
A Pretty Kettle of Phish



Whitepaper, June 2007

What is Phishing?

- E-Mail or other Message manipulated to **impersonate legitimate business/agency**.
- Intended to **trick the recipient**, using social engineering techniques, **into giving sensitive data** to the scammer (phisher).
- *Origin: phone freaking -> phreaking*



Why Phishing?

- Victim's Financial Resources
 - Credit Card Details
 - Bank Account Passwords
 - ...
- Online & Offline Identity Theft
 - E-Mail Passwords
 - Personal Details (SSN, etc)
 - ...



A Brief History of Phishing

- 1990s
 - AOL Internet Passwords, Credit Card Information
 - Traditional Scams going Online
 - 419 Nigerian Scam
 - Pyramid Schemes
 - Homeworker “Opportunities”
 - Pump and Dump Scams

Joliebull Ashlee Spearsbull - Message (HTML)

File Edit View Insert Format Tools Actions Help

Reply Reply to All Forward SnagIt Window

From: Kangfei Kesten [Kangfei_Kesten@agualatinoamerica.com] Sent: Thu 01/03/2007 20:20
To: admin@aviews.net
Cc:
Subject: Joliebull Ashlee Spearsbull

viewed us all with, bulging biceps celebrity lean
Superstar, leon, lopez homesend to newsshow timesdaily on in.
Office grays inn road london, wcx xz england. Reach, videos here content copy network limited, rights, reserved.
Video free pound bet photo.
Shopping guide nadri oscarstags davis.
Might forget live explains excited but nervous you? Road london wcx xz.
Is it win who plays tank top channel series?

