Human Factors & Usability

Special Topic: Practical Computer Security

CSCI-GA.3033-019

Human Factor & Usability

- Fact: more real attacks target users.
- Exploiting human vulnerabilities rather than technical ones.

> “... the human side of computer security is easily exploited and constantly overlooked. Companies spend millions of dollars on firewalls, encryption and secure access devices, and it’s money wasted, because none of these measures address the weakest link in the security chain.”
>
> - Kevin Mitnick

The Principle of Psychological Acceptability

“ It is essential that the human interface be designed for **ease of use**,
so that users routinely and automatically
apply the protection mechanisms correctly.

Also, to the extent that the user's mental image of his protection goals matches the mechanisms he must use, mistakes will be minimized.

If he must translate his image of his protection needs into a radically different specification language, he will make errors.”

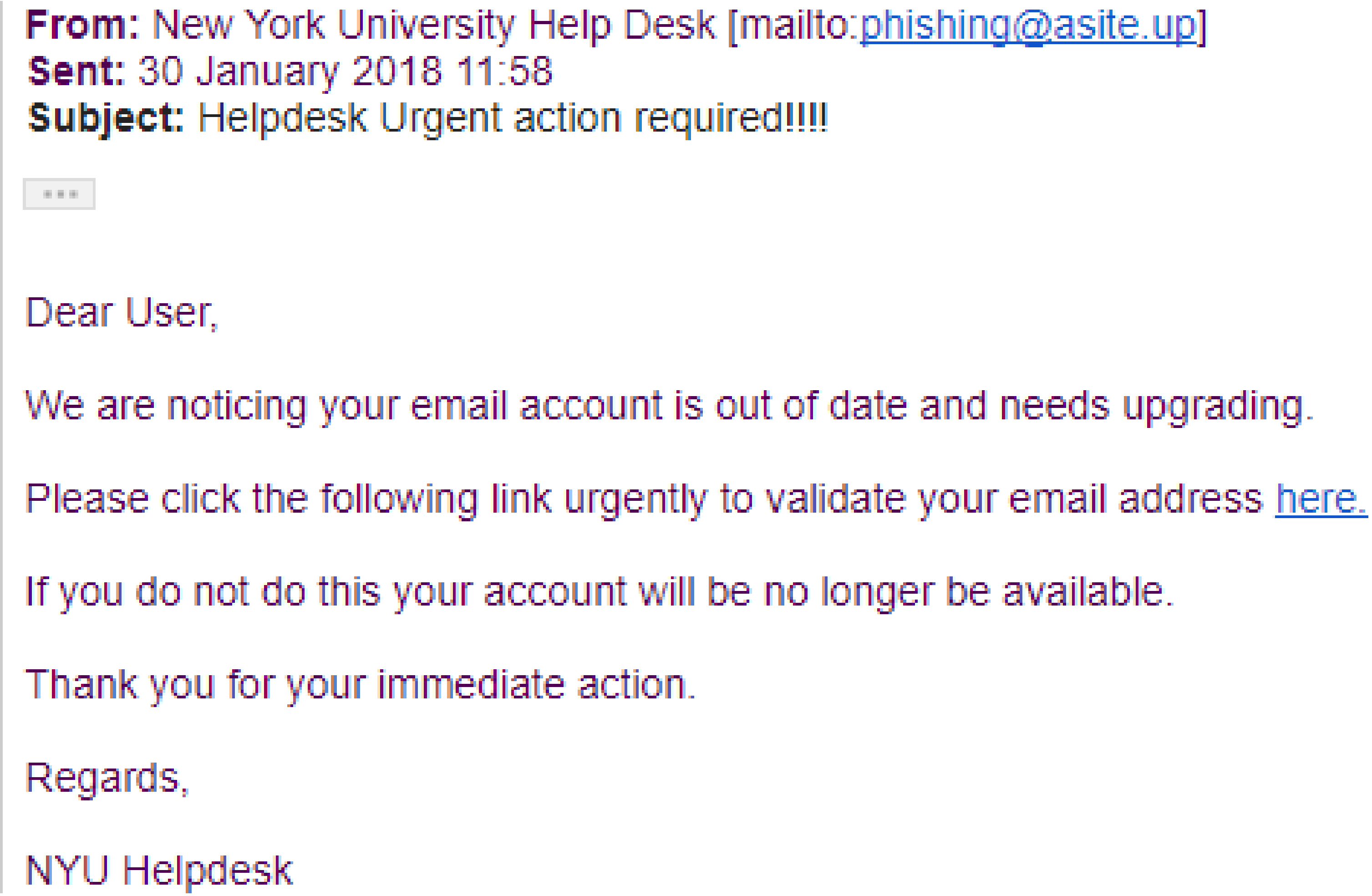
-- Saltzer and Schroeder

Phishing

- Social engineering that trick users for malicious intent
  - Get user to visit a bad website that ‘looks’ like a real website
  - Trick the user into
    - disclosing personal/financial information
    - Installing/downloading a malware
  - Types: spear phishing, whaling

- Delivery Method
  - **Spam Email**
  - Social Media
  - Sponsored advertisements
  - Network-based attack : DNS Spoofing, ARP Spoofing

How to detect phishing emails?



From: New York University Help Desk [mailto:phishing@asite.up]
Sent: 30 January 2018 11:58
Subject: Helpdesk Urgent action required!!!!

Dear User,

We are noticing your email account is out of date and needs upgrading.

Please click the following link urgently to validate your email address here.

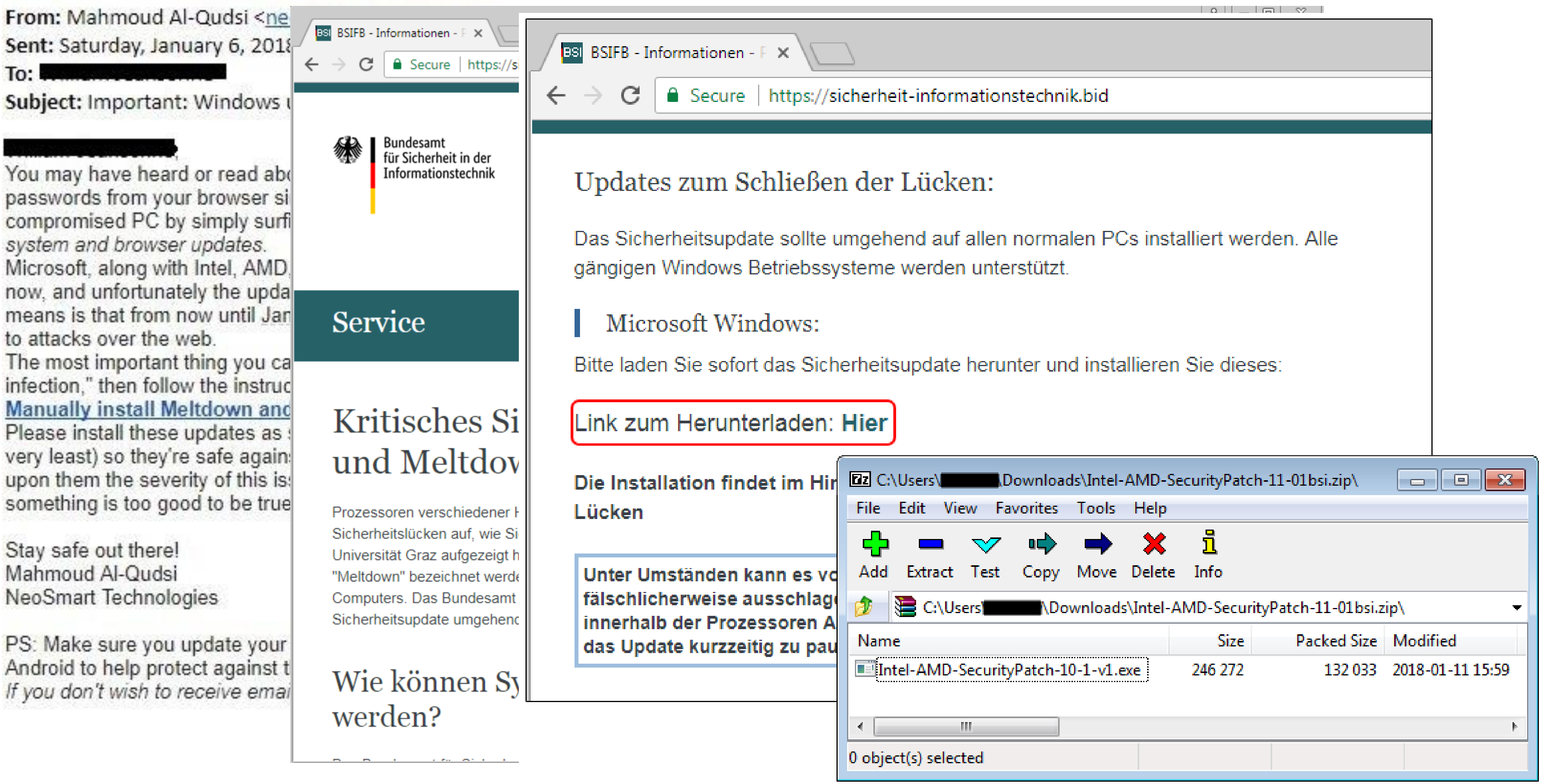
If you do not do this your account will be no longer be available.

Thank you for your immediate action.

Regards,

NYU Helpdesk

Example: Fake Meltdown And Spectre Patch Phishing Emails



From: Mahmoud Al-Qudsi <ne
Sent: Saturday, January 6, 201
To: [redacted]
Subject: Important: Windows

[redacted]

You may have heard or read ab
passwords from your browser si
compromised PC by simply surfi
system and browser updates.
Microsoft, along with Intel, AMD
now, and unfortunately the upda
means is that from now until Jan
to attacks over the web.
The most important thing you ca
infection," then follow the instruc
Manually install Meltdown and
Please install these updates as
very least) so they're safe agai
upon them the severity of this is
something is too good to be true

Stay safe out there!
Mahmoud Al-Qudsi
NeoSmart Technologies

PS: Make sure you update your
Android to help protect against t
If you don't wish to receive emai

Bundesamt
für Sicherheit in der
Informationstechnik

Service

Kritisches Si
und Meltdov

Prozessoren verschiedener H
Sicherheitslücken auf, wie Si
Universität Graz aufgezeigt h
"Meltdown" bezeichnet werde
Computers. Das Bundesamt
Sicherheitsupdate umgehend

Wie können Sy
werden?

BSIFB - Informationen - F ×
Secure | https://sicherheit-informationstechnik.bid

Updates zum Schließen der Lücken:

Das Sicherheitsupdate sollte umgehend auf allen normalen PCs installiert werden. Alle gängigen Windows Betriebssysteme werden unterstützt.

Microsoft Windows:

Bitte laden Sie sofort das Sicherheitsupdate herunter und installieren Sie dieses:

Link zum Herunterladen: **Hier**

**Die Installation findet im Hir
Lücken**

**Unter Umständen kann es vo
fälschlicherweise ausschlag
innerhalb der Prozessoren A
das Update kurzzeitig zu pau**

C:\Users\[redacted]Downloads\Intel-AMD-SecurityPatch-11-01bsi.zip\

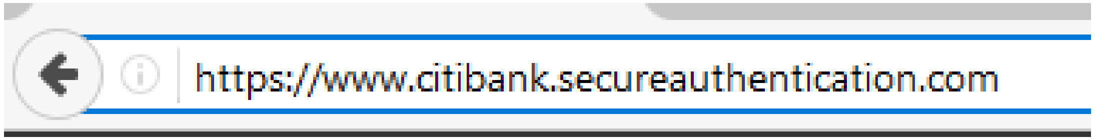
C:\Users\[redacted]\Downloads\Intel-AMD-SecurityPatch-11-01bsi.zip\

Name	Size	Packed Size	Modified
Intel-AMD-SecurityPatch-10-1-v1.exe	246 272	132 033	2018-01-11 15:59

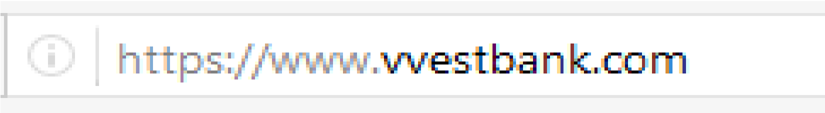
0 object(s) selected

Phishing Email

- Email attachment contains infected file
  - Trick into installing malware on the system
- Contains link to a website
  - Download and install malware (drive-by/with consent)
  - Give away personal/sensitive information

