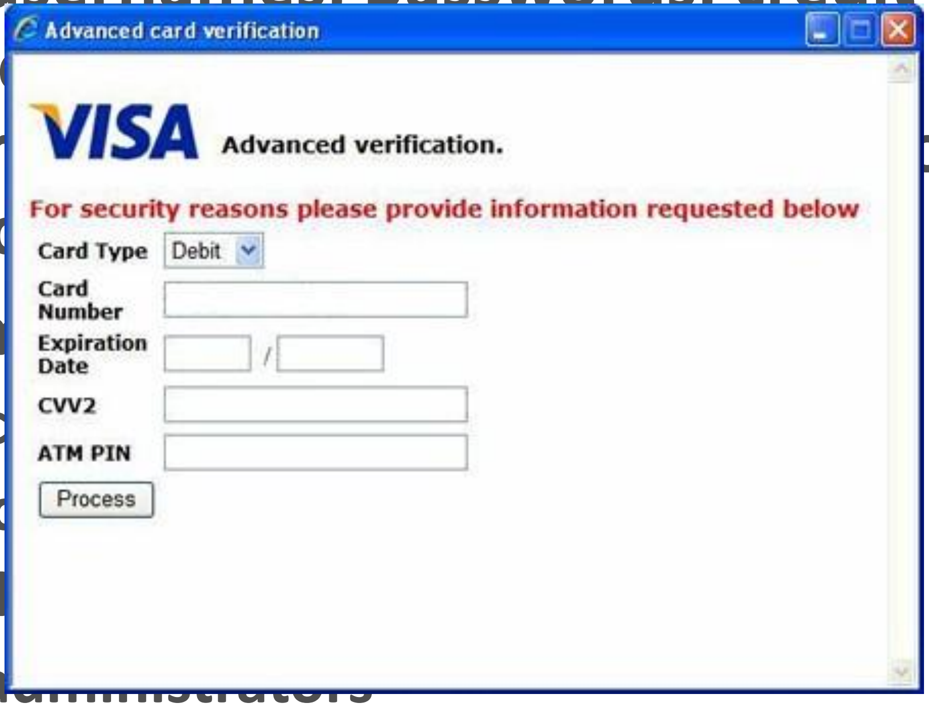
Source:
EC-Council

# 5 minutes  Social Engineering Workshop

- Phishing
- Cryptolocker
- Identity Theft
- USB Threat
- Wi-Fi Threat

# Phishing

- Criminally fraudulent process of attempting to acquire sensitive information (usernames, passwords, credit card d
  tr onic
  c
- Comm
  - Soc
  - Auc
  - Onl
  - IT administrators



Advanced card verification

VISA Advanced verification.

For security reasons please provide information requested below

Card Type Debit

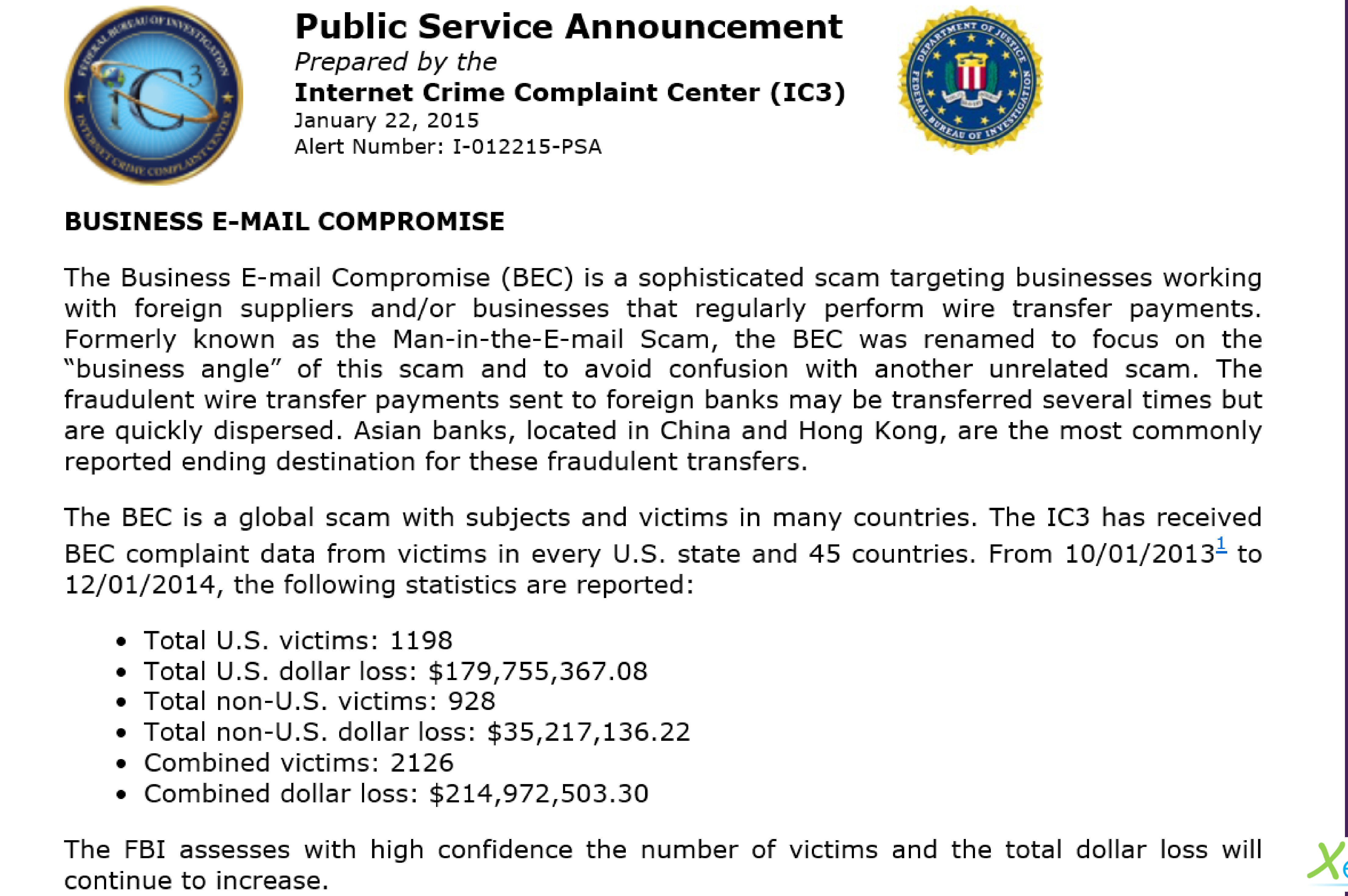
Card Number

Expiration Date /

CVV2

ATM PIN

Process



# Public Service Announcement

*Prepared by the*

**Internet Crime Complaint Center (IC3)**

January 22, 2015

Alert Number: I-012215-PSA

## BUSINESS E-MAIL COMPROMISE

The Business E-mail Compromise (BEC) is a sophisticated scam targeting businesses working with foreign suppliers and/or businesses that regularly perform wire transfer payments. Formerly known as the Man-in-the-E-mail Scam, the BEC was renamed to focus on the "business angle" of this scam and to avoid confusion with another unrelated scam. The fraudulent wire transfer payments sent to foreign banks may be transferred several times but are quickly dispersed. Asian banks, located in China and Hong Kong, are the most commonly reported ending destination for these fraudulent transfers.

The BEC is a global scam with subjects and victims in many countries. The IC3 has received BEC complaint data from victims in every U.S. state and 45 countries. From 10/01/2013[1] to 12/01/2014, the following statistics are reported:

- Total U.S. victims: 1198
- Total U.S. dollar loss: $179,755,367.08
- Total non-U.S. victims: 928
- Total non-U.S. dollar loss: $35,217,136.22
- Combined victims: 2126
- Combined dollar loss: $214,972,503.30

The FBI assesses with high confidence the number of victims and the total dollar loss will continue to increase.

