CSE508 Network Security

2021-04-22

Spam and Phishing

Michalis Polychronakis

Stony Brook University

I don’t like SPAM!

Spam Sources

Commercial entities

- Legitimate or "gray" businesses, advertisers, …

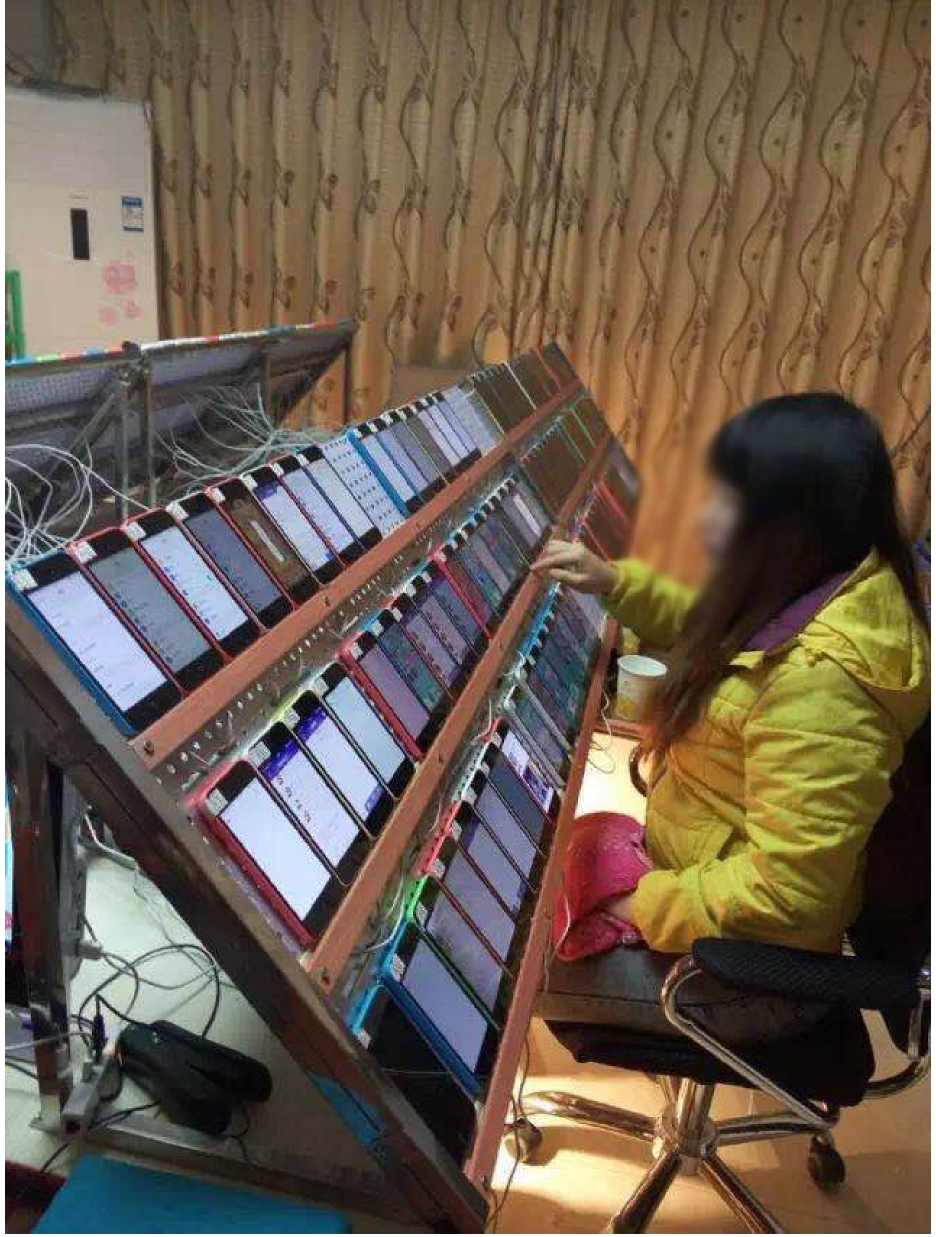
Spammers' own hosts or open relays ➔ easily blocked

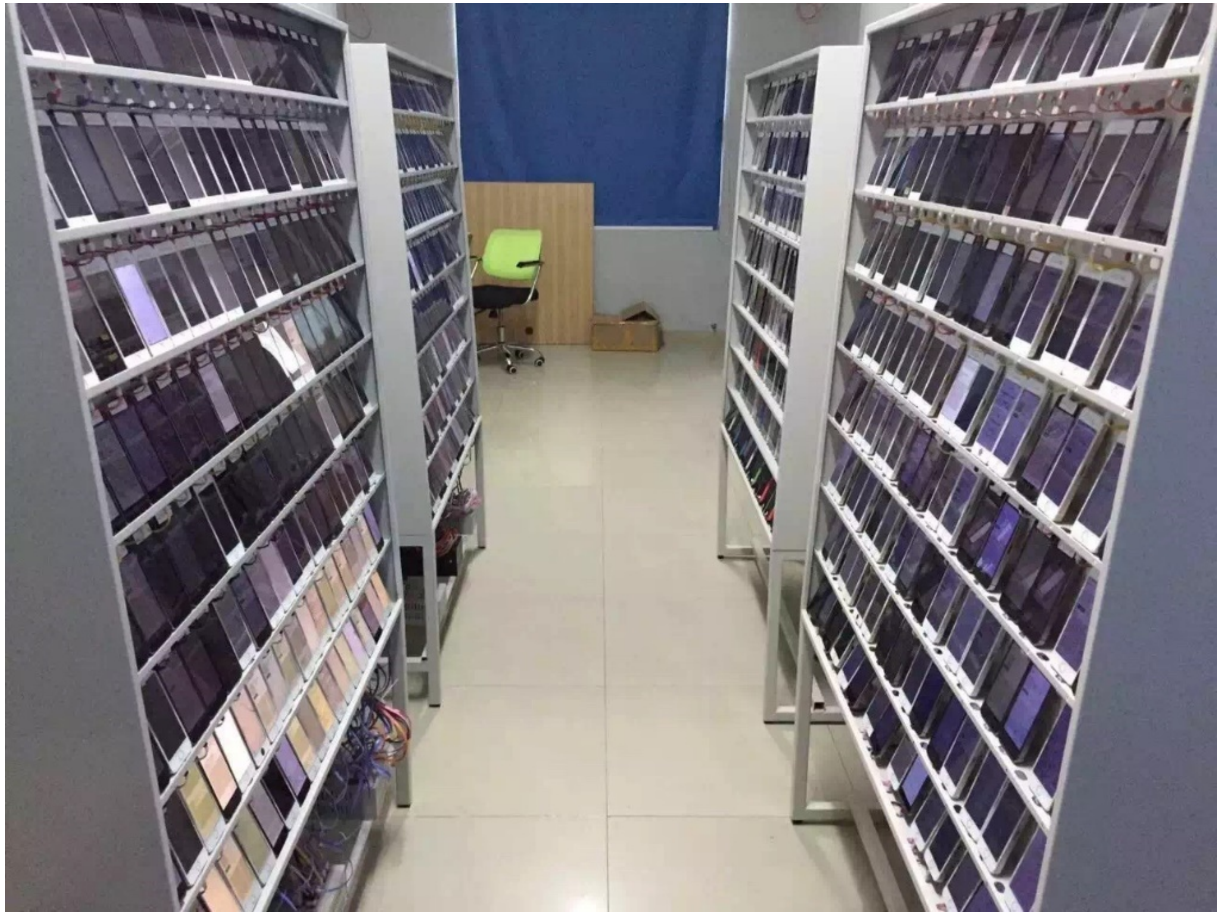
Botnets

- Abuse of ISPs and webmail providers
- Abuse of legitimate user email accounts
- Address harvesting from users' address books

Beyond email

- *Fraudulent messages:* Facebook, Twitter, Yelp, Amazon, online comments, forum messages, Apple/Google Store, …
- *Fraudulent activities:* likes, retweets, clicks, app store rankings, fake reviews, …





© TechInAsia - https://www.techinasia.com/viral-photo-china-shows-manipulate-app-store-rankings-hard
© iFeng - http://tech.ifeng.com/a/20161024/44476050_0.shtml

Spam Lifecycle

Gathering addresses

- Valid, actively used addresses are precious
- Stolen address books, web crawling, black market, …

Message content

- Advertising, 419 scams, fraud, phishing, malware, …
- Anti-spam filter evasion: content obfuscation

Spam email delivery

- Valid accounts: newly created (sweatshops), hijacked ones, …
- Fake social media accounts "primed" over time
- Open relays/proxies (not common anymore)
- Malware: most spam comes from infected machines/botnets

Email Address Protection

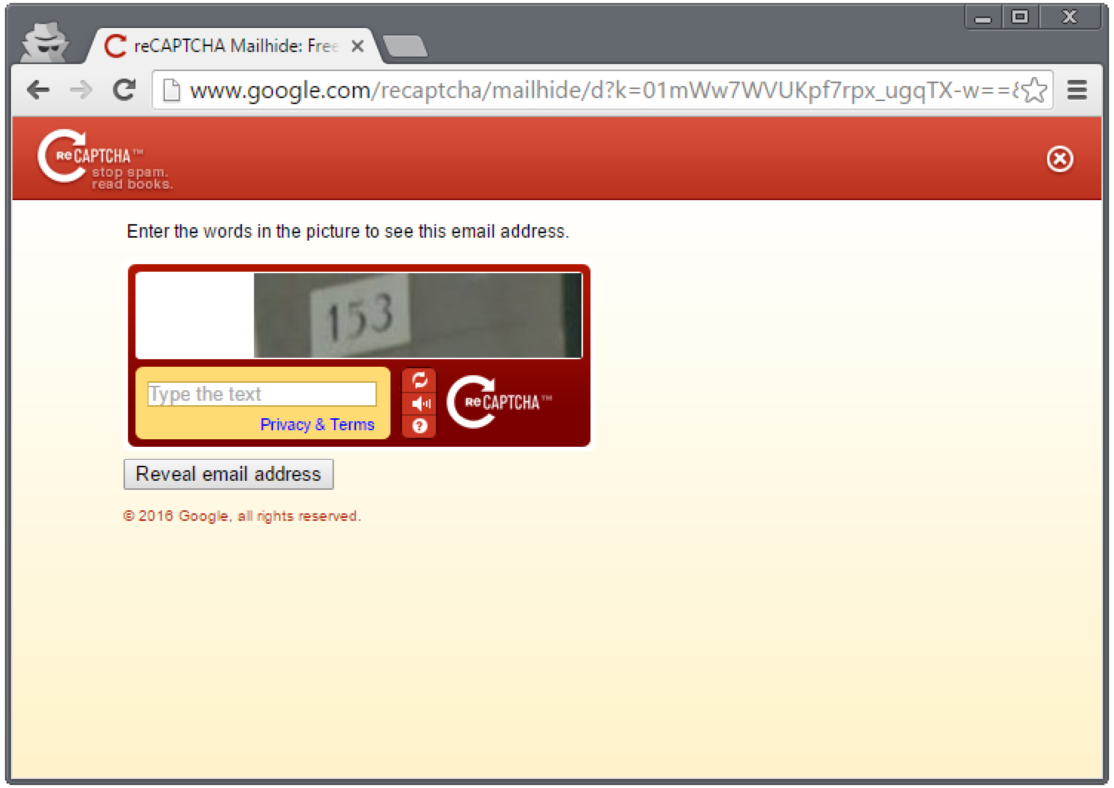
Keep it safe from automated address harvesting crawlers

Munging: `username [at] example.com`

Image instead of text

CAPTCHAs

…



Enter the words in the picture to see this email address.

© 2016 Google, all rights reserved.

Fighting Spam

Content-based filtering

- False positives vs. false negatives
- Local vs. cloud-based

Blacklisting

- IPs/domains of known spammers, open relays, zombie machines, hosts that shouldn’t be sending emails (e.g., ISP DHCP pools), …

Honeypots

- Relays, proxies, spamtraps (fake email addresses)

Outbound filtering (block port 25)

- SMTP authentication is now mandatory by most ISPs

Email authentication

Content-based Filtering

Machine learning

- Training with labeled "spam" and "ham" messages
- Feedback from user activities (e.g., "not spam" button)

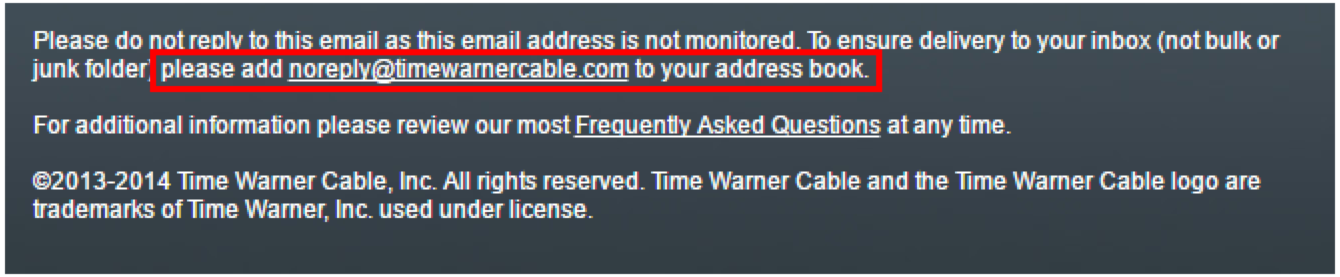
Rule-based systems

- Signatures, regular expressions, patterns, …
- Certain keywords, phrases, unusual text, …
- Example: SpamAssassin

Spam authors try to evade filters

- V1agra, Via'gra, Vi@graa, vi*gra, \/iagra
- Intentional spelling mistakes, symbols, weird punctuation, …
- Continuous arms race
- Example: attackers started using images, defenders started using OCR

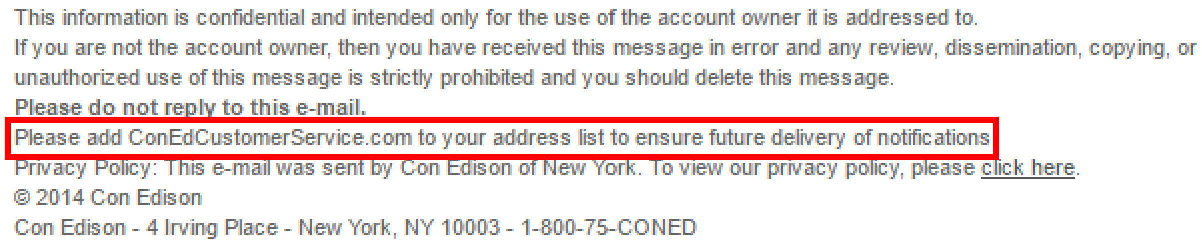
False positives are a challenging problem



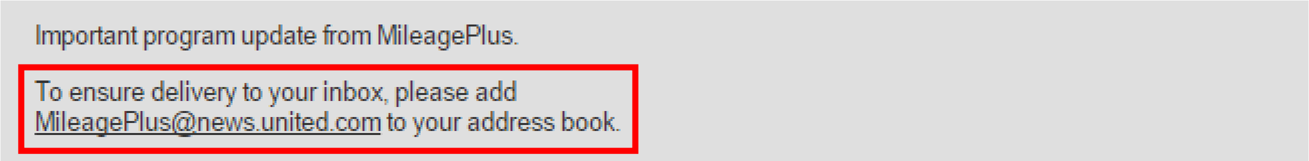
Please do not reply to this email as this email address is not monitored. To ensure delivery to your inbox (not bulk or junk folder) please add noreply@timewarnercable.com to your address book.