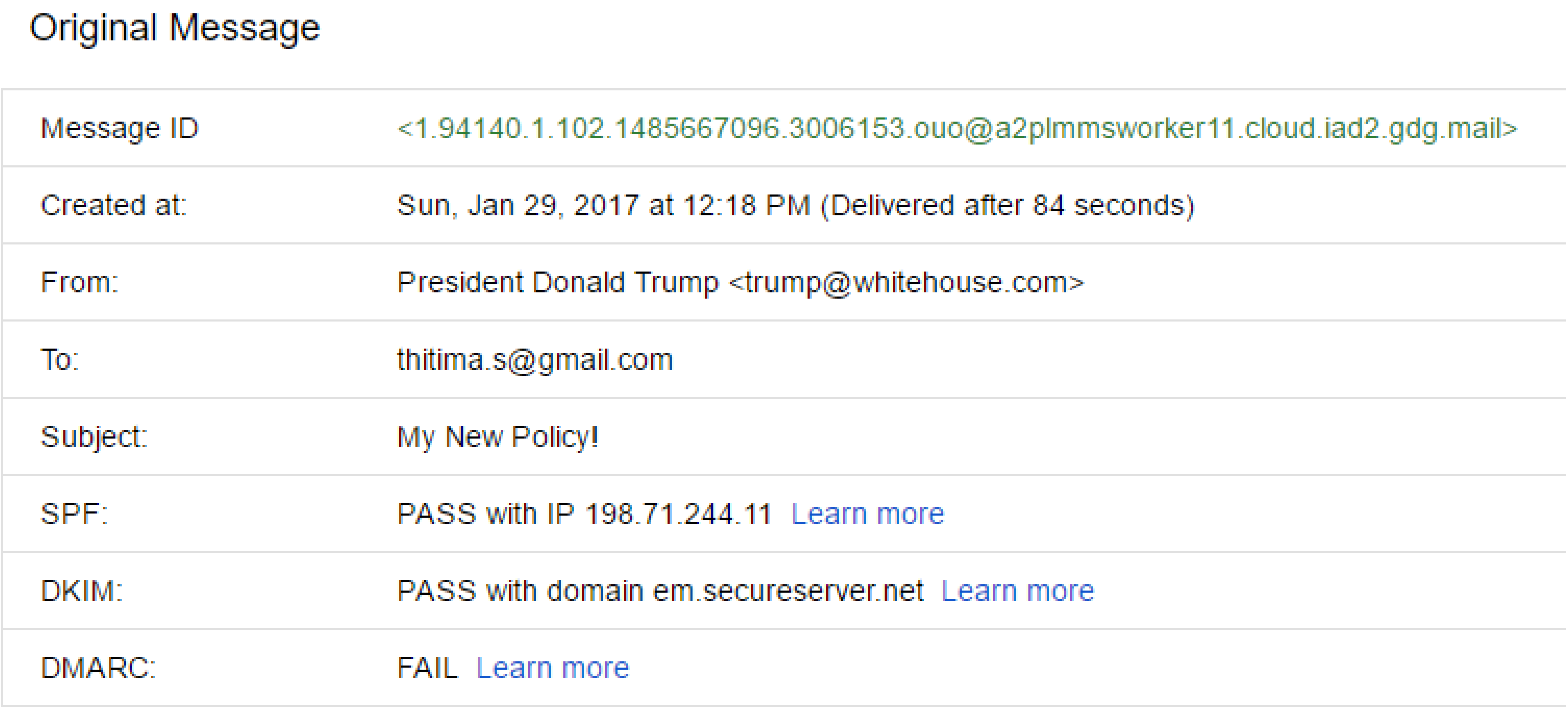


https://www.citibank.secureauthentication.com



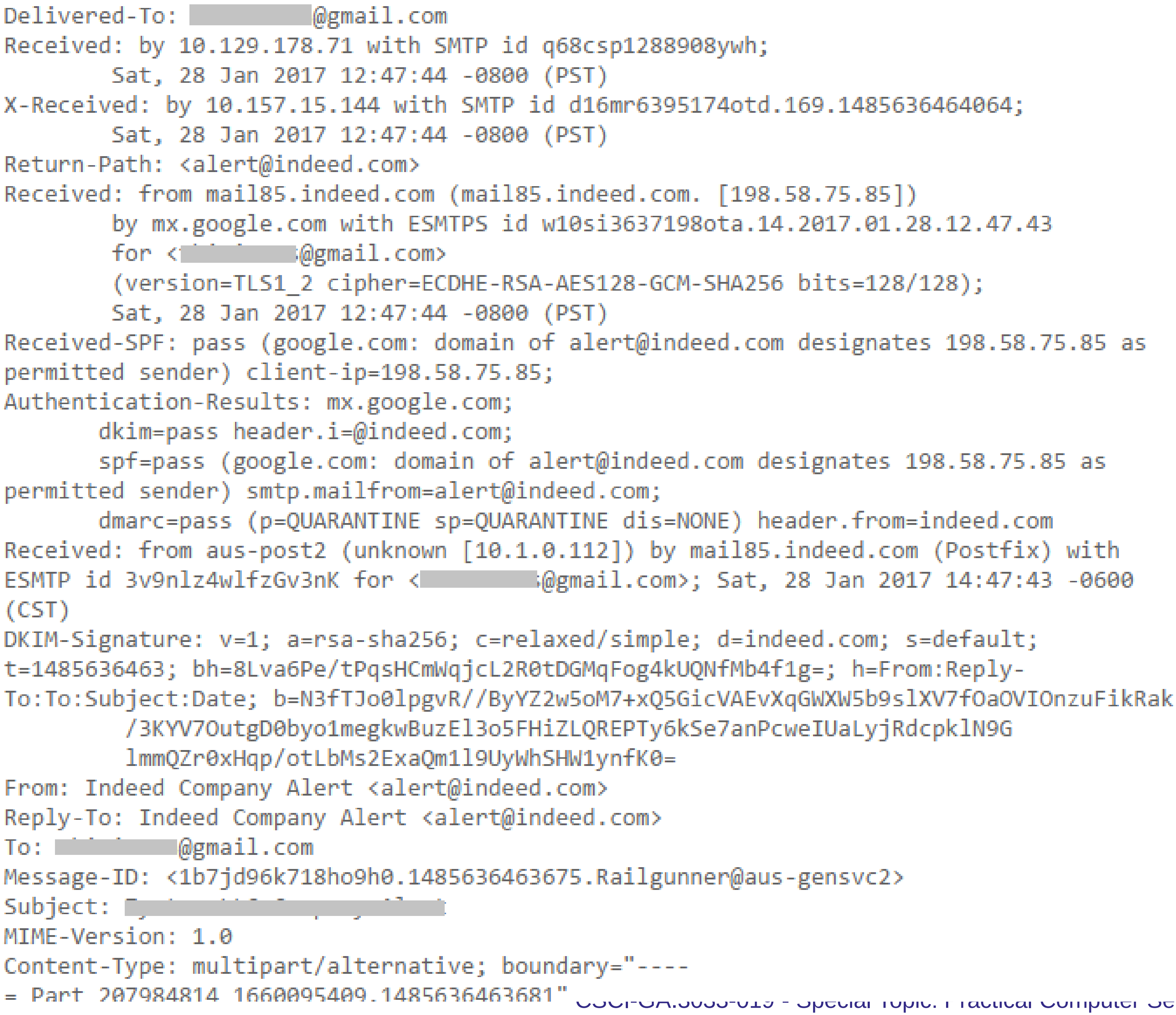
https://www.vvestbank.com

- Dropbox/Google Docs Phishing



Original Message

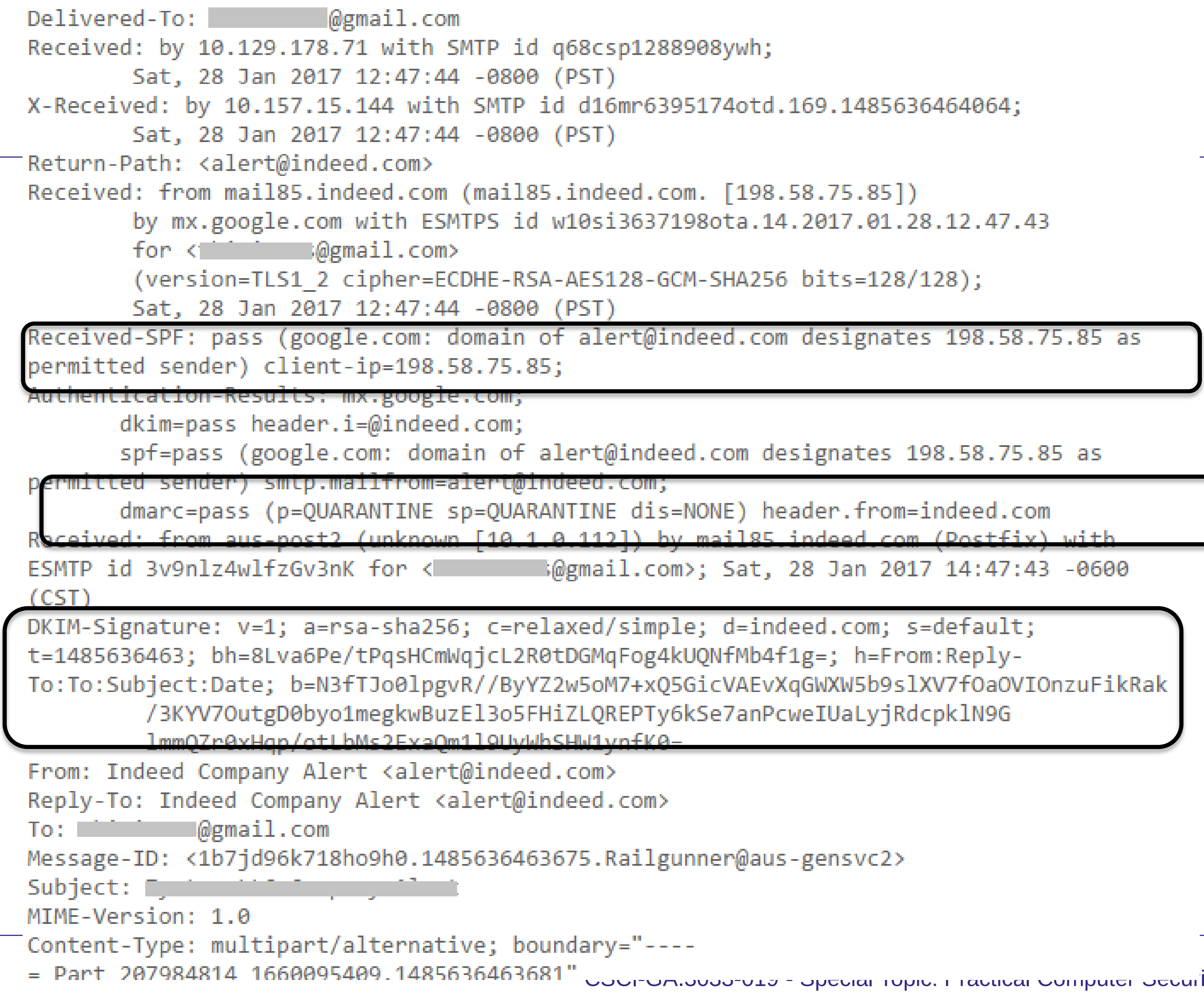
Message ID	<1.94140.1.102.1485667096.3006153.ouo@a2plmmsworker11.cloud.iad2.gdg.mail>
Created at:	Sun, Jan 29, 2017 at 12:18 PM (Delivered after 84 seconds)
From:	President Donald Trump <trump@whitehouse.com>
To:	thitima.s@gmail.com
Subject:	My New Policy!
SPF:	PASS with IP 198.71.244.11 Learn more
DKIM:	PASS with domain em.secureserver.net Learn more
DMARC:	FAIL Learn more



```
Delivered-To: [redacted]@gmail.com
Received: by 10.129.178.71 with SMTP id q68csp1288908ywh;
        Sat, 28 Jan 2017 12:47:44 -0800 (PST)
X-Received: by 10.157.15.144 with SMTP id d16mr6395174otd.169.1485636464064;
        Sat, 28 Jan 2017 12:47:44 -0800 (PST)
Return-Path: <alert@indeed.com>
Received: from mail85.indeed.com (mail85.indeed.com. [198.58.75.85])
        by mx.google.com with ESMTPS id w10si3637198ota.14.2017.01.28.12.47.43
        for <[redacted]@gmail.com>
        (version=TLS1_2 cipher=ECDHE-RSA-AES128-GCM-SHA256 bits=128/128);
        Sat, 28 Jan 2017 12:47:44 -0800 (PST)
Received-SPF: pass (google.com: domain of alert@indeed.com designates 198.58.75.85 as
permitted sender) client-ip=198.58.75.85;
Authentication-Results: mx.google.com;
       dkim=pass header.i=@indeed.com;
       spf=pass (google.com: domain of alert@indeed.com designates 198.58.75.85 as
permitted sender) smtp.mailfrom=alert@indeed.com;
       dmarc=pass (p=QUARANTINE sp=QUARANTINE dis=NONE) header.from=indeed.com
Received: from aus-post2 (unknown [10.1.0.112]) by mail85.indeed.com (Postfix) with
ESMTP id 3v9nlz4wlfzGv3nK for <[redacted]@gmail.com>; Sat, 28 Jan 2017 14:47:43 -0600
(CST)
DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/simple; d=indeed.com; s=default;
t=1485636463; bh=8Lva6Pe/tPqsHCmWqjcL2R0tDGMqFog4kUQNfMb4f1g=; h=From:Reply-
To:To:Subject:Date; b=N3fTJo0lpgvR//ByYZ2w5oM7+xQ5GicVAEvXqGWXW5b9slXV7fOaOVIOnzuFikRak
         /3KYV7OutgD0byo1megkwBuzEl3o5FHiZLQREPTy6kSe7anPcweIUaLyjRdcpklN9G
         lmmQZr0xHqp/otLbMs2ExaQm1l9UyWhSHW1ynfK0=
From: Indeed Company Alert <alert@indeed.com>
Reply-To: Indeed Company Alert <alert@indeed.com>
To: [redacted]@gmail.com
Message-ID: <1b7jd96k718ho9h0.1485636463675.Railgunner@aus-gensvc2>
Subject: [redacted]
MIME-Version: 1.0
Content-Type: multipart/alternative; boundary="----
=_Part_207984814_1660095409.1485636463681"
```

