Spam & Phishing

Aggelos Kiayias

What is Spam?

What is the relation?

- The Spam Sketch in Monty Python’s Flying Circus, 1970

Word Filtering

- Simple filtering: example: “if an e-mail contains the strings *offer* and *!!!!* it is spam.”
- Advantages: very simple to configure.
- Disadvantages: can be circumvented relatively easily. may kill useful messages.

Rule based Scoring

- Direct extension of word filtering.
  - Each e-mail has a score that starts at 0.
  - Inclusion of "*spam related words*" add to the score of the e-mail.
  - If the score exceeds a threshold then the e-mail is classified as spam.
- Advantage: can be calibrated according to user; catches spam better than word-filtering.

spamassasin

Black/White-listings

Black-listing:
reject all e-mails
from this list

Problem:
spammers change e-mails rapidly; catches only small amount of spam

a@a.com
b@b.com
c@c.com
d@d.com

...

White-listing:
accept all e-mails
from this list

Problem:
receiving e-mail from people you don’t know!

a@a.com
b@b.com
c@c.com
d@d.com

...

Possible way-out:
ask for e-mail verification

Example: Active Spam Killer   http://a-s-k.sourceforge.net/

Bayesian Filtering

- More sophisticated than rule-based scoring.
- More easy to configure.
- Can be tuned to a specific users' e-mail traffic.

bogofilter

http://bogofilter.sourceforge.net/

also incorporated into
Thunderbird, Mac-OS, Windows etc.

Bayesian Spam Filtering

Message is treated as a set of words

$$\text{email} = \{w_1, \ldots, w_N\}$$

Message is classified as spam if the "SPAM" probability given the words of the e-mail exceeds a threshold.

$$\mathbf{Prob}[\text{SPAM} \mid w_1, w_2, \ldots w_N] \geq \text{threshold}$$

Computing SPAM Probability

$$\mathbf{Prob}[\mathrm{SPAM} \mid w_1, w_2, \ldots w_N] =$$

$$\frac{\mathbf{Prob}[w_1, w_2, \ldots, w_N \mid \mathrm{SPAM}] \cdot \mathbf{Prob}[\mathrm{SPAM}]}{\mathbf{Prob}[w_1, w_2, \ldots, w_N]}$$

$$= \frac{\mathbf{Prob}[\mathrm{SPAM}] \cdot \prod_{i=1}^{n} \mathbf{Prob}[w_i \mid \mathrm{SPAM}]}{\prod_{i=1}^{n} \mathbf{Prob}[w_i]}$$

independence assumption

$$= \frac{\mathbf{Prob}[\mathrm{SPAM}] \cdot \prod_{i=1}^{n} \overline{\mathbf{Prob}[w_i \mid \mathrm{SPAM}]}}{\prod_{i=1}^{n}(\mathbf{Prob}[w_i|\mathrm{SPAM}] \cdot \mathbf{Prob}[\mathrm{SPAM}] + \underline{\mathbf{Prob}[w_i|\neg\mathrm{SPAM}]} \cdot \mathbf{Prob}[\neg\mathrm{SPAM}]}$$

Training

Estimation of Probabilities

$\mathbf{Prob}[w \mid \mathrm{SPAM}]$	probability word appears in a SPAM
$\mathbf{Prob}[w \mid \neg\mathrm{SPAM}]$	probability word appears in a non-SPAM message

Training can be achieved by using test-data, interactively etc.