For additional information please review our most Frequently Asked Questions at any time.

©2013-2014 Time Warner Cable, Inc. All rights reserved. Time Warner Cable and the Time Warner Cable logo are trademarks of Time Warner, Inc. used under license.



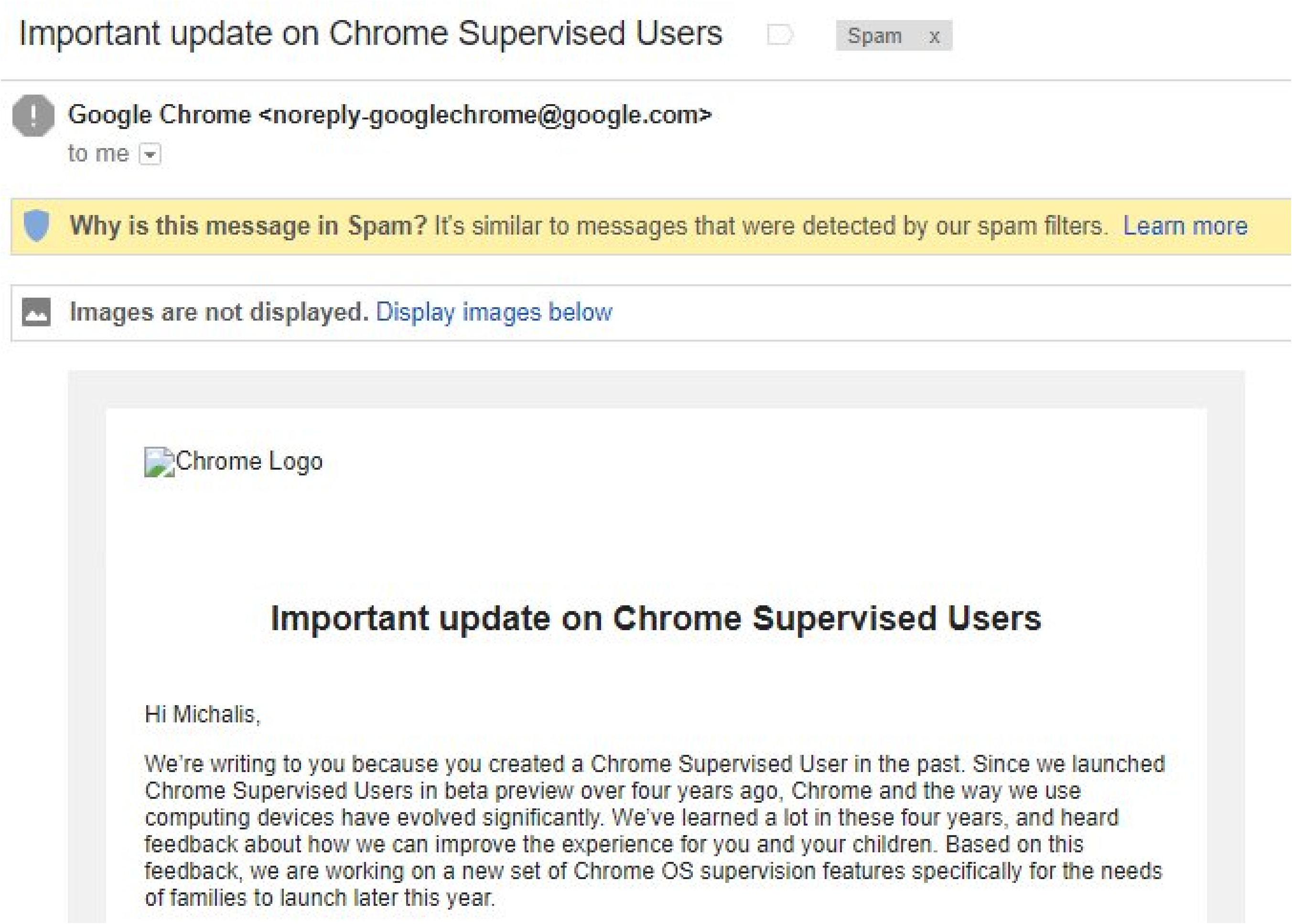
This information is confidential and intended only for the use of the account owner it is addressed to.
If you are not the account owner, then you have received this message in error and any review, dissemination, copying, or unauthorized use of this message is strictly prohibited and you should delete this message.
Please do not reply to this e-mail.
Please add ConEdCustomerService.com to your address list to ensure future delivery of notifications
Privacy Policy: This e-mail was sent by Con Edison of New York. To view our privacy policy, please click here.
© 2014 Con Edison
Con Edison - 4 Irving Place - New York, NY 10003 - 1-800-75-CONED



Important program update from MileagePlus.

To ensure delivery to your inbox, please add MileagePlus@news.united.com to your address book.

Personal example: Google's own message classified as spam by Gmail



Important update on Chrome Supervised Users

Google Chrome <noreply-googlechrome@google.com>

to me

Why is this message in Spam? It's similar to messages that were detected by our spam filters. Learn more

Images are not displayed. Display images below

Chrome Logo

Important update on Chrome Supervised Users

Hi Michalis,

We're writing to you because you created a Chrome Supervised User in the past. Since we launched Chrome Supervised Users in beta preview over four years ago, Chrome and the way we use computing devices have evolved significantly. We've learned a lot in these four years, and heard feedback about how we can improve the experience for you and your children. Based on this feedback, we are working on a new set of Chrome OS supervision features specifically for the needs of families to launch later this year.

https://twitter.com/polychronakis/status/950873453648850944

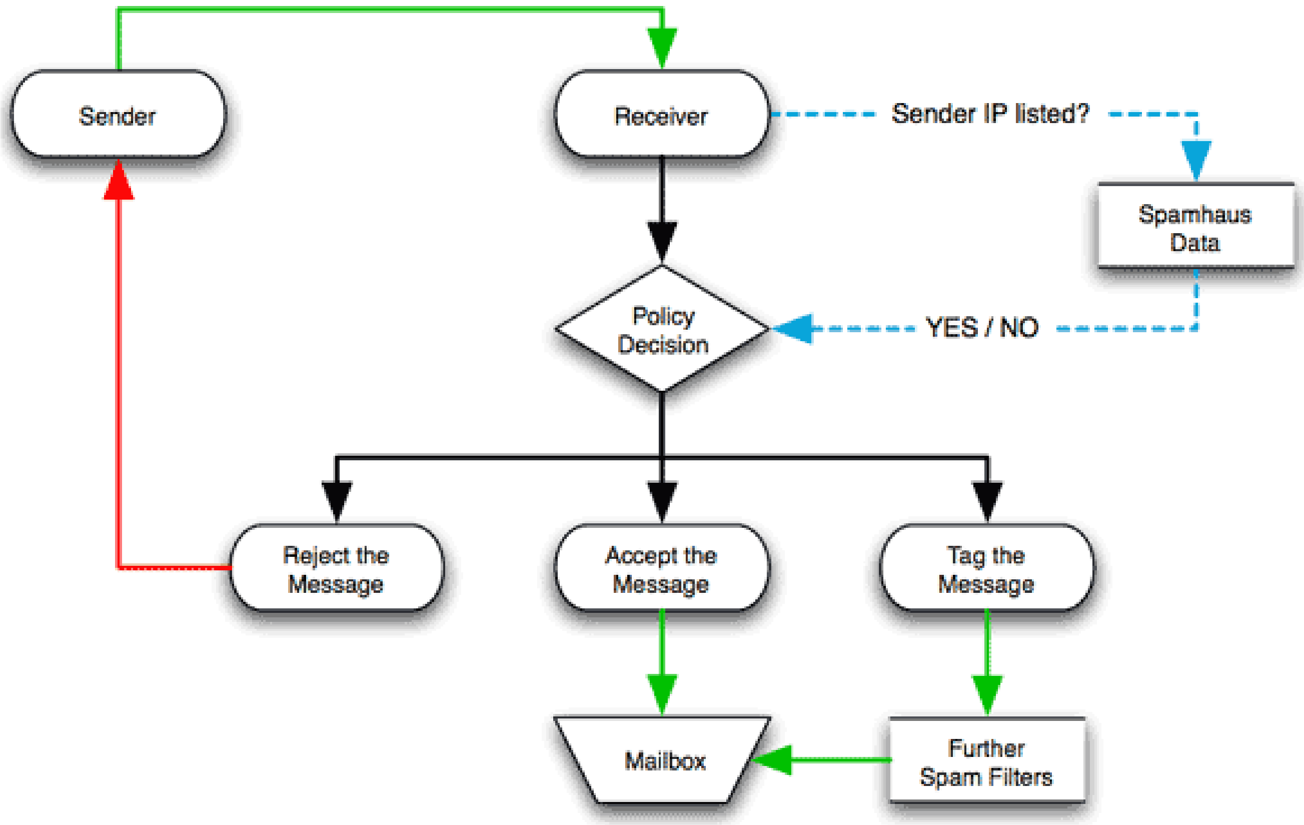
DNSBL Filtering

DNS Block List

- IP addresses, domain names, and other information compiled as a DNS zone

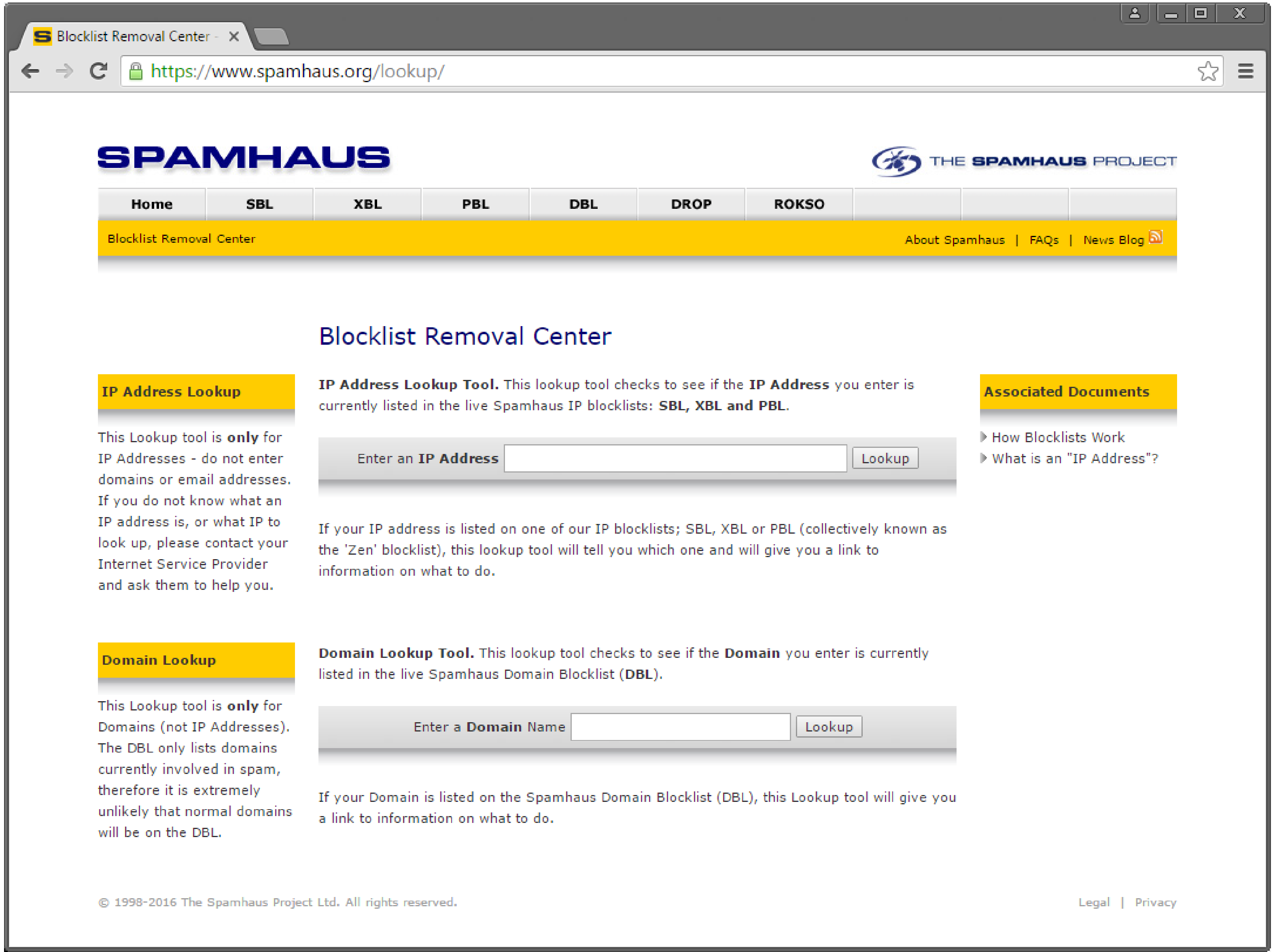
DNS-based

- Easy to query
- Light on bandwidth/resources



© Spamhaus - https://www.spamhaus.org/whitepapers/dnsbl_function/

False positives, IP addresses change owners, …


Blocklist Removal Center -
https://www.spamhaus.org/lookup/
SPAMHAUS
THE SPAMHAUS PROJECT
Home
SBL
XBL
PBL
DBL
DROP
ROKSO
Blocklist Removal Center
About Spamhaus | FAQs | News Blog
Lookup
Lookup

Blocklist Removal Center

IP Address Lookup

This Lookup tool is **only** for IP Addresses - do not enter domains or email addresses. If you do not know what an IP address is, or what IP to look up, please contact your Internet Service Provider and ask them to help you.

