The Evolving Cyber Threat

August 8, 2016

FTA Technology Conference

Pittsburg, PA

John Moynihan

President, Minuteman Governance @Jmoynihan_cyber

Background

- Founded firm in 2008
- Mass DOR – CISO (1997 – 2007)
- Internal Audit Director (1995 – 1997)

Today's Session

Interactive

Session Goals

- Alert you to escalating threats
- Discuss evolving methods and campaigns
- Provide practical mitigation strategy

Your Risk

- All sectors
- State Agencies and Municipalities
- Proceed as if attack is imminent

Current Environment

- Campaigns are dynamic and sophisticated

- Targeted and thoroughly

- Proactive risk mitigation essential

Uptick in Incidents

- Rogue file sharing
- Credential Theft
- Remote desktop compromise
- Unauthorized access

Targeting Users

Potential Adversaries

- **Internal** – Employees, privileged users, IT Vendors, Temporary Employees, Interns
- **External** – Ex-employees, cyber criminals, foreign governments
- **Radicalized Insiders –** IT staff “inspired” by extremist groups

Consequences

- Unauthorized access
- Ransom
- Disruption of essential operations
- Sabotage

Dilemma

Does this mean that you are defenseless?

Answer

YES…….

If you continue to rely on a technical approach.

Customized Malware

Malicious software that has been reengineered, altered or modified to evade security technologies

Top Targets

1.Healthcare

2. Retail

3. Education

4. Government/public sector

5. Financial Services

Reality

- Security technologies can’t detect

- Undetectable variants have proliferated

- “Signature - Based Detection” has failed

Signature Based Detection

- Anti-Virus detects only “known signatures”

- Many “new” variants escape detection

- 30-90 days to update security software

Dynamic

- 95% of variants disappear in 30 days
- 80% of variants are gone in a week
- Very dynamic situation

New Variants Annually

317,000,000

Target

- Malware within network October-December

- The detection rate was 0 %

- No AV detected it

ISight Partners

Sony

- Most destructive attack in US history
- Network compromised from September-December
- Undetectable variant

Tactics

Focus has shifted to “users”

Social Engineering

- The art of manipulating people into performing certain actions, such as executing links, attachments, videos, jpegs …….

- Employees must be cautioned

Inbound email

- Inbound email – most common delivery
- Phishing/Spear-Phishing
- Must educate workforce

Types

- E-card
- UPS, FedEx
- Banking scam
- Celebrity
- You’ve won a prize

Impulsiveness

- Adversaries rely on this trait
- Users need to act for attack to occur
- Employees need to be cautioned
- Take a deep breath – Prevent an attack

There is no “Silver Bullet”

- Multifaceted strategy required
- “Layers” of controls
- Technical and non-technical

Common Vulnerabilities

- Lack of workforce awareness
- Poor segmentation
- Inadequate monitoring

Measures to Mitigate Threat

1. Awareness

2. Containment

3. Detection

Layer 1

Prevention through workforce education

Educate Workforce

- Employees are malware catalysts

- Must explain risk - layman's terms

- Show them delivery methods

- Will prevent attacks

How?

- Acceptable-use policies
- Ongoing training
- Provide examples of overtures
- Accountability - Consequences

Suggested Policy Language

- “The opening of non-business links, attachments or executable programs, is prohibited. Opening a link or attachment may result in the installation of malicious software.”

- “Employees must exercise caution when receiving email from unknown, or non-business, sources. Although there may be a legitimate business purpose to open an email message from an unknown party, employees are prohibited from clicking on links, or opening attachments, contained therein.”