Example

E-mail contains
viagra
funny
jason

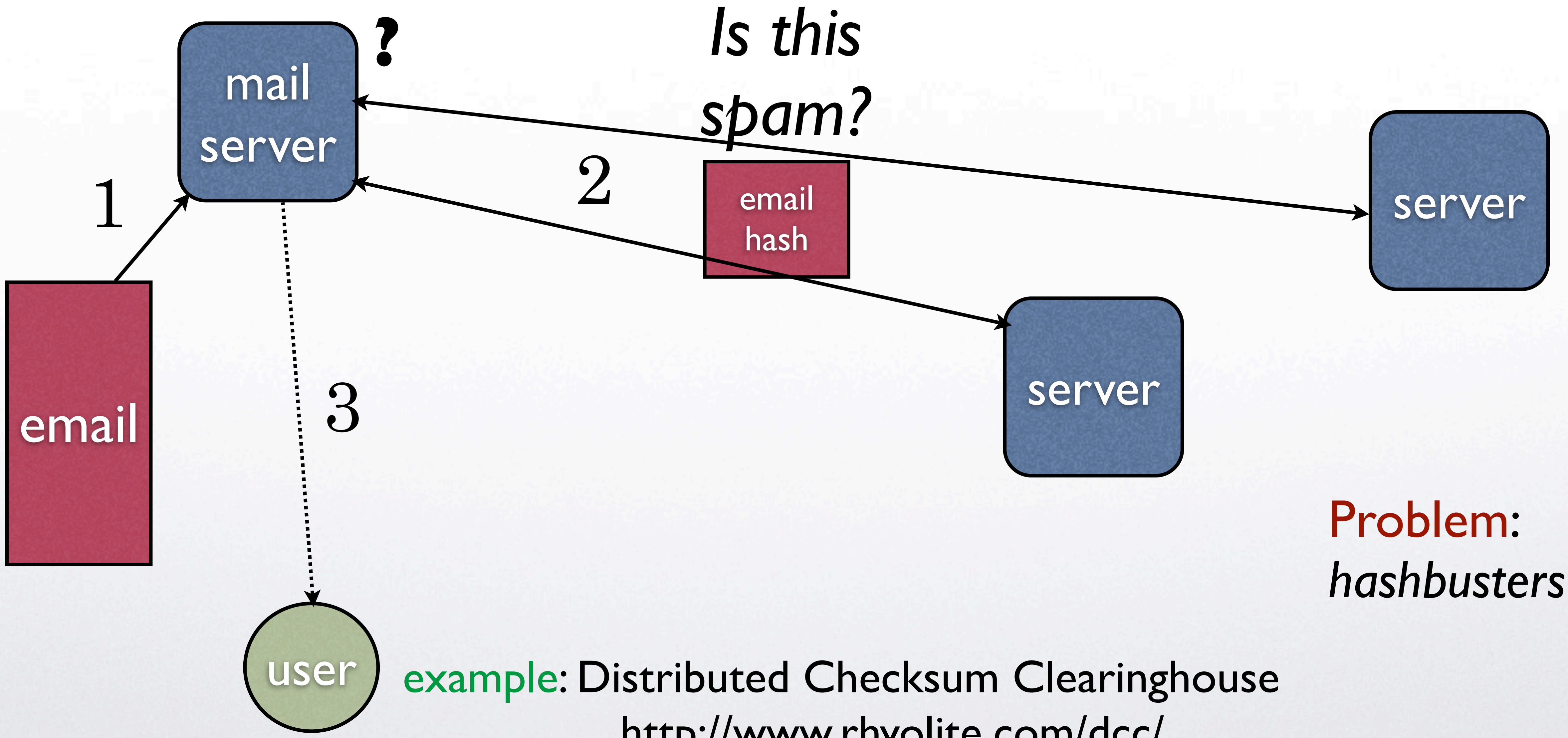
Training:

Prob[viagra | SPAM] = 0.81
Prob[funny | SPAM] = 0.62
Prob[jason | SPAM] = 0.25
Prob[viagra | ¬ SPAM] = 0.10
Prob[funny | ¬ SPAM] = 0.43
Prob[jason | ¬ SPAM] = 0.80

$$\frac{0.3 \cdot 0.81 \cdot 0.62 \cdot 0.25}{(0.81 \cdot 0.3 + 0.1 \cdot 0.7)(0.62 \cdot 0.3 + 0.43 \cdot 0.7)(0.25 \cdot 0.3 + 0.80 \cdot 0.7)} = 38.9\%$$

Without "jason" $$\frac{0.3 \cdot 0.81 \cdot 0.62}{(0.81 \cdot 0.3 + 0.1 \cdot 0.7)(0.62 \cdot 0.3 + 0.43 \cdot 0.7)} = 98.8\%$$

Hash-based Identification



Problem: *hashbusters*

example: Distributed Checksum Clearinghouse
http://www.rhyolite.com/dcc/

Cost-Based

- Sending e-mails is too cheap!
  - Solution 1: pay for e-mails with electronic coins. *Will make it too costly to send spam.*
  - Solution 2: in order to send an e-mail do some work (e.g., solve a puzzle). *Will require too much computational effort to send spam.*