IP Address Lookup Tool. This lookup tool checks to see if the **IP Address** you enter is currently listed in the live Spamhaus IP blocklists: **SBL, XBL and PBL**.

Enter an **IP Address**

If your IP address is listed on one of our IP blocklists; SBL, XBL or PBL (collectively known as the 'Zen' blocklist), this lookup tool will tell you which one and will give you a link to information on what to do.

Associated Documents

- How Blocklists Work
- What is an "IP Address"?

Domain Lookup

This Lookup tool is **only** for Domains (not IP Addresses). The DBL only lists domains currently involved in spam, therefore it is extremely unlikely that normal domains will be on the DBL.

Domain Lookup Tool. This lookup tool checks to see if the **Domain** you enter is currently listed in the live Spamhaus Domain Blocklist (**DBL**).

Enter a **Domain** Name

If your Domain is listed on the Spamhaus Domain Blocklist (DBL), this Lookup tool will give you a link to information on what to do.

© 1998-2016 The Spamhaus Project Ltd. All rights reserved.

Legal | Privacy

SPF: Origin Authentication

SMTP allows anyone to send an email with an arbitrary “From” address

Sender Policy Framework

- DNS TXT record pointing to the *hosts* that are allowed to send email from the domain
- Receiving SMTP servers compare the IP address that attempts to send an email with the allowed (by SPF) addresses of the domain(s) provided in the `HELO` and `MAIL FROM` commands
- Helps to block spam at it source

```
mikepo@styx:~> dig google.com TXT
;; ANSWER SECTION:
google.com.            3599    IN     TXT    "v=spf1 include:_spf.google.com ~all"
```

DKIM: Email Validation

DomainKeys Identified Mail: digitally sign some email headers and message body

Allows the recipient to verify that

- The message is sent from the domain it claims to be sent from
- The message has not been tampered with

Domain’s public key is stored in a DNS TXT record

```
X-Google-DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed; d=1e100.net; s=20161025;
h=x-gm-message-state:mime-version:from:date:message-id:subject:to;
bh=0BSnrwLTQ7KblIwINxoPJN40a/K5PZCIV8atL6a1Dvg=;
b=Nch9yEorgibAjkh90ukDL6SU0FYn70qP6AMsWFfpLO+W3iroMoVdKIjKk8Cv6Gc1TW ...
```

```
mikepo@styx:~> dig 20161025._domainkey.1e100.net TXT
;; ANSWER SECTION:
20161025._domainkey.1e100.net. 21599 IN TXT     "k=rsa;
p=MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAnOv6+Txyz+SEc7mT719QQtOj6g2MjpErYUGVrRGGc7f5rmE...
```

SPF + DKIM = DMARC

Domain-based Message Authentication, Reporting & Conformance

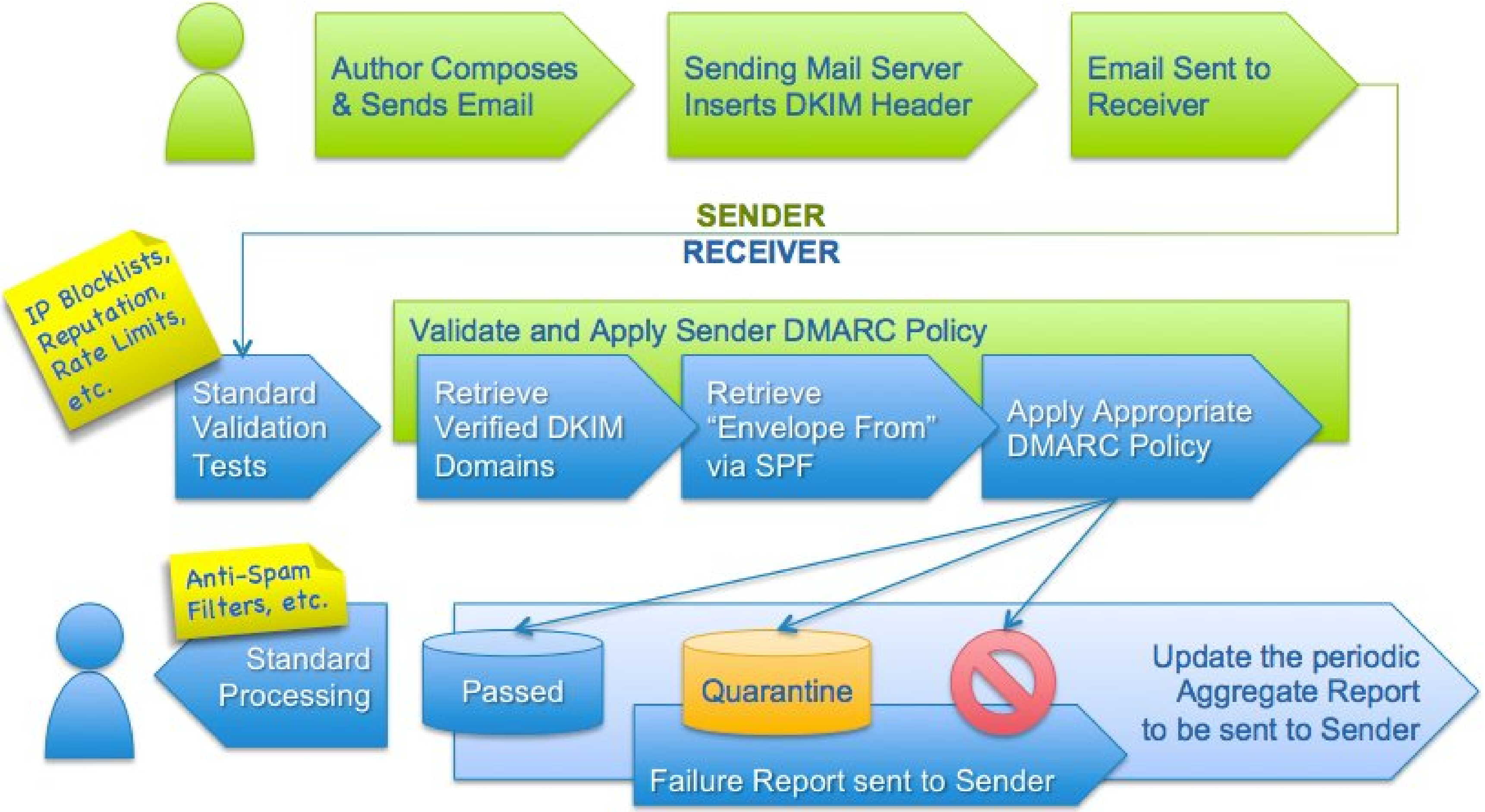
Standardizes how email receivers perform email authentication using SPF and DKIM

Tells receivers what to do if neither of those authentication methods passes (possible actions: mark as junk, or reject the message)

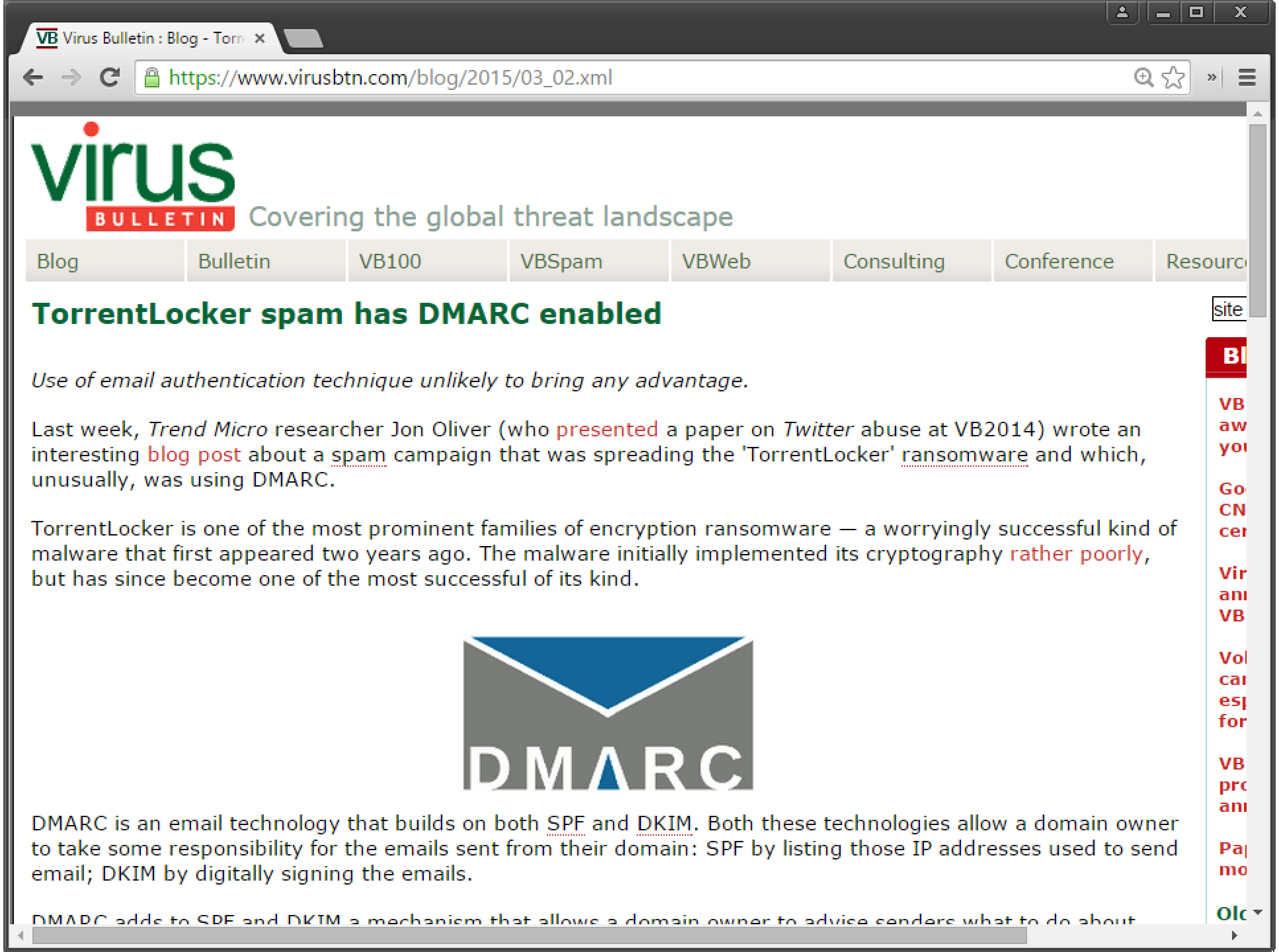
DMARC policies are published as DNS TXT records

```
mikepo@styx:~> dig _dmarc.google.com TXT
;; ANSWER SECTION:
_dmarc.google.com.      299     IN      TXT     "v=DMARC1; p=reject;
rua=mailto:mailauth-reports@google.com"
```

DMARC Email Authentication Process


Author Composes & Sends Email
Sending Mail Server Inserts DKIM Header
Email Sent to Receiver
SENDER
RECEIVER
IP Blocklists, Reputation, Rate Limits, etc.
Standard Validation Tests
Validate and Apply Sender DMARC Policy
Retrieve Verified DKIM Domains
Retrieve "Envelope From" via SPF
Apply Appropriate DMARC Policy
Anti-Spam Filters, etc.
Standard Processing
Passed
Quarantine
Update the periodic Aggregate Report to be sent to Sender
Failure Report sent to Sender

http://dmarc.org/overview/


Virus Bulletin : Blog - Torr
https://www.virusbtn.com/blog/2015/03_02.xml
virus BULLETIN Covering the global threat landscape
Blog
Bulletin
VB100
VBSpam
VBWeb
Consulting
Conference
Resourc
site

TorrentLocker spam has DMARC enabled

Use of email authentication technique unlikely to bring any advantage.

Last week, *Trend Micro* researcher Jon Oliver (who presented a paper on *Twitter* abuse at VB2014) wrote an interesting blog post about a spam campaign that was spreading the 'TorrentLocker' ransomware and which, unusually, was using DMARC.

TorrentLocker is one of the most prominent families of encryption ransomware — a worryingly successful kind of malware that first appeared two years ago. The malware initially implemented its cryptography rather poorly, but has since become one of the most successful of its kind.

DMARC is an email technology that builds on both SPF and DKIM. Both these technologies allow a domain owner to take some responsibility for the emails sent from their domain: SPF by listing those IP addresses used to send email; DKIM by digitally signing the emails.