# Social Engineering Red Flags

## FROM:

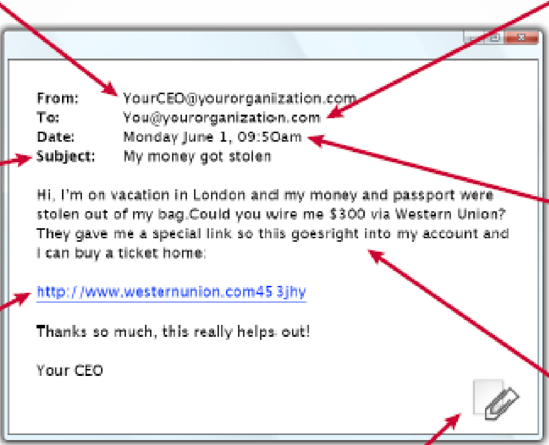
- I don't recognize the sender's email address as someone **I ordinarily communicate with.**
- This email is from **someone outside my organization and it's not related to my job responsibilities.**
- This email was sent from **someone inside the organization** or from a customer, vendor, or partner and is **very unusual or out of character.**
- Is the sender's email address **from a suspicious domain**? (like micorsoft-support.om)
- **I don't know the sender personally** and they **were not vouched for** by someone I trust.
- **I don't have a business relationship** nor any **past communications** with the sender.
- This is an **unexpected or unusual email** with an **embedded hyperlink or an attachment** from someone I hadn't communicated with recently.

## TO:

- I was cc'd on an email sent to one or more people, but I **don't personally know** the other people it was sent to.
- I received an email that was also sent to an **unusual mix of people.** For instance a seemingly random group of people at your organization whose last names start with the same letter, or a whole list of unrelated addresses.

## SUBJECT:

- Did I get an email with a subject line that is **irrelevant** or **does not match** the content?
- Is the email message a reply to something I **never sent or request**?



**From:** YourCEO@yourorganization.com
**To:** You@yourorganization.com
**Date:** Monday June 1, 09:50am
**Subject:** My money got stolen

Hi, I'm on vacation in London and my money and passport were stolen out of my bag.Could you wire me $300 via Western Union? They gave me a special link so this goesright into my account and I can buy a ticket home:

http://www.westernunion.com45 3jhy

Thanks so much, this really helps out!

Your CEO

## DATE:

- Did I receive an email that I normally would get during regular business hours, but it was **sent at an unusual time** like 3 a.m.?

## HYPERLINKS:

- I hover my mouse over a hyperlink that's displayed in the email message, but the **link to address is for a different web site.** (This is a **big** red flag.)
- I received an email that only has **long hyperlinks with no further information** and the rest of the email is completely blank.
- I received an email with a **hyperlink that is a misspelling** of a known web site. For instance, www.bankofarnerica.com - the "m" is really two characters – "r & n")

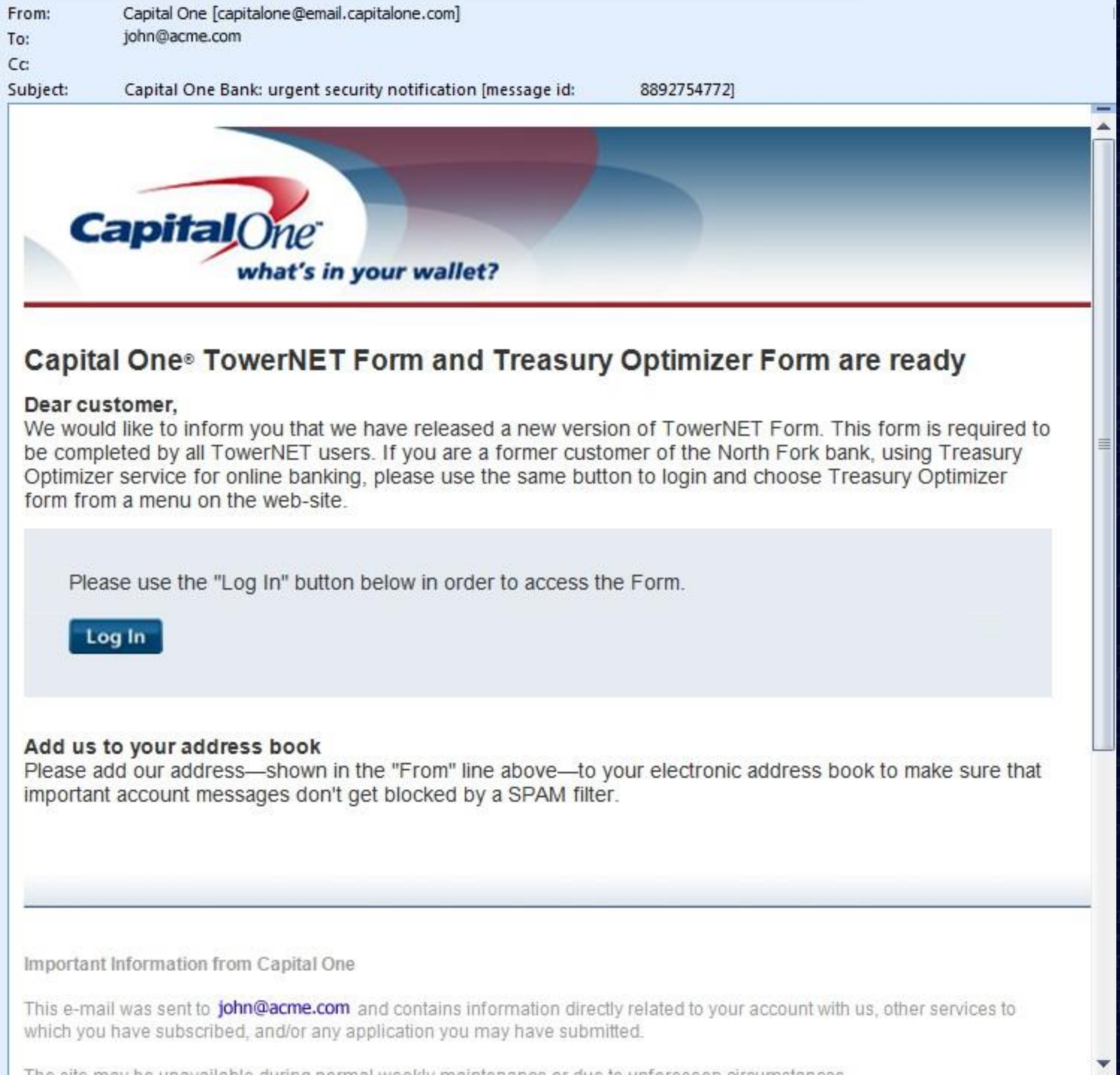
## CONTENT:

- Is the sender asking me to click on a link or open an attachment to **avoid a negative consequence**, or to **gain something of value**?
- Is the email **out of the ordinary**, or does it have **bad grammar** or **spelling errors**?
- Is the sender asking me to click a link or open up an attachment that **seems odd** or **illogical**?
- Do I have an **uncomfortable gut feeling** about the sender's request to open an attachment or click a link?
- Is the email asking me to look at a **compromising or embarrassing picture** of myself or someone I know?

## ATTACHMENTS:

- The sender included an email attachment that I **was not expecting** or that **makes no sense** in relation to the email message. (This sender doesn't ordinarily send me these types of attachment(s).)
- I see an attachment with a **possibly dangerous file type**. The only file type that is **always safe to click on is a .TXT** file.)