Actual Overture

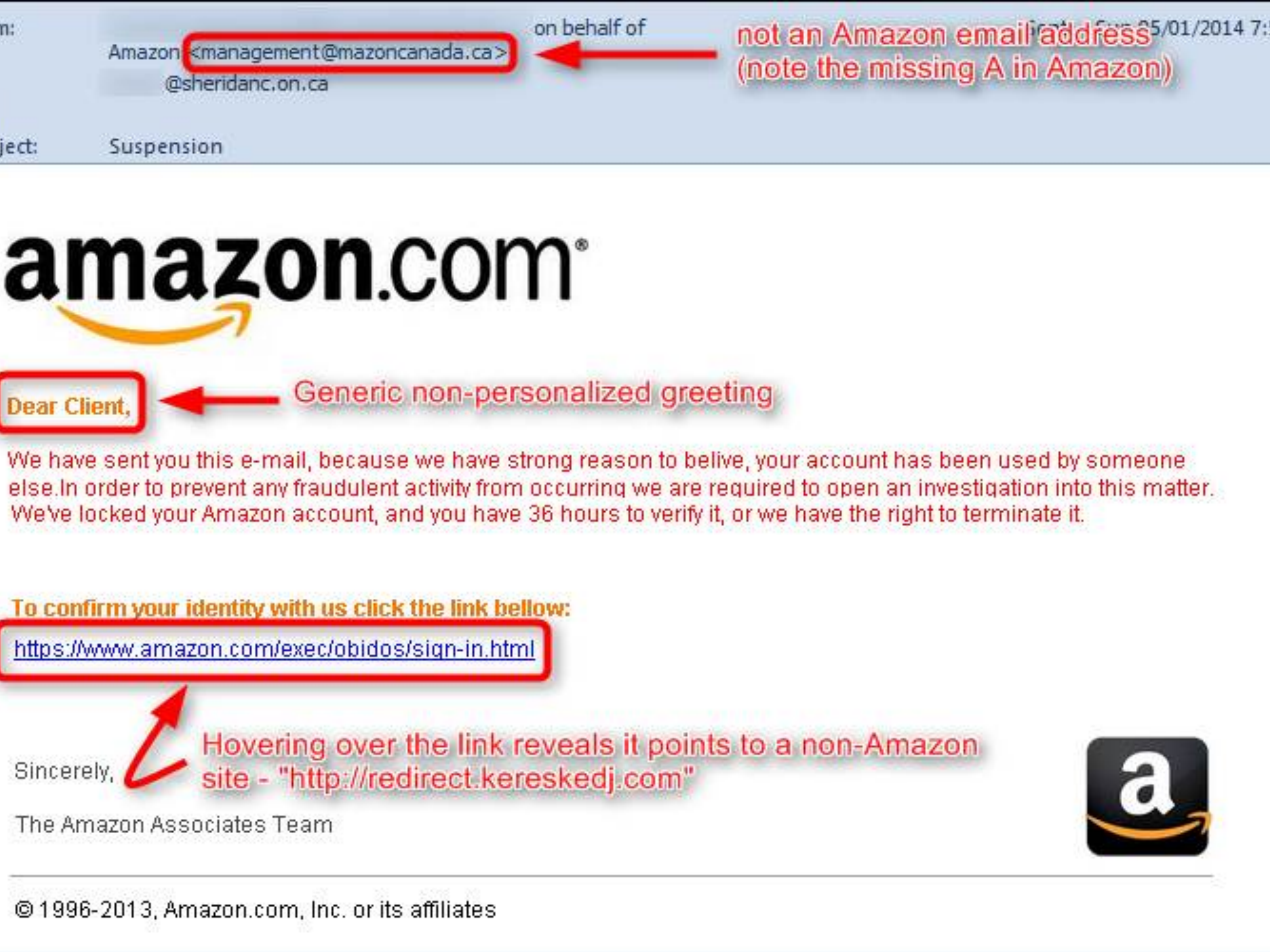
Hi Mike,

I noticed you at last week's meeting, but I didn't get a chance to speak with you. You sure are a popular member of the group… I have provided my email and would like to talk. Thanks!

Brittany

What Did Mike Do?

- Acted impulsively
- Clicked email address to respond
- Malware installed
- Significant disruption throughout company



m: [redacted] on behalf of Amazon <management@mazoncanada.ca> Sent: Sun 05/01/2014 7:

[redacted]@sheridanc.on.ca

ject: Suspension

not an Amazon email address (note the missing A in Amazon)

Dear Client,

Generic non-personalized greeting

We have sent you this e-mail, because we have strong reason to belive, your account has been used by someone else.In order to prevent any fraudulent activity from occurring we are required to open an investigation into this matter. We've locked your Amazon account, and you have 36 hours to verify it, or we have the right to terminate it.