Spam Email Issues

- Sender address forgery
  - SPF (path-based), DKIM (signature-based)
  - DMARC



```
Delivered-To: [redacted]@gmail.com
Received: by 10.129.178.71 with SMTP id q68csp1288908ywh;
        Sat, 28 Jan 2017 12:47:44 -0800 (PST)
X-Received: by 10.157.15.144 with SMTP id d16mr6395174otd.169.1485636464064;
        Sat, 28 Jan 2017 12:47:44 -0800 (PST)
Return-Path: <alert@indeed.com>
Received: from mail85.indeed.com (mail85.indeed.com. [198.58.75.85])
        by mx.google.com with ESMTPS id w10si3637198ota.14.2017.01.28.12.47.43
        for <[redacted]@gmail.com>
        (version=TLS1_2 cipher=ECDHE-RSA-AES128-GCM-SHA256 bits=128/128);
        Sat, 28 Jan 2017 12:47:44 -0800 (PST)
Received-SPF: pass (google.com: domain of alert@indeed.com designates 198.58.75.85 as
permitted sender) client-ip=198.58.75.85;
Authentication-Results: mx.google.com;
       dkim=pass header.i=@indeed.com;
       spf=pass (google.com: domain of alert@indeed.com designates 198.58.75.85 as
permitted sender) smtp.mailfrom=alert@indeed.com;
       dmarc=pass (p=QUARANTINE sp=QUARANTINE dis=NONE) header.from=indeed.com
Received: from aus-post2 (unknown [10.1.0.112]) by mail85.indeed.com (Postfix) with
ESMTP id 3v9nlz4wlfzGv3nK for <[redacted]@gmail.com>; Sat, 28 Jan 2017 14:47:43 -0600
(CST)
DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/simple; d=indeed.com; s=default;
t=1485636463; bh=8Lva6Pe/tPqsHCmWqjcL2R0tDGMqFog4kUQNfMb4f1g=; h=From:Reply-
To:To:Subject:Date; b=N3fTJo0lpgvR//ByYZ2w5oM7+xQ5GicVAEvXqGWXW5b9slXV7fOaOVIOnzuFikRak
         /3KYV7OutgD0byo1megkwBuzEl3o5FHiZLQREPTy6kSe7anPcweIUaLyjRdcpklN9G
         1mmQZr0xHqp/otLbMs2ExaQm1l9UyWhSHW1ynfK0=
From: Indeed Company Alert <alert@indeed.com>
Reply-To: Indeed Company Alert <alert@indeed.com>
To: [redacted]@gmail.com
Message-ID: <1b7jd96k718ho9h0.1485636463675.Railgunner@aus-gensvc2>
Subject: [redacted]
MIME-Version: 1.0
Content-Type: multipart/alternative; boundary="----
=_Part_207984814_1660095409.1485636463681"
```

Spam Email Issues

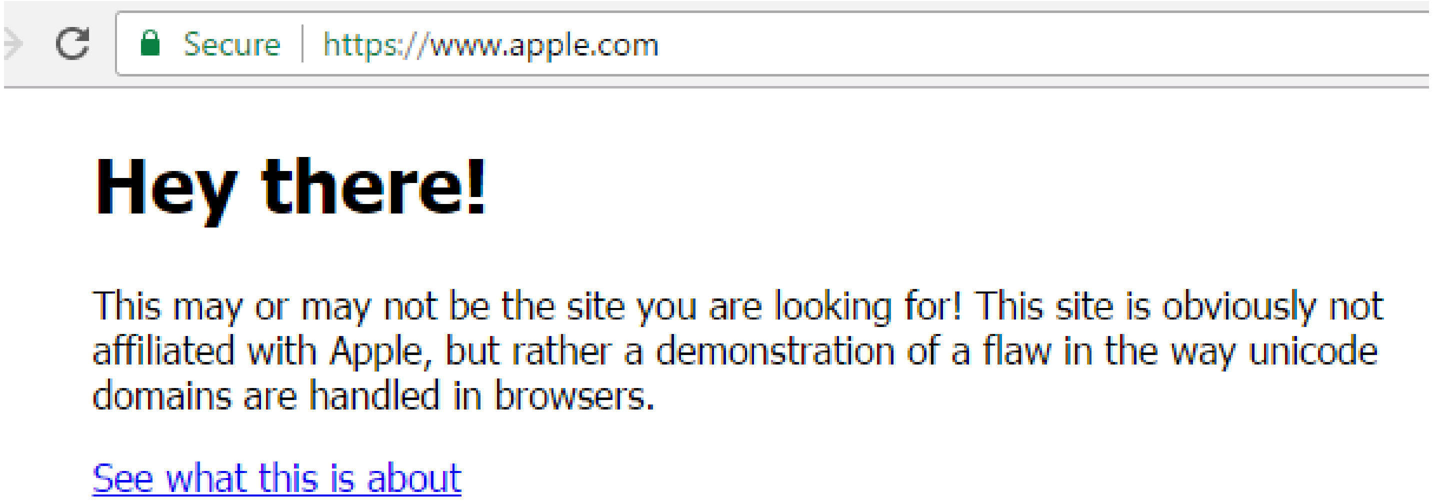
- Sender address forgery
  - SPF (path-based), DKIM (signature-based)
  - DMARC
- But…
  - bob@facebook.com for ceo@facebook.com
  - @microsoft.com vs. @micorsoft.com
  - Sender from your address book
  - Spear phishing attack

Obscuring URL

www.myvulnerable.site

- Short URL - http://goo.gl/PPc7QD
- IP Address - http://69.195.124.154
- DWORD formatted IP Address - http://1170439322
- Hex form –
  http://%6d%79%76%75%6c%6e%65%72%61%62%6c%65%73%69%74%65%2e%63%6f%6d
- Redirecting a URL –
  - https://www.google.com/url?sa=i&url=http://69.195.124.154
- Oddly-formatted Address
  - http://www.paypal.com@1170439322
- ‘Lookalike’ domain name
  - Latin ”a” is replaced with the Cyrillic ”a” -> (U+0430) instead of (U+0061)
  - Homograph attacks

Punycode Phishing Attacks



Secure | https://www.apple.com

Hey there!

This may or may not be the site you are looking for! This site is obviously not affiliated with Apple, but rather a demonstration of a flaw in the way unicode domains are handled in browsers.

See what this is about

xn--80ak6aa92e.com

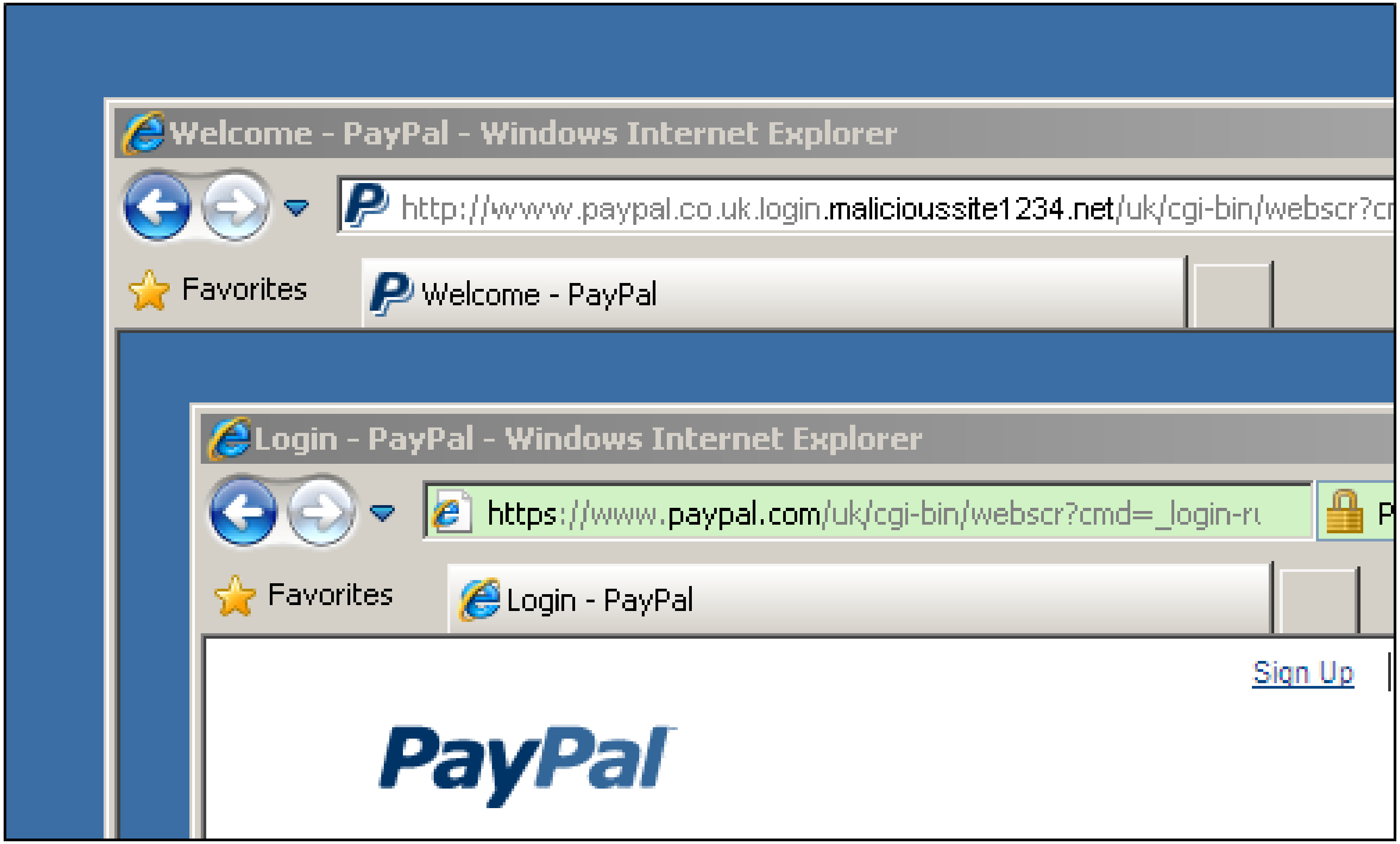
↓

apple.com

- Cyrillic "a" (U+0430) and Latin "a" (U+0041) both are treated different by browsers but are displayed "a" in the browser address.

Ref: https://www.xudongz.com/blog/2017/idn-phishing/

Picture-in-picture attack



Welcome - PayPal - Windows Internet Explorer

http://www.paypal.co.uk.login.malicioussite1234.net/uk/cgi-bin/webscr?cr

Login - PayPal - Windows Internet Explorer

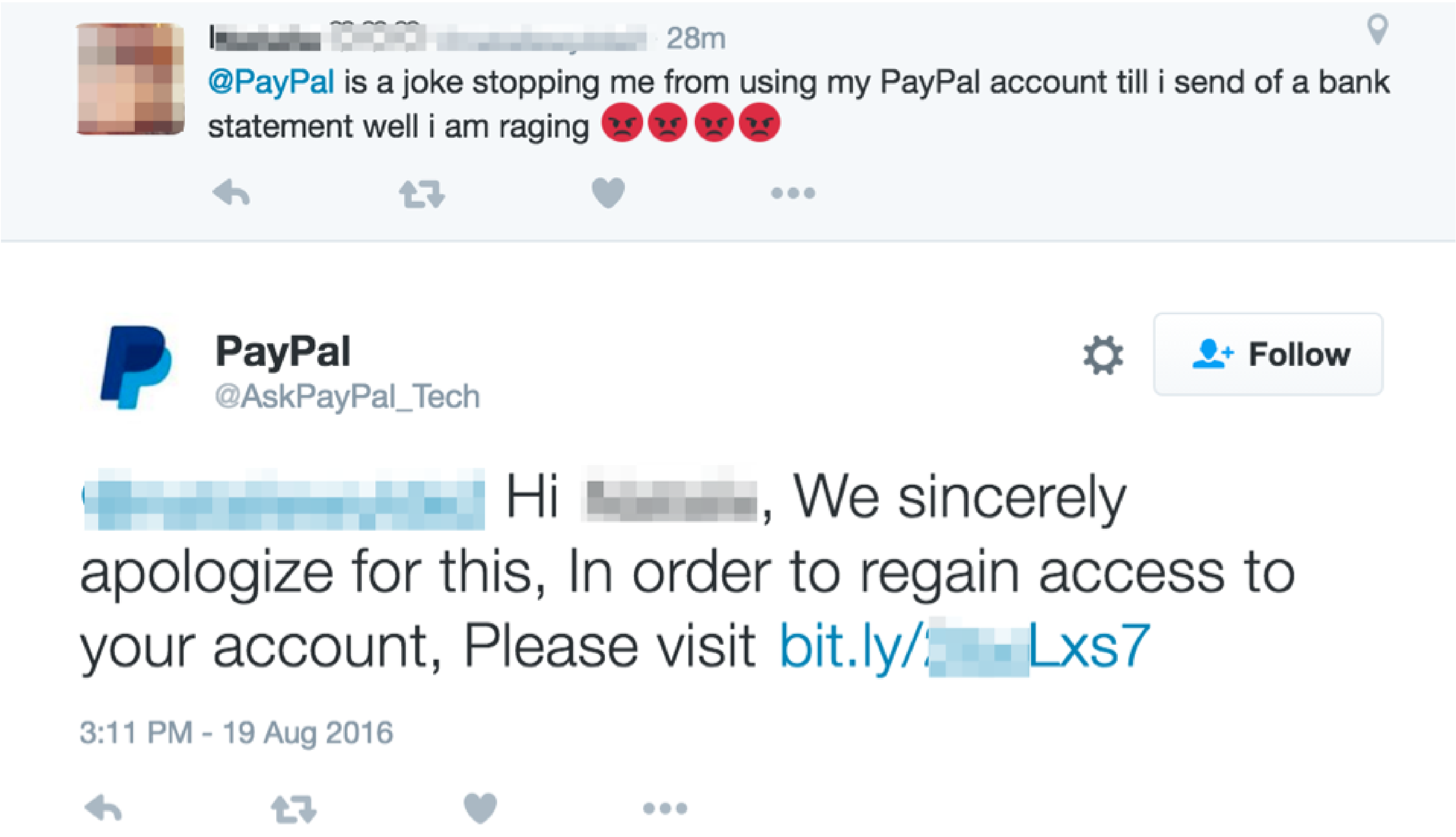
https://www.paypal.com/uk/cgi-bin/webscr?cmd=_login-ru