Source:
Knowbe4



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

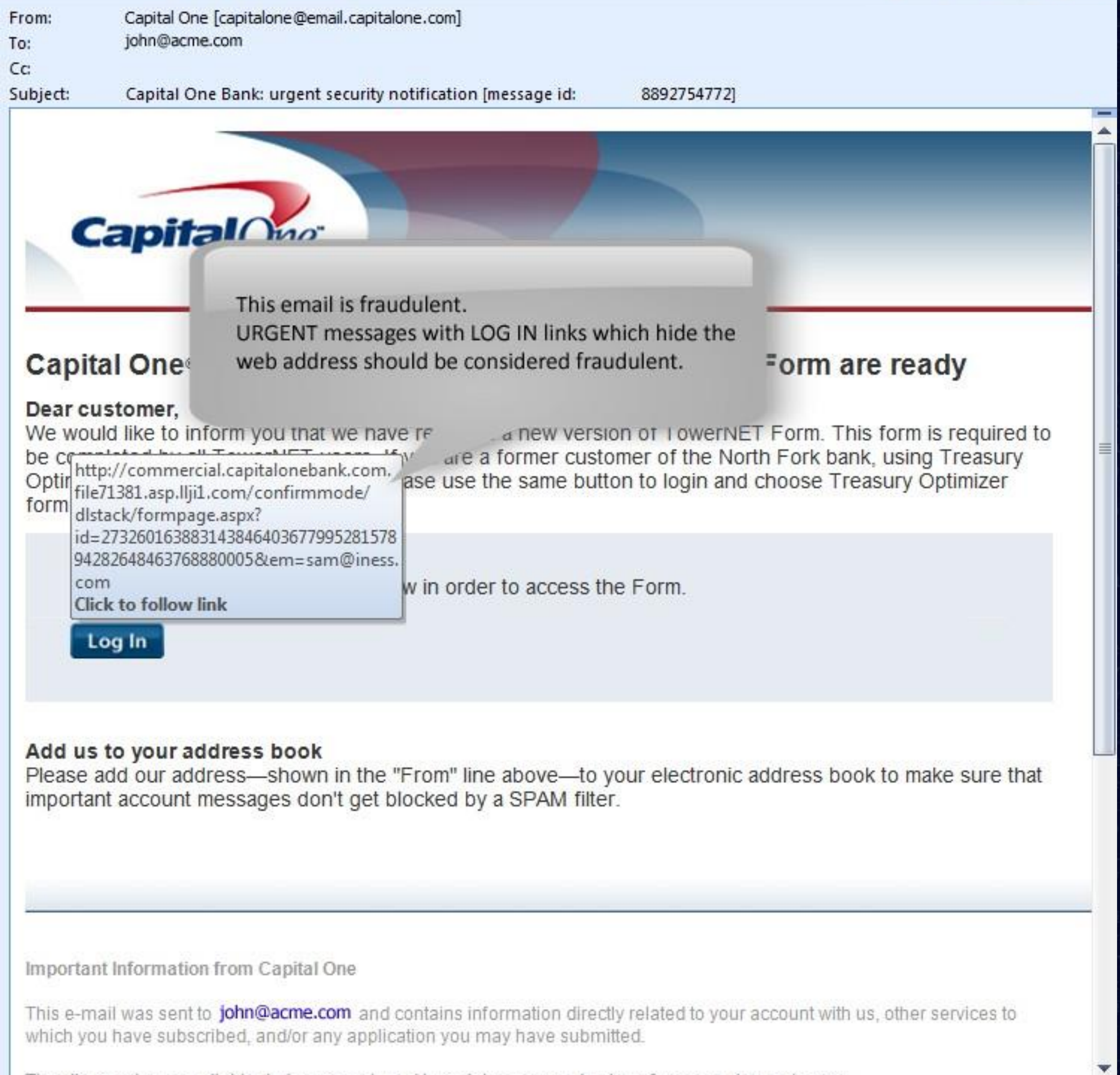
Please use the "Log In" button below in order to access the Form.

**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.



From: Capital One [capitalone@email.capitalone.com]
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 co are a former customer of the North Fork bank, using Treasury Opti ase use the same button to login and choose Treasury Optimizer form

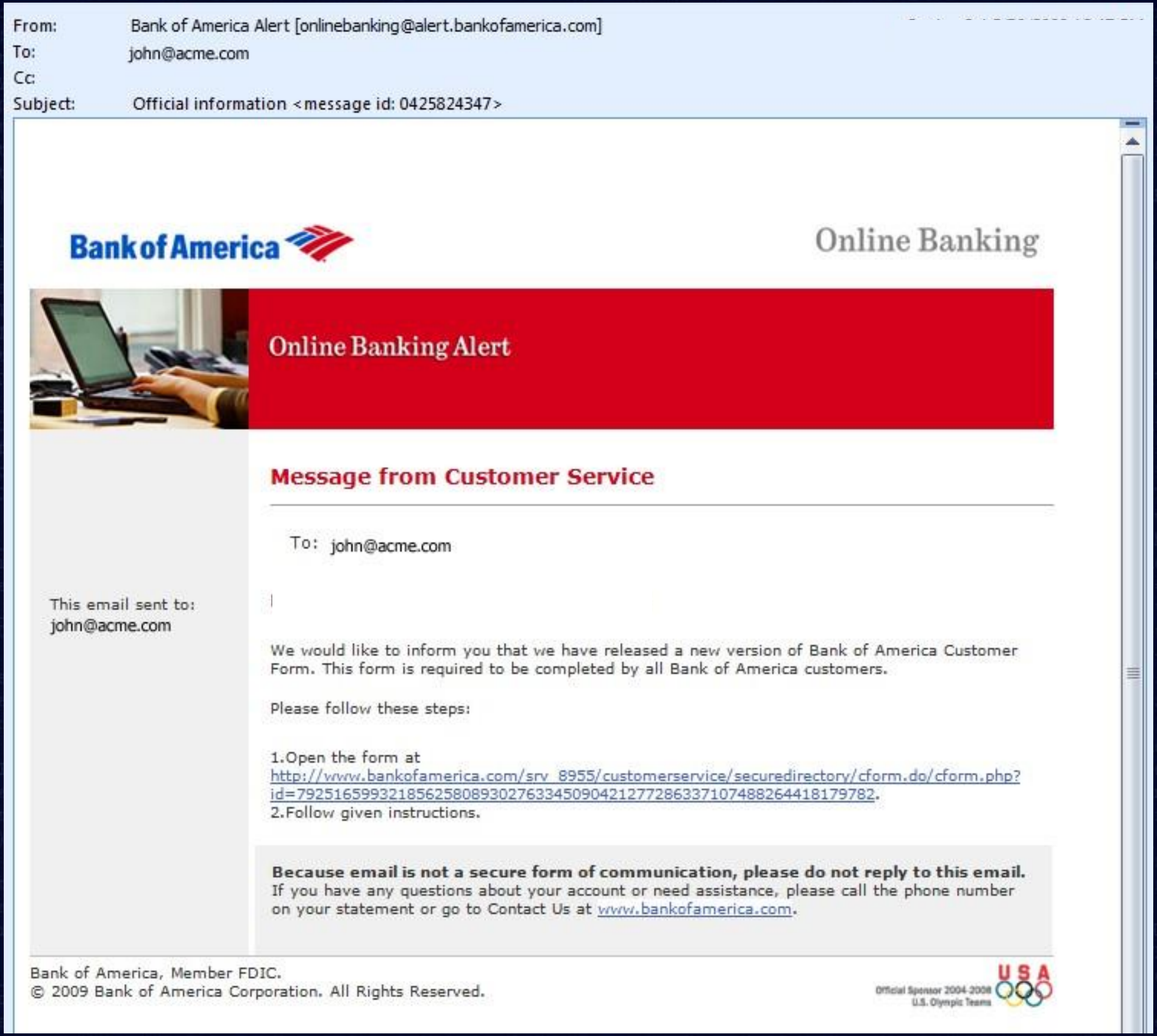
http://commercial.capitalonebank.com.file71381.asp.llji1.com/confirmmode/dlstack/formpage.aspx?id=2732601638831438464036779952815789428264846376888000 5&em=sam@iness.com
**Click to follow link**

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.