DMARC adds to SPF and DKIM a mechanism that allows a domain owner to advise senders what to do about

Recap: SPF, DKIM, DMARC

SPF validates MAIL FROM vs. its source server (“envelope” information)

DKIM validates the “From:” message header

- Plus other message headers and the message body

Not effective against spammers who

- Use their own domains
- Use legitimate email services, such as webmail
- Pretend to be another user on the same domain

Good for whitelisting and verifying email from trusted sources (.gov, banks, other trusted sources …)

Besides spam, we also care about phishing…

6’0”
5’6”
5’0”
4’6”
4’0”
3’6
3’0
6’0”
5’6”
5’0”
’6”
’0”
’6”
3’0”

Social Engineering

Exploit human behavior to breach security

- Psychological manipulation of people into performing actions or divulging confidential information
- *"…the art and science of getting people to comply with your wishes"*
- *“A euphemism for non-technical or low-technology means (lies, impersonation, tricks, bribes, blackmail, and threats) used to attack information systems”*

Human-based deception

- Take advantage of the victim’s ignorance and the natural human inclination to be helpful and liked

Technology-based deception

- Trick users into believing that they are interacting with a “real” computer system and are experiencing “legitimate” behavior

Basic Types of Social Engineering

Phishing

Sending emails appearing to be from reputable sources with the goal of influencing or gaining personal information

Example: emails, text messages, websites, …

Voice/phone phishing

Eliciting information or influencing action by talking to someone over the phone

Example: call to reset password, transfer phone number, change credit card, …

Impersonation

Pretending to be another person, or pretexting, with the goal of gaining physical access to a system or building

Example: pose as delivery persons, fire marshals, technicians, …

Address Obfuscation

Misspelled/similar domain names (typosquatting)

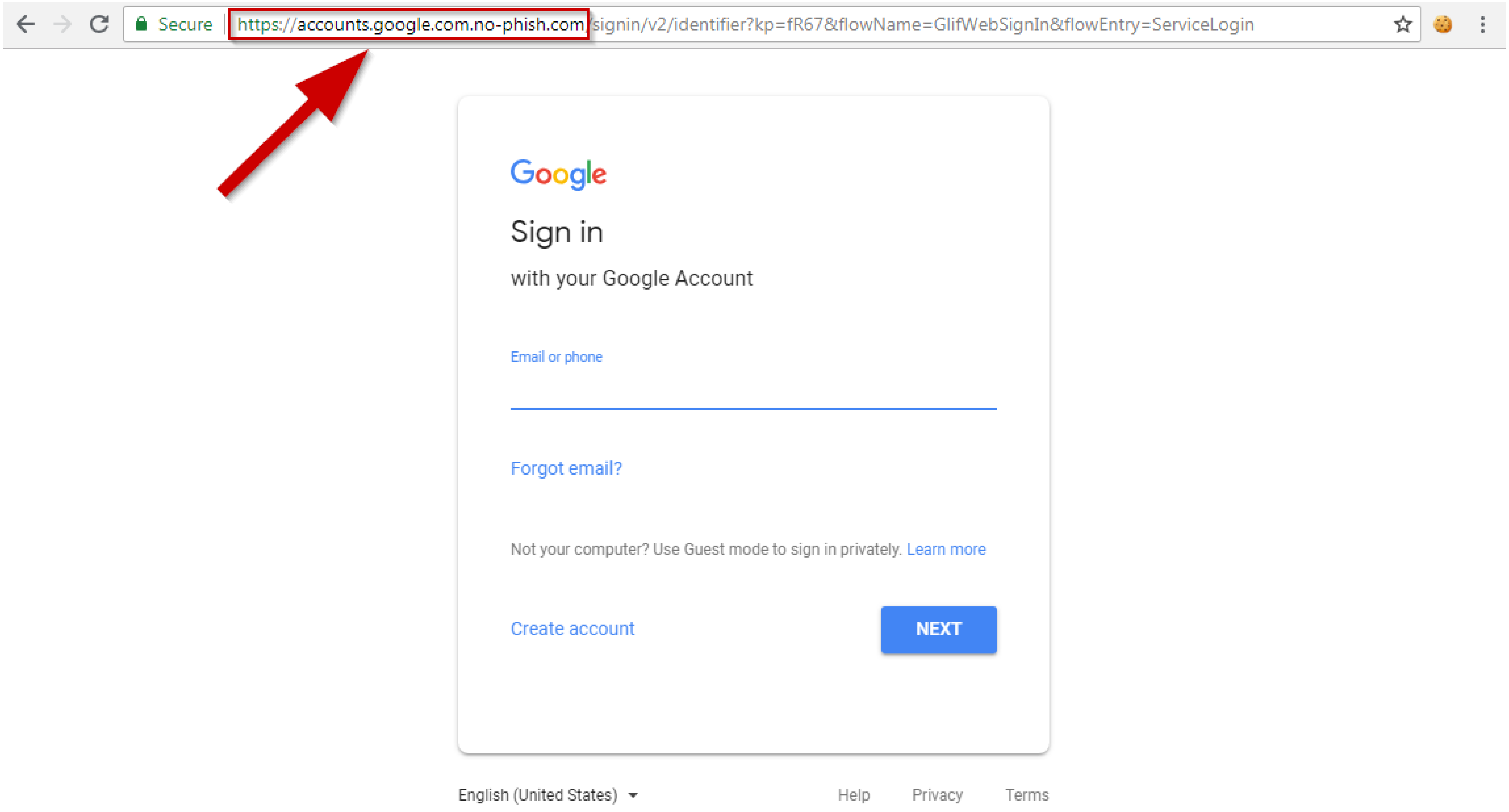
```
From: info@paypa1.com
http://www.citybank.com
```

Misleading <A> tags

```
<a href=“http://www.attacker.com”>http://www.bank.com</a>
```

Seemingly legitimate/complex/long URLs

```
http://www.bankofamerica.com.attacker.net/
http://www.visa.com:UserSession=2f6q988316484495&usersoption=
SecurityUpdate&From@61.252.126.191/verified_by_visa.html
```



Secure https://accounts.google.com.no-phish.com/signin/v2/identifier?kp=fR67&flowName=GlifWebSignIn&flowEntry=ServiceLogin

Google

Sign in

with your Google Account

Not your computer? Use Guest mode to sign in privately. Learn more

© Kuba Gretzky - https://breakdev.org/evilginx-2-next-generation-of-phishing-2fa-tokens/

Address Obfuscation

Homographs, internationalized domain names (IDN), punycode

- `http://ebay.com` (`http://xn--eby-7cd.com/`) – Cyrillic “a” vs. Latin “a”
- Most browsers now display IDNs only for the system’s configured language
- Punycode is shown if a non-default language or mixed languages are used

Dot-less addresses and other URL encoding tricks

- `www.cs.stonybrook.edu` ➔ `http://130.245.27.2` ➔ `http://2197101314`

URL shorteners and redirection chains

- `https://bit.ly/1PibSU0` ➔ `https://definitely-not-a-phishing-site.com`
- Completely hide the actual destination URL (even hovering doesn’t work)

Typosquatting and Fake URLs

Besides phishing: opportunistic "hijacking" of typos when writing a website address into the URL bar

- Misspelling or foreign language spelling: `exemple.com`
- Common typos/permutations: `examlpe.com`
- Differently phrased names: `examples.com`
- Different top-level domains: `example.org`, `example.cm`, `example.co`, …

Many other variations

- Combosquatting: combining seemingly legitimate/gripe/random words: `example-security.com`, `example-sucks.com`, `examplenext.com`, …
- Doppelganger domains by omitting a period: `financeexample.com` (instead of `finance.example.com`)
- Extra period: `e.xample.com`

Spear Phishing

Meticulously prepared, carefully personalized, highly convincing messages targeted to specific individuals

- Seemingly coming from trusted colleagues/sources
- May come from their real accounts if they have been compromised
- Personalized according to their target: mention real names, personal and business information, recent activity (e.g., real purchases), …

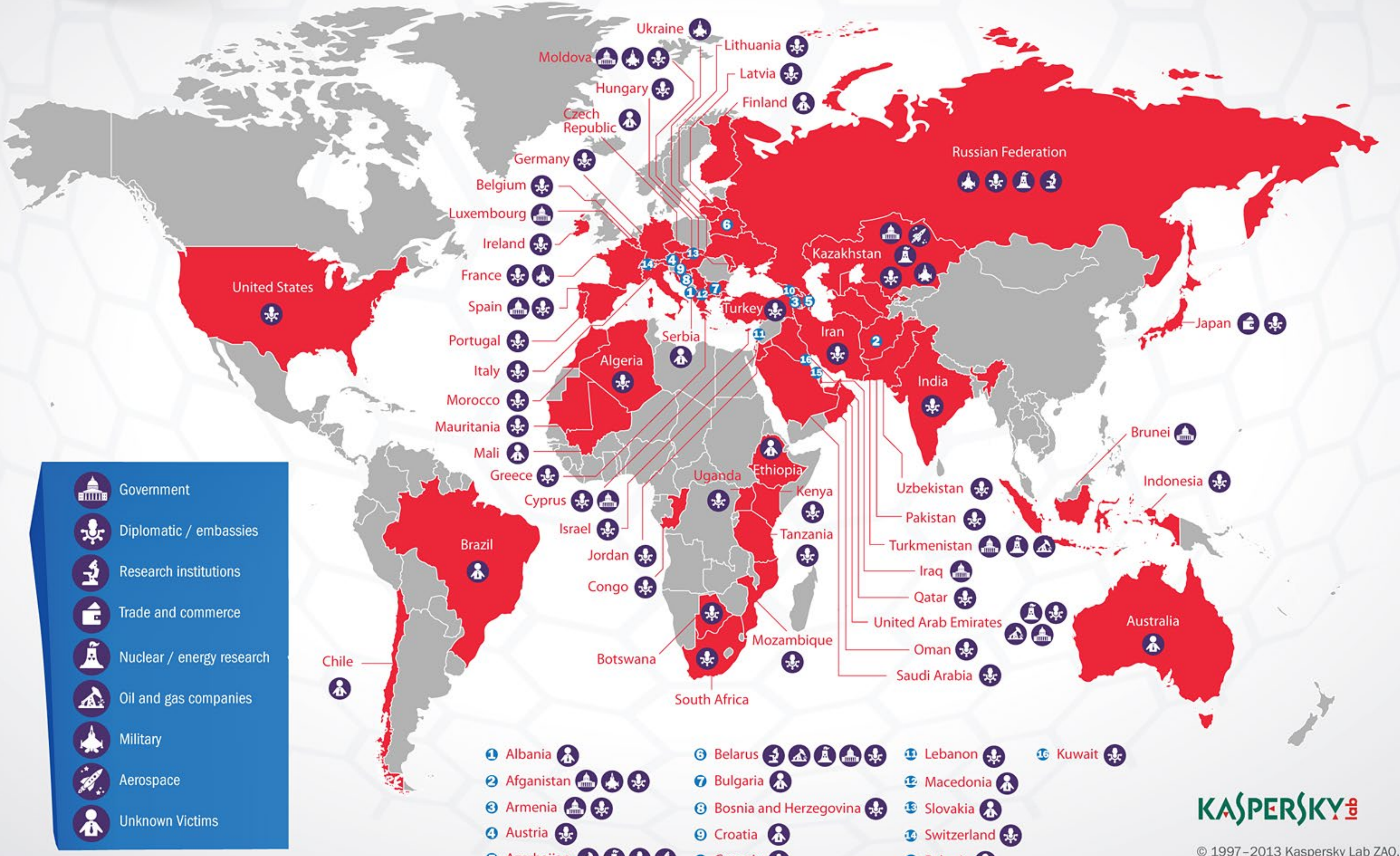
Highly effective! Used extensively in targeted attacks

- Document attachments exploiting 0day vulnerabilities
- Links to fake login pages for stealing credentials

Numerous recent incidents

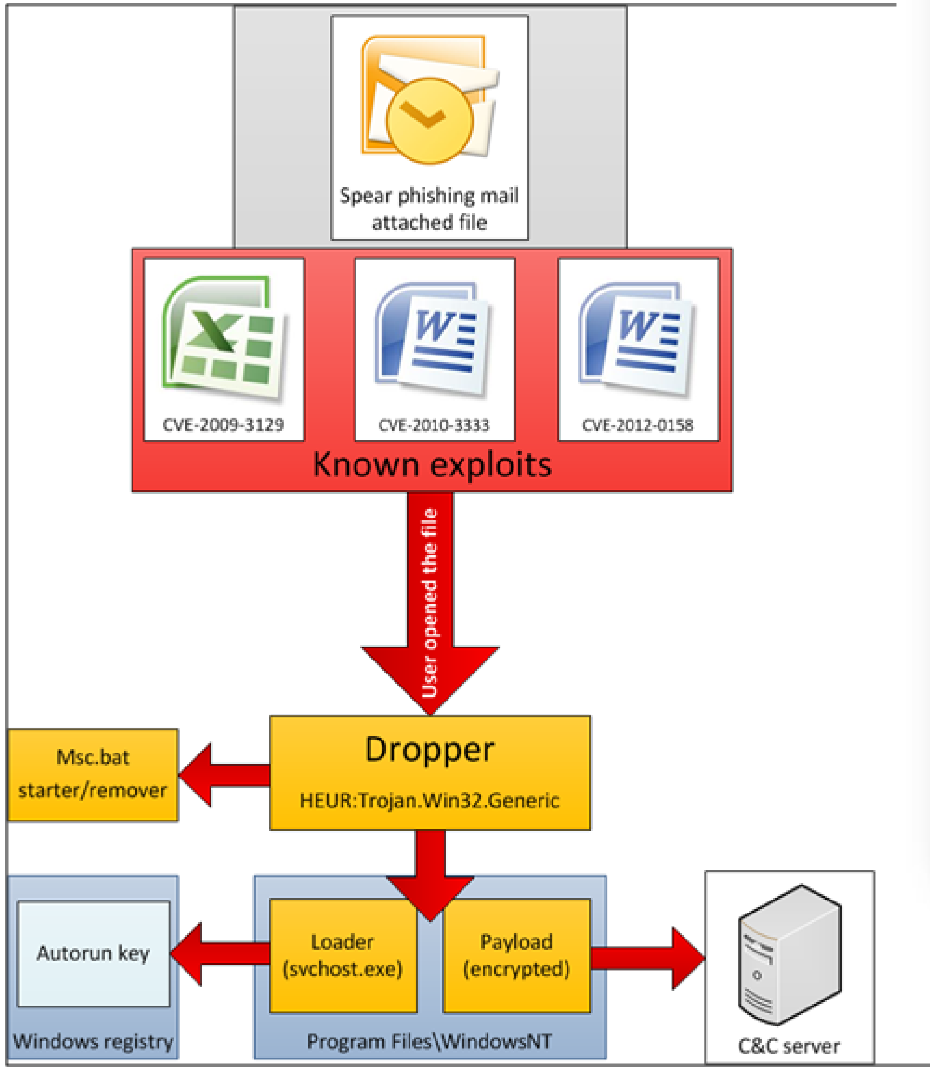
Operation “Red October”

