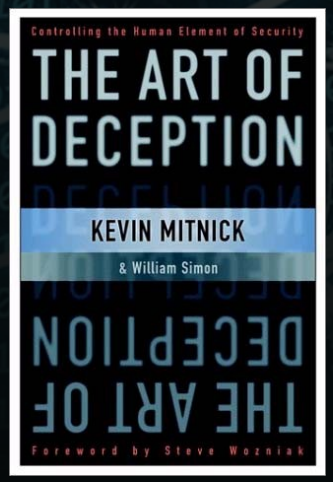
Social engineering

Marek Zachara
http://marek.zachara.name

„Controlling the human Element of Security”

- Kevin Mitnick



A system is only as strong
As the weakest link -
- users are usually
„the weakest links”

And there is always a user who
is not skilled / knowledgeable
enough in the matters of security

Co to jest

Methods of obtaining access or credentials

Passive: Observation

- Workspace (notes), gossips

Active: Preparing a trap

- Building trust
- Severity of the predicament
- Cut-off from important resources

Casting a net - phishing

- General, targeting a web site
- Spearhead phishing
- “Dumb” phishing

Too much hardening can cause trouble

Periodical password changes

- „Amy, what is the password today”
- Writing it down in a notepad
- Sticking it on the screen cover

Masked passwords

- Table “helper” form at one bank's branch

Conclusion:

- Password and procedures complexities have positive influence only up to a certain point (Laffer curve analogy)

This first anecdote involves a security officer at a top secret government facility. Suspecting that some employees were not abiding by the password rules for network login, I decided to run LOphtCrack, an administrative tool that can sometimes be used to find lost passwords. Lo and behold, the chief of facility was using "87654321" as his login code. When I pointed out to him that this was not acceptable, he said "It's such a simple password, nobody would guess I would use it." And when I asked him to change it, he said "No, I like it and besides, I use it for all my accounts." Those included, as he later admitted, his personal AOL logon and his ATM PIN.

Spectacular failures

Trust as an attack vector

- “Foot-in-the-door” technique – gradually increasing the weight of the requests
- Use of internal, even though not confidential information (e.g. the company structure) to pose as an “insider”
- Request for actions the victim considers to be under his/her control (e.g. typing in commands)
- Help with solving a problem (deliberately engineered)

“Stochastic” approach – a call from the support

Virtual trust via social sites

- Creating a virtual profile
- Building trust among the followers
- Delivering (semi) valuable content
- Finally – reaping the benefits

Experiment by BitDefender:

- 97% of the followers 'clicked' a link leading to a dangerous website

Password please...

Ninety per cent of office workers at London's Waterloo Station gave away their computer password for a cheap pen, compared with 65 per cent last year. The survey also found the majority of workers (80 per cent) would take confidential information with them when they change jobs and would not keep salary details confidential if they came across them.

source: *http://www.theregister.co.uk/2003/04/18/office_workers_give_away_passwords/*

Password please...

More than 70% of people would reveal their computer password in exchange for a bar of chocolate, a survey has found.
It also showed that 34% of respondents volunteered their password when asked without even needing to be bribed.
A second survey found that 79% of people unwittingly gave away information that could be used to steal their identity when questioned.
The survey on passwords was carried out for the Infosecurity Europe trade show due to take place at Olympia in London from 27-29 April.
The survey data was gathered by questioning commuters passing through Liverpool Street station in London and found that many were happy to share login and password information with those carrying out the research.

source: *http://news.bbc.co.uk/2/hi/technology/3639679.stm*

Password please (solutions)

How to protect against “handing over” of the passwords

- Minimal user rights
- Limiting access to a list of selected machines
- Procedures for handling the staff leaving the company
- Single sign-on
- Fraud detection (behavioral patterns)