From: Bank of America Alert [onlinebanking@alert.bankofamerica.com]
To: john@acme.com
Cc:
Subject: Official information <message id: 0425824347>

Bank of America

Online Banking

## Online Banking Alert

### Message from Customer Service

To: john@acme.com

This email sent to:
john@acme.com

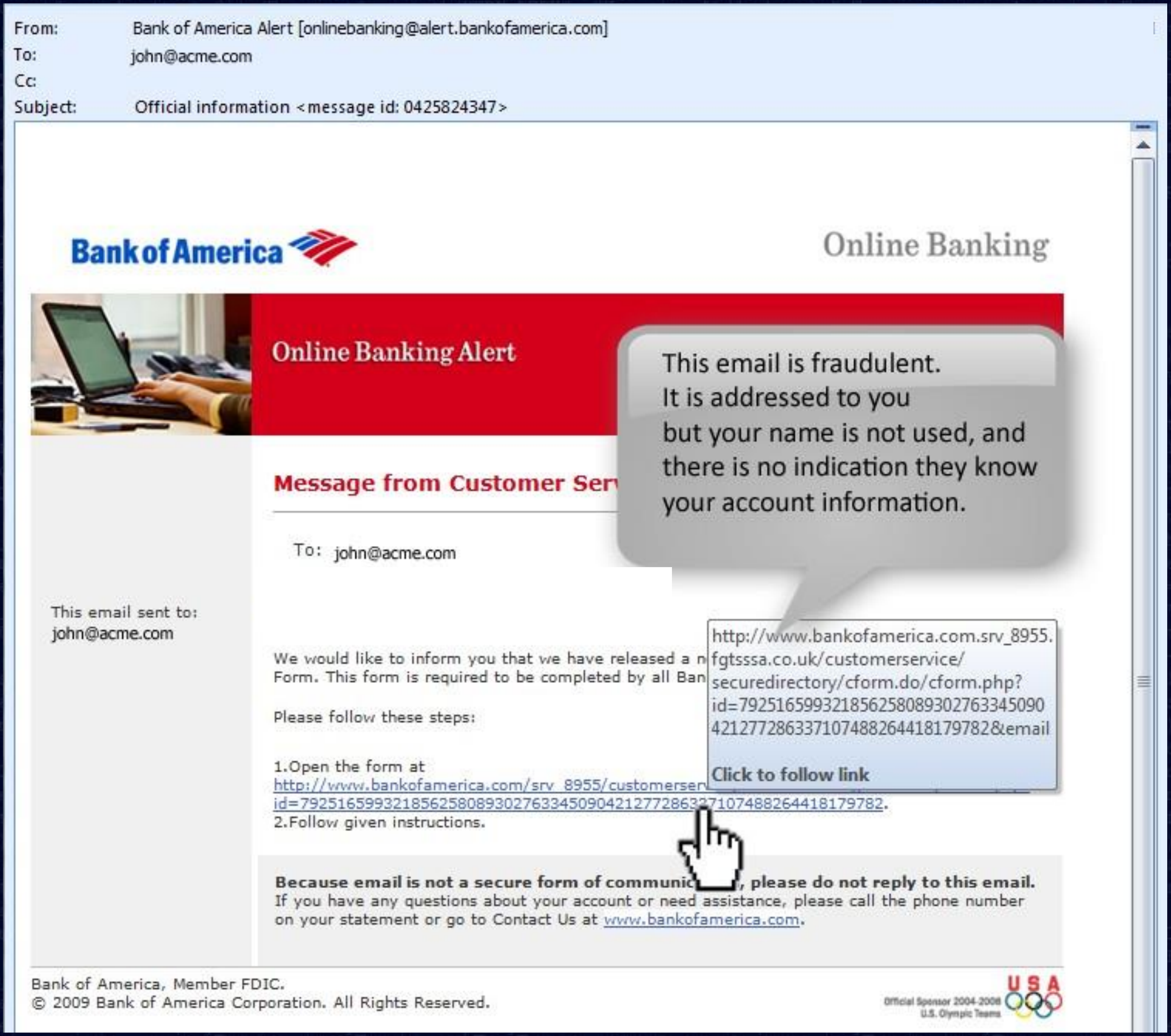
We would like to inform you that we have released a new version of Bank of America Customer Form. This form is required to be completed by all Bank of America customers.

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.



From: Bank of America Alert [onlinebanking@alert.bankofamerica.com]
To: john@acme.com
Cc:
Subject: Official information <message id: 0425824347>

Bank of America

Online Banking

Online Banking Alert

Message from Customer Ser

To: john@acme.com

This email sent to:
john@acme.com

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/customerser
id=792516599321856258089302763345090421277286337107488264418179782.
2.Follow given instructions.

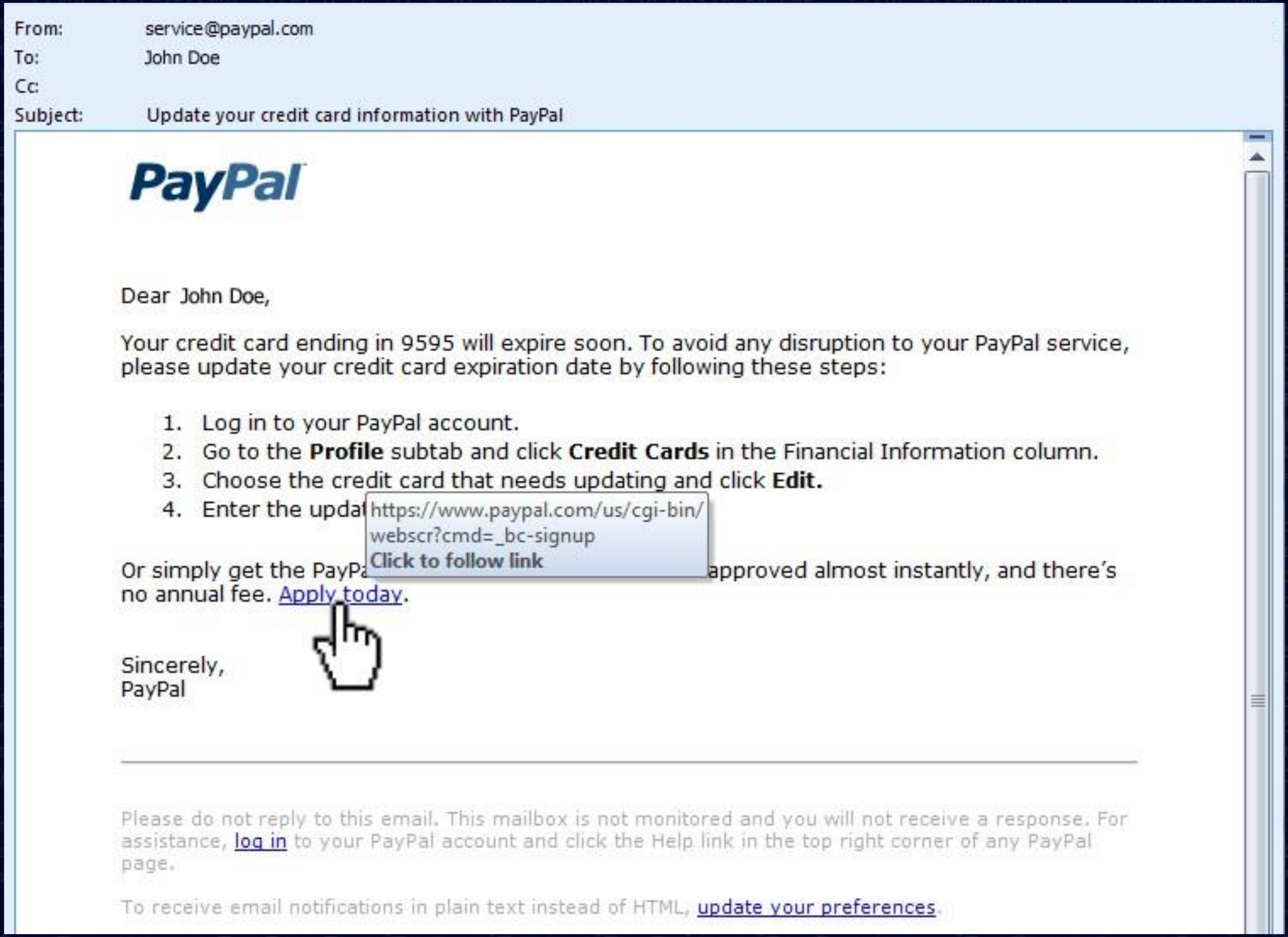
**Because email is not a secure form of communic , please do not reply to this email.**
If you have any questions about your account or need assistance, please call the phone number on your statement or go to Contact Us at www.bankofamerica.com.