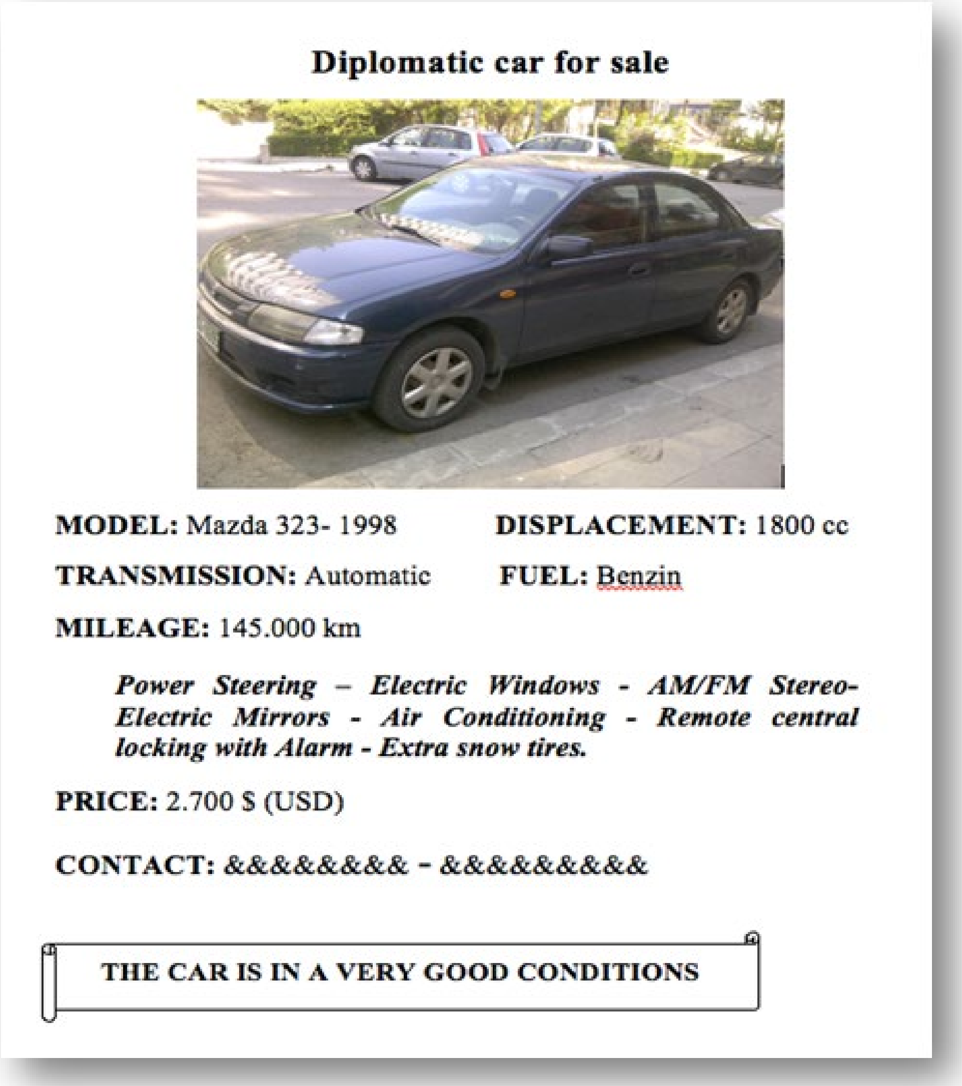
Victims of advanced cyber–espionage network



KASPERSKY lab

Operation “Red October” (2012)





Diagnomatic car for sale

MODEL: Mazda 323- 1998 **DISPLACEMENT:** 1800 cc

TRANSMISSION: Automatic **FUEL:** Benzin

MILEAGE: 145.000 km

Power Steering – Electric Windows - AM/FM Stereo- Electric Mirrors - Air Conditioning - Remote central locking with Alarm - Extra snow tires.

PRICE: 2.700 $ (USD)

CONTACT: &&&&&&&& - &&&&&&&&&

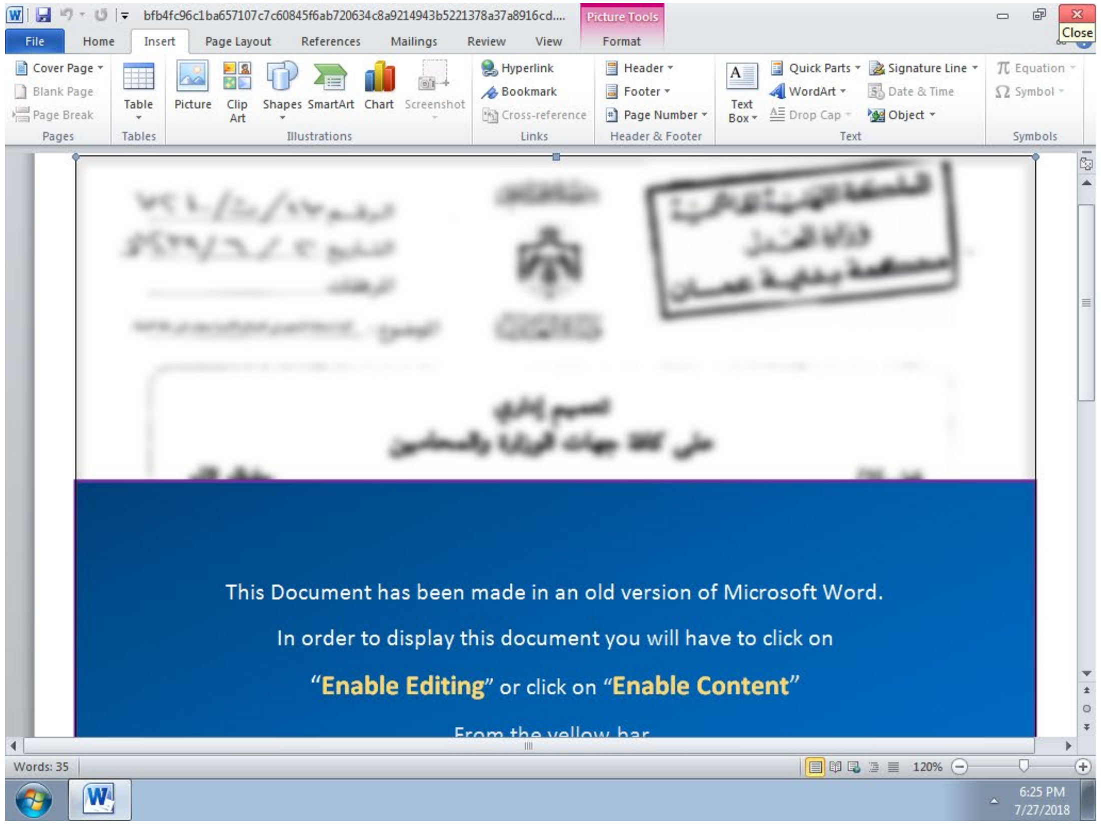
THE CAR IS IN A VERY GOOD CONDITIONS

© https://securelist.com/red-october-diplomatic-cyber-attacks-investigation/36740/

MuddyWater (2018)

Social engineering to enable macros

Decoy document images according to the target's country



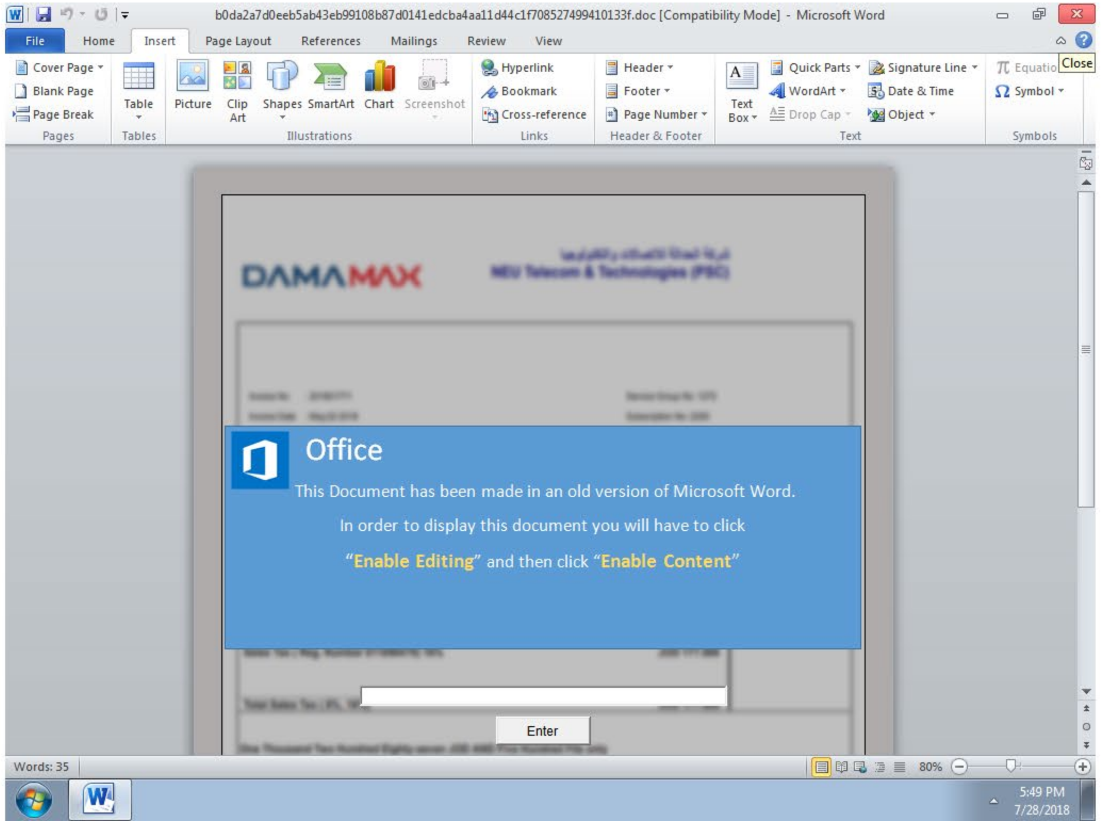
bfb4fc96c1ba657107c7c60845f6ab720634c8a9214943b5221378a37a8916cd....

This Document has been made in an old version of Microsoft Word.

In order to display this document you will have to click on

"Enable Editing" or click on "Enable Content"

From the yellow bar



b0da2a7d0eeb5ab43eb99108b87d0141edcba4aa11d44c1f708527499410133f.doc [Compatibility Mode] - Microsoft Word

Office

This Document has been made in an old version of Microsoft Word.

In order to display this document you will have to click

"Enable Editing" and then click "Enable Content"

© https://securelist.com/muddywater/88059/

Personal example #1: Phishing message targeting SBU users

From: **SBU Team <ebrahle2@kent.edu>**
Date: Tue, Feb 2, 2016 at 8:42 PM
Subject: cyber security
To: XXXXXXXXXXXX

We've detected spam-like activity in your webmail account,
which is against our Acceptable Use Policy (AUP).

Kindly click on the link below to verify that you're the owner of the account and
not a spammer.

http://is.gd/stonybrooksecure

We apologize for any inconvenience this may have cause you.

Thanks,
SBU Team

Personal (counter) example #2: *Legitimate* message from an IT department

From: XXXXXXXXXX
Date: XXXXXXXXXX
Subject: Important! You must change your XXXXXXX password
To: XXXXXXXXXXXX

[This is not a spam mail, this email is from me, XXXXXXXXXXXX]

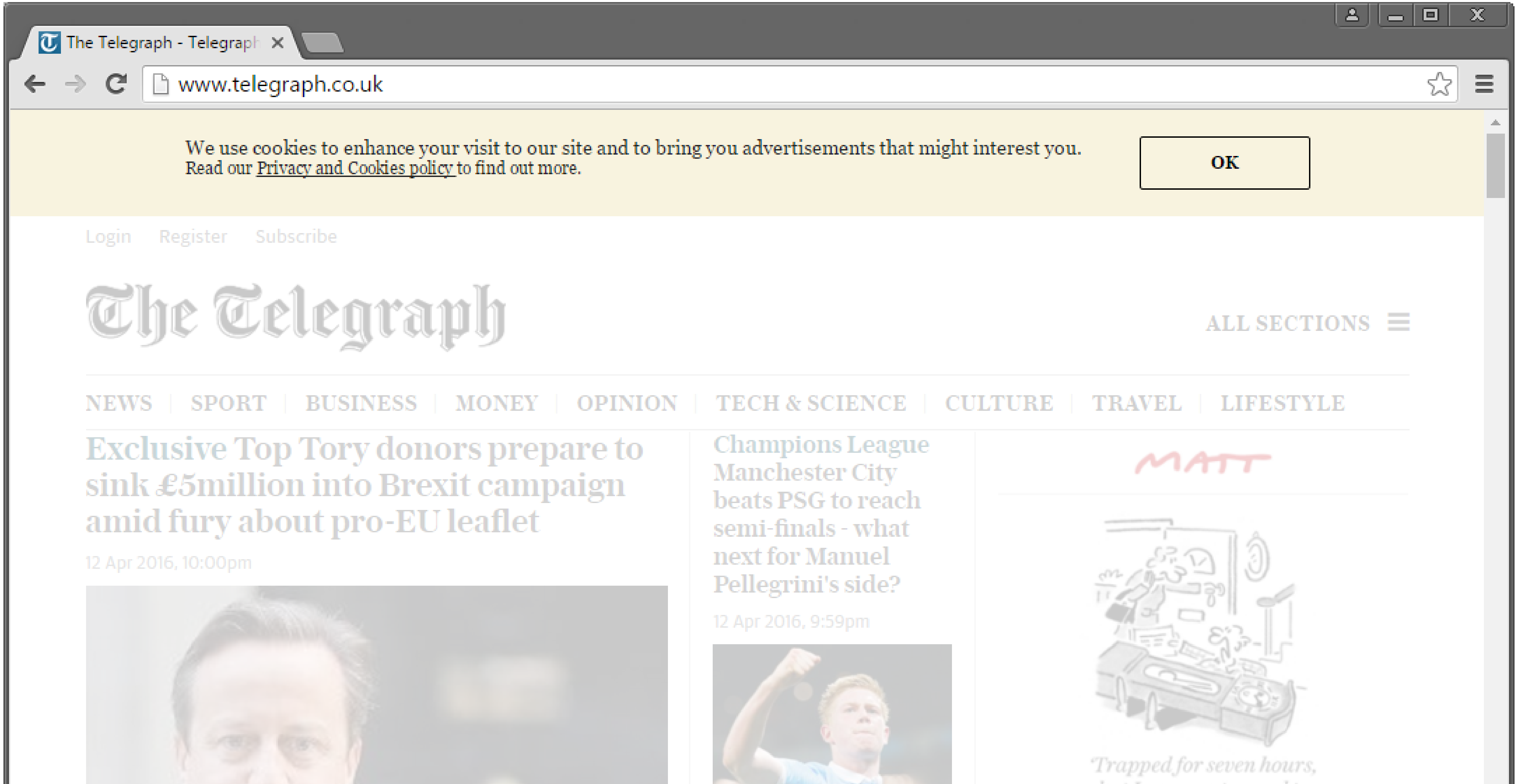
Member of XXXXXXXXX Department,

PLEASE CHANGE YOUR XXXXXX PASSWORD!

