

Social engineering

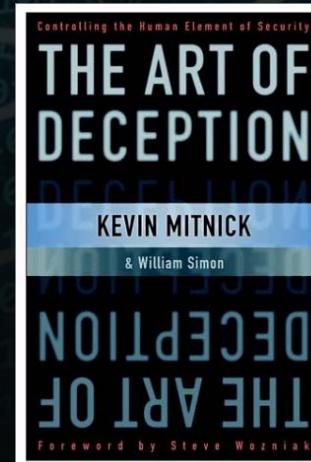
Marek Zachara
<http://marek.zachara.name>



„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

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 LOptCrack, 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



source: <http://securityaffairs.co/>

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.

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.

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

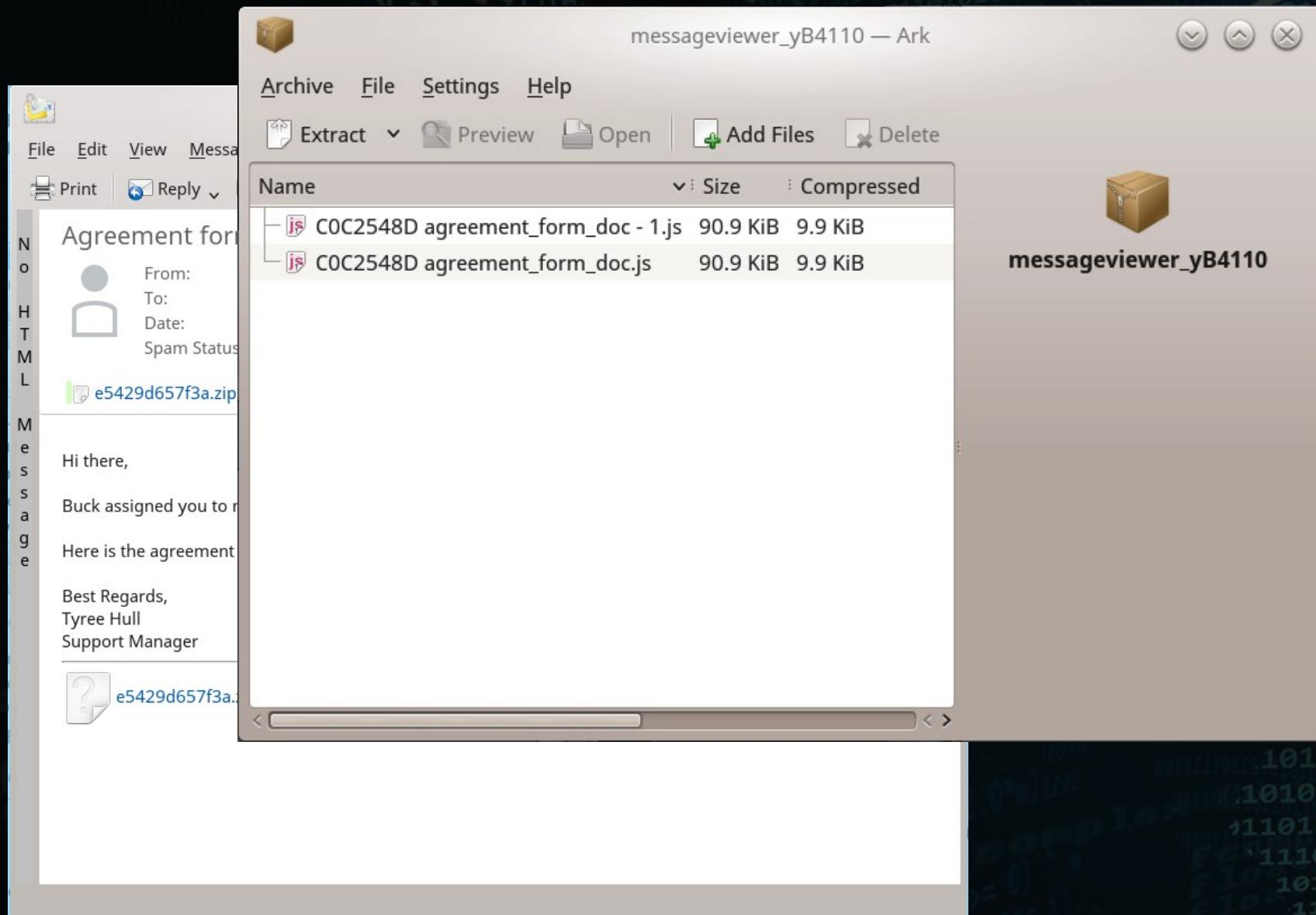
Phishing

- 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)

MAREK, Unable to deliver your item, #000794681 - Orion/Inbox - Kontact

File Edit View Message Settings Help

Print Reply Forward Trash Create To-do

MAREK, Unable to d

From: FedEx

To: marek.zachara@cor

Date: 9/15/2016

Spam Status: Spamassassin

FedEx_ID_000794681.zip

Dear Marek,

This is to confirm that one or more items you have sent us have been delivered.