Protection against data copying

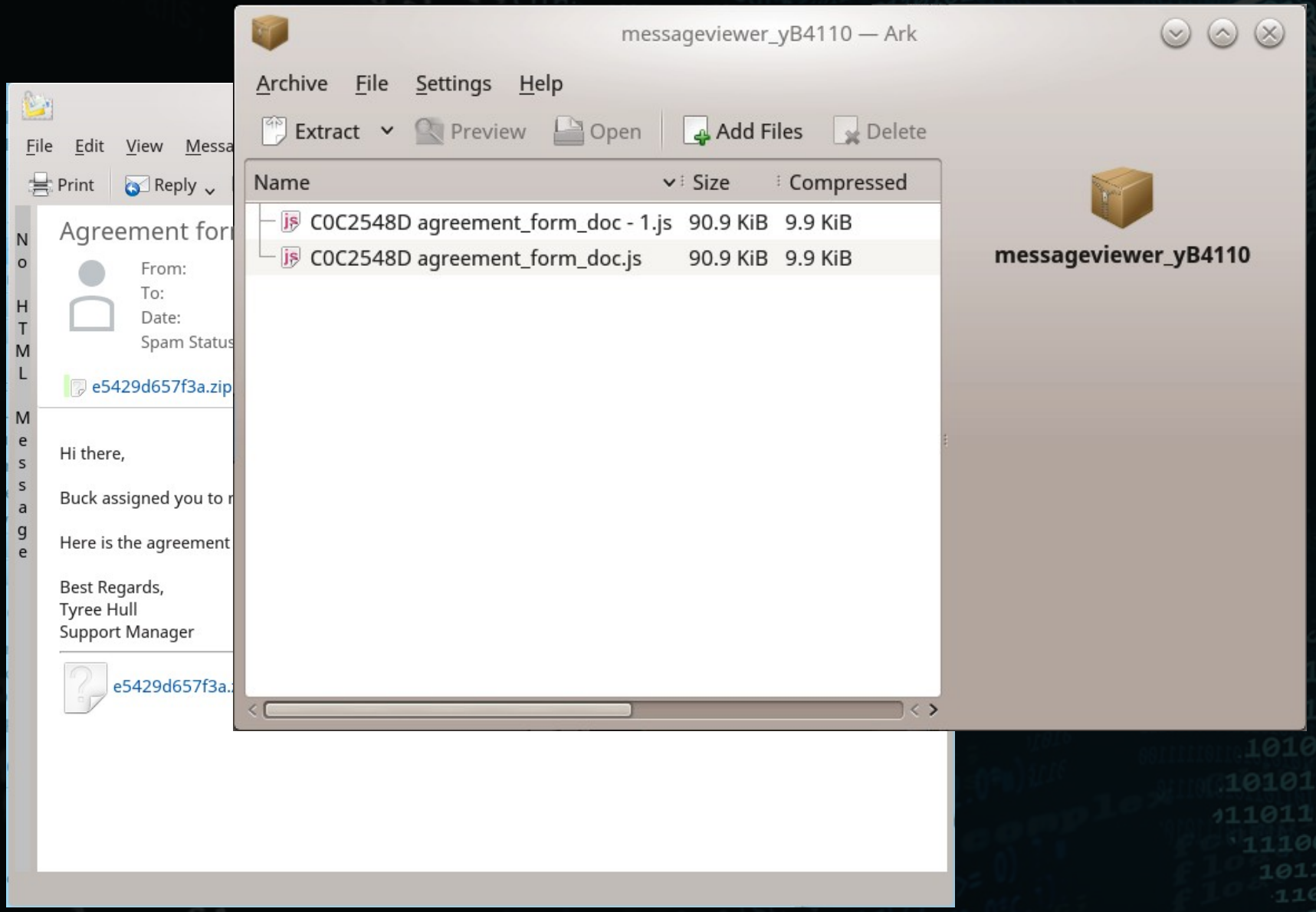
Phishing

- Often relies on convincing the victim to log into a fabricated copy of a legitimate service
- Usually utilizes e-mail as means of reaching the victims
- E-mails include links to the “login page” of the target application/service

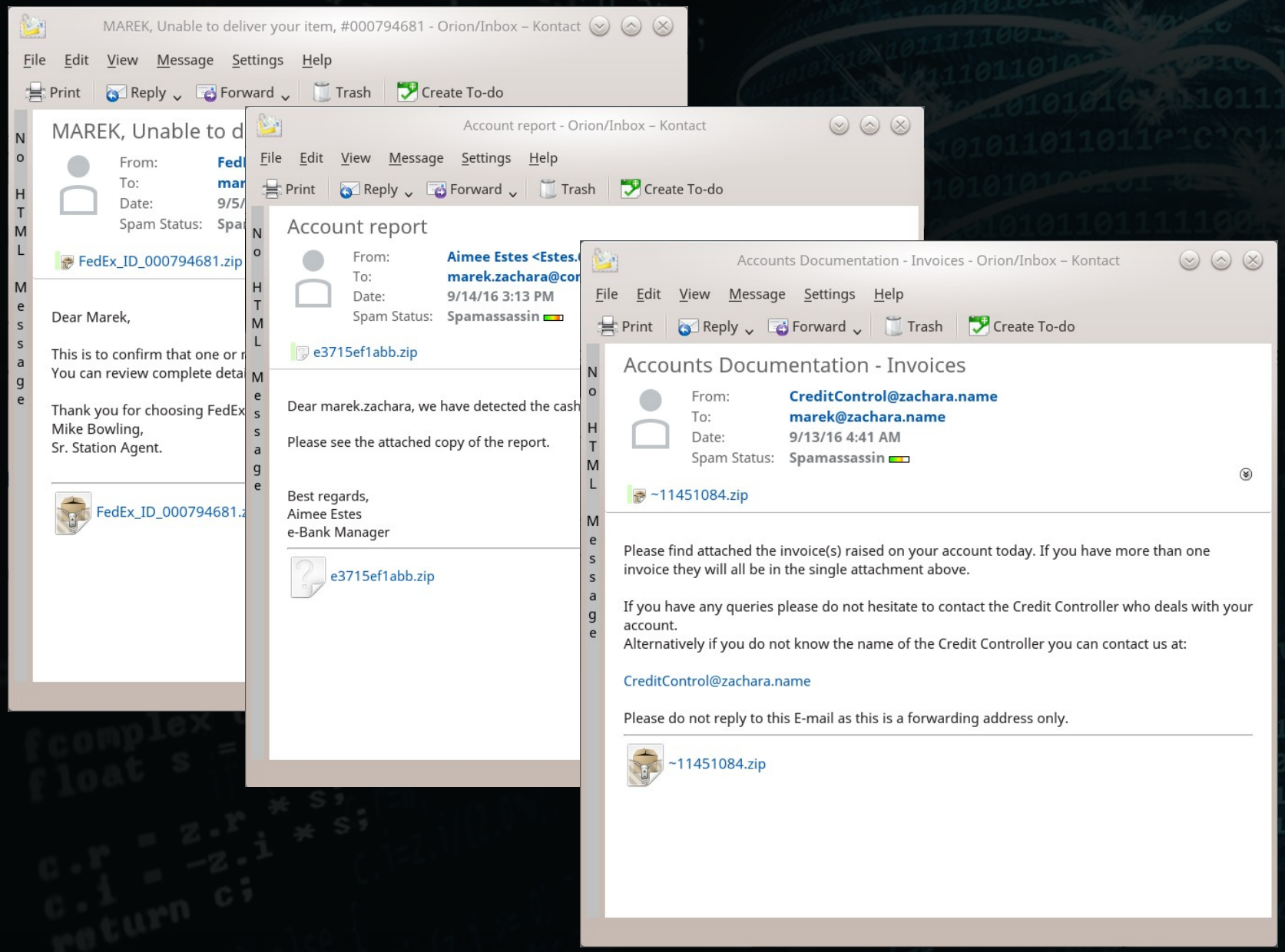
The content of the e-mail is meant to cause worry or anxiousness:

- 'periodical verification of user accounts'
- 'your data has been compromised'
- 'you just won a $10'

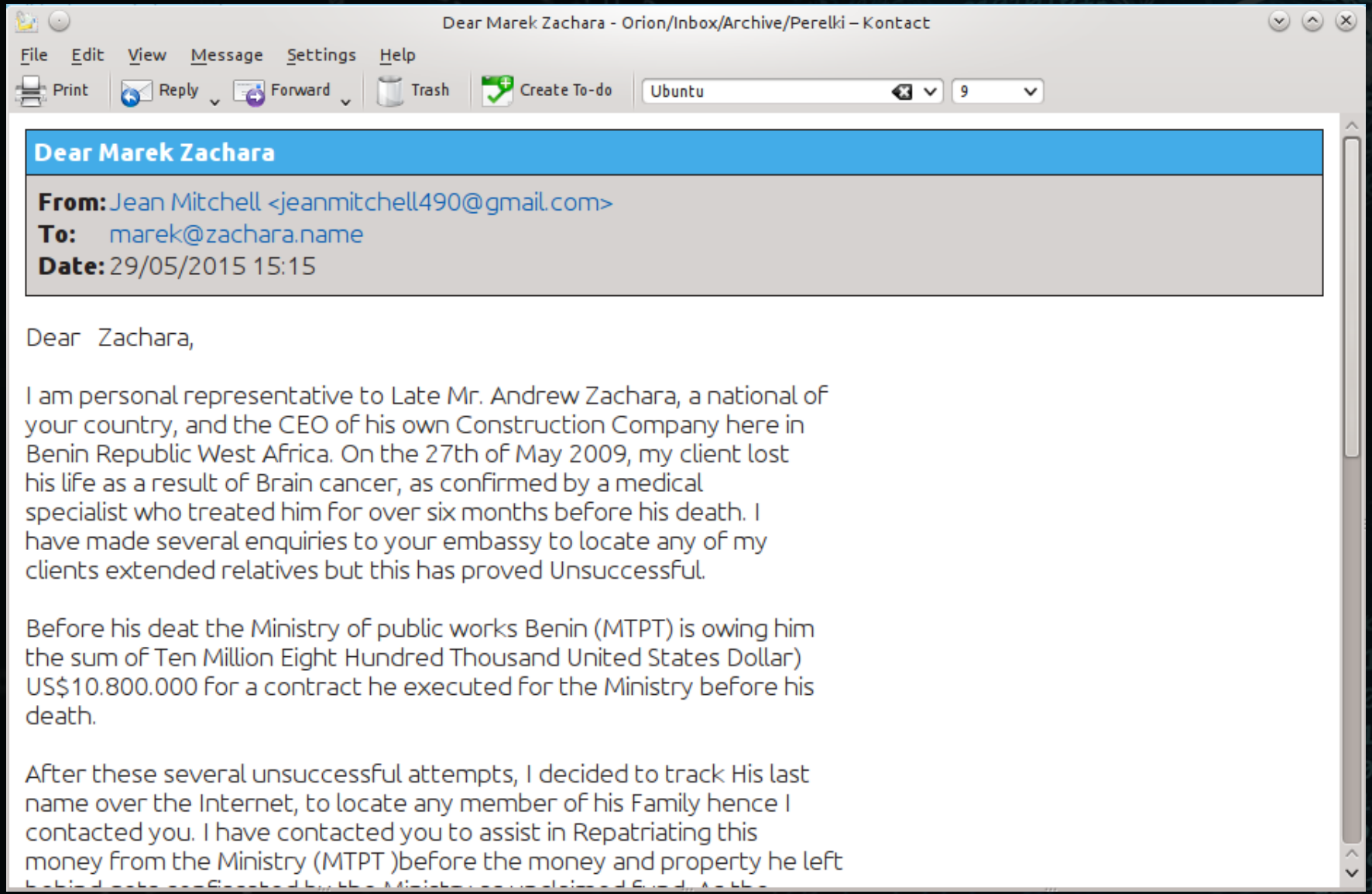
Attachment-based phishing



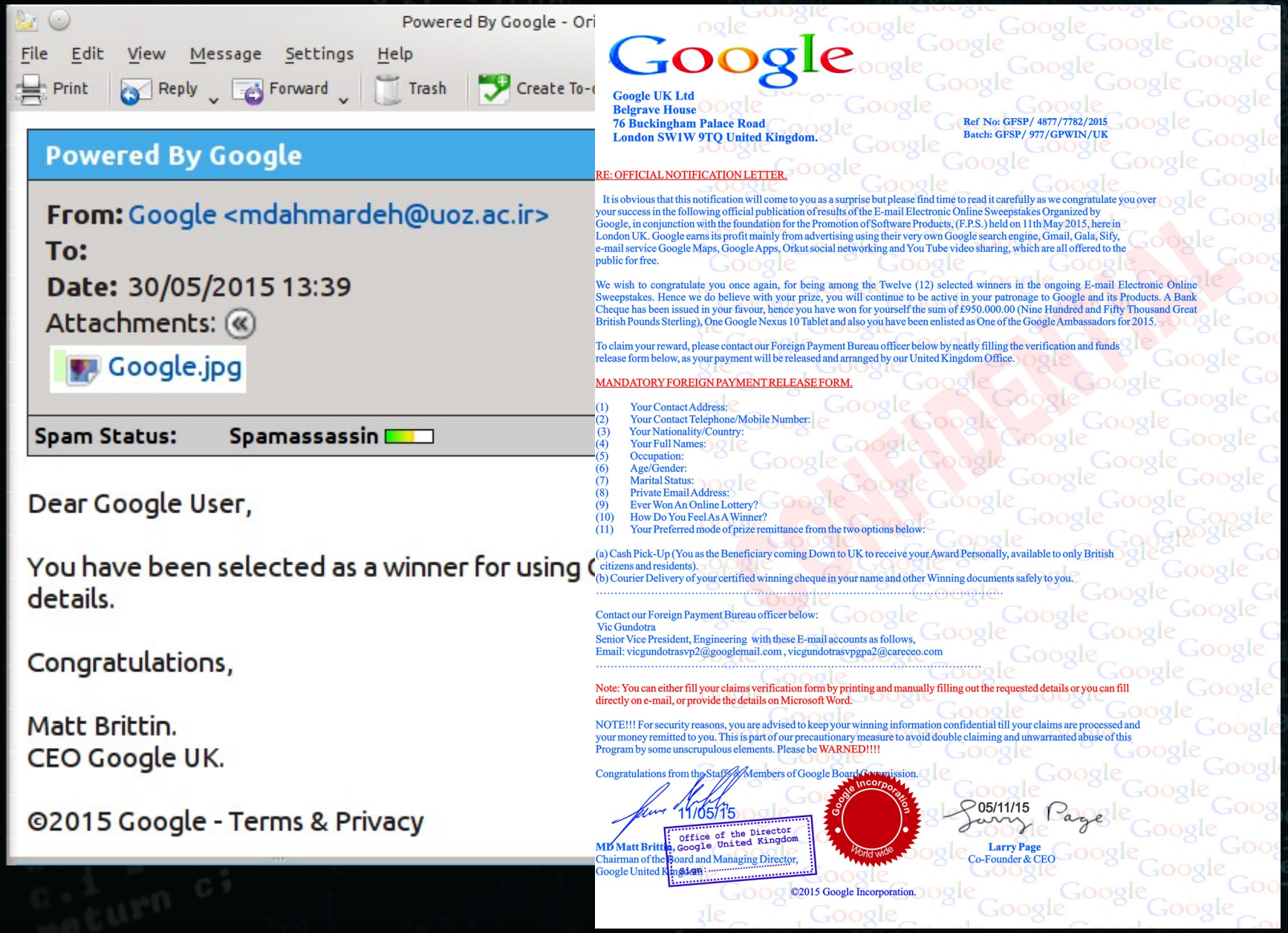
Attachment-based phishing (variations)



Sample phishing (2)



Sample phishing (3)



Powered By Google - Ori

File Edit View Message Settings Help

Print Reply Forward Trash Create To-

Powered By Google

From: Google <mdahmardeh@uoz.ac.ir>
To:
Date: 30/05/2015 13:39
Attachments:
Google.jpg

Spam Status: Spamassassin

Dear Google User,

You have been selected as a winner for using (
details.

Congratulations,

Matt Brittin.
CEO Google UK.

©2015 Google - Terms & Privacy

Google

Google UK Ltd
Belgrave House
76 Buckingham Palace Road
London SW1W 9TQ United Kingdom.

Ref No: GFSP/ 4877/7782/2015
Batch: GFSP/ 977/GPWIN/UK

RE: OFFICIAL NOTIFICATION LETTER.

It is obvious that this notification will come to you as a surprise but please find time to read it carefully as we congratulate you over your success in the following official publication of results of the E-mail Electronic Online Sweepstakes Organized by Google, in conjunction with the foundation for the Promotion of Software Products, (F.P.S.) held on 11th May 2015, here in London UK. Google earns its profit mainly from advertising using their very own Google search engine, Gmail, Gala, Sify, e-mail service Google Maps, Google Apps, Orkut social networking and You Tube video sharing, which are all offered to the public for free.