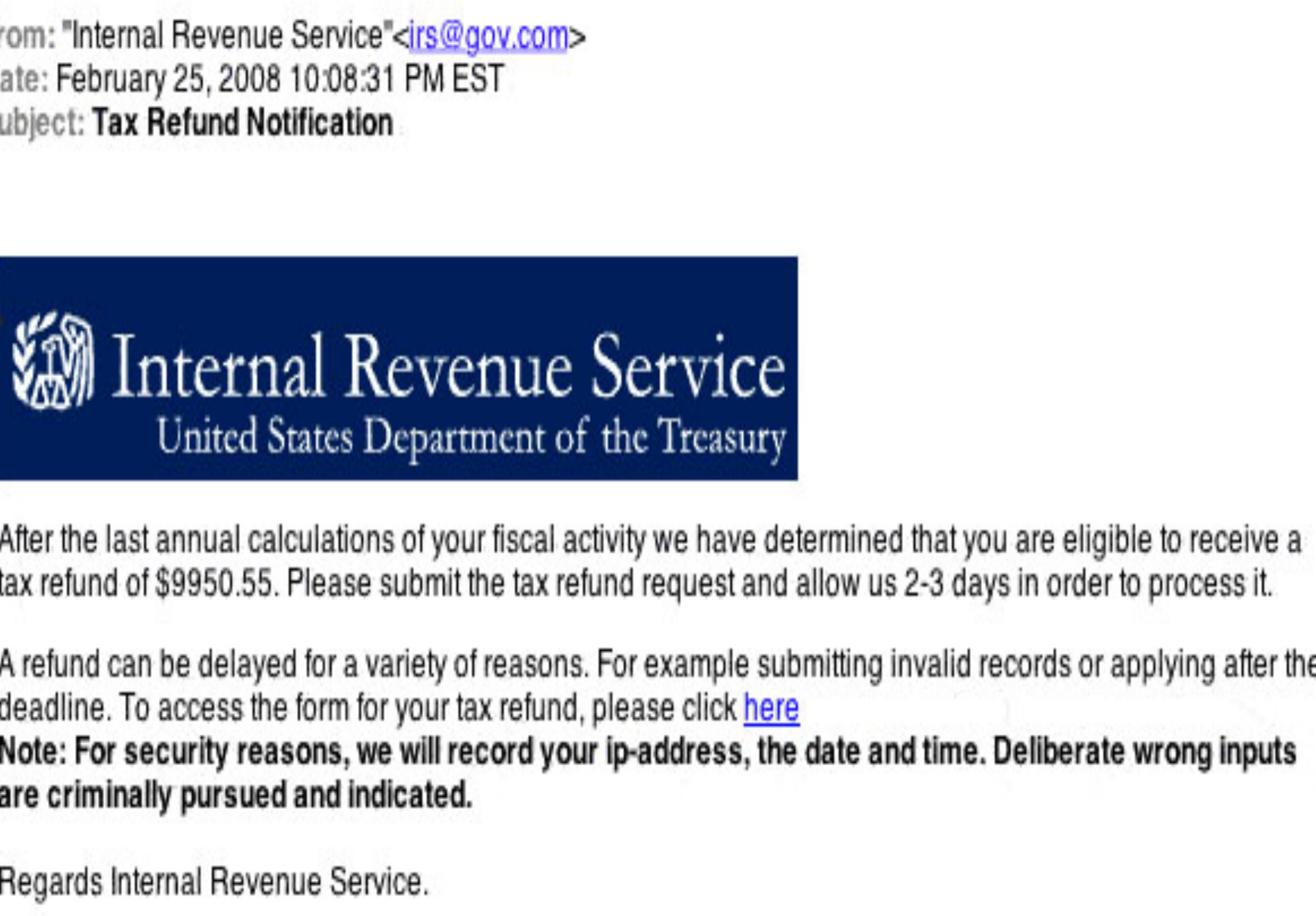
To confirm your identity with us click the link bellow:

https://www.amazon.com/exec/obidos/sign-in.html

Hovering over the link reveals it points to a non-Amazon site - "http://redirect.kereskedj.com"