Phishing

- Social engineering that trick users for malicious intent
  - Get user to visit a bad website that ‘looks’ like a real website
  - Trick the user into
    - disclosing personal/financial information
    - Installing/downloading a malware

- Delivery Method
  - Spam Email
  - **Social Media**
  - Sponsored advertisements
  - Network-based attack: DNS Spoofing, ARP Spoofing

Social Media-based Phishing



[redacted] 28m

@PayPal is a joke stopping me from using my PayPal account till i send of a bank statement well i am raging 😡😡😡😡

PayPal
@AskPayPal_Tech

[redacted] Hi [redacted], We sincerely apologize for this, In order to regain access to your account, Please visit bit.ly/[redacted]Lxs7

3:11 PM - 19 Aug 2016

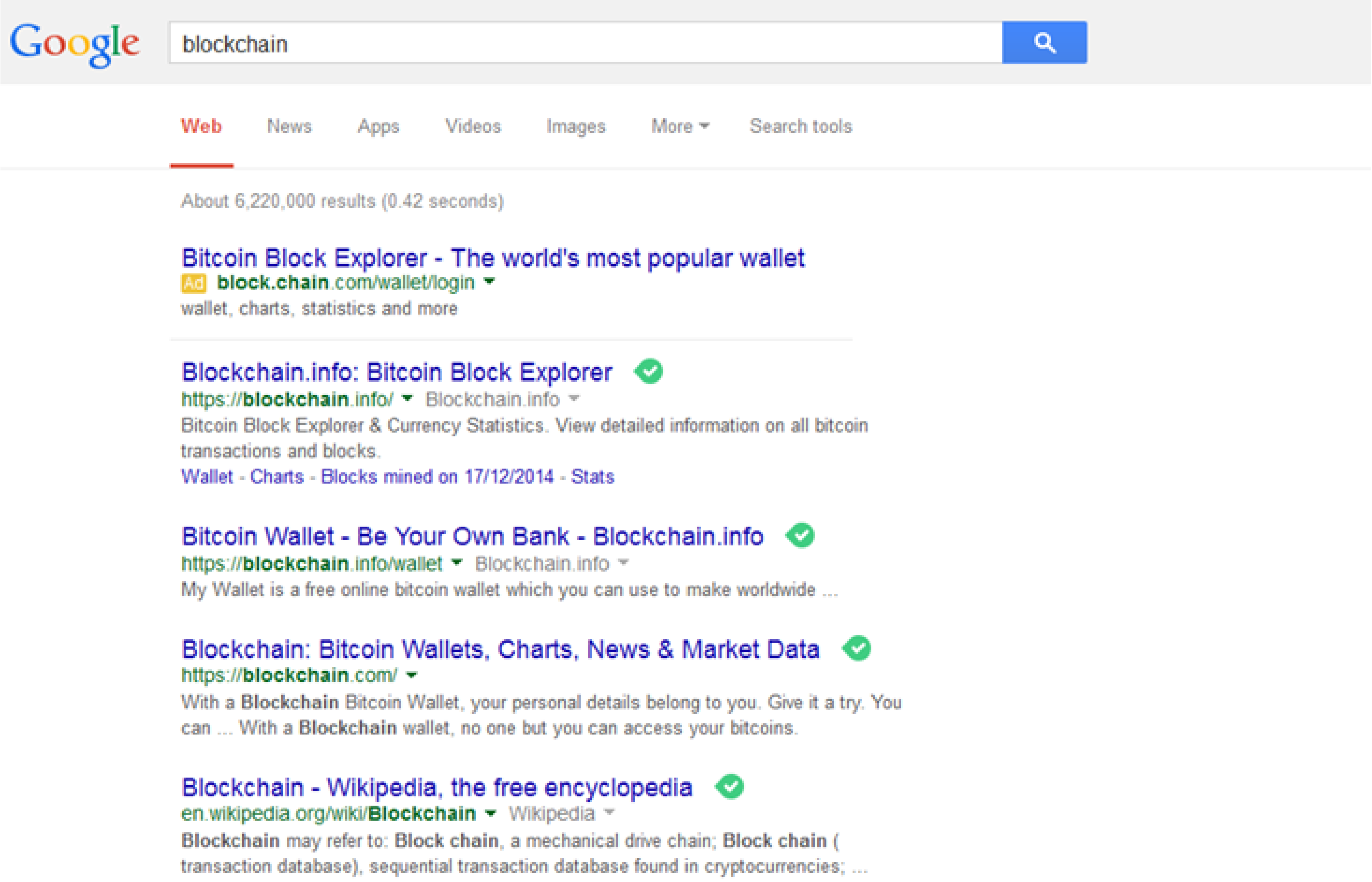
Image Souce: https://www.proofpoint.com/us/threat-insight/post/fraudulent-social-media-accounts-continue-phish-banking-credentials

Phishing

- Social engineering that trick users for malicious intent
  - Get user to visit a bad website that ‘looks’ like a real website
  - Trick the user into
    - disclosing personal/financial information
    - Installing/downloading a malware

- Delivery Method
  - Spam Email
  - Social Media
  - **Sponsored advertisements**
  - Network-based attack: DNS Spoofing, ARP Spoofing

Sponsored ads



About 6,220,000 results (0.42 seconds)

Bitcoin Block Explorer - The world's most popular wallet
Ad **block.chain**.com/wallet/login
wallet, charts, statistics and more

Blockchain.info: Bitcoin Block Explorer ✓
https://**blockchain**.info/ Blockchain.info
Bitcoin Block Explorer & Currency Statistics. View detailed information on all bitcoin transactions and blocks.
Wallet - Charts - Blocks mined on 17/12/2014 - Stats

Bitcoin Wallet - Be Your Own Bank - Blockchain.info ✓
https://**blockchain**.info/wallet Blockchain.info
My Wallet is a free online bitcoin wallet which you can use to make worldwide ...

Blockchain: Bitcoin Wallets, Charts, News & Market Data ✓
https://**blockchain**.com/
With a **Blockchain** Bitcoin Wallet, your personal details belong to you. Give it a try. You can ... With a **Blockchain** wallet, no one but you can access your bitcoins.

Blockchain - Wikipedia, the free encyclopedia ✓
en.wikipedia.org/wiki/**Blockchain** Wikipedia
Blockchain may refer to: **Block chain**, a mechanical drive chain; **Block chain** (transaction database), sequential transaction database found in cryptocurrencies; ...

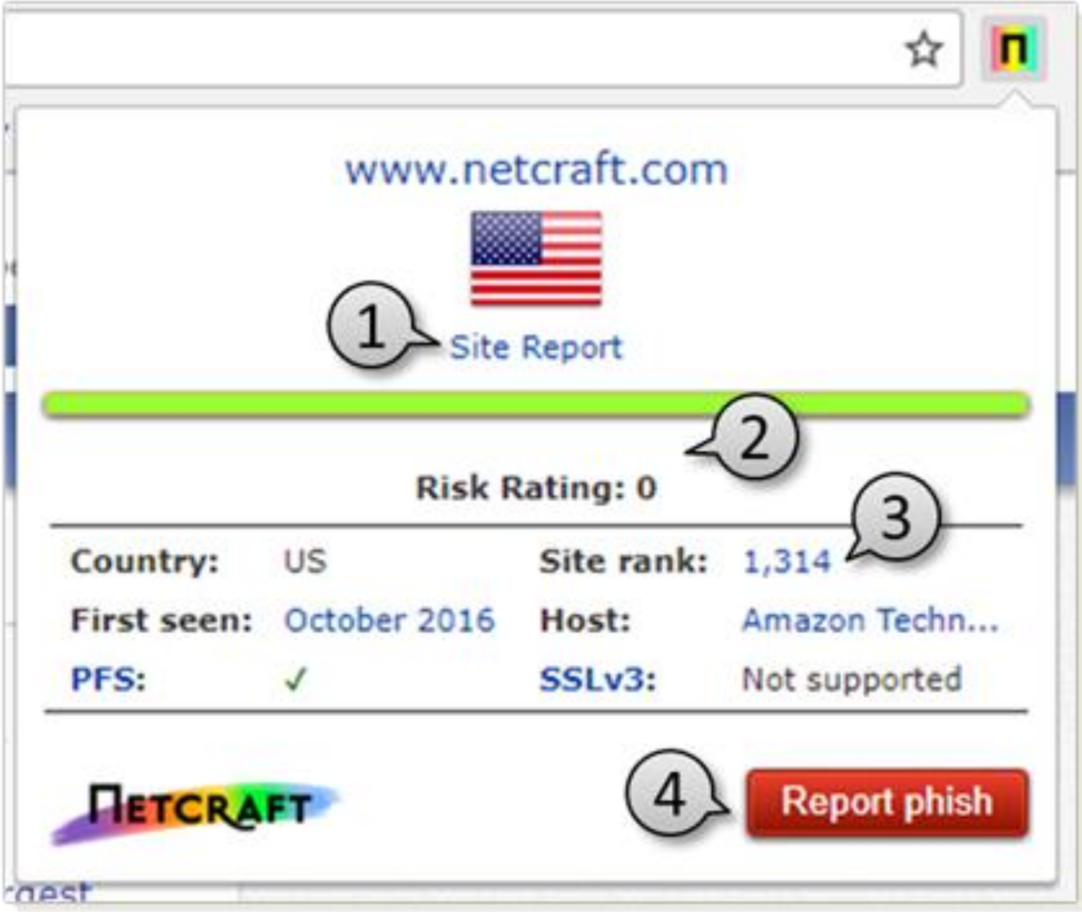
Phishing

- Social engineering that trick users for malicious intent
  - Get user to visit a bad website that ‘looks’ like a real website
  - Trick the user into
    - disclosing personal/financial information
    - Installing/downloading a malware

- Delivery Method
  - Spam Email
  - Social Media
  - Sponsored advertisements
  - **Network-based attack: DNS Spoofing, ARP Spoofing**

Phishing Countermeasures

- Phishing Alert Toolbars
- Password Management Tool
- Two-factor Authentication
- Security Awareness Program/Training

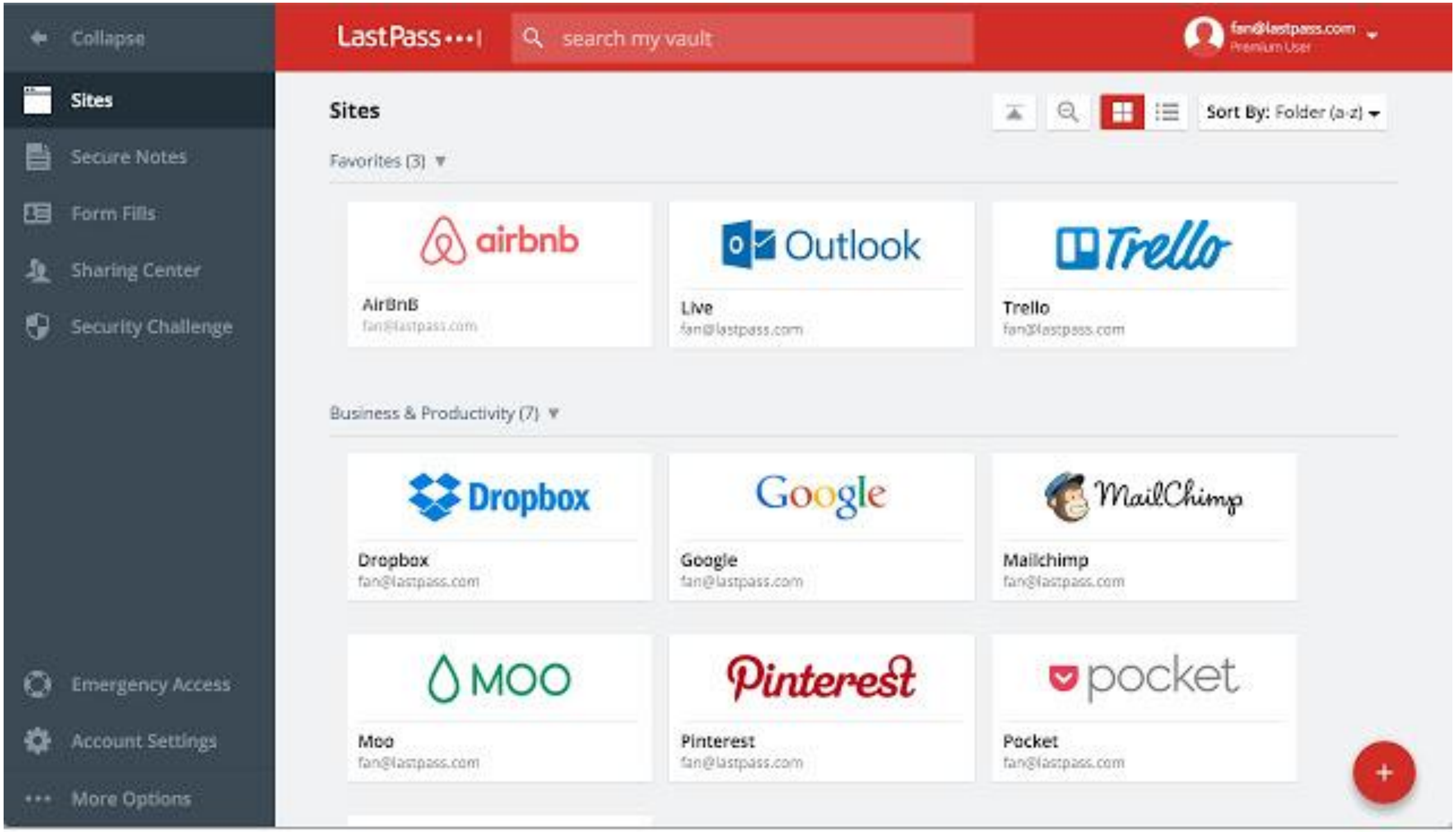


www.netcraft.com

Site Report

Risk Rating: 0

Country:	US	Site rank:	1,314
First seen:	October 2016	Host:	Amazon Techn...
PFS:	✓	SSLv3:	Not supported