You can review complete details in the attached report.

Thank you for choosing FedEx.

Mike Bowling,
Sr. Station Agent.

FedEx_ID_000794681.zip

Aimee Estes <Estes.Aimee@fedex.com>

marek.zachara@corporate.zachara.name

9/14/16 3:13 PM

Spam Status: Spamassassin

e3715ef1abb.zip

Dear marek.zachara, we have detected the cash in transit.

Please see the attached copy of the report.

Best regards,
Aimee Estes
e-Bank Manager

e3715ef1abb.zip

Account report - Orion/Inbox - Kontact

File Edit View Message Settings Help

Print Reply Forward Trash Create To-do

Account report

From: Aimee Estes <Estes.Aimee@fedex.com>

To: marek.zachara@corporate.zachara.name

Date: 9/14/16 3:13 PM

Spam Status: Spamassassin

e3715ef1abb.zip

Accounts Documentation - Invoices - Orion/Inbox - Kontact

File Edit View Message Settings Help

Print Reply Forward Trash Create To-do

Accounts Documentation - Invoices

From: CreditControl@zachara.name

To: marek.zachara@zachara.name

Date: 9/13/16 4:41 AM

Spam Status: Spamassassin

~11451084.zip

Please find attached the invoice(s) raised on your account today. If you have more than one invoice they will all be in the single attachment above.

If you have any queries please do not hesitate to contact the Credit Controller who deals with your account.

Alternatively if you do not know the name of the Credit Controller you can contact us at:

CreditControl@zachara.name

Please do not reply to this E-mail as this is a forwarding address only.

~11451084.zip

Sample phishing (2)

Dear Marek Zachara - Orion/Inbox/Archive/Perelki – Kontact

File Edit View Message Settings Help

Print **Reply** **Forward** **Trash** **Create To-do** **Ubuntu**

Dear Marek Zachara

From: Jean Mitchell <jeanmitchell490@gmail.com>
To: marek@zachara.name
Date: 29/05/2015 15:15

Dear Zachara,

I am personal representative to Late Mr. Andrew Zachara, a national of your country, and the CEO of his own Construction Company here in Benin Republic West Africa. On the 27th of May 2009, my client lost his life as a result of Brain cancer, as confirmed by a medical specialist who treated him for over six months before his death. I have made several enquiries to your embassy to locate any of my clients extended relatives but this has proved Unsuccessful.

Before his deat the Ministry of public works Benin (MTPT) is owing him the sum of Ten Million Eight Hundred Thousand United States Dollar) US\$10.800.000 for a contract he executed for the Ministry before his death.

After these several unsuccessful attempts, I decided to track His last name over the Internet, to locate any member of his Family hence I contacted you. I have contacted you to assist in Repatriating this money from the Ministry (MTPT)before the money and property he left

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:

Spam Status: Spamassassin

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, vicgundotrasvp2@carecco.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 Of Directors.

11/05/15
MD Matt Brittin, Office of the Director, Chairman of the Board and Managing Director, Google United Kingdom

Google Incorporation Worldwide
05/11/15 Larry Page
Larry Page Co-Founder & CEO

©2015 Google Inc.

©2015 Google - Terms & Privacy

Sample phishing (4)

SPAM marek@zachara.name:mit

File Edit View Message Settings Help

https://haveibeenpwned.com

Data Enrichment Exposure From PDL Customer: In October 2019, security researchers Vinny Troia and Bob Diachenko identified an unprotected Elasticsearch server holding 1.2 billion records of personal data. The exposed data included an index indicating it was sourced from data enrichment company People Data Labs (PDL) and contained 622 million unique email addresses. The server was not owned by PDL and it's believed a customer failed to properly secure the database. Exposed information included email addresses, phone numbers, social media profiles and job history data.

Compromised data: Email addresses, Employers, Geographic locations, Job titles, Names, Phone numbers, Social media profiles

Exploit.In (unverified): In late 2016, a huge list of email address and password pairs appeared in a "combo list" referred to as "Exploit.In". The list contained 593 million unique email addresses, many with multiple different passwords hacked from various online systems. The list was broadly circulated and used for "credential stuffing", that is attackers employ it in an attempt to identify other online systems where the account owner had reused their password. For detailed background on this incident, read [Password reuse, credential stuffing and another billion records in Have I Been Pwned](#).