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.



From: service@paypal.com
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

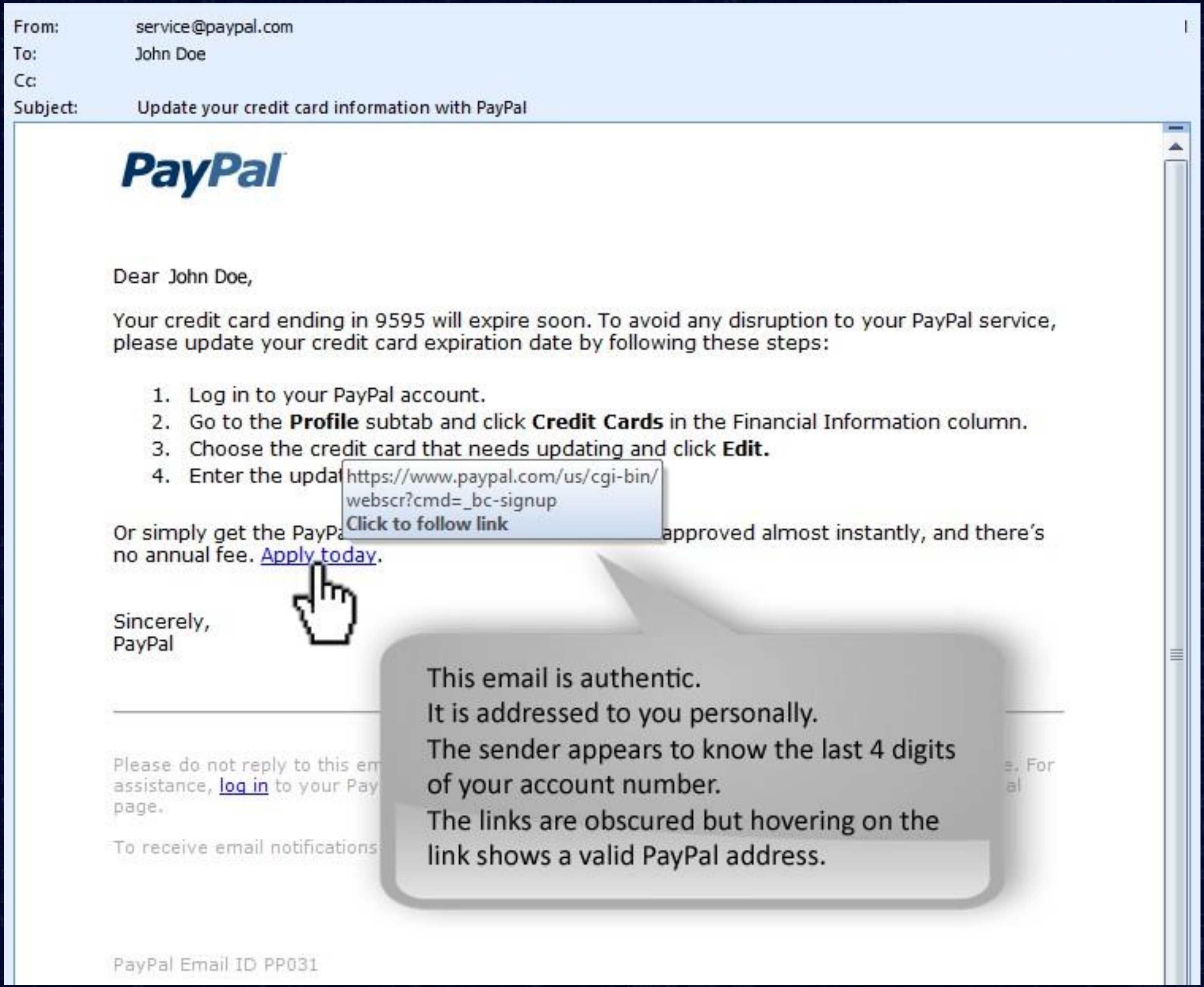
https://www.paypal.com/us/cgi-bin/webscr?cmd=_bc-signup
**Click to follow link**

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.



From: service@paypal.com

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.