We just upgraded the security of XXXXXX. Your current password is no longer working. You must change your password if you want to log into XXXXXX. [...]

To change your XXXXX password:
http://XXXXXXXXX.XXX -> forgot your password -> follow the instructions

More training of users to click on things…


The Telegraph - Telegraph
www.telegraph.co.uk
OK

We use cookies to enhance your visit to our site and to bring you advertisements that might interest you.
Read our Privacy and Cookies policy to find out more.

Login Register Subscribe
The Telegraph
ALL SECTIONS
NEWS | SPORT | BUSINESS | MONEY | OPINION | TECH & SCIENCE | CULTURE | TRAVEL | LIFESTYLE
MATT

Exclusive Top Tory donors prepare to sink £5million into Brexit campaign amid fury about pro-EU leaflet

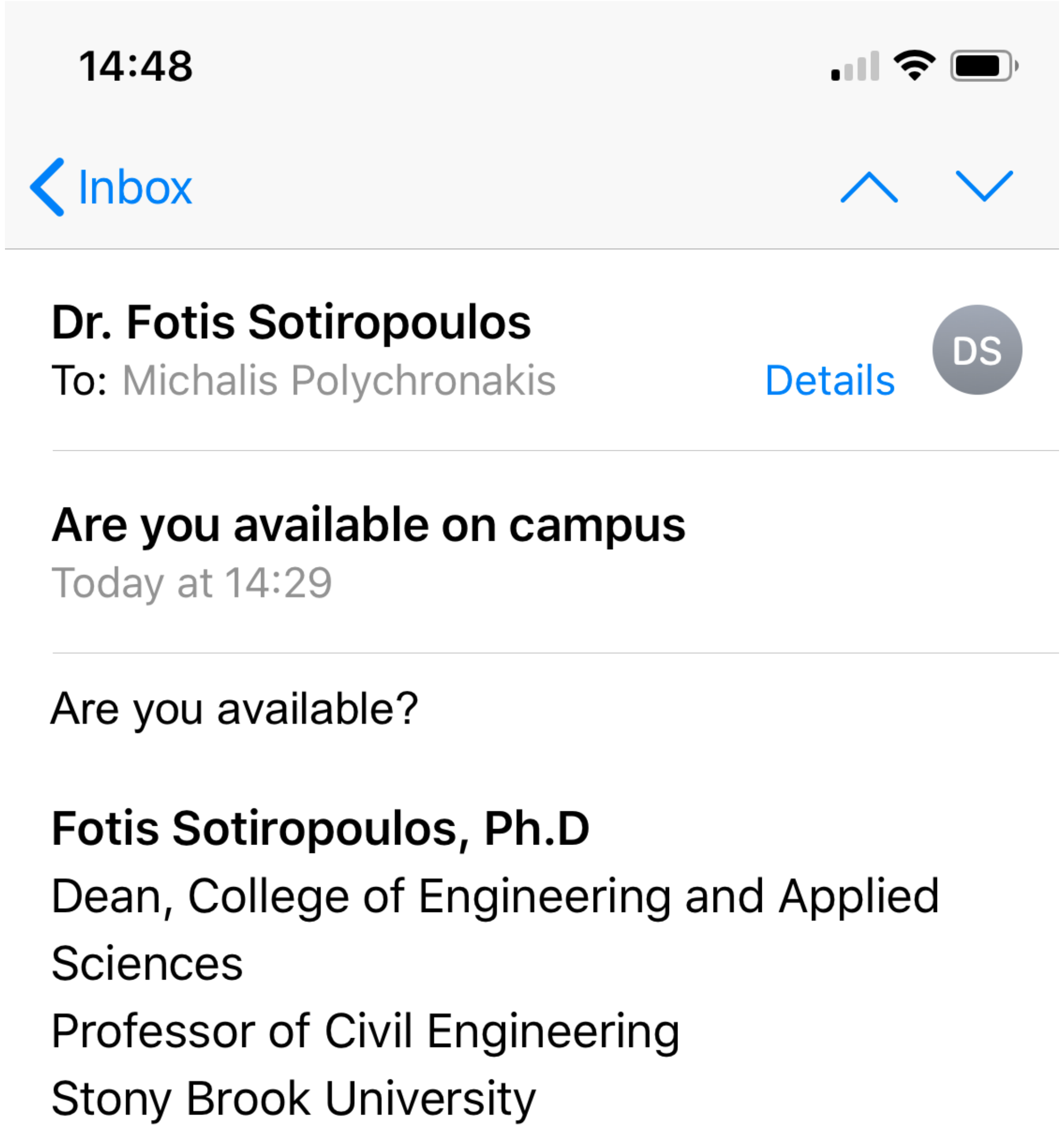
12 Apr 2016, 10:00pm

Champions League Manchester City beats PSG to reach semi-finals - what next for Manuel Pellegrini's side?

12 Apr 2016, 9:59pm

'Trapped for seven hours,

Personal example #3: targeted phishing message (which I opened on iPhone)



Dr. Fotis Sotiropoulos

To: Michalis Polychronakis

Are you available on campus

Today at 14:29

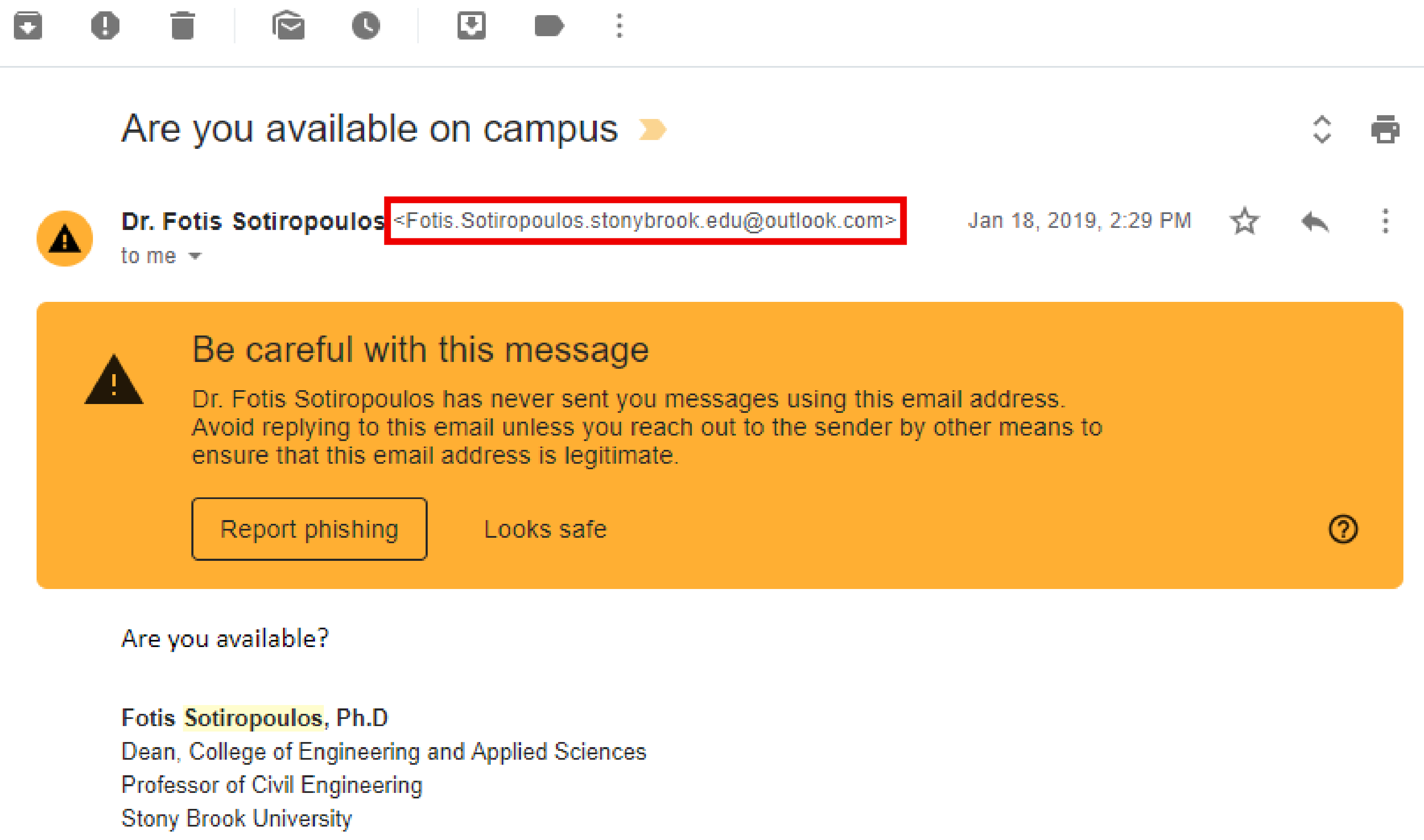
Are you available?

Fotis Sotiropoulos, Ph.D

Dean, College of Engineering and Applied Sciences

Professor of Civil Engineering

Stony Brook University



Are you available on campus

Dr. Fotis Sotiropoulos <Fotis.Sotiropoulos.stonybrook.edu@outlook.com>

to me

Jan 18, 2019, 2:29 PM

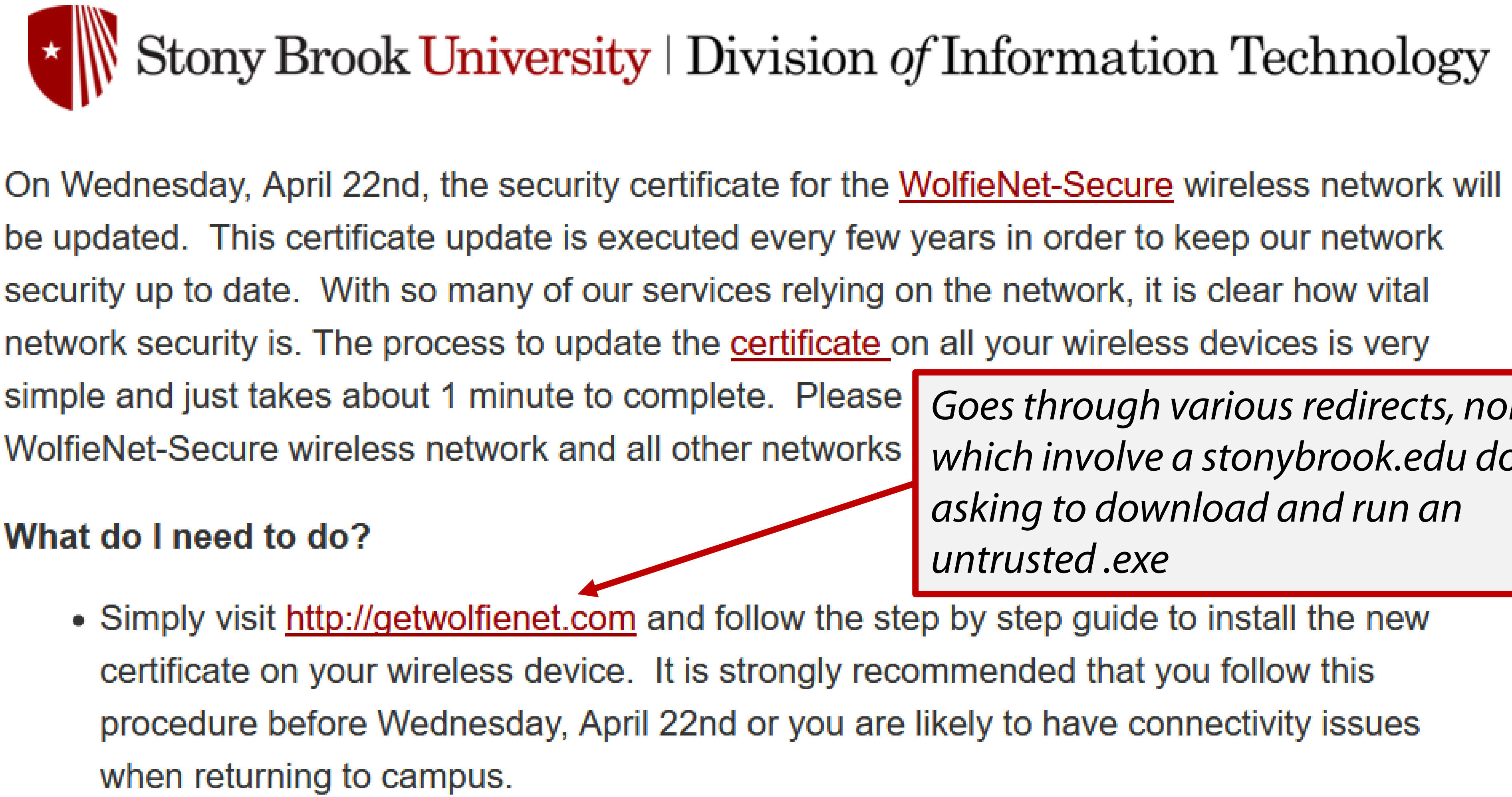
Be careful with this message

Dr. Fotis Sotiropoulos has never sent you messages using this email address. Avoid replying to this email unless you reach out to the sender by other means to ensure that this email address is legitimate.