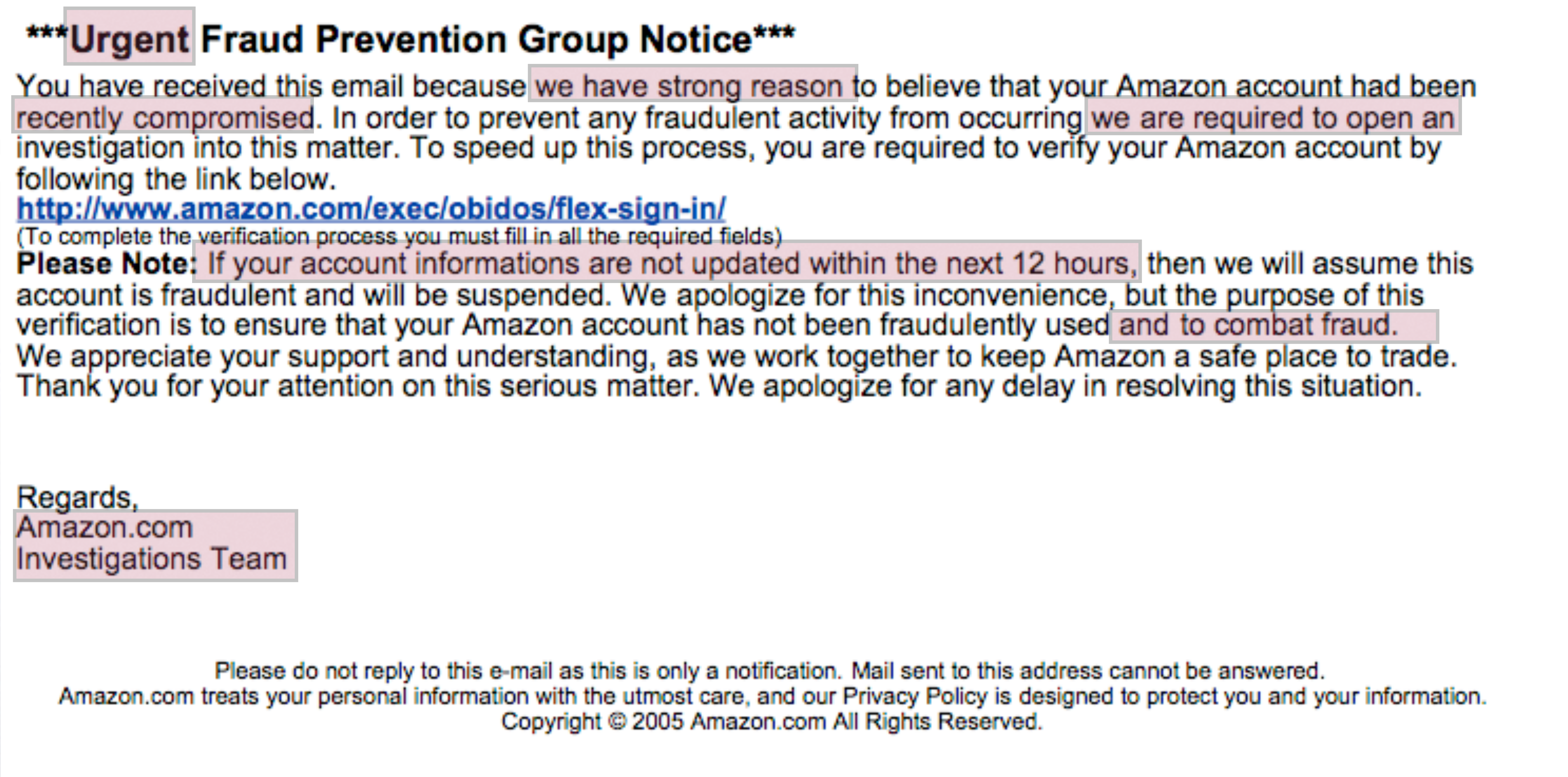
Phishing

- “Phish” personal information out of users.
- Typically uses spam as a lure to get a user hooked up.
- The next level of *social engineering*.
- Projected damages > $1,000,000,000