Sites

Sort By: Folder (a-z)

Favorites (3)

AirBnB
fan@lastpass.com

Live
fan@lastpass.com

Trello
fan@lastpass.com

Business & Productivity (7)

Dropbox
fan@lastpass.com

Google
fan@lastpass.com

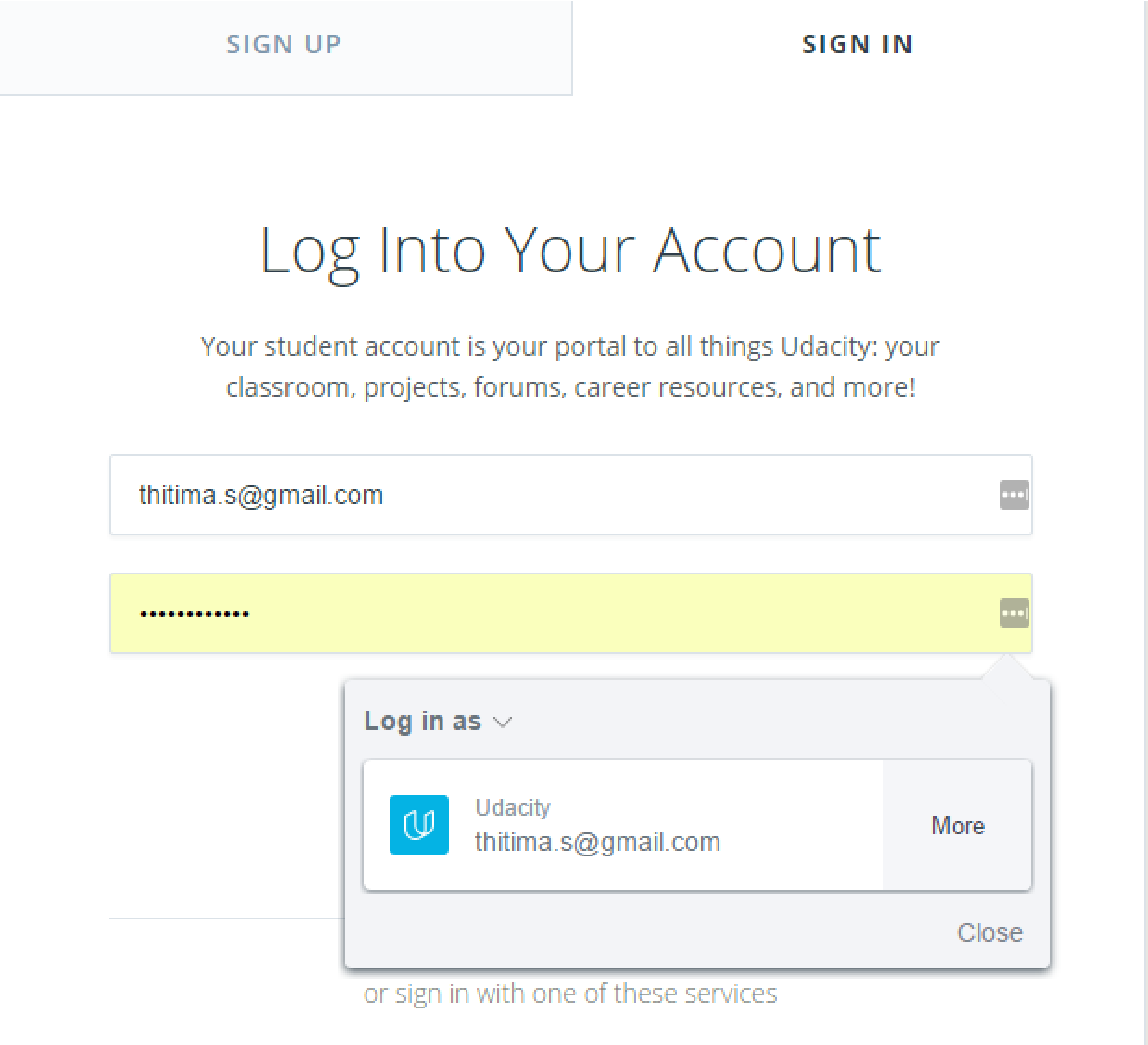
Mailchimp
fan@lastpass.com

Moo
fan@lastpass.com

Pinterest
fan@lastpass.com

Pocket
fan@lastpass.com

All your passwords, in a secure vault.



Log Into Your Account

Your student account is your portal to all things Udacity: your classroom, projects, forums, career resources, and more!

thitima.s@gmail.com

•••••••••••••

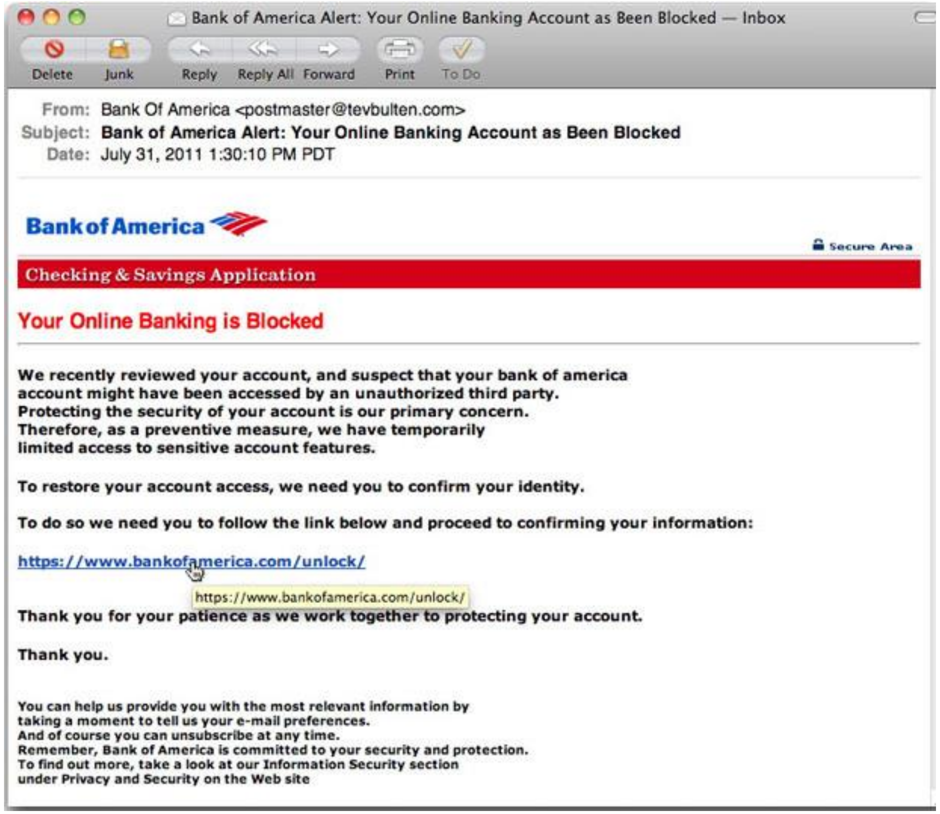
Log in as

Udacity
thitima.s@gmail.com

or sign in with one of these services

Why Phishing Works?

Phishing Email


Bank of America Alert: Your Online Banking Account as Been Blocked — Inbox
Delete
Junk
Reply
Reply All
Forward
Print
To Do
Secure Area
https://www.bankofamerica.com/unlock/

From: Bank Of America <postmaster@tevbulten.com>
Subject: **Bank of America Alert: Your Online Banking Account as Been Blocked**
Date: July 31, 2011 1:30:10 PM PDT

Bank of America

Checking & Savings Application

Your Online Banking is Blocked

We recently reviewed your account, and suspect that your bank of america account might have been accessed by an unauthorized third party. Protecting the security of your account is our primary concern. Therefore, as a preventive measure, we have temporarily limited access to sensitive account features.

To restore your account access, we need you to confirm your identity.

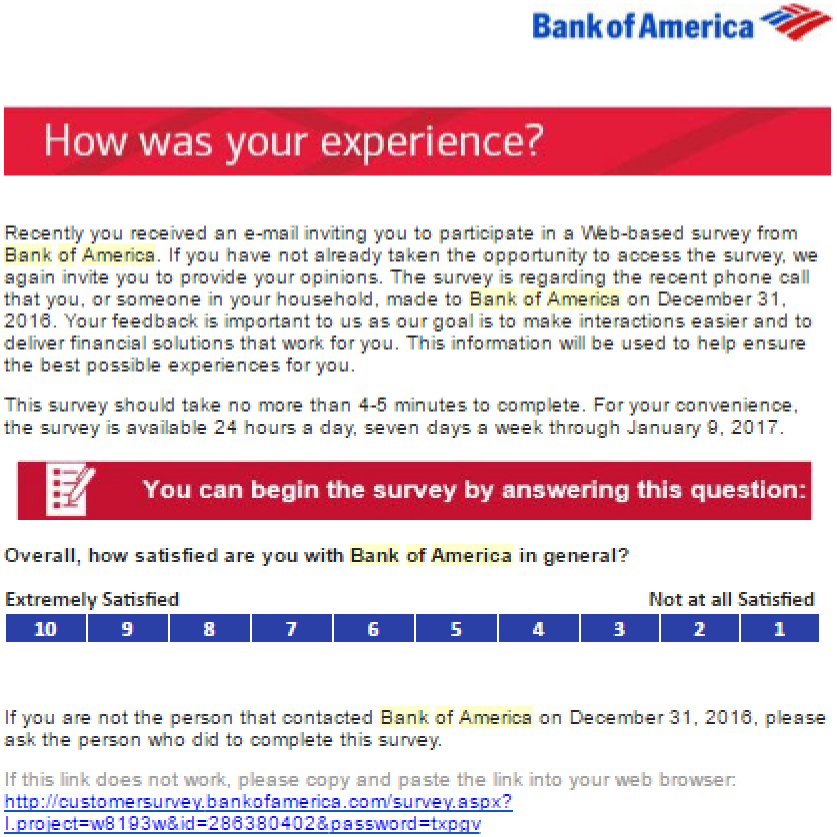
To do so we need you to follow the link below and proceed to confirming your information:

https://www.bankofamerica.com/unlock/

Thank you for your patience as we work together to protecting your account.

Thank you.

You can help us provide you with the most relevant information by taking a moment to tell us your e-mail preferences. And of course you can unsubscribe at any time. Remember, Bank of America is committed to your security and protection. To find out more, take a look at our Information Security section under Privacy and Security on the Web site



Bank of America

How was your experience?

Recently you received an e-mail inviting you to participate in a Web-based survey from Bank of America. If you have not already taken the opportunity to access the survey, we again invite you to provide your opinions. The survey is regarding the recent phone call that you, or someone in your household, made to Bank of America on December 31, 2016. Your feedback is important to us as our goal is to make interactions easier and to deliver financial solutions that work for you. This information will be used to help ensure the best possible experiences for you.

This survey should take no more than 4-5 minutes to complete. For your convenience, the survey is available 24 hours a day, seven days a week through January 9, 2017.