Are you available?

Fotis Sotiropoulos, Ph.D
Dean, College of Engineering and Applied Sciences
Professor of Civil Engineering
Stony Brook University

Personal (counter) example #4: *Legitimate* message to SBU users



Stony Brook University | Division *of* Information Technology

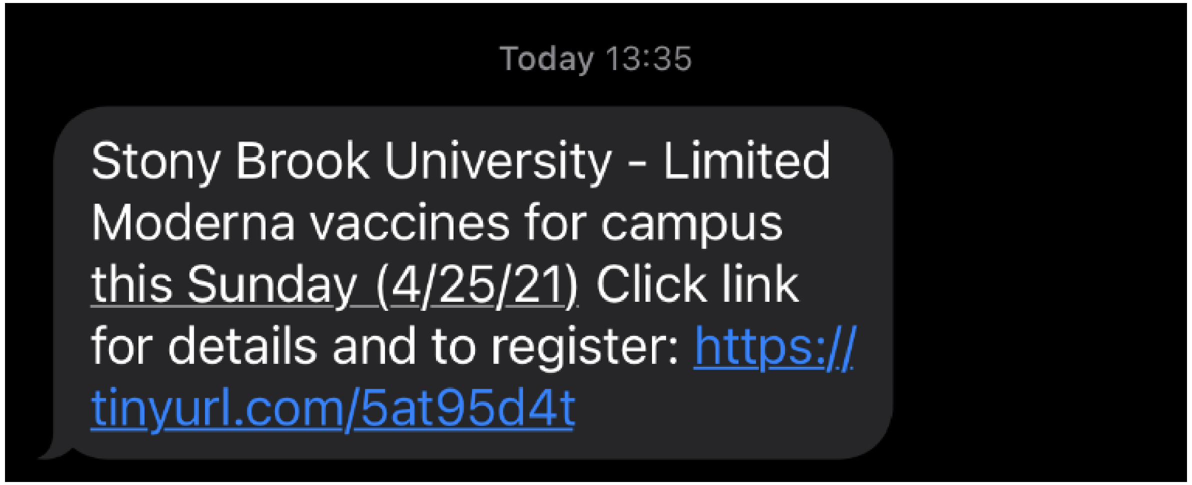
On Wednesday, April 22nd, the security certificate for the WolfieNet-Secure wireless network will be updated. This certificate update is executed every few years in order to keep our network security up to date. With so many of our services relying on the network, it is clear how vital network security is. The process to update the certificate on all your wireless devices is very simple and just takes about 1 minute to complete. Please
WolfieNet-Secure wireless network and all other networks

What do I need to do?

- Simply visit http://getwolfienet.com and follow the step by step guide to install the new certificate on your wireless device. It is strongly recommended that you follow this procedure before Wednesday, April 22nd or you are likely to have connectivity issues when returning to campus.

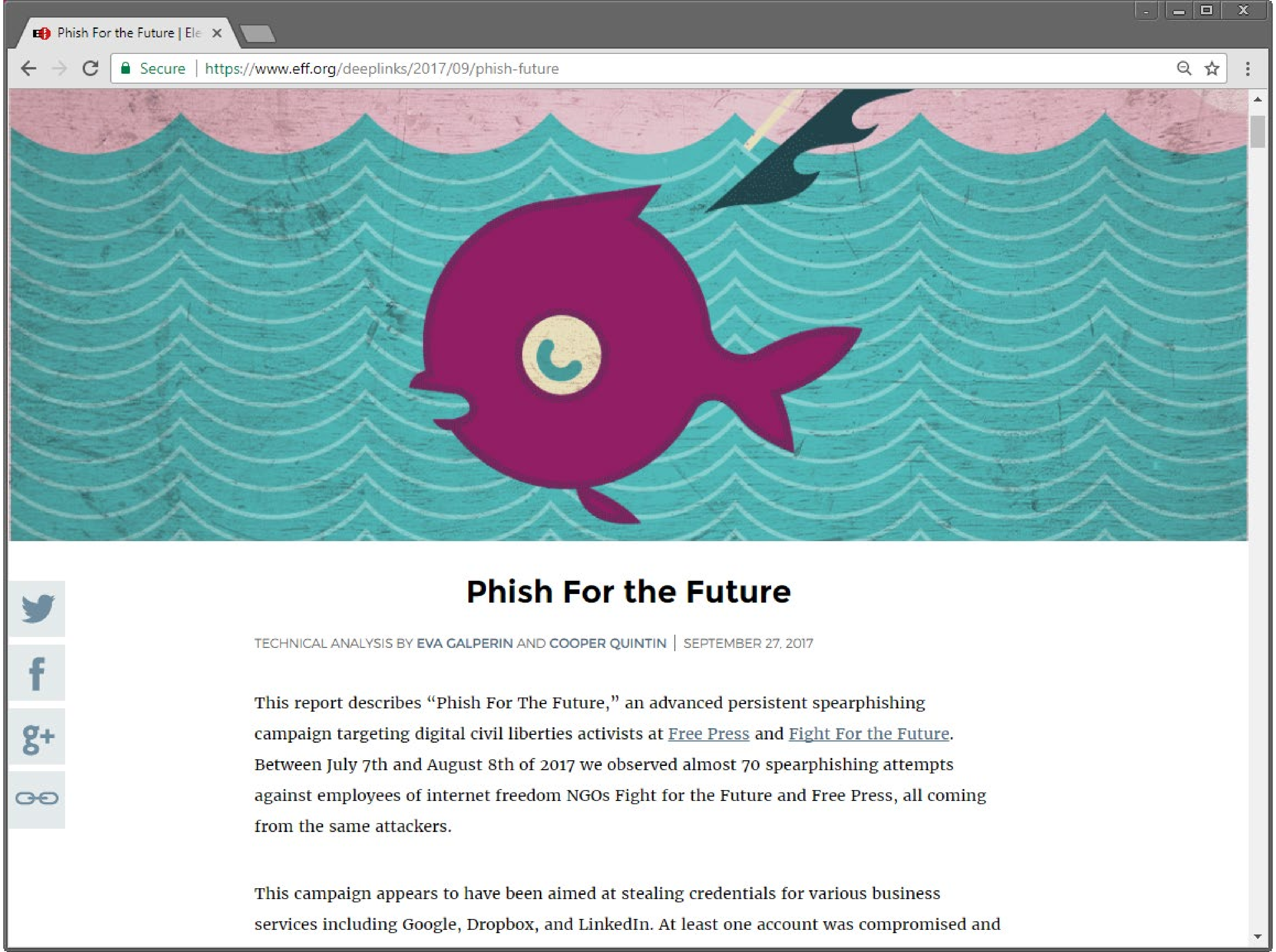
Goes through various redirects, none of which involve a stonybrook.edu domain, asking to download and run an untrusted .exe

Personal (counter) example #5: SMS received a few hours before this lecture



Today 13:35

Stony Brook University - Limited Moderna vaccines for campus this Sunday (4/25/21) Click link for details and to register: https://tinyurl.com/5at95d4t



Phish For the Future | Ele
Secure
https://www.eff.org/deeplinks/2017/09/phish-future

Phish For the Future

TECHNICAL ANALYSIS BY EVA GALPERIN AND COOPER QUINTIN | SEPTEMBER 27, 2017

This report describes “Phish For The Future,” an advanced persistent spearphishing campaign targeting digital civil liberties activists at Free Press and Fight For the Future. Between July 7th and August 8th of 2017 we observed almost 70 spearphishing attempts against employees of internet freedom NGOs Fight for the Future and Free Press, all coming from the same attackers.

This campaign appears to have been aimed at stealing credentials for various business services including Google, Dropbox, and LinkedIn. At least one account was compromised and

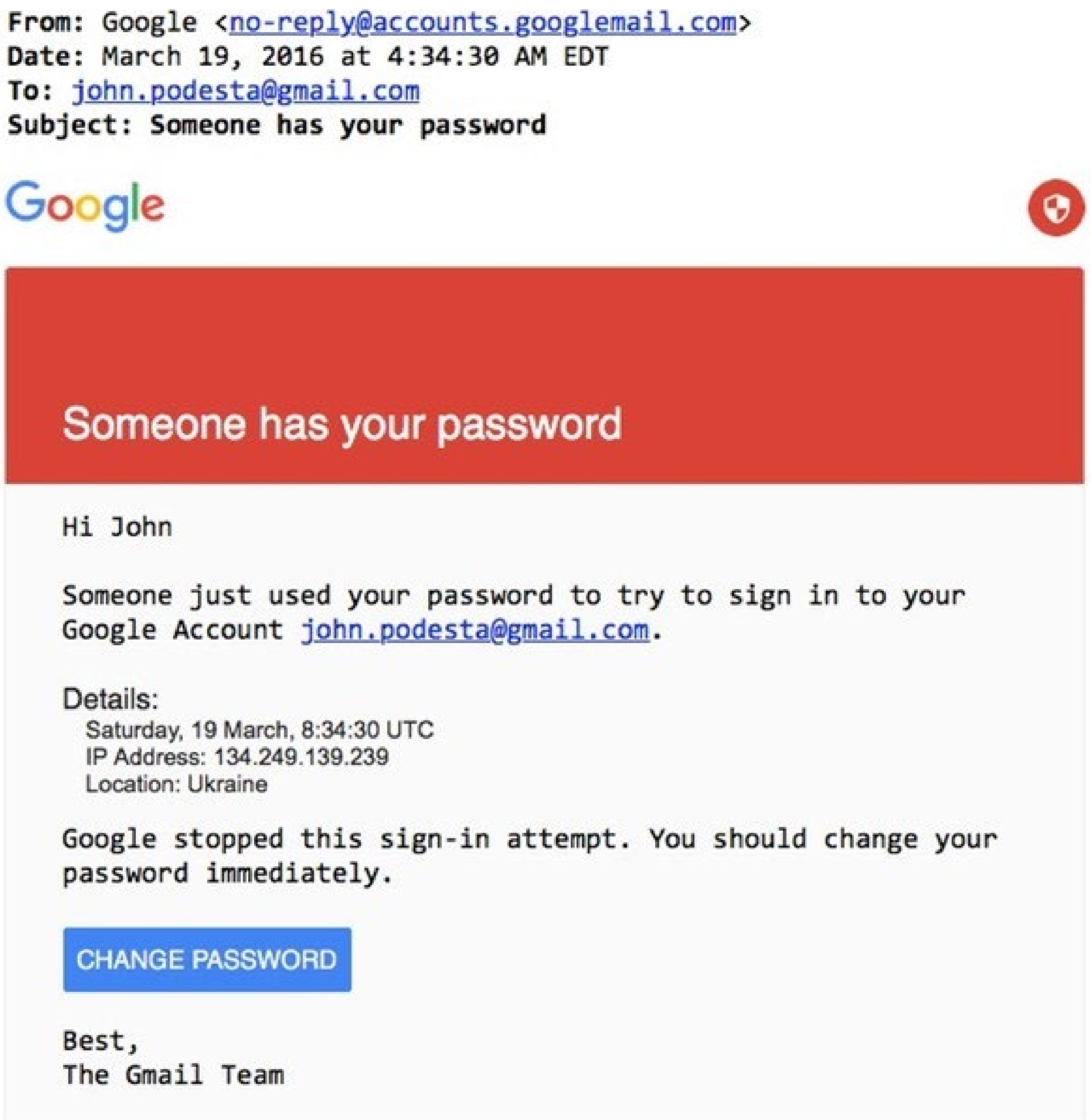
Some of the attacks were generic, such as a link to view a Gmail document supposedly sent by a co-worker or a LinkedIn notification message from a colleague.

Another attack pretended to be from a target's husband, sharing family photos; the email was forged to include the husband's name.

Yet another attack pretended to be a YouTube comment for a real YouTube video that the target had uploaded.

Some of the headlines are designed to appeal to the political interests of the targets, such as: "George W. Bush ON TRUMP'S TWEET: A FREE PRESS IS 'INDISPENSABLE TO DEMOCRACY,'"

The attackers sent emails titled "You have been successfully subscribed to Pornhub.com" and "You have been successfully subscribed to Redtube.com" to the victims. This was followed up minutes later with several emails all disguised as coming from Pornhub or Redtube with explicit subject lines. Each of the emails contained an unsubscribe link which directed the target to a Google credential phishing page.



From: Google <no-reply@accounts.googlemail.com>
Date: March 19, 2016 at 4:34:30 AM EDT
To: john.podesta@gmail.com
Subject: Someone has your password

Someone has your password

Hi John

Someone just used your password to try to sign in to your Google Account john.podesta@gmail.com.