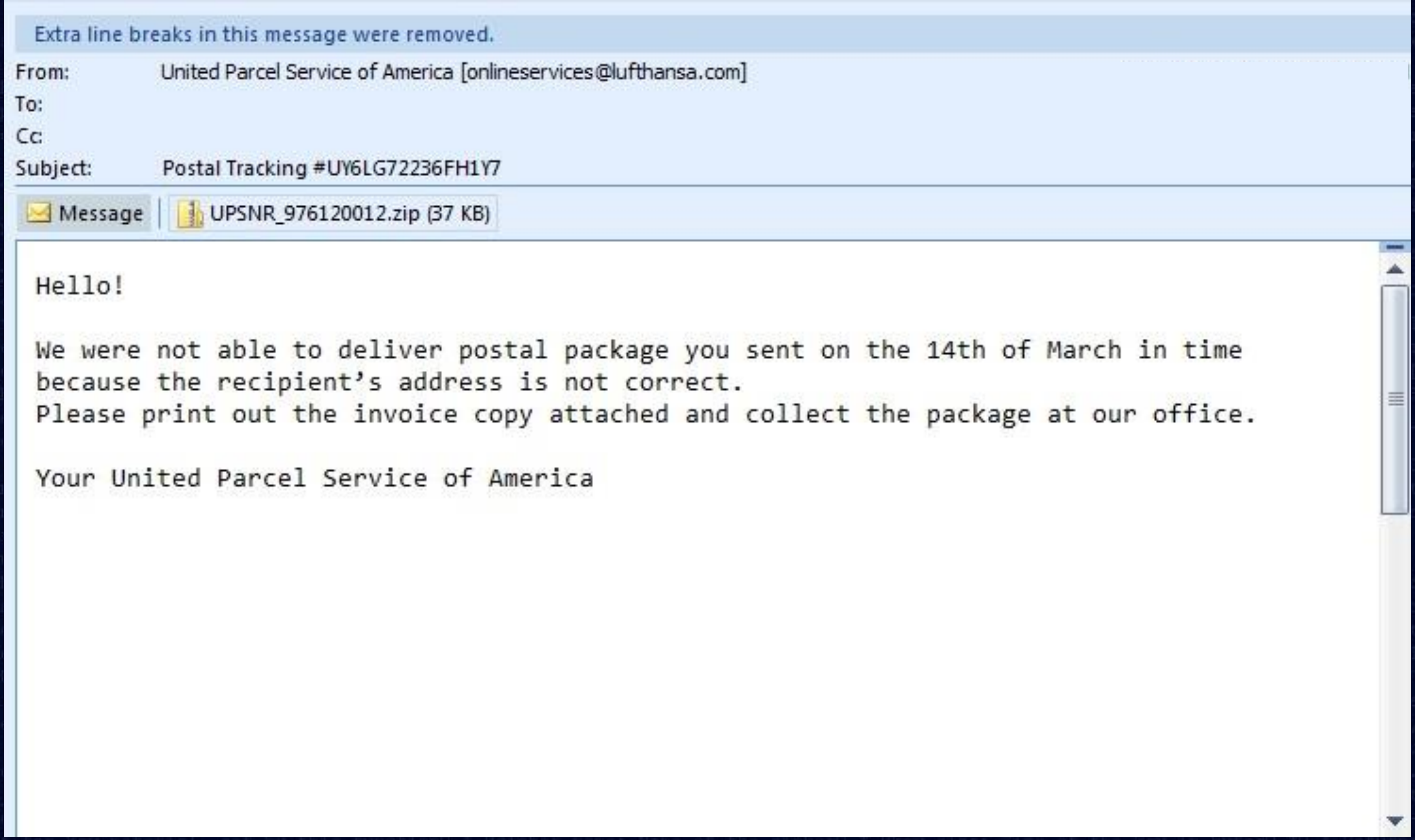
Sincerely,
PayPal

Please do not reply to this em . 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.



Extra line breaks in this message were removed.

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

To:

Cc:

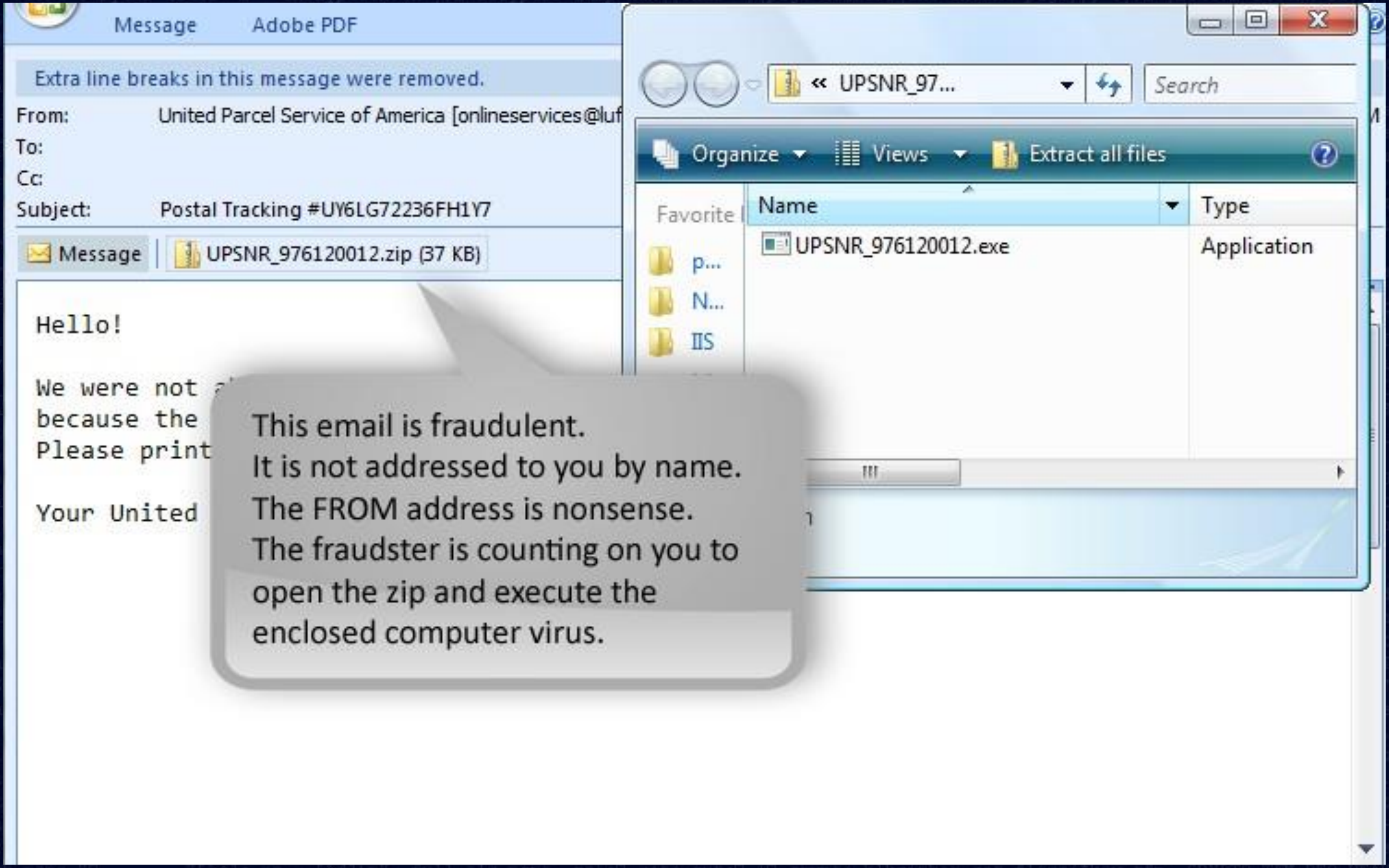
Subject: Postal Tracking #UY6LG72236FH1Y7

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



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)

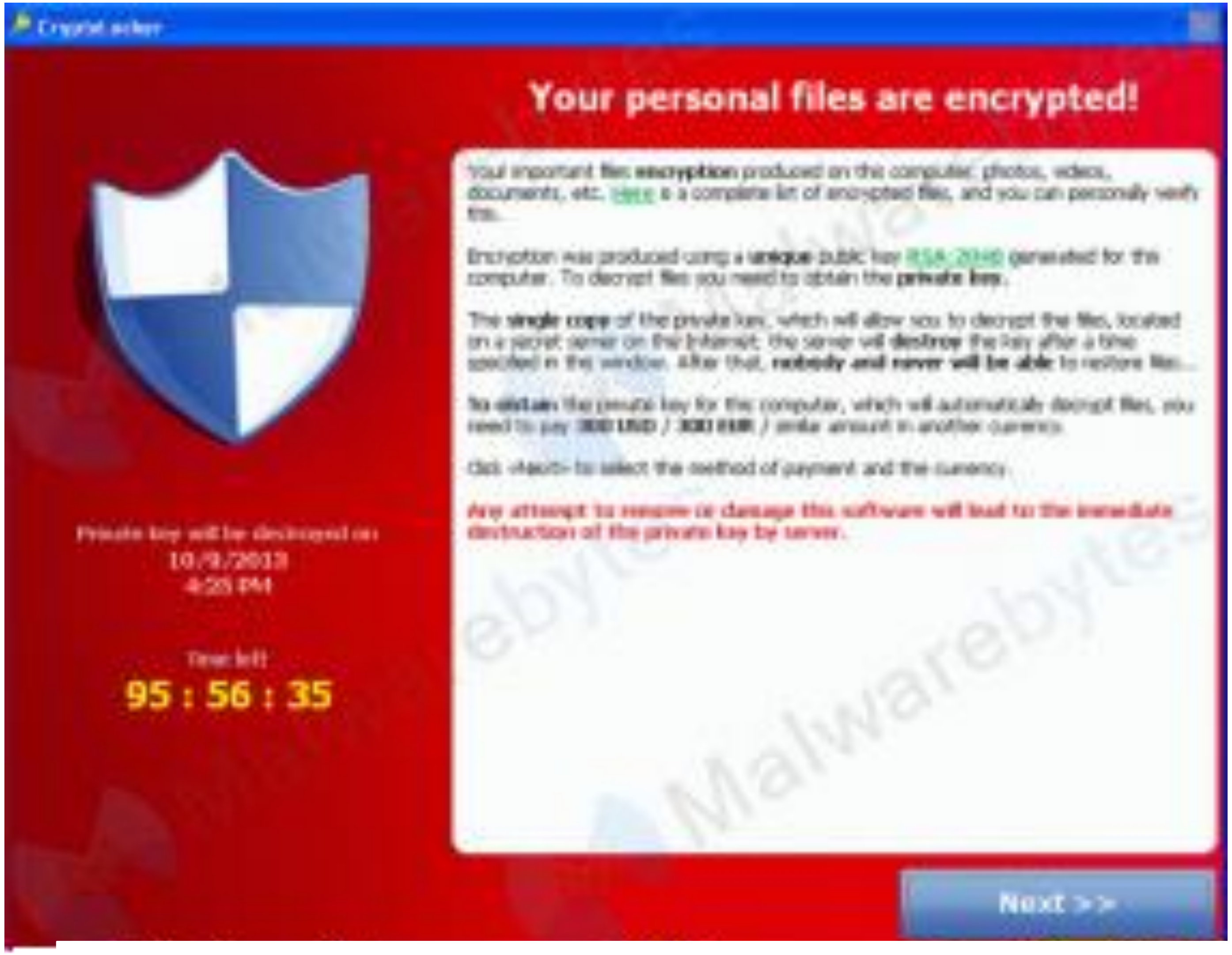
```
Hello!

We were not a
because the
Please print

Your United
```