source http://www.gartner.com/5_about/press_releases/asset_71087_11.jsp

Phishing Example

emphasis added



*****Urgent Fraud Prevention Group Notice*****

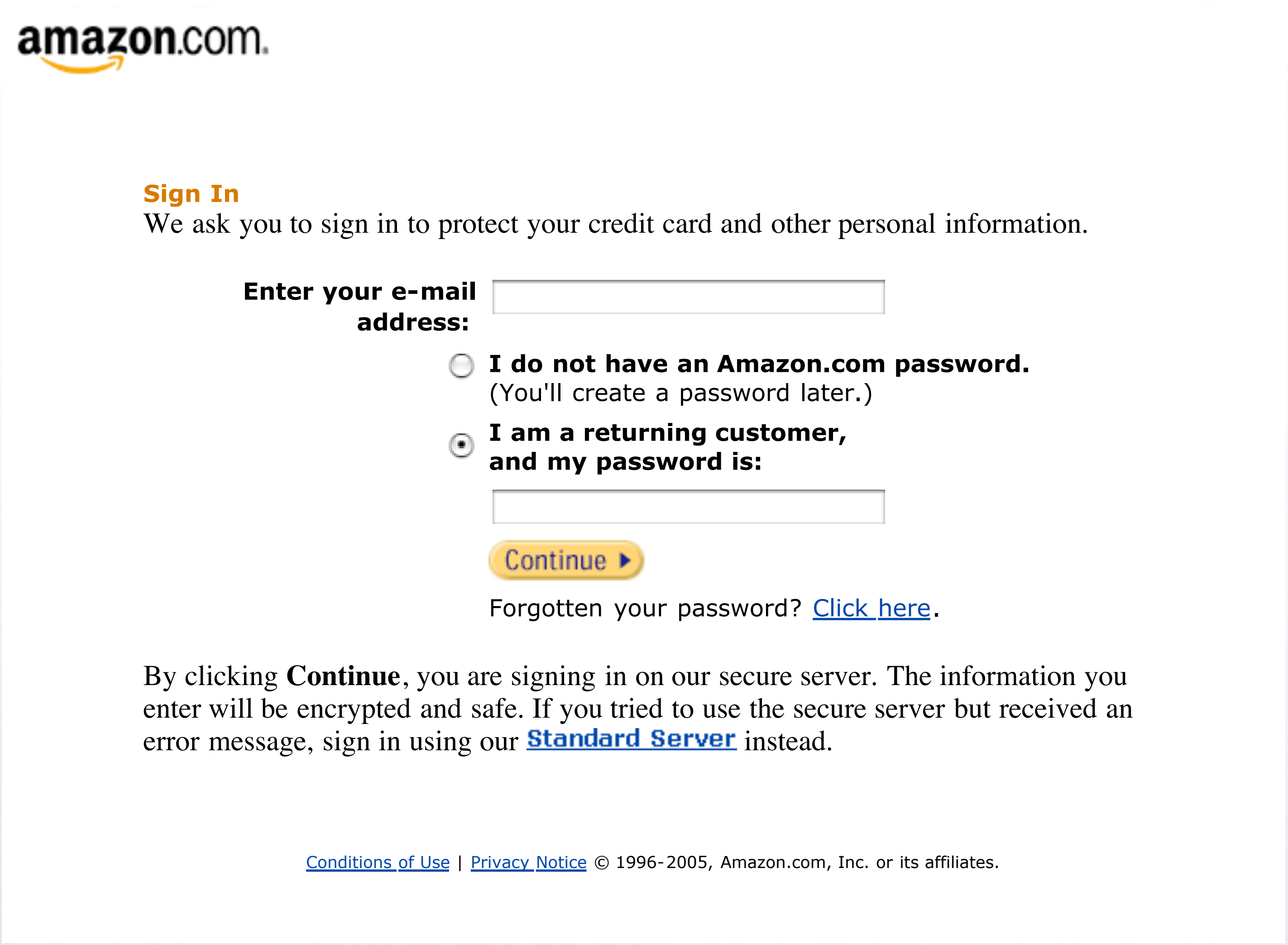
You have received this email because we have strong reason to believe that your Amazon account had been recently compromised. In order to prevent any fraudulent activity from occurring we are required to open an investigation into this matter. To speed up this process, you are required to verify your Amazon account by following the link below.
http://www.amazon.com/exec/obidos/flex-sign-in/
(To complete the verification process you must fill in all the required fields)
Please Note: If your account informations are not updated within the next 12 hours, then we will assume this account is fraudulent and will be suspended. We apologize for this inconvenience, but the purpose of this verification is to ensure that your Amazon account has not been fraudulently used and to combat fraud.
We appreciate your support and understanding, as we work together to keep Amazon a safe place to trade.
Thank you for your attention on this serious matter. We apologize for any delay in resolving this situation.