Sincerely,

The Amazon Associates Team



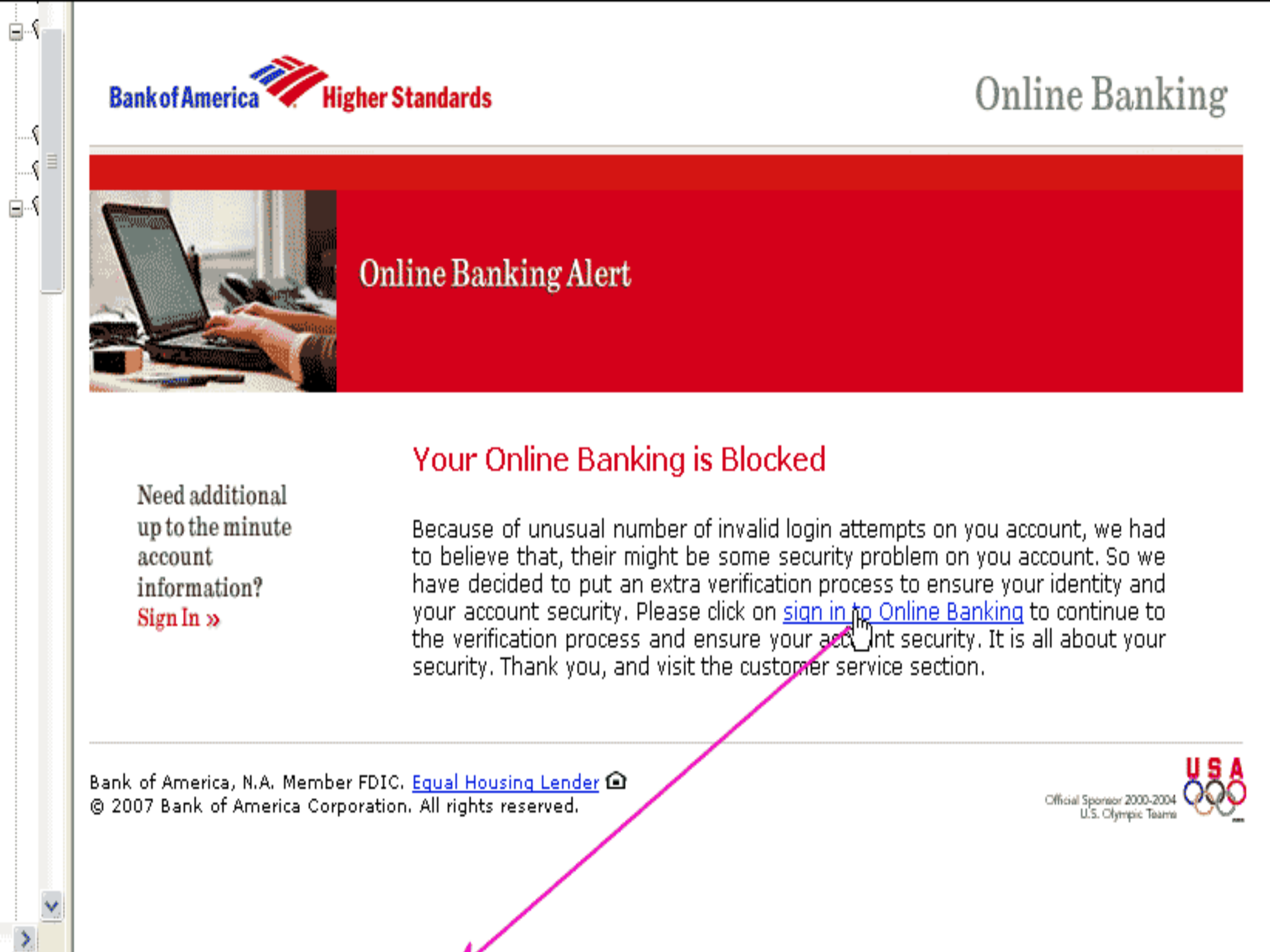
rom: "Internal Revenue Service"<irs@gov.com>
ate: February 25, 2008 10:08:31 PM EST
ubject: **Tax Refund Notification**

Internal Revenue Service
United States Department of the Treasury

After the last annual calculations of your fiscal activity we have determined that you are eligible to receive a tax refund of $9950.55. Please submit the tax refund request and allow us 2-3 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
Note: For security reasons, we will record your ip-address, the date and time. Deliberate wrong inputs are criminally pursued and indicated.

Regards Internal Revenue Service.