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.

# Cryptolocker Case



**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.

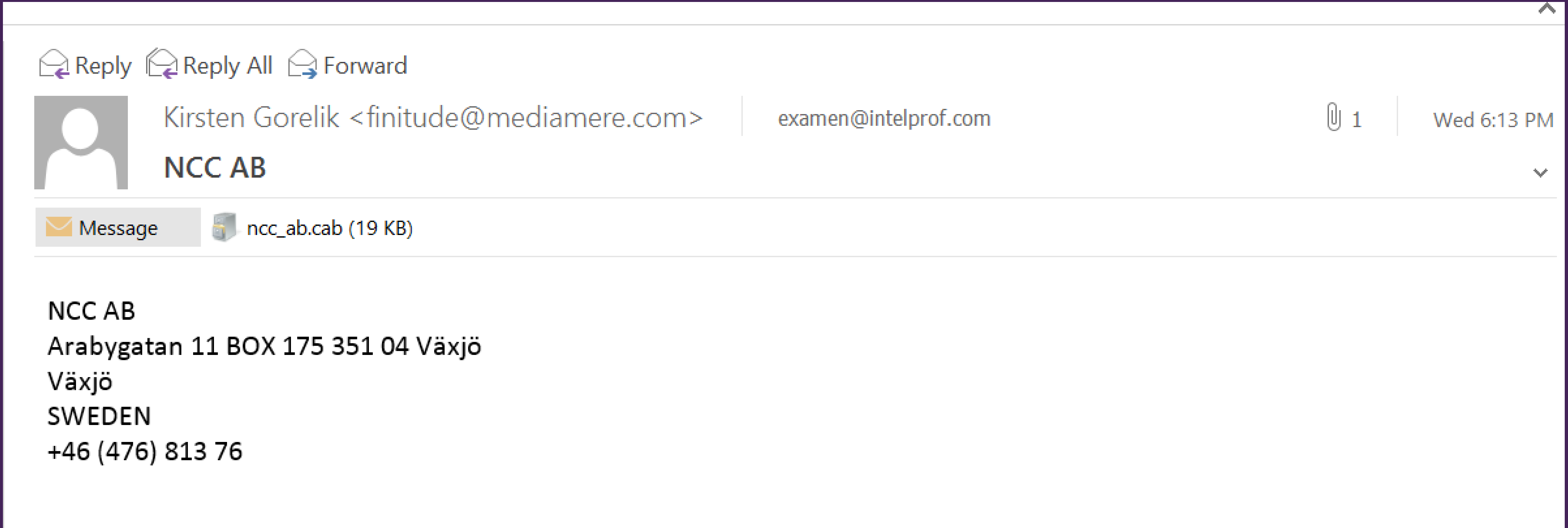
Any attempt to remove or damage this software will lead to the immediate destruction of the private key by server.

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

Time left
95 : 56 : 35

- Massachusetts police have admitted to paying a bitcoin ransom after being infected by the Cryptolocker ransomware.
- "(The virus) is so complicated and successful that you have to buy these bitcoins, which we had never heard of," Swansea Police Lt. Gregory Ryan talking to the Herald News.

# Sample Phishing Email w. Malware Attachment



Kirsten Gorelik <finitude@mediamere.com>

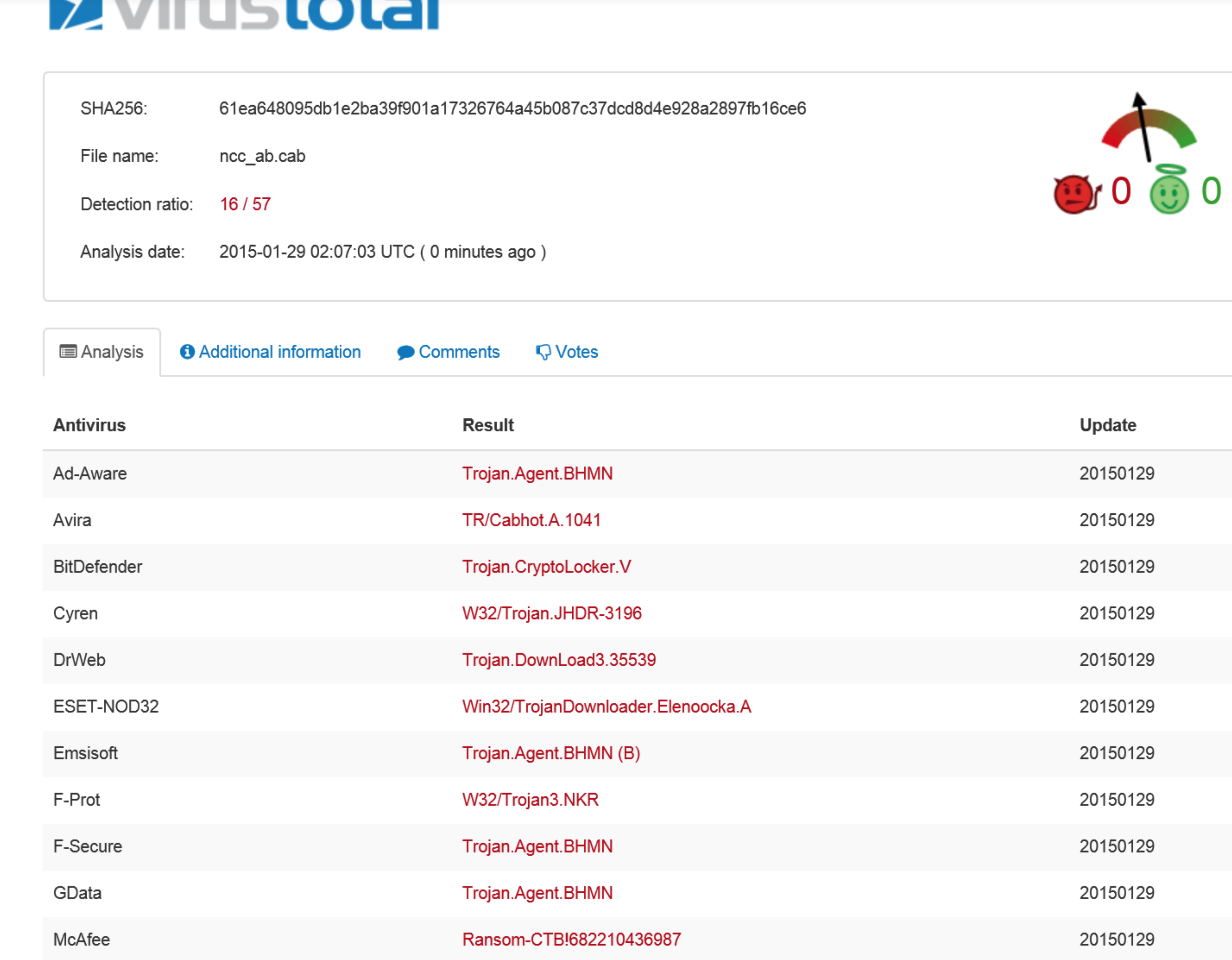
examen@intelprof.com

Wed 6:13 PM

NCC AB

ncc_ab.cab (19 KB)