We wish to congratulate you once again, for being among the Twelve (12) selected winners in the ongoing E-mail Electronic Online Sweepstakes. Hence we do believe with your prize, you will continue to be active in your patronage to Google and its Products. A Bank Cheque has been issued in your favour, hence you have won for yourself the sum of £950.000.00 (Nine Hundred and Fifty Thousand Great British Pounds Sterling), One Google Nexus 10 Tablet and also you have been enlisted as One of the Google Ambassadors for 2015.

To claim your reward, please contact our Foreign Payment Bureau officer below by neatly filling the verification and funds release form below, as your payment will be released and arranged by our United Kingdom Office.

MANDATORY FOREIGN PAYMENT RELEASE FORM.

(1) Your Contact Address:
(2) Your Contact Telephone/Mobile Number:
(3) Your Nationality/Country:
(4) Your Full Names:
(5) Occupation:
(6) Age/Gender:
(7) Marital Status:
(8) Private Email Address:
(9) Ever Won An Online Lottery?
(10) How Do You Feel As A Winner?
(11) Your Preferred mode of prize remittance from the two options below:

(a) Cash Pick-Up (You as the Beneficiary coming Down to UK to receive your Award Personally, available to only British citizens and residents).
(b) Courier Delivery of your certified winning cheque in your name and other Winning documents safely to you.