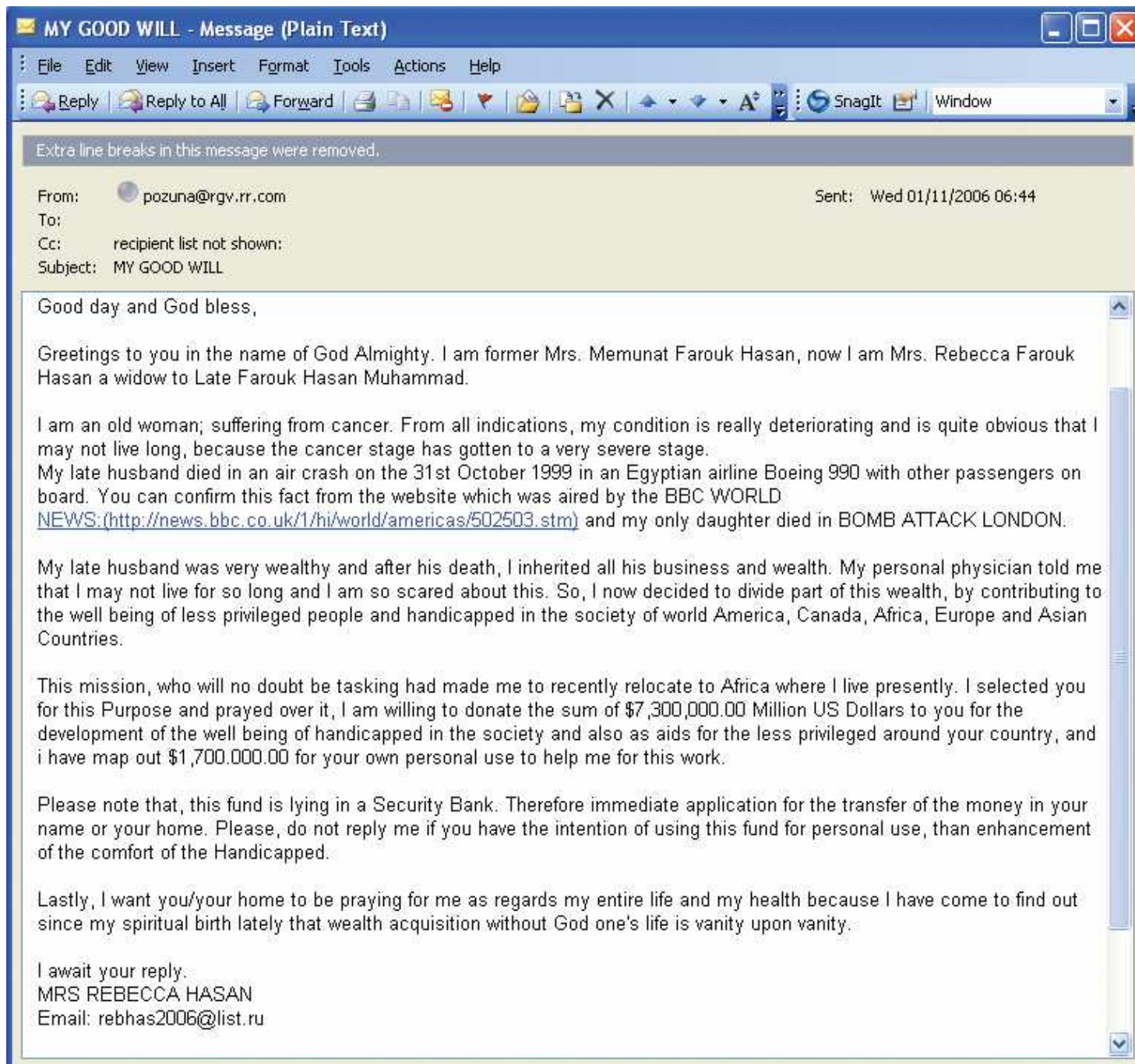
**INCREDIBLE INVESTMENT OPPORTUNITIES
ONLY A CLICK AWAY!**

Visit the address below and sign up now for your free guide on emerging companies!
Our last feature **gained 250% in two-weeks**, and our current feature is poised
to match or beat that! The Sign-up process is entirely free, and you have no obligations
at all! Spend the next 45 seconds signing up and securing the rest of your financial life!

Visit

[URL removed]

and be impressed with our current feature!!!



Old Phish

- Expect Personal Contact
- Social Engineering than Technical Attacks
- Originate from Fake Organizations

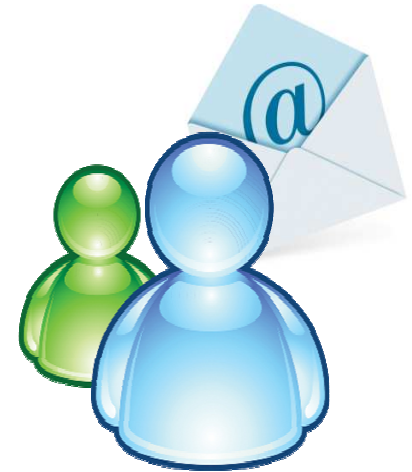
Phresher Phish

- 2000
 - Targets: Major Financial Organizations
 - Impersonating requests for client data
 - Malicious Web sites identical to the genuine
 - Malicious Pop-up forms inside the genuine site
 - Deceptive links that resemble legitimate ones
 - Injection of malicious fields in genuine site

Phishing Attack Components

- Bait Distribution

- E-mail, Instant Messaging, VoIP



- Data Collection

- Fake Web Site, Direct response to Bait, Spyware

- Use of misappropriated information

- Fraud
- Identity Theft



Phishing Attack: Bait Distribution

- From: badly-spelled plain-text
- To: sophisticated graphic-rich messages

- Sent through networks of compromised computers (Botnets)

Phishing Attack: Bait Distribution

Σημαντική Μήνυμα! Spam | X 2Me | X CSD-All | X

★ NATIONAL BANK OF GREECE S.A. Αγαπητοί πελάτες, Τα αρχεία μας δείχνει Feb 16

★ from NATIONAL BANK OF GREECE S.A. hide details Feb 16 Reply

<NBGservice@upenn.edu>

to

date Tue, Feb 16, 2010 at 7:32 PM

subject Σημαντική Μήνυμα!

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.