Regards,
Amazon.com
Investigations Team

Please do not reply to this e-mail as this is only a notification. Mail sent to this address cannot be answered.
Amazon.com treats your personal information with the utmost care, and our Privacy Policy is designed to protect you and your information.
Copyright © 2005 Amazon.com All Rights Reserved.

Phishing Example

http://202.85.152.20/.www.amazon.com/amaz/index.html



amazon.com

Sign In
We ask you to sign in to protect your credit card and other personal information.

Enter your e-mail address:

○ **I do not have an Amazon.com password.**
(You'll create a password later.)

● **I am a returning customer, and my password is:**

Continue ▸

Forgotten your password? Click here.

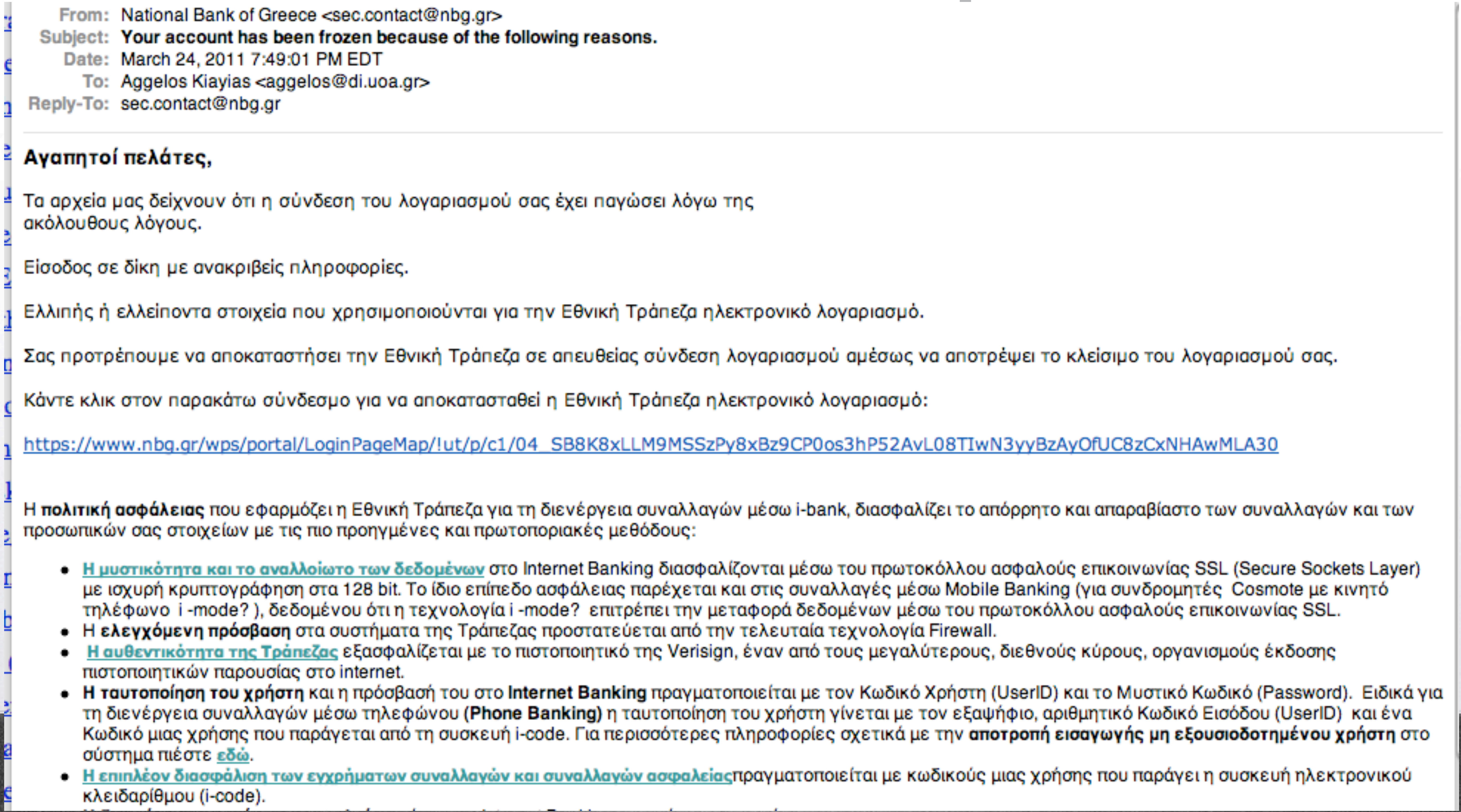
By clicking **Continue**, you are signing in on our secure server. The information you enter will be encrypted and safe. If you tried to use the secure server but received an error message, sign in using our **Standard Server** instead.