NCC AB
Arabygatan 11 BOX 175 351 04 Växjö
Växjö
SWEDEN
+46 (476) 813 76



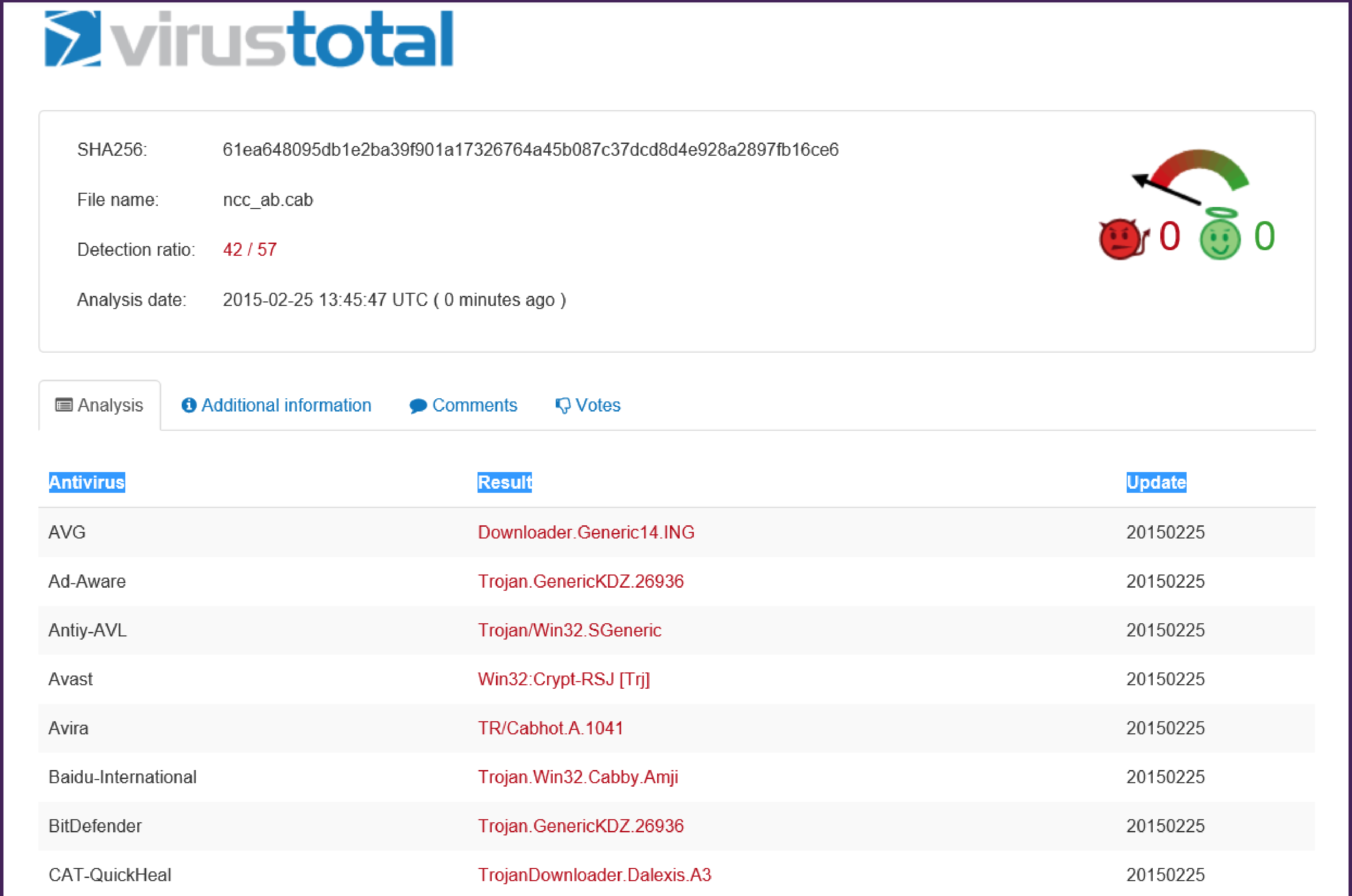
SHA256: 61ea648095db1e2ba39f901a17326764a45b087c37dcd8d4e928a2897fb16ce6

File name: ncc_ab.cab

Detection ratio: 16 / 57

Analysis date: 2015-01-29 02:07:03 UTC ( 0 minutes ago )

| Antivirus | Result | Update |
|---|---|---|
| Ad-Aware | Trojan.Agent.BHMN | 20150129 |
| Avira | TR/Cabhot.A.1041 | 20150129 |
| BitDefender | Trojan.CryptoLocker.V | 20150129 |
| Cyren | W32/Trojan.JHDR-3196 | 20150129 |
| DrWeb | Trojan.DownLoad3.35539 | 20150129 |
| ESET-NOD32 | Win32/TrojanDownloader.Elenoocka.A | 20150129 |
| Emsisoft | Trojan.Agent.BHMN (B) | 20150129 |
| F-Prot | W32/Trojan3.NKR | 20150129 |
| F-Secure | Trojan.Agent.BHMN | 20150129 |
| GData | Trojan.Agent.BHMN | 20150129 |
| McAfee | Ransom-CTB!682210436987 | 20150129 |



SHA256: 61ea648095db1e2ba39f901a17326764a45b087c37dcd8d4e928a2897fb16ce6

File name: ncc_ab.cab

Detection ratio: 42 / 57

Analysis date: 2015-02-25 13:45:47 UTC ( 0 minutes ago )

| Antivirus | Result | Update |
|---|---|---|
| AVG | Downloader.Generic14.ING | 20150225 |
| Ad-Aware | Trojan.GenericKDZ.26936 | 20150225 |
| Antiy-AVL | Trojan/Win32.SGeneric | 20150225 |
| Avast | Win32:Crypt-RSJ [Trj] | 20150225 |
| Avira | TR/Cabhot.A.1041 | 20150225 |
| Baidu-International | Trojan.Win32.Cabby.Amji | 20150225 |
| BitDefender | Trojan.GenericKDZ.26936 | 20150225 |
| CAT-QuickHeal | TrojanDownloader.Dalexis.A3 | 20150225 |

# Remember the mandatory steps to take before you become the next victim ☺

- Make sure you encrypt computers, hard drives, databases and all the data.
- Run and test frequent backups and disaster recovery plans.
- Manage the **BYOD** (Bring Your Own Device) dilemma
- Make sure you enforce better password management policies.
- Create and manage corporate security policies around the standards such as ISO 27001 or COBIT.
- Educate employees against social engineering and phishing attacks.

# Call To Action: In order to better protect your business data and assets, Start thinking like a hacker ☺ !

Questions?

gdobrea@xeduco.net

Xeduco

www.xeduco.net