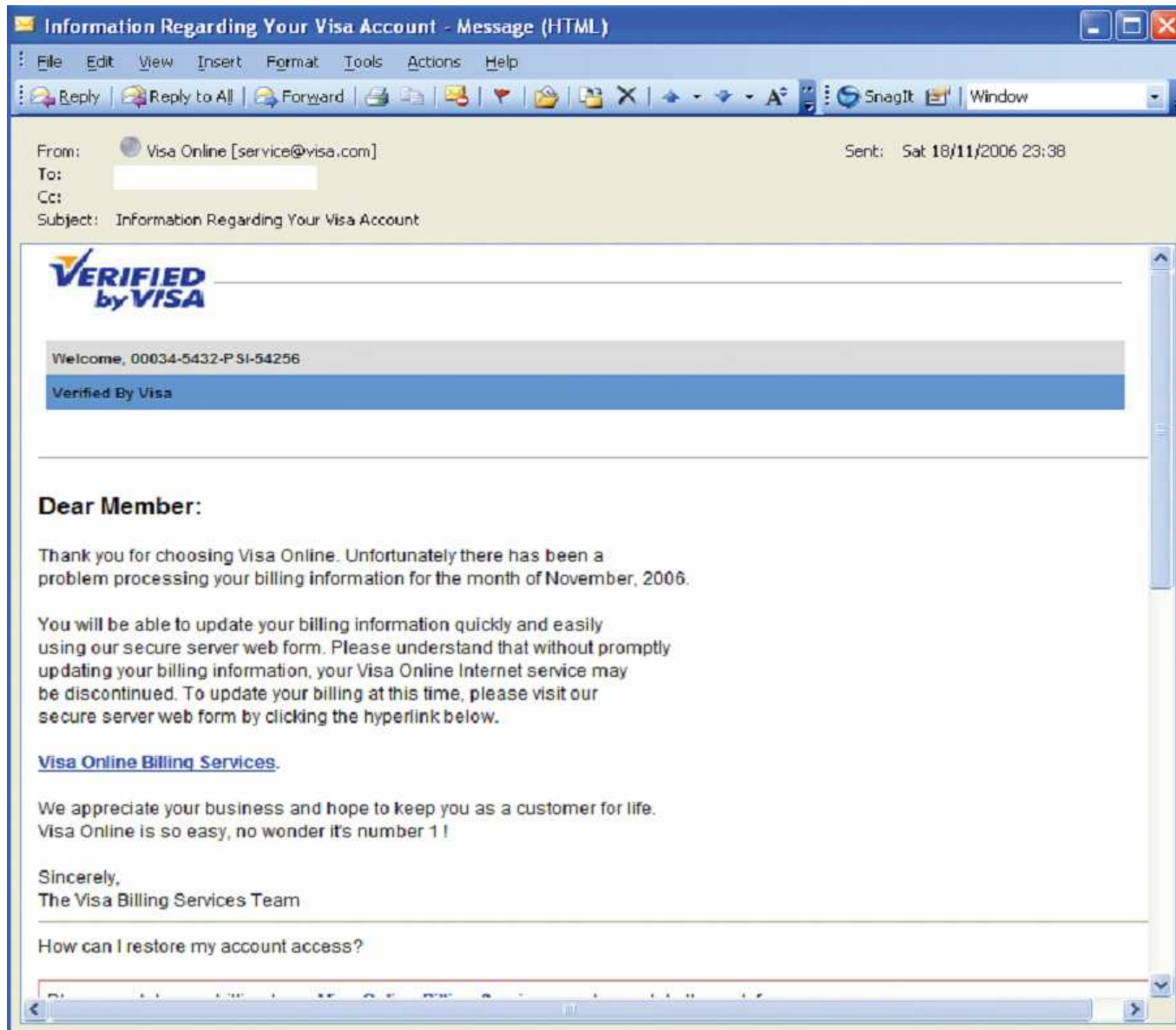
Σας προτρέπουμε να αποκαταστήσει την Εθνική Τράπεζα σε απευθείας σύνδεση λογαριασμού αμέσως να αποτρέψει το κλείσιμο του λογαριασμού σας.

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

<http://www.nbg9.gr.y-sisul.or.kr/wps/portal/LoginPageMap.php?loginPage=true>

© 2010 Εθνική Τράπεζα.

Phishing Attack: Bait Distribution



Phishing Attack: Evade Detection

- Hash Busters: text randomizers
- HTML Display Hacks
- Hidden Safewords



Phishing Attack: Targets

- Remember: it's all about the money!