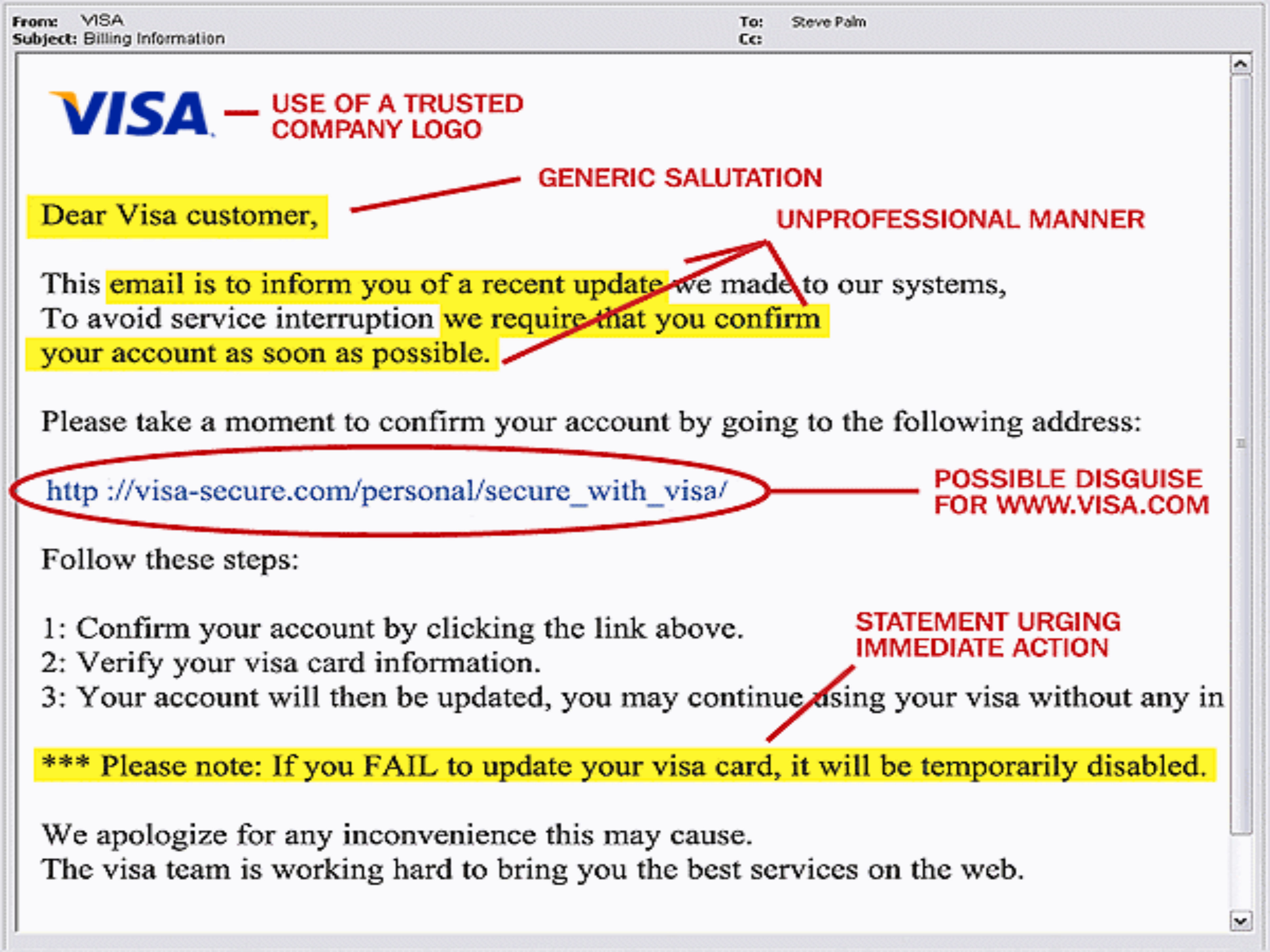
Online Banking Alert

Need additional up to the minute account information?
Sign In »

Your Online Banking is Blocked

Because of unusual number of invalid login attempts on you account, we had to believe that, their might be some security problem on you account. So we have decided to put an extra verification process to ensure your identity and your account security. Please click on sign in to Online Banking to continue to the verification process and ensure your account security. It is all about your security. Thank you, and visit the customer service section.

Bank of America, N.A. Member FDIC. Equal Housing Lender
© 2007 Bank of America Corporation. All rights reserved.



From: VISA
To: Steve Palm
Subject: Billing Information
Cc:

USE OF A TRUSTED COMPANY LOGO

GENERIC SALUTATION

Dear Visa customer,

UNPROFESSIONAL MANNER

This email is to inform you of a recent update we made to our systems,
To avoid service interruption we require that you confirm
your account as soon as possible.

Please take a moment to confirm your account by going to the following address:

http ://visa-secure.com/personal/secure_with_visa/

POSSIBLE DISGUISE FOR WWW.VISA.COM

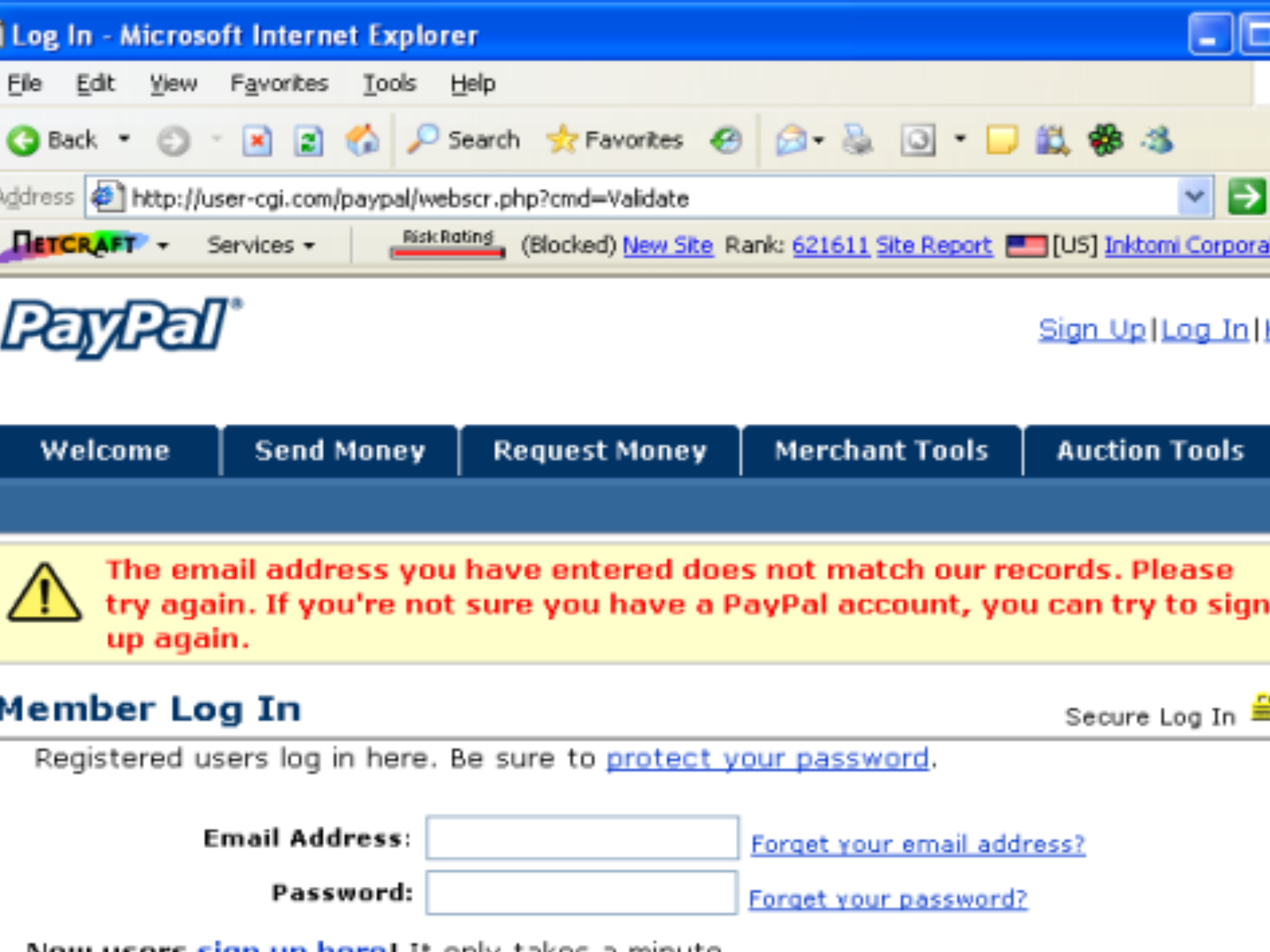
Follow these steps:

1: Confirm your account by clicking the link above.
2: Verify your visa card information.
3: Your account will then be updated, you may continue using your visa without any in

STATEMENT URGING IMMEDIATE ACTION

*** Please note: If you FAIL to update your visa card, it will be temporarily disabled.

We apologize for any inconvenience this may cause.
The visa team is working hard to bring you the best services on the web.



Address http://user-cgi.com/paypal/webscr.php?cmd=Validate

(Blocked) New Site Rank: 621611 Site Report [US] Inktomi Corpora

The email address you have entered does not match our records. Please try again. If you're not sure you have a PayPal account, you can try to sign up again.