Compromised data: Email addresses, Passwords

LinkedIn: In May 2016, LinkedIn had 164 million email addresses and passwords exposed. Originally hacked in 2012, the data remained out of sight until being offered for sale on a dark market site 4 years later. The passwords in the breach were stored as SHA1 hashes without salt, the vast majority of which were quickly cracked in the days following the release of the data.

Compromised data: Email addresses, Passwords

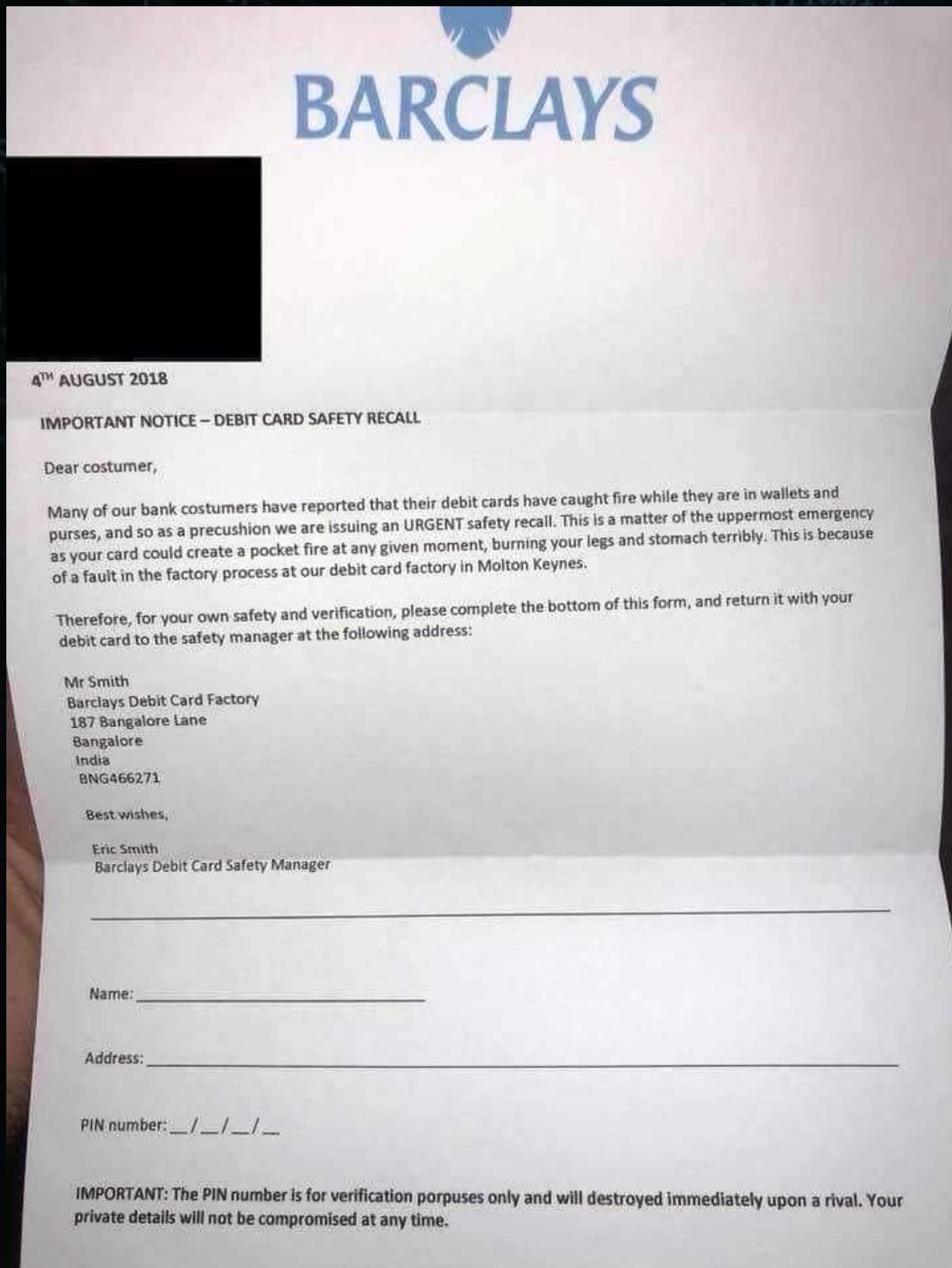
A phishing site

The image shows a desktop environment with multiple windows open, illustrating a phishing attack. The background features a dark theme with a faint watermark of binary code. In the foreground, there are four distinct windows:

- Top Left Window:** A 'Kontakt' application window with a standard menu bar: File, Edit, View, Message, Settings, Help.
- Second Window:** A Mozilla Firefox browser window titled 'Serwis internetowy iPKO - Mozilla Firefox'. It displays a login form for 'cooperativenserviceproviders.nl' with fields for 'Numer telefonu' and 'Podaj kod nr' (with a placeholder '04').
- Third Window:** Another Mozilla Firefox browser window titled 'Serwis internetowy iPKO - Mozilla Firefox'. It also displays a login form for 'cooperativenserviceproviders.nl' with similar fields.
- Fourth Window:** A third Mozilla Firefox browser window titled 'Serwis internetowy iPKO - Mozilla Firefox'. This one displays a login form for 'cooperativevserviceproviders.nl'.

All three iPKO-like windows appear to be phishing attempts, as they lack legitimate branding and contain placeholder text where actual user input would be expected.

Phishing variation



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:

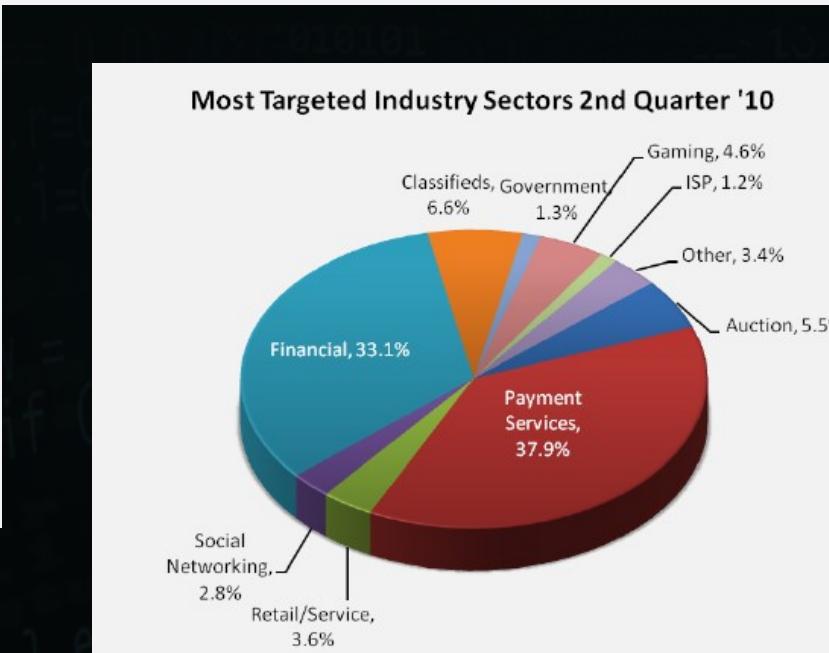
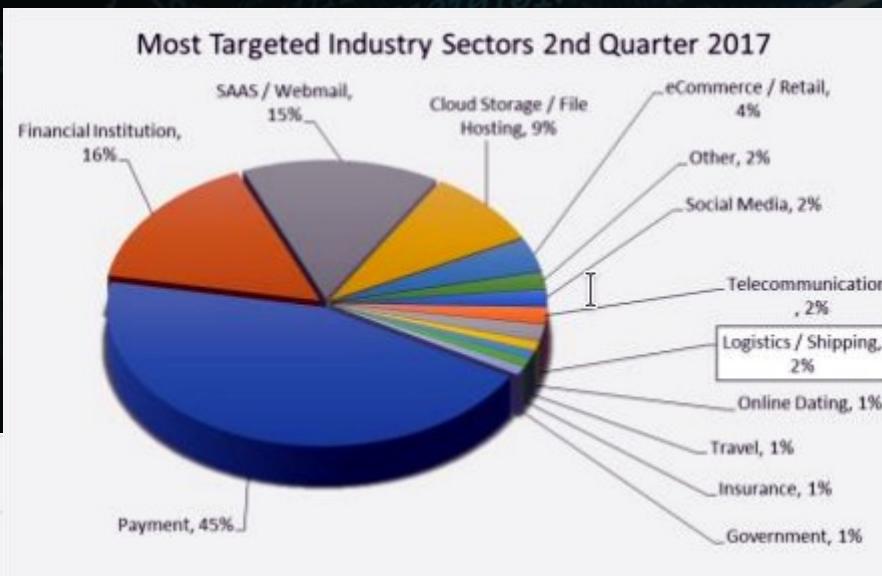
*E-mail Password:

*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



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."*

A bait

- Various data storage units (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 control 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



Published
under the
following
license:

Creative
Commons
Attribution
Share-Alike