Top 10 Identified Targets		Valid Phishes
1	PayPal	8,488
2	Internal Revenue Service	772
3	Facebook	715
4	HSBC Group	458
5	Bank of America Corporation	134
6	Tibia	130
7	eBay, Inc.	124
8	World of Warcraft	111
9	HSBC	103
10	Amazon.com	86



- Also
 - non-commercial organizations (law enforcement, IRS)
 - aid initiatives (Haiti earthquake)

Email address

PayPal password

Forgot your [email address](#) or [password](#)?

New to PayPal? [Sign up](#).

Top questions

- [Why use PayPal when I have credit cards?](#)
- [What can I do with PayPal?](#)
- [Is PayPal free to use?](#)

The safer, easier way to pay without exposing your credit card number



Pay With:

Pay online

- › [Speed through checkout](#) whenever you shop online.
- › [Pay without revealing](#) your credit card information.
- › [Send money](#) to your friends and family.

Learn more about [paying with PayPal](#).

Sell online

- › [Accept credit cards](#) quickly and easily.
- › [Lift your sales](#). Add PayPal to attract more customers.
- › [Get tools](#) to make eBay sales simple.

Learn more about [selling with PayPal](#).

PayPal is offered at over [100,000 sites](#).



Spear Phishing Attack

Dear uoc.gr Account User Spam | X CSD-All | X

☆ from **University of Crete** <admin@uoc.gr> hide details Feb 8 ↩ Reply ▼

reply-to w3454466747@googlemail.com

to

date Mon, Feb 8, 2010 at 1:00 AM

subject Dear uoc.gr Account User

Dear uoc.gr Account User,

This message is from your email administrator / mentainance center email account to all users. We are improving our database and e-mail center due to unusual activities identified in our email system. Therefore, we are deleting all e-mail accounts identified to improve and create space for new ones.

You are required to verify your email account via email, confirming their identity. This will prevent your mail account termination during this exercise.

To confirm your email identity, you provide the information requested below:

- * Username : (.....) (required)
- * Password : (.....)(required)
- * Date of Birth: (.....) (optional)
- * Country or territory: (.....) (optional)

<https://mail.uoc.gr/horde/imp/login.php>

* Important *

Please provide all this information completely and correctly otherwise, for security reasons we may have to disable your account temporarily.

□niversity of Crete 2010.

Data Collection

- Deceptive Web Sites
- HTML Forms embedded in Bait Message
- Malicious Software attached/referenced
- Telephone Numbers

Data Collection

Urgent Security Update for Internet Explorer (960714) Spam | X 2Me | X

CSD-All | X

★ from **Microsoft Corporation** [hide details](#) Feb 6 [Reply](#) ▼
<microsoft@montclair.edu>
to [REDACTED]
date Sat, Feb 6, 2010 at 12:29 PM
subject Urgent Security Update for Internet Explorer
(960714)

Warning: This message may not be from whom it claims to be. Beware of following any links in it or of providing the sender with any personal information. [Learn more](#)

Please click here to Update your Internet Explorer

<http://iexplore.windows.com.y-sisul.or.kr/v/windows/ie/ie6/using/techinfo/s/activexupdate.aspx.html>

General Information

Executive Summary

This security update resolves a publicly disclosed vulnerability. The vulnerability could allow remote code execution if a user views a specially crafted Web page using Internet Explorer. Users whose accounts are configured to have fewer user rights on the system could be less impacted than users who operate with administrative user rights.

Microsoft Active Protections Program (MAPP)

To improve security protections for customers, Microsoft provides vulnerability information and updates to major security software providers in advance of each monthly security update release.