Member Log In

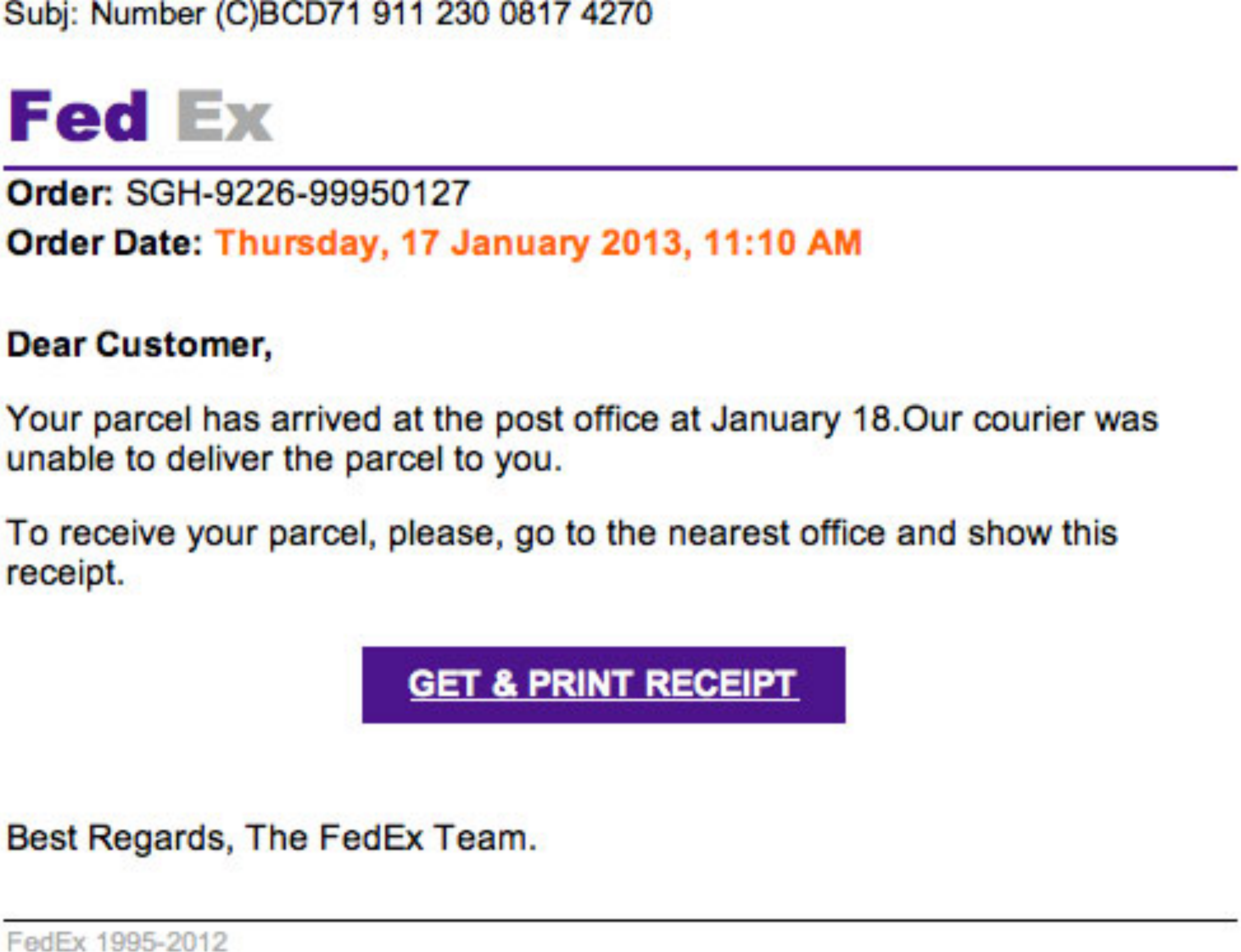
Secure Log In

Registered users log in here. Be sure to protect your password.

Email Address: Forget your email address?

Password: Forget your password?

New users sign up here! It only takes a minute.