Conditions of Use | Privacy Notice © 1996-2005, Amazon.com, Inc. or its affiliates.

Phishing archive for more

http://www.antiphishing.org/phishing_archive.html

NBG Example



From: National Bank of Greece <sec.contact@nbg.gr>
Subject: **Your account has been frozen because of the following reasons.**
Date: March 24, 2011 7:49:01 PM EDT
To: Aggelos Kiayias <aggelos@di.uoa.gr>
Reply-To: sec.contact@nbg.gr

Αγαπητοί πελάτες,

Τα αρχεία μας δείχνουν ότι η σύνδεση του λογαριασμού σας έχει παγώσει λόγω της
ακόλουθους λόγους.

Είσοδος σε δίκη με ανακριβείς πληροφορίες.

Ελλιπής ή ελλείποντα στοιχεία που χρησιμοποιούνται για την Εθνική Τράπεζα ηλεκτρονικό λογαριασμό.

Σας προτρέπουμε να αποκαταστήσει την Εθνική Τράπεζα σε απευθείας σύνδεση λογαριασμού αμέσως να αποτρέψει το κλείσιμο του λογαριασμού σας.

Κάντε κλικ στον παρακάτω σύνδεσμο για να αποκατασταθεί η Εθνική Τράπεζα ηλεκτρονικό λογαριασμό:

https://www.nbg.gr/wps/portal/LoginPageMap/!ut/p/c1/04_SB8K8xLLM9MSSzPy8xBz9CP0os3hP52AvL08TIwN3yyBzAyOfUC8zCxNHAwMLA30

Η **πολιτική ασφάλειας** που εφαρμόζει η Εθνική Τράπεζα για τη διενέργεια συναλλαγών μέσω i-bank, διασφαλίζει το απόρρητο και απαραβίαστο των συναλλαγών και των προσωπικών σας στοιχείων με τις πιο προηγμένες και πρωτοποριακές μεθόδους:

- Η μυστικότητα και το αναλλοίωτο των δεδομένων στο Internet Banking διασφαλίζονται μέσω του πρωτοκόλλου ασφαλούς επικοινωνίας SSL (Secure Sockets Layer) με ισχυρή κρυπτογράφηση στα 128 bit. Το ίδιο επίπεδο ασφάλειας παρέχεται και στις συναλλαγές μέσω Mobile Banking (για συνδρομητές Cosmote με κινητό τηλέφωνο i -mode?), δεδομένου ότι η τεχνολογία i -mode? επιτρέπει την μεταφορά δεδομένων μέσω του πρωτοκόλλου ασφαλούς επικοινωνίας SSL.
- Η **ελεγχόμενη πρόσβαση** στα συστήματα της Τράπεζας προστατεύεται από την τελευταία τεχνολογία Firewall.
- Η αυθεντικότητα της Τράπεζας εξασφαλίζεται με το πιστοποιητικό της Verisign, έναν από τους μεγαλύτερους, διεθνούς κύρους, οργανισμούς έκδοσης πιστοποιητικών παρουσίας στο internet.
- **Η ταυτοποίηση του χρήστη** και η πρόσβασή του στο **Internet Banking** πραγματοποιείται με τον Κωδικό Χρήστη (UserID) και το Μυστικό Κωδικό (Password). Ειδικά για τη διενέργεια συναλλαγών μέσω τηλεφώνου (**Phone Banking)** η ταυτοποίηση του χρήστη γίνεται με τον εξαψήφιο, αριθμητικό Κωδικό Εισόδου (UserID) και ένα Κωδικό μιας χρήσης που παράγεται από τη συσκευή i-code. Για περισσότερες πληροφορίες σχετικά με την **αποτροπή εισαγωγής μη εξουσιοδοτημένου χρήστη** στο σύστημα πιέστε εδώ.
- Η επιπλέον διασφάλιση των εγχρήματων συναλλαγών και συναλλαγών ασφαλείαςπραγματοποιείται με κωδικούς μιας χρήσης που παράγει η συσκευή ηλεκτρονικού κλειδαρίθμου (i-code).

Phishing Checklist

- Prepare fake web-site (HTML editors + ripping a legitimate web-site).
- Setup a web-server on a compromised host.
- Redirect traffic to fake web-server. How?
  - DNS Poisoning
  - Spam

For more information see

http://www.honeynet.org/papers/phishing/

Phishing Defenses

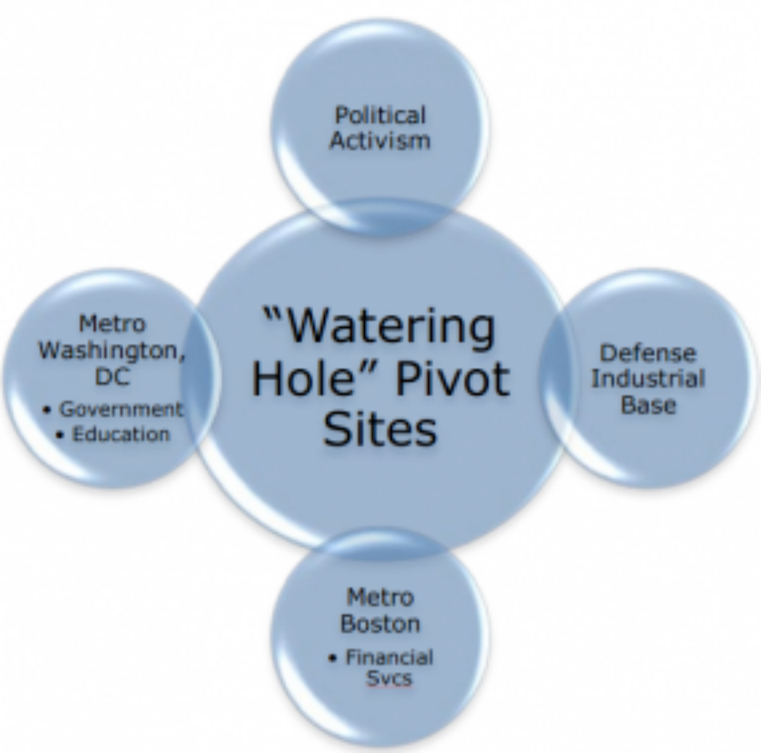
- Anti-spamming.
- User education.
- Improved branding techniques:
  - User-based branding.
  - Certification authority branding (requires modifications in the web-browser).

Spear Phishing

- Targeted Attacks
  - RSA Attack 2011
    http://blogs.rsa.com/anatomy-of-an-attack/
  - Uconn - “Your Inbox Almost Full”
  - Mandiant Report - “Mandiant_APT2_Report.pdf”
    http://www.itbusinessedge.com/blogs/data-security/spearphishing-attack-spoofs-mandiant-report.html

Watering Hole Attack

- "planting malware at sites deemed most likely to be visited by the targets of interest"
  http://krebsonsecurity.com/tag/watering-hole-attack/


Political Activism
Metro Washington, DC
• Government
• Education
"Watering Hole" Pivot Sites
Defense Industrial Base
Metro Boston
• Financial Svcs