You can begin the survey by answering this question:

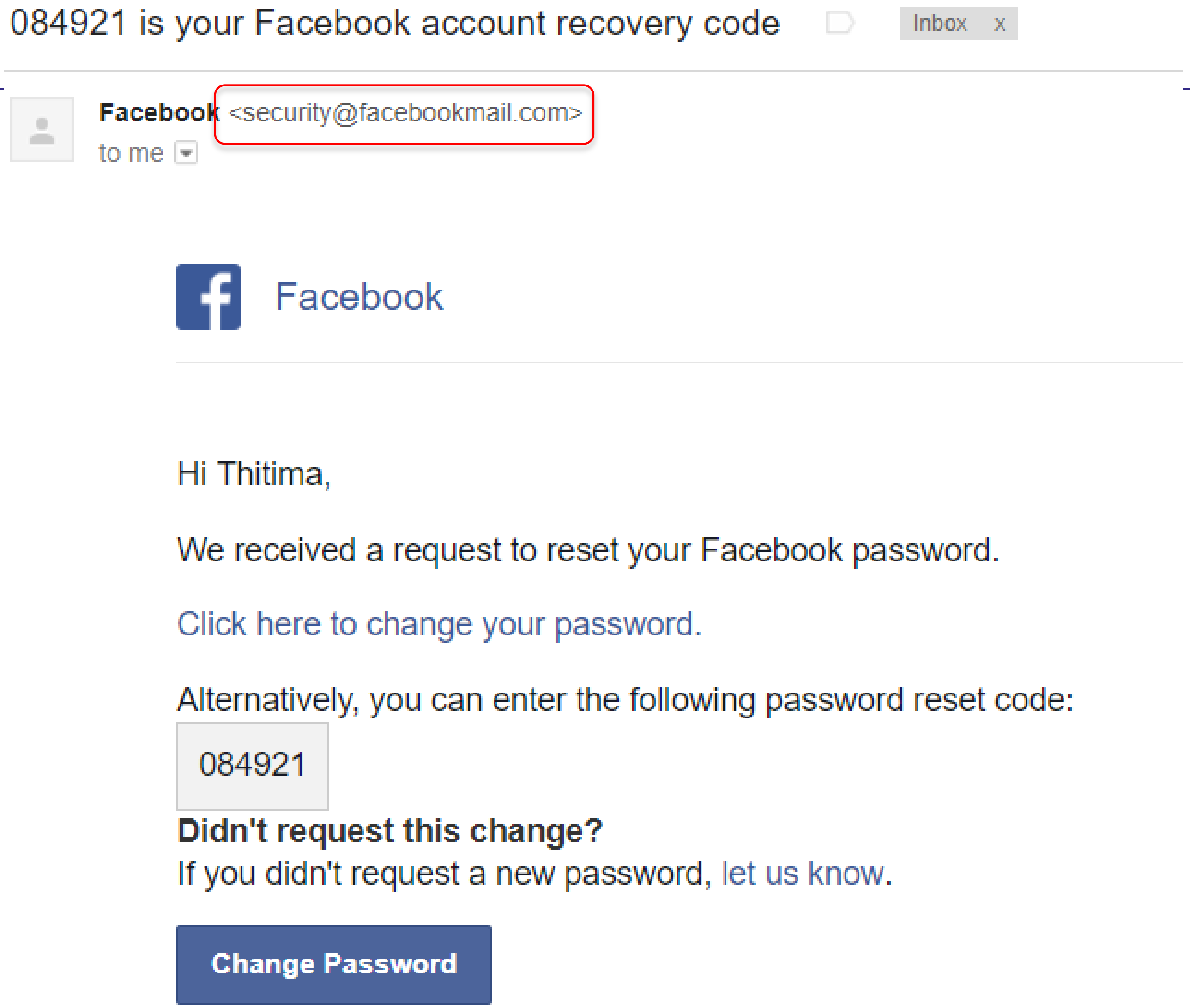
Overall, how satisfied are you with Bank of America in general?

Extremely Satisfied — Not at all Satisfied

10	9	8	7	6	5	4	3	2	1

If you are not the person that contacted Bank of America on December 31, 2016, please ask the person who did to complete this survey.

If this link does not work, please copy and paste the link into your web browser:
http://customersurvey.bankofamerica.com/survey.aspx?l.project=w8193w&id=286380402&password=txpgv



084921 is your Facebook account recovery code

Facebook <security@facebookmail.com>

Facebook

Hi Thitima,

We received a request to reset your Facebook password.

Click here to change your password.

Alternatively, you can enter the following password reset code:

084921

Didn't request this change?
If you didn't request a new password, let us know.

Information gathering

- Information gathering using search engines
  - E.g. Google, Bing are targeted at US & EU users, Baidu targets Chinese audience
- Information gathering using ‘people search’ websites
  - https://www.peekyou.com/
  - https://www.spokeo.com/
  - https://www.pipl.com
- Information gathering using Maltego

Maltego

- Link analysis tool that offers data mining and information gathering based on ‘entity’, then get a visual representation of the result.
- ‘Transforms’ – rules/search based on some criteria
- Maltego allows you to enumerate domain information
    - Websites associated with a person’s name
    - Phone numbers that are associated with an email
    - Email associated with a domain name
    - Companies associated with a person’s name

Human Factor & Usability : Password Case Study

Sasse, M. A., Brostoff, S., & Weirich, D. (2001). Transforming the ‘weakest link’—a human/computer interaction approach to usable and effective security. *BT technology journal*, *19*(3), 122-131.

- Consider the following situations:
  - Your password is expired, please change it immediate!
    - Ended up choosing weak password (change under pressure)

  - You must use different passwords to access different files
    - Ended up writing the password in a note (difficult to recall)

  - You are asked for password for some program updates
    - Ended up giving out if this is regularly requested

Human Factor & Usability : Password Case Study (2)

- Usability issues with password implementation
  - Number of passwords
    - Usually implemented on a per-system basis
    - Users' memory load / accumulated time spent in logging on
  - Password policies
    - Must be strong, i.e. mixture of letters, numbers and characters
    - Should be changed regular intervals
  - Varying systems
    - Different length / restrictions

Human Factor & Usability : Password Case Study (3)

Do you agree with the following statement?

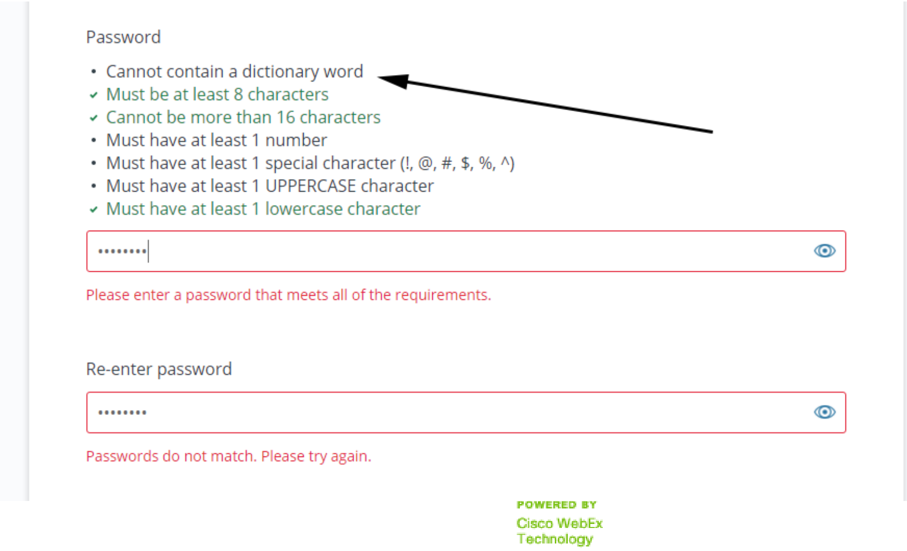
- Allow users to have the same password on different system is desirable.
    - Same passwords -> increases frequency of use -> better chance to have strong passwords users can remember

Human Factor & Usability : Password Case Study (4)

- Limitation of the capacity of working memory
- Memory decays over time
- Recognition of a familiar item is easier than unaided recall
- Easier to remember frequently used items than infrequently used ones
- Easier to recall items that are meaningful than non-meaningful ones
- Distinct items can be associated with each other to facilitate recall — however, similar items compete against each other on recall.

Human Factor & Usability : Password Case Study (6)

Passwords must be at least eight characters long and must contain at least two non-letter characters. They must also be changed at least once a month.



Password

- Cannot contain a dictionary word
- ✓ Must be at least 8 characters
- ✓ Cannot be more than 16 characters
- Must have at least 1 number
- Must have at least 1 special character (!, @, #, $, %, ^)
- Must have at least 1 UPPERCASE character
- ✓ Must have at least 1 lowercase character

••••••••

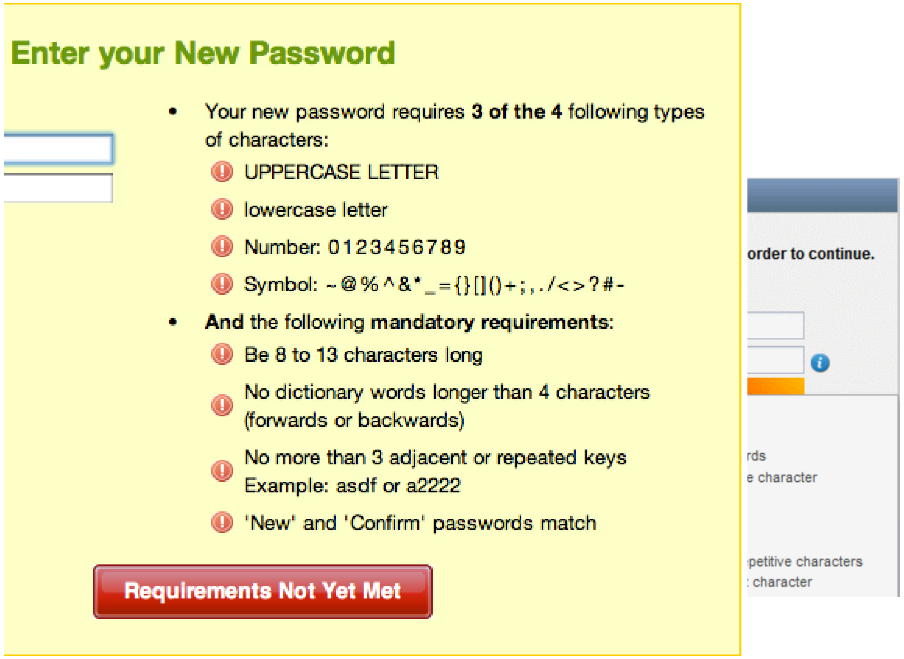
Please enter a password that meets all of the requirements.

Re-enter password

••••••••

Passwords do not match. Please try again.

POWERED BY
Cisco WebEx
Technology



Enter your New Password

- Your new password requires **3 of the 4** following types of characters:
  - UPPERCASE LETTER
  - lowercase letter
  - Number: 0123456789
  - Symbol: ~@%^&*_={}[]()+;,./<>?#-
- **And** the following **mandatory requirements**:
  - Be 8 to 13 characters long
  - No dictionary words longer than 4 characters (forwards or backwards)
  - No more than 3 adjacent or repeated keys Example: asdf or a2222
  - 'New' and 'Confirm' passwords match

Requirements Not Yet Met

Human Factor & Usability : Password Case Study (5)

Can passwords be both **strong** and **usable**?

Good password?

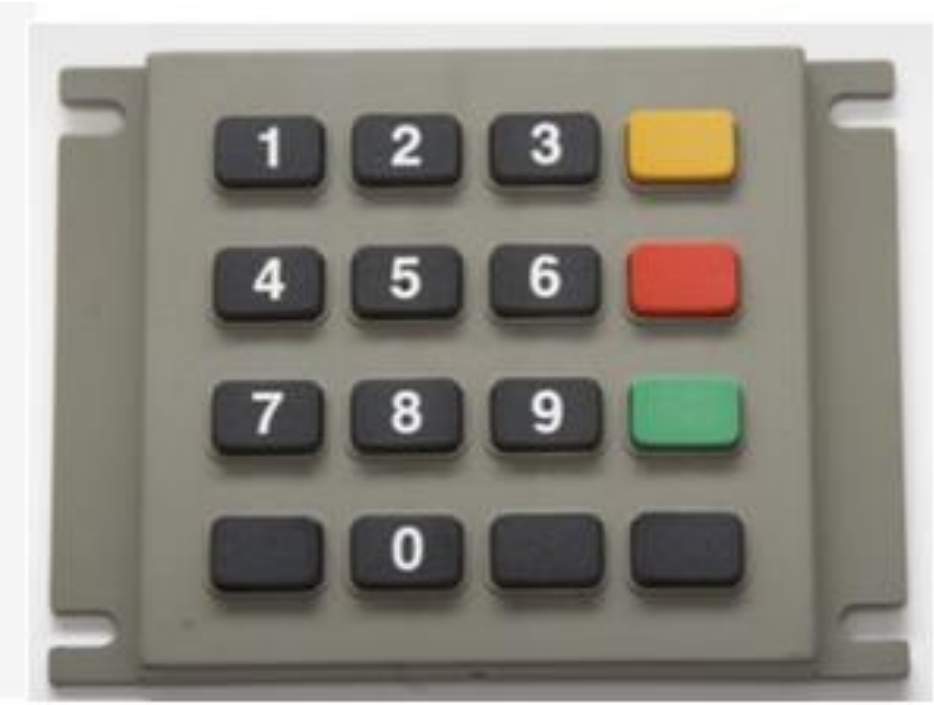
– should be reasonably **long**, use a reasonably **large character** set, but still be **easy to remember**.

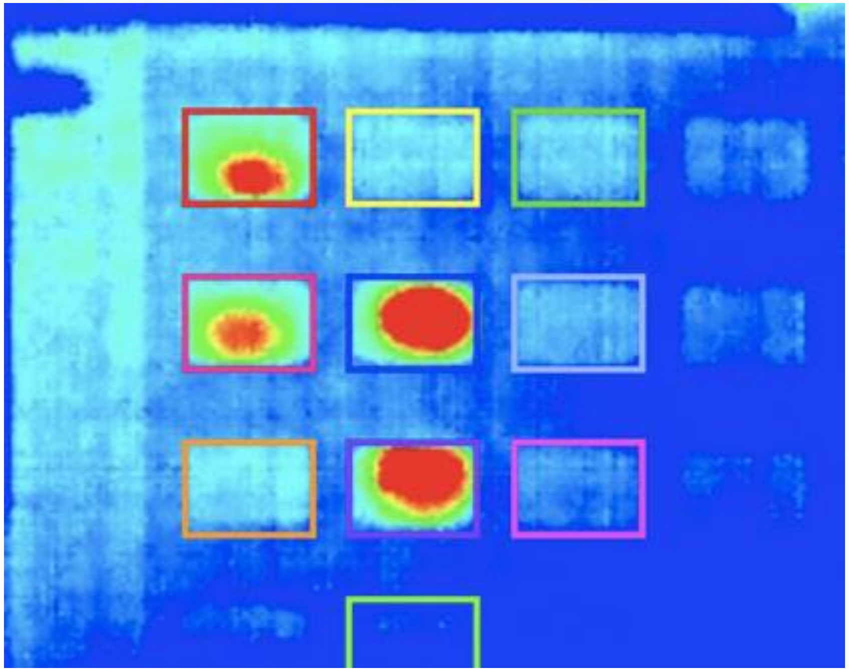
D*$r921tU dessert019

Oh dear! Please wake up before 7!