Subj: Number (C)BCD71 911 230 0817 4270

Fed Ex

Order: SGH-9226-99950127

Order Date: **Thursday, 17 January 2013, 11:10 AM**

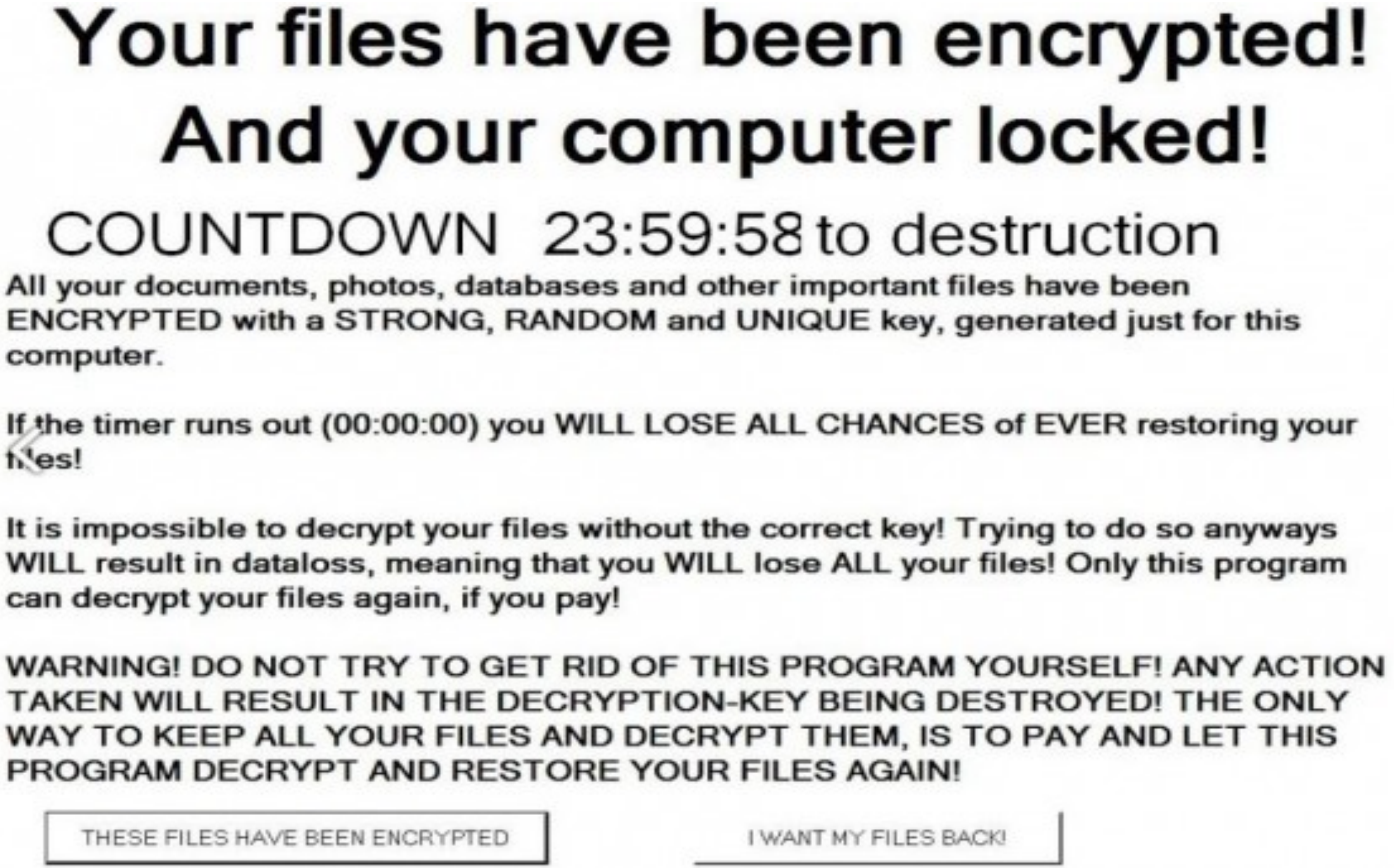
Dear Customer,

Your parcel has arrived at the post office at January 18.Our courier was unable to deliver the parcel to you.

To receive your parcel, please, go to the nearest office and show this receipt.

Best Regards, The FedEx Team.

FedEx 1995-2012



Your files have been encrypted! And your computer locked!

COUNTDOWN 23:59:58 to destruction

All your documents, photos, databases and other important files have been ENCRYPTED with a STRONG, RANDOM and UNIQUE key, generated just for this computer.

If the timer runs out (00:00:00) you WILL LOSE ALL CHANCES of EVER restoring your files!

It is impossible to decrypt your files without the correct key! Trying to do so anyways WILL result in dataloss, meaning that you WILL lose ALL your files! Only this program can decrypt your files again, if you pay!

WARNING! DO NOT TRY TO GET RID OF THIS PROGRAM YOURSELF! ANY ACTION TAKEN WILL RESULT IN THE DECRYPTION-KEY BEING DESTROYED! THE ONLY WAY TO KEEP ALL YOUR FILES AND DECRYPT THEM, IS TO PAY AND LET THIS PROGRAM DECRYPT AND RESTORE YOUR FILES AGAIN!

Employer Negligence

- No training provided on this risk
- Employee was unequipped

Layer 2

Containment through network segmentation

Reality

Network Intrusions Happen

Containment is Critical

- Must contain threat
- Must avoid a "flat network"
- Isolate critical data – tax databases
- Protect outward facing applications

Limit Network Access

- Configure network to limit access
- Prevent lateral movement
- Protect databases with tax data

Target

- Tested network post breach
- Navigated from deli scale to POS
- Example of open network

Layer 3

Identification Through Monitoring

Prioritize

- Identify critical assets and technologies
- Tax data
- Employee information

Monitor

- Exports/transmission of data
- Unusual ports and services
- Access from unknown hosts
- Any network anomalies

Identify

- Generate automated alerts
- Immediately verify activity
- Will identify intrusions

Disrupt Attack

Intervene and Eradicate

What will you do?

- You occupy a unique role
- Your members are at risk
- What will you do?

Questions and Discussion

John Moynihan

John@minutemangovernance.com
minutemangovernance.com
(617) 645-4422