Contact our Foreign Payment Bureau officer below:
Vic Gundotra
Senior Vice President, Engineering with these E-mail accounts as follows,
Email: vicgundotrasvp2@googlemail.com , vicgundotrasvpgpa2@careceo.com

Note: You can either fill your claims verification form by printing and manually filling out the requested details or you can fill directly on e-mail, or provide the details on Microsoft Word.

NOTE!!! For security reasons, you are advised to keep your winning information confidential till your claims are processed and your money remitted to you. This is part of our precautionary measure to avoid double claiming and unwarranted abuse of this Program by some unscrupulous elements. Please be WARNED!!!!

Congratulations from the Staff Members of Google Board Commission.

11/05/15

Office of the Director Google United Kingdom

Google Incorporation World wide

05/11/15 Larry Page

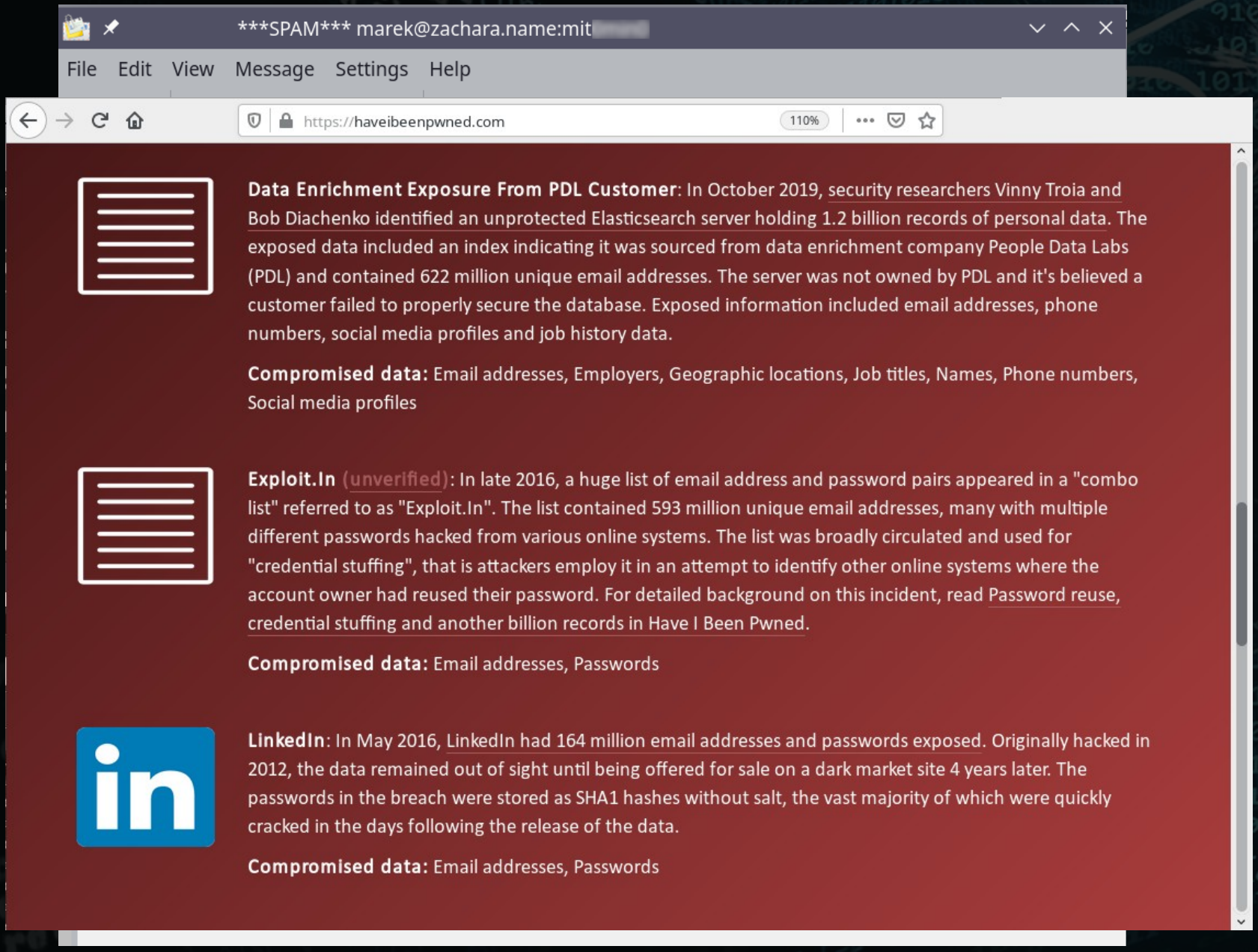
MD Matt Brittin,
Chairman of the Board and Managing Director,
Google United Kingdom