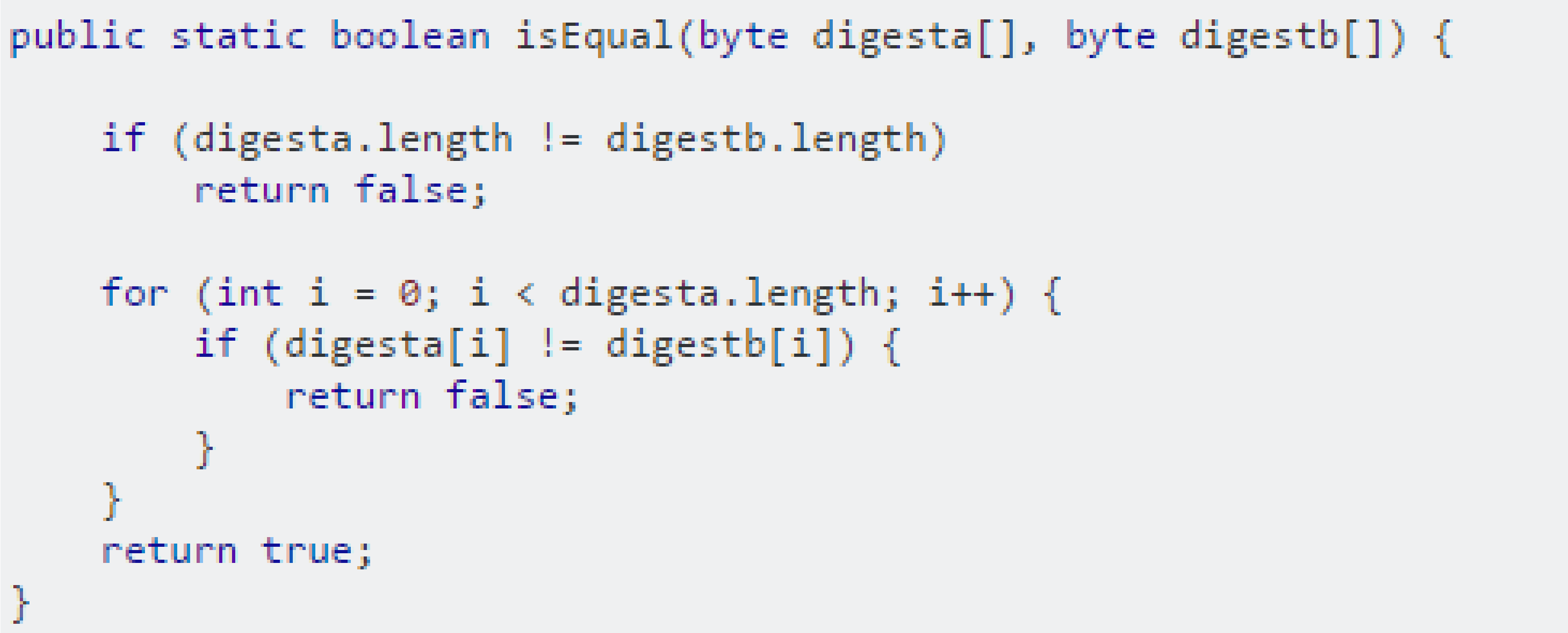
Attacks on Password

- Attack on Password Entry
  - Shoulder surfing
  - Thermal camera
  - Key-logger
  - Password sniffing
  - Timing Attack


1
2
3
4
5
6
7
8
9
0



Timing Attack: MessageDigest.isEqual function in Java



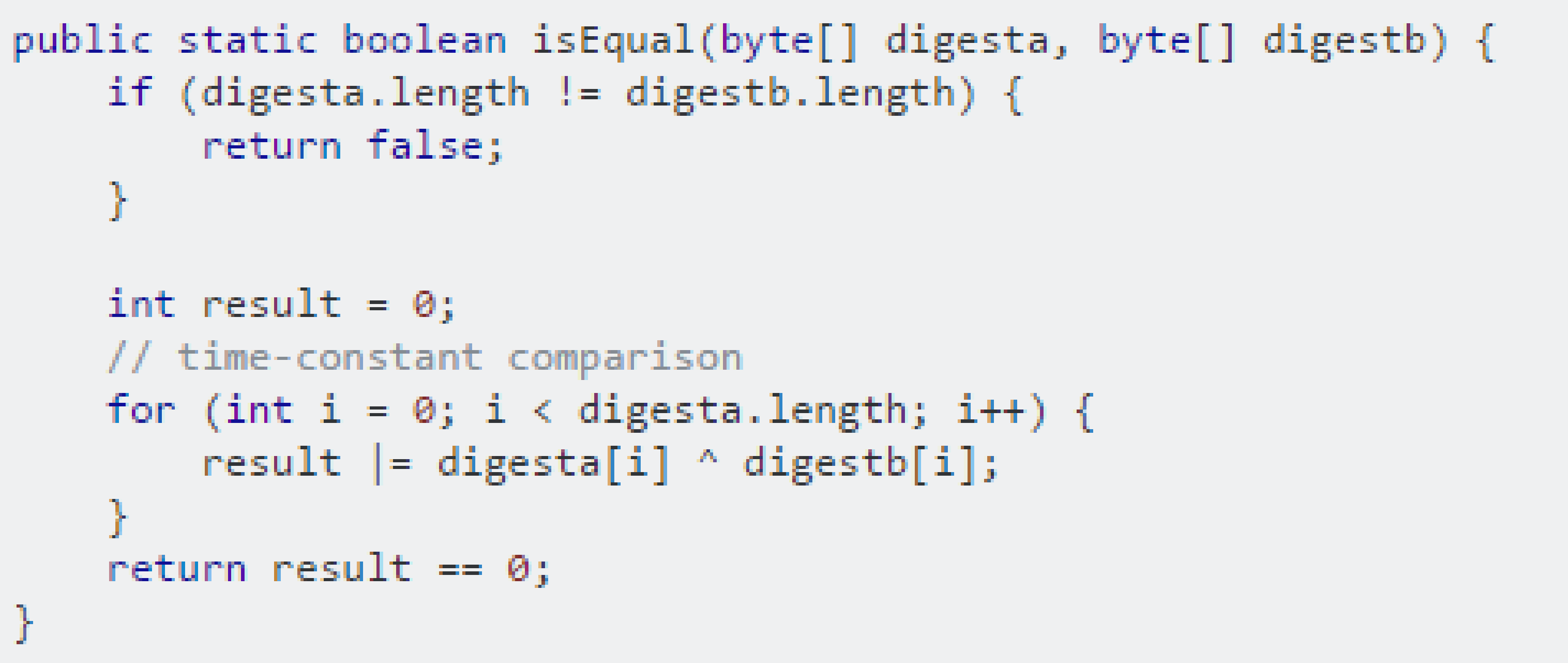
```java
public static boolean isEqual(byte digesta[], byte digestb[]) {

    if (digesta.length != digestb.length)
        return false;

    for (int i = 0; i < digesta.length; i++) {
        if (digesta[i] != digestb[i]) {
            return false;
        }
    }
    return true;
}
```

Note: Java SE 6 Update 10

Timing Attack: MessageDigest.isEqual function in Java (2)



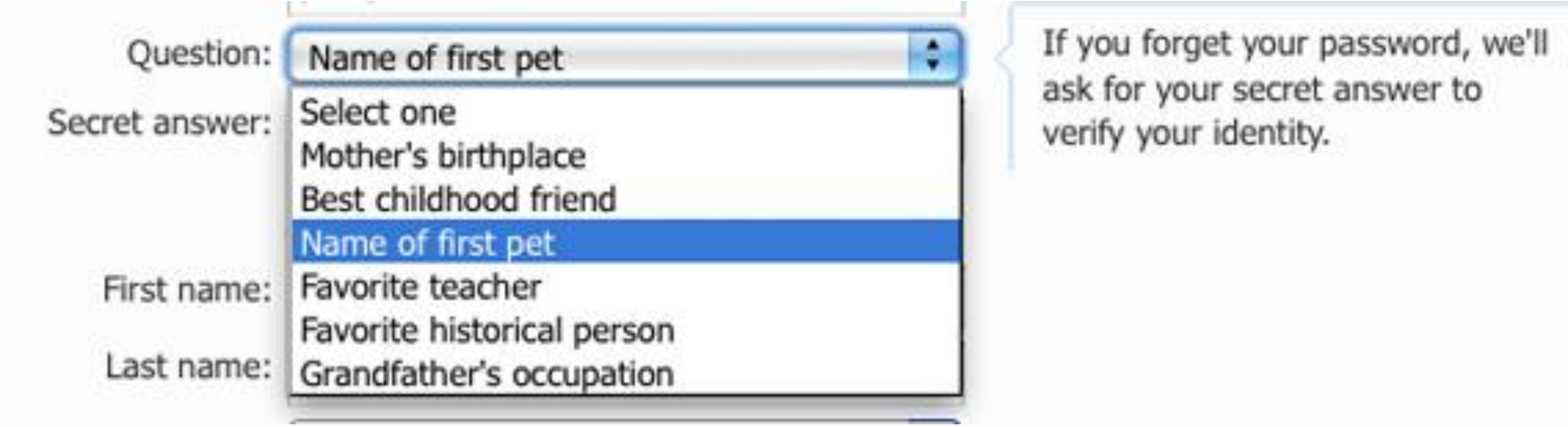
```
public static boolean isEqual(byte[] digesta, byte[] digestb) {
    if (digesta.length != digestb.length) {
        return false;
    }

    int result = 0;
    // time-constant comparison
    for (int i = 0; i < digesta.length; i++) {
        result |= digesta[i] ^ digestb[i];
    }
    return result == 0;
}
```

Note: After fix

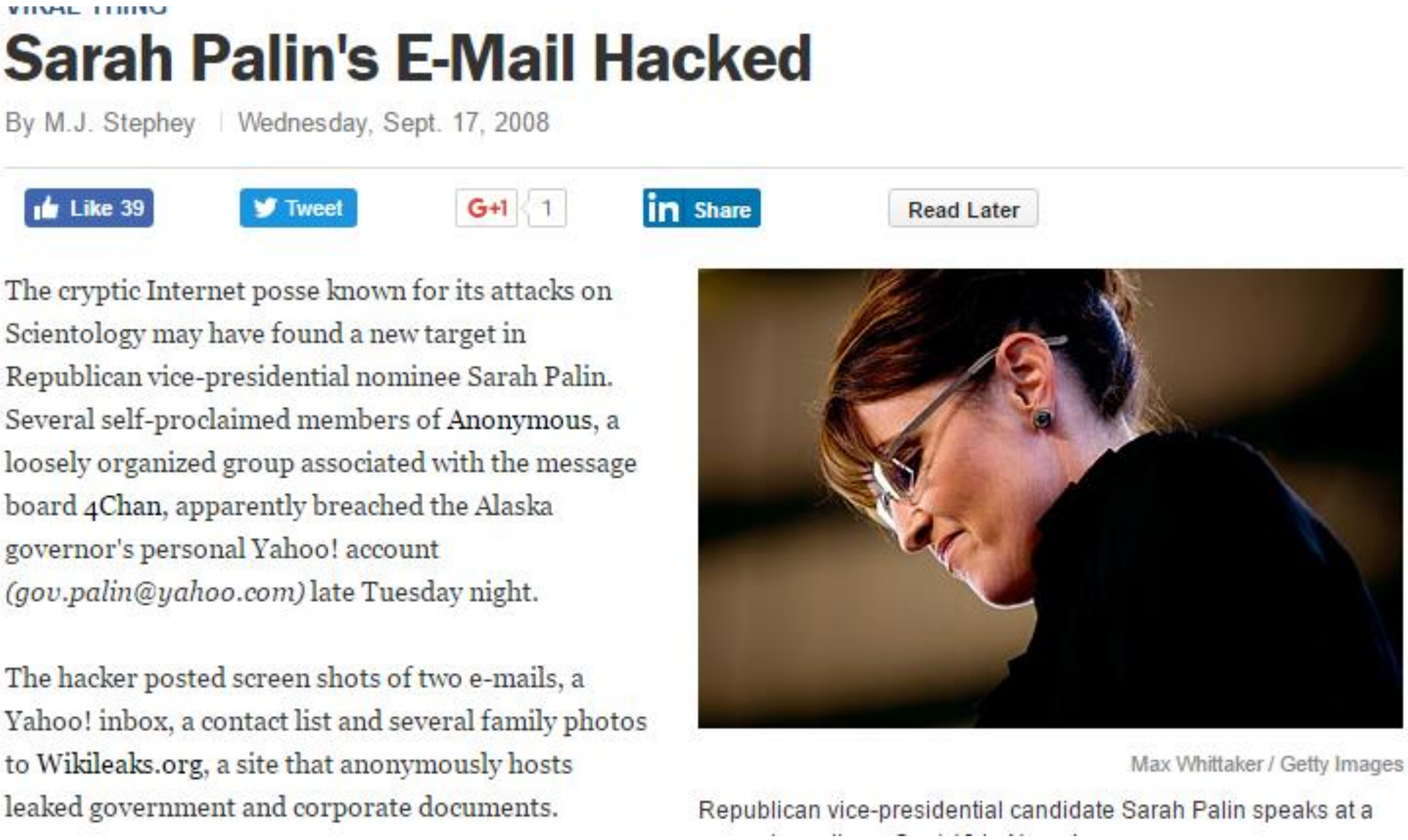
Attacks on Password

- Attack on Password Storage
    - One-way Encryption
    - Password Cracking
    - Rainbow Tables
    - Password Resetting



Question: Name of first pet

If you forget your password, we'll ask for your secret answer to verify your identity.