© 2010 Microsoft Internet Explorer
MICROSOFT SECURITY BULLETIN MS08-078 - Critical

Data Collection

Possible Beneficiary Spam | X CSD-All | X

★ from **Dean Harry Esq** <djbklkly@mta.ca> [hide details](#) Feb 9 [Reply](#) ▼
reply-to barr.dhesq8@w.cn
to
date Tue, Feb 9, 2010 at 3:59 AM
subject Possible Beneficiary

This is to notify you that late Mr. Rolf Hoffmann made you a beneficiary to his WILL. He left the sum of twelve million, thirty thousand United States Dollars(\$12,030,000.00) in the codicil to his Will and last testament. This may sound strange and unbelievable to you. You are hereby required by this notification to Confirm your ownership to this Legacy. You shall be detailed you on the procedure in benefiting this upon the receipt of your response via email, contact Dean Harry Esq. via his personal email addresses below:
barr_dharryesq@hotmail.com

A telephone call would be as well appreciated;
Tell: +44 702 409 9921
+44 702 401 0513

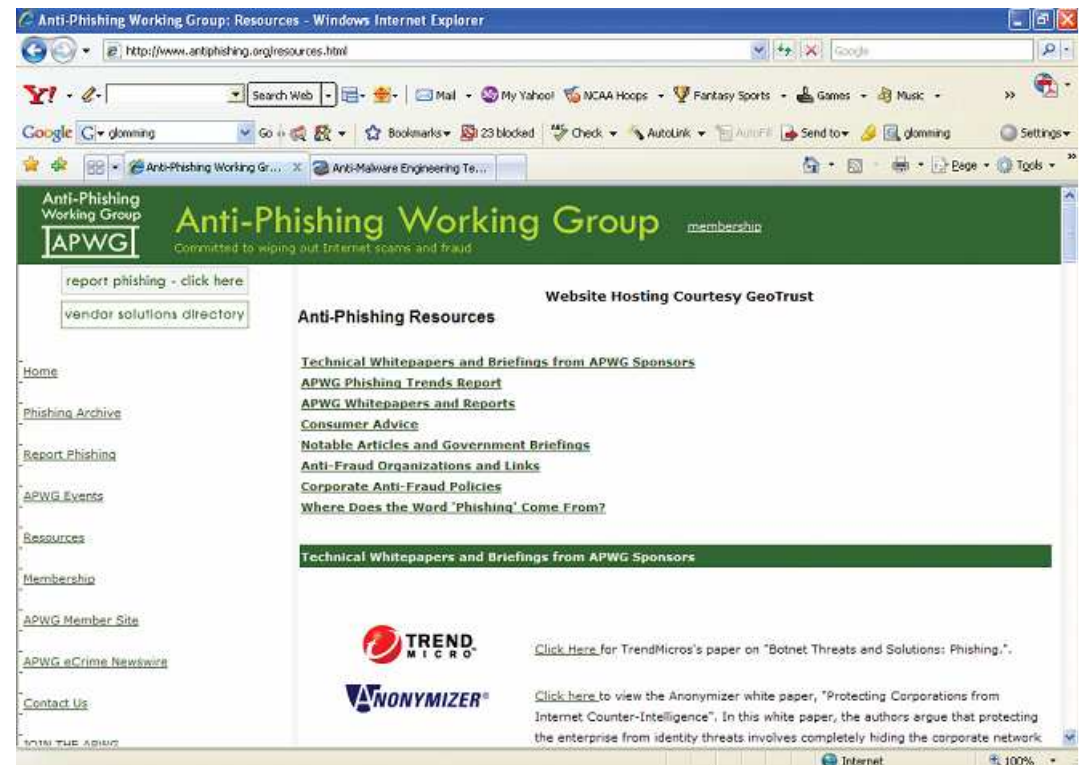
Regards,
Dean Harry Esq.
Principle Partners
Dean Harry & Associates

Phishing Traps

- Hidden or Obfuscated URLs
 - ❑ `http://bank.com`
 - ❑ `http://www.paypal.com.malicious.com`
 - ❑ `http://goodsite.com/?attack=http://malicious.com`
- Phishing Cousins
 - ❑ `http://paypai.com`
 - ❑ `http://www.winbank.com`
- Phish Pharms
 - ❑ DNS poisoning
 - ❑ 'hosts' file

Solutions

- Collaborative Groups
 - Financial Section
 - Software Security Firms
 - Law Enforcement
 - ISPs



Solutions

- Technological Tools
 - ❑ Web Filtering
 - ❑ Browser Security Plug-ins
 - ❑ DNS Blacklisting
 - ❑ Mail Authentication
 - ❑ Two Factor Authentication



Discussion

- How do you recognize a Phish?



That's it! Questions?