Larry Page
Co-Founder & CEO

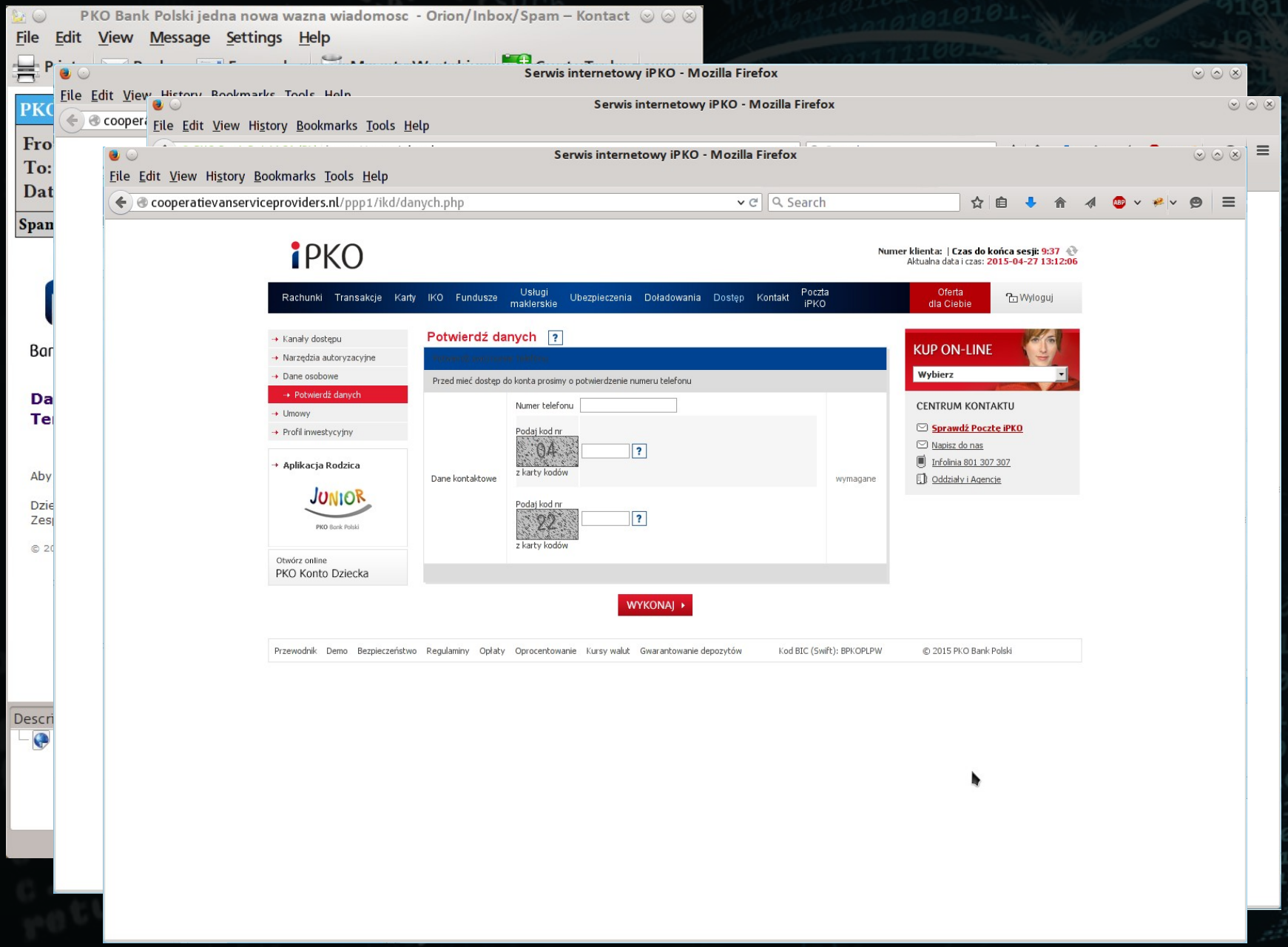
©2015 Google Incorporation.

CONFIDENTIAL

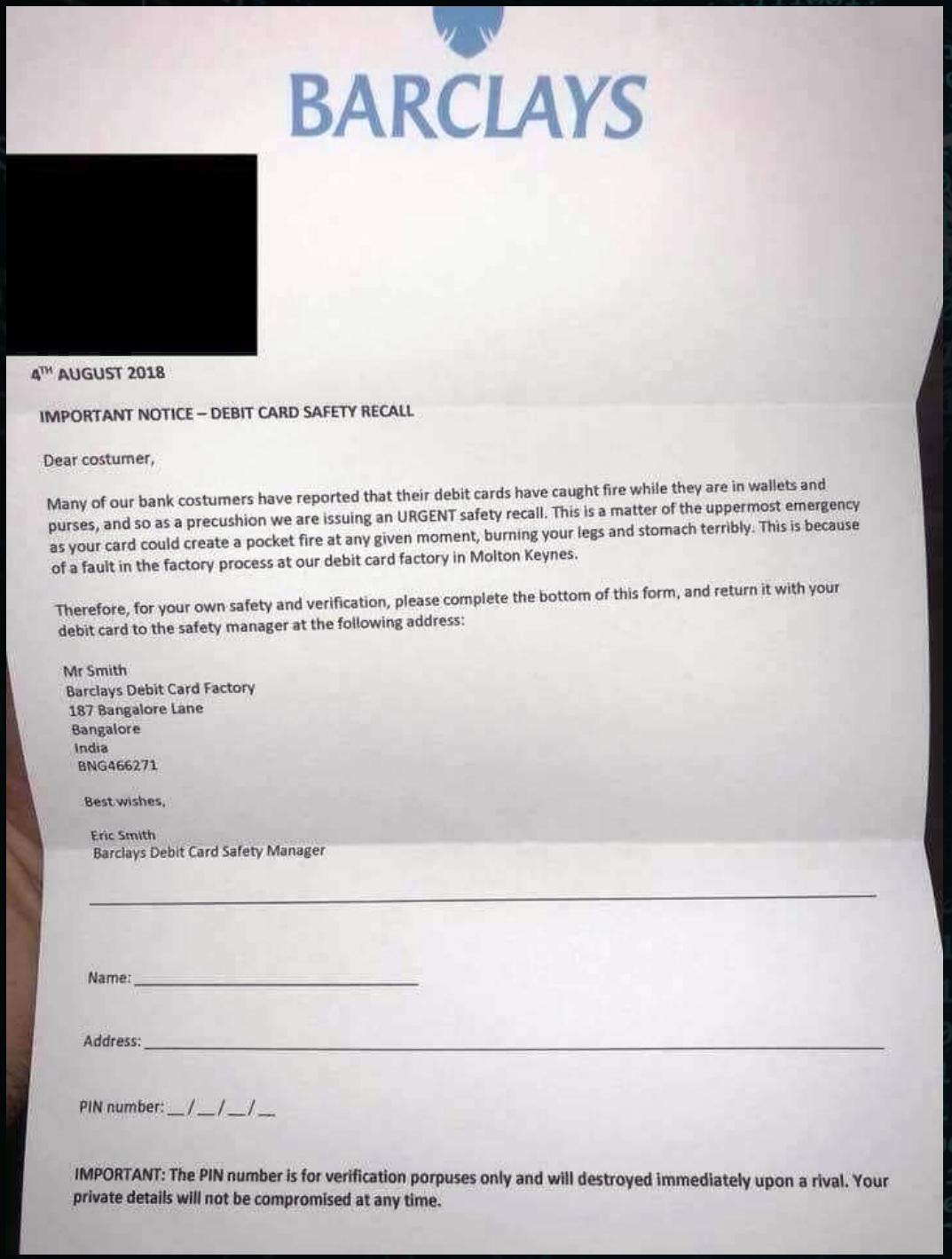
Sample phishing (4)