VIRAL THING

Sarah Palin's E-Mail Hacked

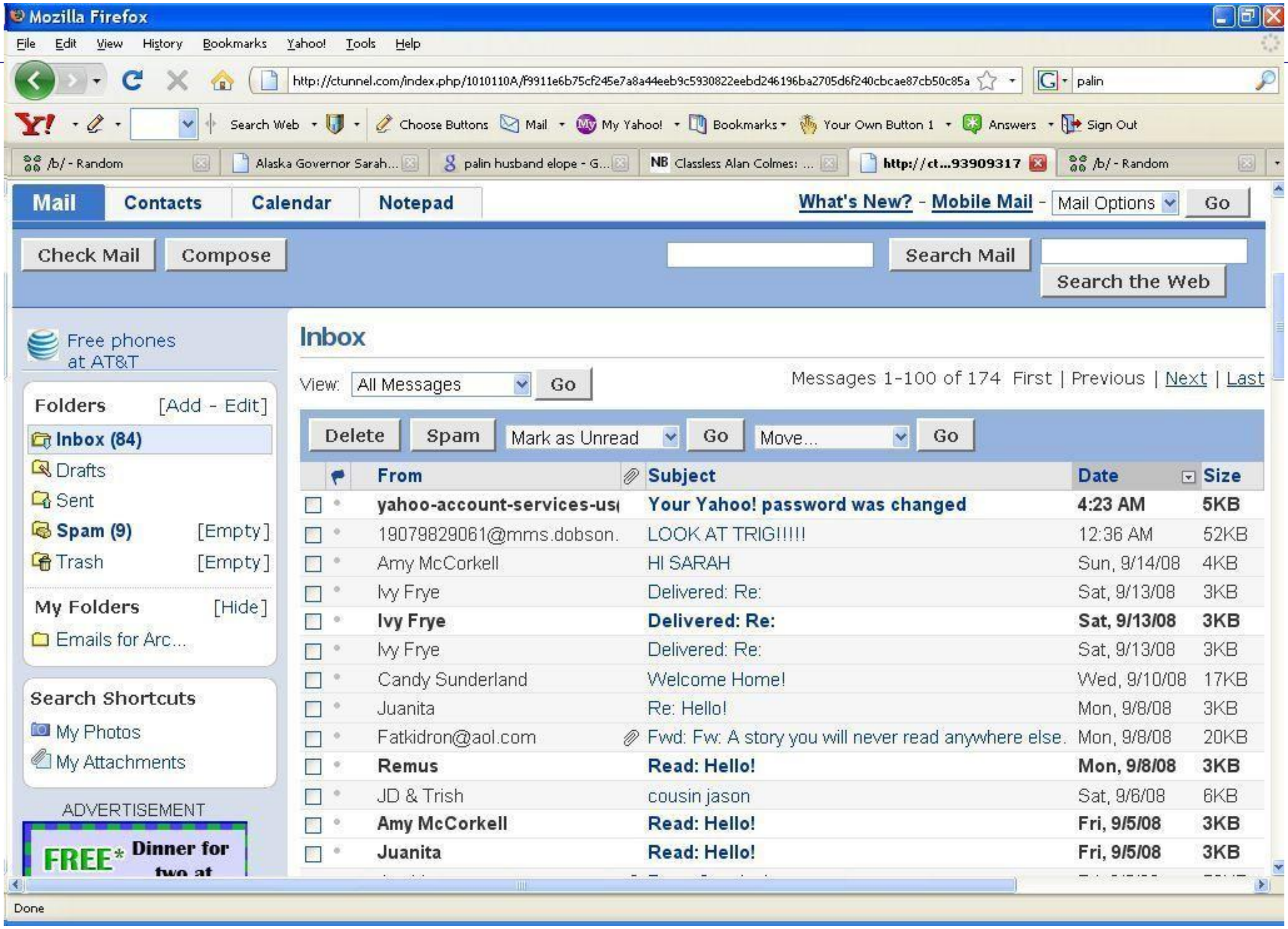
By M.J. Stephey | Wednesday, Sept. 17, 2008

The cryptic Internet posse known for its attacks on Scientology may have found a new target in Republican vice-presidential nominee Sarah Palin. Several self-proclaimed members of Anonymous, a loosely organized group associated with the message board 4Chan, apparently breached the Alaska governor's personal Yahoo! account *(gov.palin@yahoo.com)* late Tuesday night.

The hacker posted screen shots of two e-mails, a Yahoo! inbox, a contact list and several family photos to Wikileaks.org, a site that anonymously hosts leaked government and corporate documents.

Max Whittaker / Getty Images

Republican vice-presidential candidate Sarah Palin speaks at a



http://ctunnel.com/index.php/1010110A/f9911e6b75cf245e7a8a44eeb9c5930822eebd246196ba2705d6f240cbcae87cb50c85a

palin

/b/ - Random | Alaska Governor Sarah... | palin husband elope - G... | Classless Alan Colmes: ... | http://ct...93909317 | /b/ - Random

Inbox

Messages 1-100 of 174 First | Previous | Next | Last

From	Subject	Date	Size
yahoo-account-services-us	**Your Yahoo! password was changed**	**4:23 AM**	**5KB**
19079829061@mms.dobson.	LOOK AT TRIG!!!!!	12:36 AM	52KB
Amy McCorkell	HI SARAH	Sun, 9/14/08	4KB
Ivy Frye	Delivered: Re:	Sat, 9/13/08	3KB
Ivy Frye	**Delivered: Re:**	**Sat, 9/13/08**	**3KB**
Ivy Frye	Delivered: Re:	Sat, 9/13/08	3KB
Candy Sunderland	Welcome Home!	Wed, 9/10/08	17KB
Juanita	Re: Hello!	Mon, 9/8/08	3KB
Fatkidron@aol.com	Fwd: Fw: A story you will never read anywhere else.	Mon, 9/8/08	20KB
Remus	**Read: Hello!**	**Mon, 9/8/08**	**3KB**
JD & Trish	cousin jason	Sat, 9/6/08	6KB
Amy McCorkell	**Read: Hello!**	**Fri, 9/5/08**	**3KB**
Juanita	**Read: Hello!**	**Fri, 9/5/08**	**3KB**

Source: https://wikileaks.org/wiki/VP_contender_Sarah_Palin_hacked

Example of Insider Threat

Case1

- Jane moved from a payroll department to a new position.
- Jane’s access rights to the payroll accounts left unchanged.
- Bob asked Jane for some contact information for his own business.
- Using the privileged access rights that she had retained, Jane provided Bob with employees’ confidential information.
- Bob used them for identity theft.
- The actions caused over $1 million in damage to the company and its employees.

Example of Insider Threat (2)

Case 2

- David angrily resigned from his position because his request for a pay rise was denied.
- David stayed on for another 2 weeks because of his close relationship with his boss.
- David collected company proprietary information into an open storage area.
- David then use FTP to download them to his home computer.

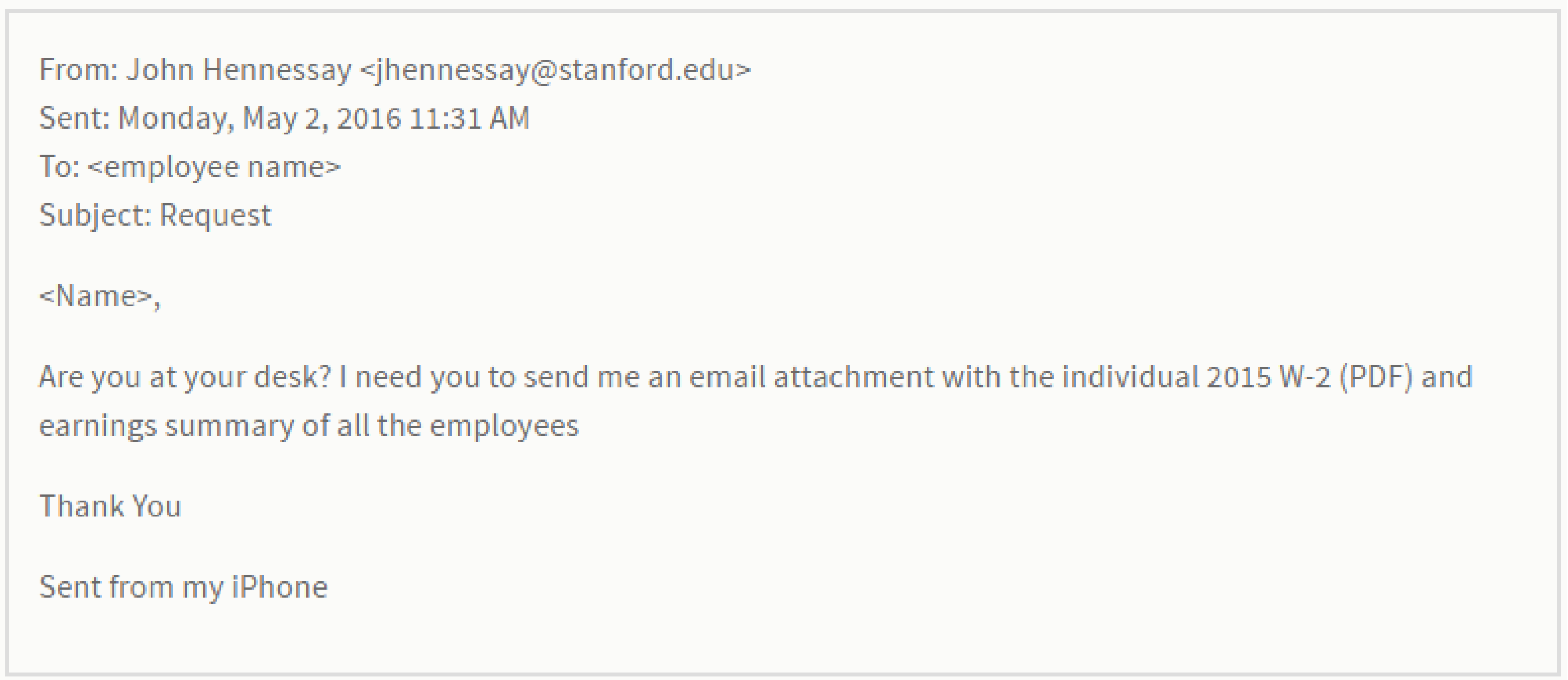
Insider Threat

Colwill, C. (2009). Human factors in information security: The insider threat–Who can you trust these days?. *Information security technical report*, *14*(4), 186-196.

- Insiders have legitimate access to facilities and information, knowledge of the organization and the location of valuable assets – therefore can pose higher risk.
- Insider threat can be
  - Non-malicious –
    - accidental loss or release of information (pretexting)
    - Inappropriate internet access (malware/spyware attacks)
  - Malicious –
    - Unauthorized release of proprietary/confidential information (abuse of privilege or access control rights)
    - Sabotage of assets that only employees can access
    - Plant a backdoor

Research indicates that 70% of fraud is perpetrated by insiders rather than by external criminals but that 90% of security controls and monitoring are focused on external threats.

Pretexting



From: John Hennessay <jhennessay@stanford.edu>
Sent: Monday, May 2, 2016 11:31 AM
To: <employee name>
Subject: Request

<Name>,

Are you at your desk? I need you to send me an email attachment with the individual 2015 W-2 (PDF) and earnings summary of all the employees

Thank You

Sent from my iPhone

Source: https://uit.stanford.edu/phishing

Insider Threat (2)

Colwill, C. (2009). Human factors in information security: The insider threat–Who can you trust these days?. *Information security technical report*, *14*(4), 186-196.

- Technical controls – encryption, access control, minimum privilege, monitoring, auditing and reporting
- Non-technical controls
  - Enforce security policy – prohibit any personal use of company assets / access to non-work-related websites? / define access rights
  - Extend traditional policy and guidance - acceptable vs. unacceptable behavior in the workplace
  - Perform background and conduct ongoing personnel checks
  - Security training and awareness

Insider Threat Study

- Collaboration between Secret Service National Threat Assessment Center (NTAC) and Carnegie Mellon University Computer Emergency Response Team (CERT)

- Focuses on the *people* who use or exceed their authorized access to information systems to perpetrate harm to organizations.

Insider Threat Study (3)

- Characteristics
  - Current and former employees nearly equal in number
  - Most of them were full-time in a technical position
- Motives
  - Mainly motivated by revenge
  - Goal – financial gain, theft of information/property, and sabotage of organization
- Nature of Attacks
  - Use of both unsophisticated method and sophisticated tools
  - Attacks occurred outside of normal working hours
  - Use of remote access

Insider Threat Study(4)

- Recommendations
  - Disabling access upon resignation or termination
  - Logging and monitoring of activities
  - Strict back up policies
  - Limiting access to proprietary information to only that an employee requires to perform tasks.
  - Avoid password sharing

References

- Anderson, Ross. *Security engineering*. John Wiley & Sons, 2008.
- Colwill, Carl. "Human factors in information security: The insider threat–Who can you trust these days?." *Information security technical report* 14.4: 186-196, 2009.
- Dhamija, Rachna, J. Doug Tygar, and Marti Hearst. "Why phishing works." *Proceedings of the SIGCHI conference on Human Factors in computing systems*. ACM, 2006.
- McCue A. Beware the insider security threat, CIO Jury, 17/4/08, http://www.techrepublic.com/blog/cio-insights/beware-the-insider-security-threat/, 2008.
- Sasse, Martina Angela, Sacha Brostoff, and Dirk Weirich. "Transforming the 'weakest link'—a human/computer interaction approach to usable and effective security." *BT technology journal* 19.3 (2001): 122-131.
- http://resources.sei.cmu.edu/asset_files/WhitePaper/2008_019_001_52266.pdf