A phishing site



Phishing variation



BARCLAYS

[redacted]

4TH AUGUST 2018

IMPORTANT NOTICE – DEBIT CARD SAFETY RECALL

Dear costumer,

Many of our bank costumers have reported that their debit cards have caught fire while they are in wallets and purses, and so as a precushion we are issuing an URGENT safety recall. This is a matter of the uppermost emergency as your card could create a pocket fire at any given moment, burning your legs and stomach terribly. This is because of a fault in the factory process at our debit card factory in Molton Keynes.

Therefore, for your own safety and verification, please complete the bottom of this form, and return it with your debit card to the safety manager at the following address:

Mr Smith
Barclays Debit Card Factory
187 Bangalore Lane
Bangalore
India
BNG466271

Best wishes,

Eric Smith
Barclays Debit Card Safety Manager

_____

Name: _____

Address: _____

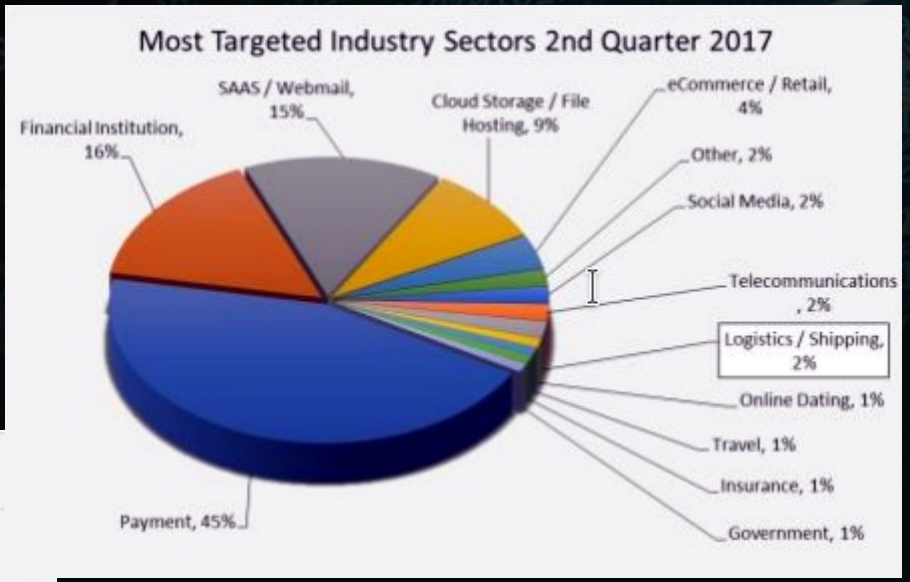
PIN number: __/__/__/__

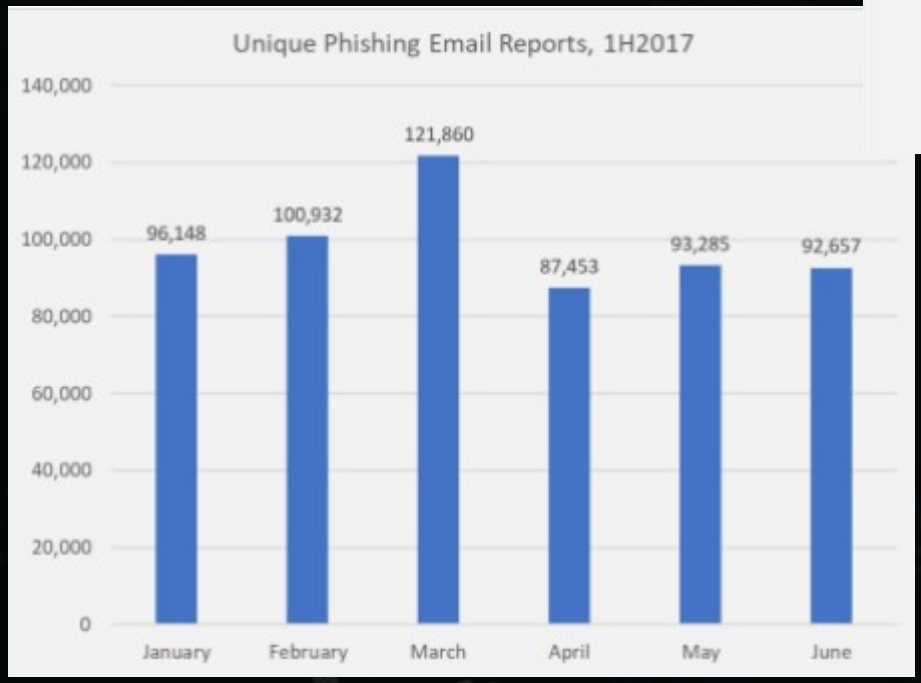
IMPORTANT: The PIN number is for verification porpuses only and will destroyed immediately upon a rival. Your private details will not be compromised at any time.

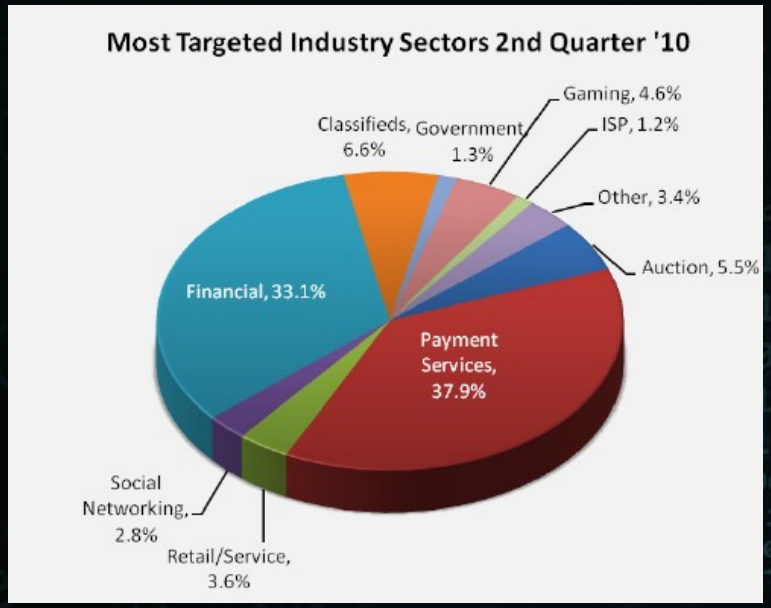
A 'dumb' phishing

Subject: Maintenance Notice.
From: "Admin Helpdesk" <helpdesk@webmaster.com>
To: undisclosed-recipients:
Dear Account User,
This message is from the Office of the Webmail Admin Helpdesk Center to all webmail account owners. Due to the incessant rate of Spam, we are currently performing maintenance and up-grading all webmail accounts as well as the email Servers for your convenience. All email services will be interrupted during this period, To prevent your account from closing during this exercise you will have to update it below to know it's status as a currently used account with a hard spam protector.
This Maintenance commenced on October 23rd to end October 30th 2011 beginning at 9:00 p.m. until approximately 12:00 midnight to enable us increase the storage size of your webmail account. Be informed also that we will not hesitate to delete your email account if not functioning to create more space for new users.
Confirm Your email account Details by clicking on the reply button and follow by your;
*Full Name:
*E-mail ID/Username:
*E-mail Password:
*Confirm Password:
*Date of Birth:
After upgrading, a password reset link will be sent to your email for new password. Please understand that this is a security measure intended to help protect your email Account.

Phishing statistics







source: http://www.antiphishing.org

Vishing

- An IVR based phishing
- Requires convincing the victim to contact (preferably a toll-free) access number to the “Customer Service”

Request for action (samples)

- Authorization of a recent transaction
- Confirmation of personal data
- Extension of service

Spearhead fishing

- Targeted for certain group or individual
  - Specific group of firms or individuals (e.g.: law firms)
  - Single individuals
    - Executives
    - Resource controllers (accountants)
- Requires some investigation
- More likely to succeed

How to get $17M ... easily

The three wire transfers, the FBI says, happened in June 2014. They were prompted by emails sent to Scoular's corporate controller, identified in the FBI statement as McMurtry. The emails purported to be from Scoular CEO Elsea, but were sent from an email address that wasn't his normal company one.

The first email on June 26 instructed McMurtry to wire $780,000, which the FBI statement says he did. The next day, McMurtry was told to wire $7 million, which he also did. Three days later, another email was sent to McMurtry, instructing him to wire $9.4 million. McMurtry again complied.

The first two emails from the faux CEO contain the swindle's setup, swearing the recipient to secrecy over a blockbuster international deal.

"I need you to take care of this," read emails from the party pretending to be Elsea. *"For the last months we have been working, in coordination and under the supervision of the SEC, on acquiring a Chinese company. ... This is very sensitive, so please only communicate with me through this email, in order for us not to infringe SEC regulations."*

Source: http://www.omaha.com/money/impostors-bilk-omaha-s-scoular-co-out-of-million/article_25af3da5-d475-5f9d-92db-52493258d23d.html

A bait

- Various data storage untis (Pen-drives, CDs) left in common places
- Possibly suggesting an interesting content
- But their primary purpose is to carry a malware into the targeted organization

Mitigation method: Identification and controll of all “entry points”

Thank you for your attention.

Any questions?

Included content came from
- Clipart – openclipart.org
- Internet map – The Opte Project

Licensed (royalty-free) content, cannot be distributed separately:
- Presentation background, people's avatars