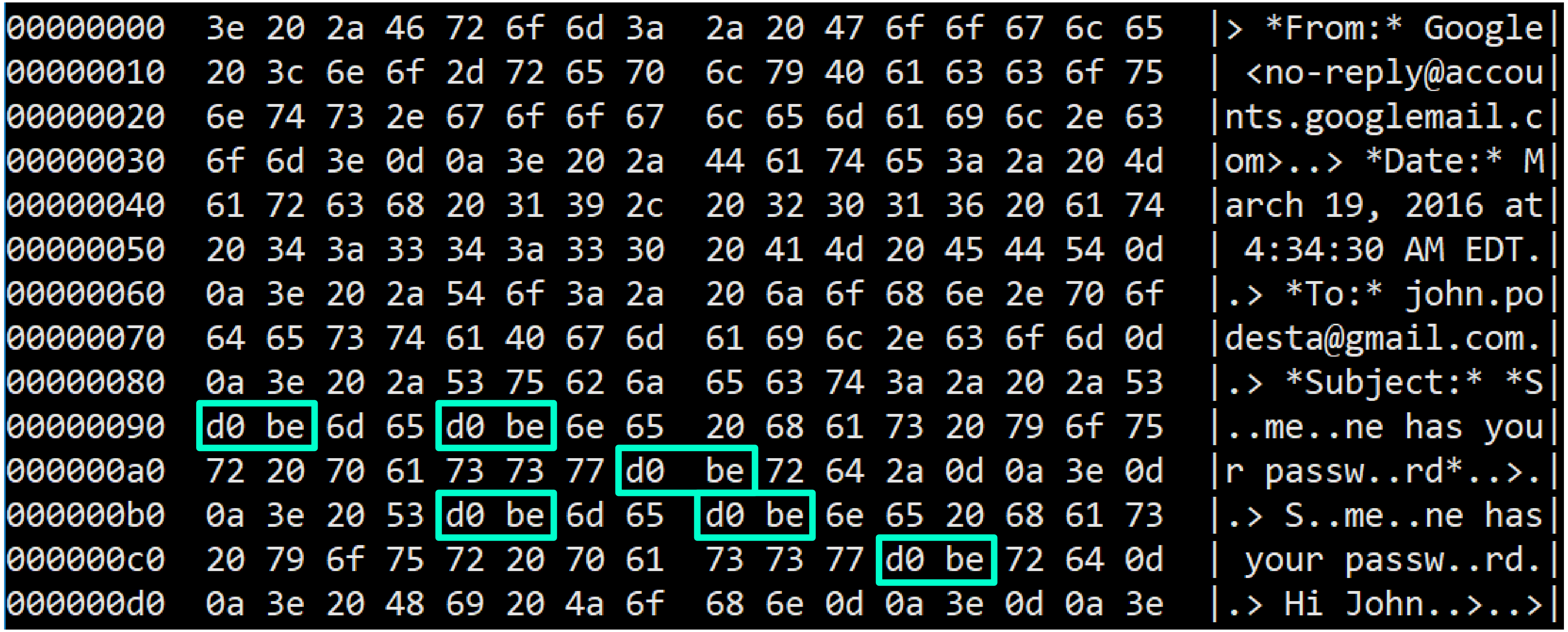
Details:
Saturday, 19 March, 8:34:30 UTC
IP Address: 134.249.139.239
Location: Ukraine

Google stopped this sign-in attempt. You should change your password immediately.

Best,
The Gmail Team

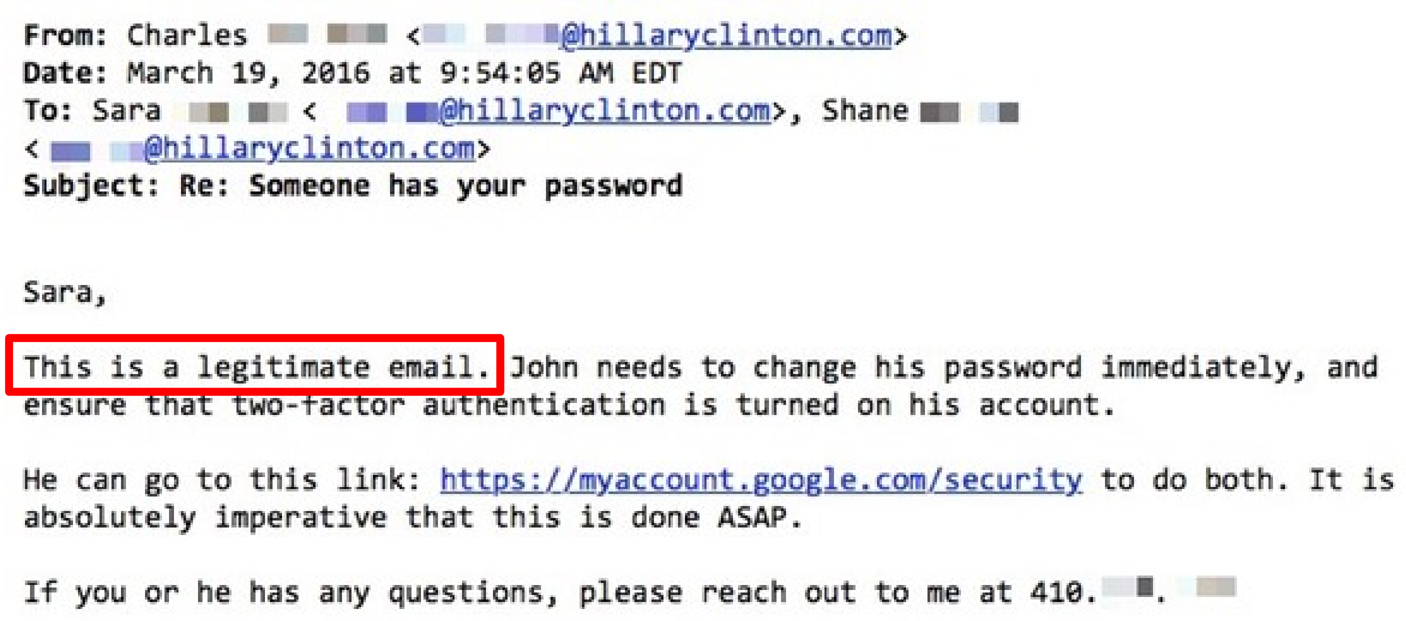
© https://hotforsecurity.bitdefender.com/blog/this-is-the-email-that-hacked-hillary-clintons-campaign-chief-17039.html

Gmail’s filters didn’t catch it…



```
00000000  3e 20 2a 46 72 6f 6d 3a  2a 20 47 6f 6f 67 6c 65  |> *From:* Google|
00000010  20 3c 6e 6f 2d 72 65 70  6c 79 40 61 63 63 6f 75  | <no-reply@accou|
00000020  6e 74 73 2e 67 6f 6f 67  6c 65 6d 61 69 6c 2e 63  |nts.googlemail.c|
00000030  6f 6d 3e 0d 0a 3e 20 2a  44 61 74 65 3a 2a 20 4d  |om>..> *Date:* M|
00000040  61 72 63 68 20 31 39 2c  20 32 30 31 36 20 61 74  |arch 19, 2016 at|
00000050  20 34 3a 33 34 3a 33 30  20 41 4d 20 45 44 54 0d  | 4:34:30 AM EDT.|
00000060  0a 3e 20 2a 54 6f 3a 2a  20 6a 6f 68 6e 2e 70 6f  |.> *To:* john.po|
00000070  64 65 73 74 61 40 67 6d  61 69 6c 2e 63 6f 6d 0d  |desta@gmail.com.|
00000080  0a 3e 20 2a 53 75 62 6a  65 63 74 3a 2a 20 2a 53  |.> *Subject:* *S|
00000090  d0 be 6d 65 d0 be 6e 65  20 68 61 73 20 79 6f 75  |..me..ne has you|
000000a0  72 20 70 61 73 73 77 d0  be 72 64 2a 0d 0a 3e 0d  |r passw..rd*..>.|
000000b0  0a 3e 20 53 d0 be 6d 65  d0 be 6e 65 20 68 61 73  |.> S..me..ne has|
000000c0  20 79 6f 75 72 20 70 61  73 73 77 d0 be 72 64 0d  | your passw..rd.|
000000d0  0a 3e 20 48 69 20 4a 6f  68 6e 0d 0a 3e 0d 0a 3e  |.> Hi John..>..>|
```

Sensibly, Podesta forwarded the email, asking what to do



From: Charles [redacted] [redacted] <[redacted] [redacted]@hillaryclinton.com>
Date: March 19, 2016 at 9:54:05 AM EDT
To: Sara [redacted] [redacted] < [redacted] [redacted]@hillaryclinton.com>, Shane [redacted] [redacted]
< [redacted] [redacted]@hillaryclinton.com>
Subject: Re: Someone has your password

Sara,

This is a legitimate email. John needs to change his password immediately, and ensure that two-factor authentication is turned on his account.

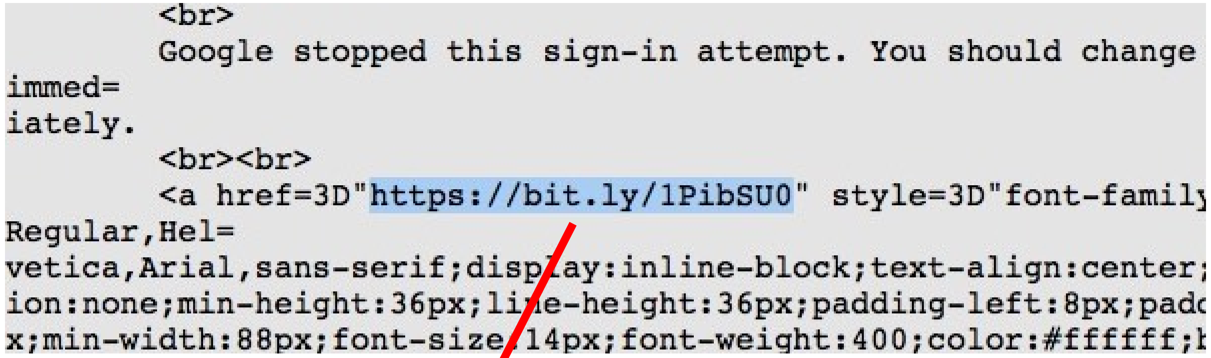
He can go to this link: https://myaccount.google.com/security to do both. It is absolutely imperative that this is done ASAP.

If you or he has any questions, please reach out to me at 410.[redacted]. [redacted]

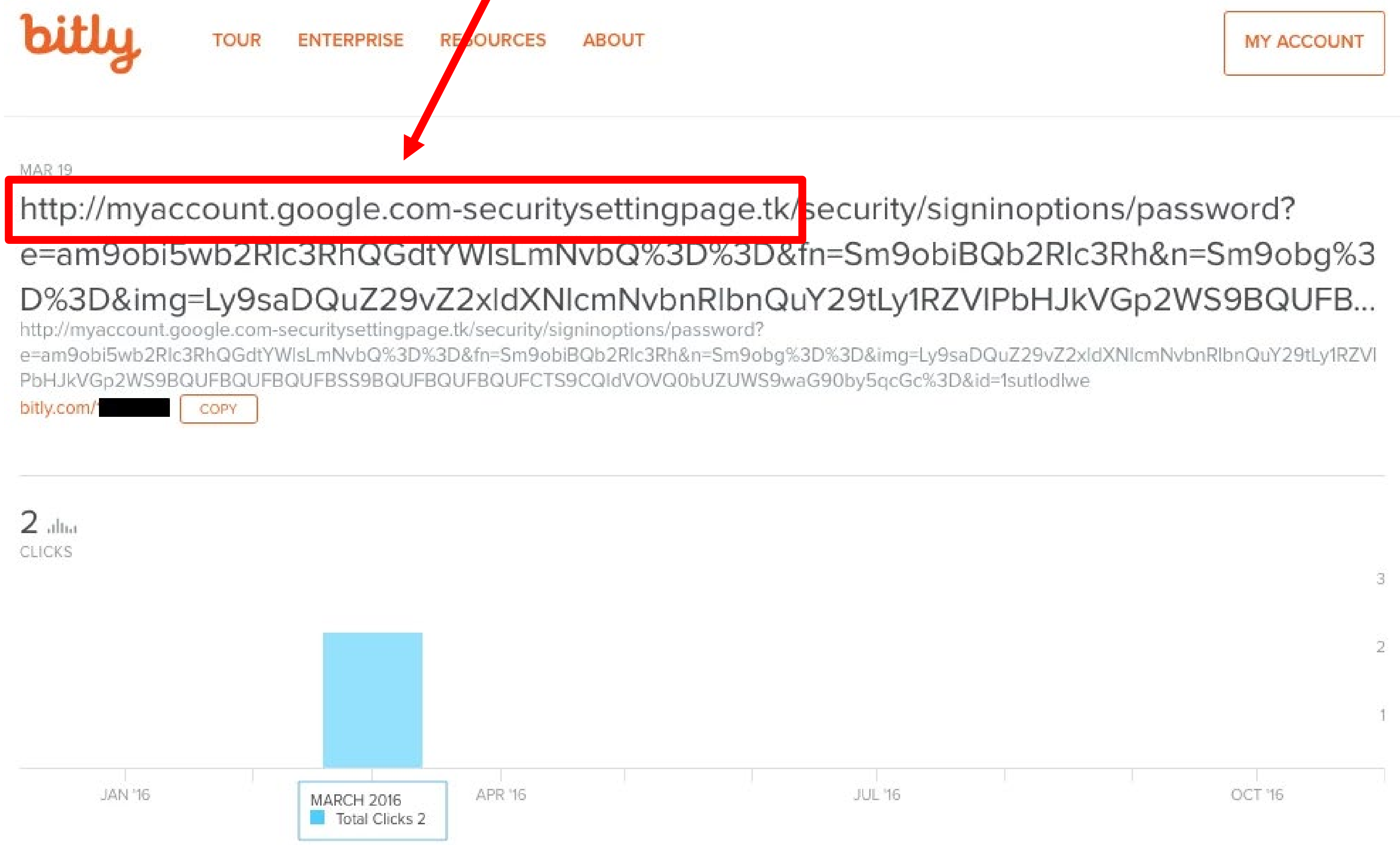
Campaign aide Charles Delavan told the NYT he knew the email was a phishing attack, given that the Clinton campaign was getting a steady stream of them. He meant to reply that the email was "illegitimate."

The IT team did send a legitimate Google link, but that's not the one Podesta clicked

© https://hotforsecurity.bitdefender.com/blog/this-is-the-email-that-hacked-hillary-clintons-campaign-chief-17039.html



```
        <br>
        Google stopped this sign-in attempt. You should change
immed=
iately.
        <br><br>
        <a href=3D"https://bit.ly/1PibSU0" style=3D"font-family
Regular,Hel=
vetica,Arial,sans-serif;display:inline-block;text-align:center;
ion:none;min-height:36px;line-height:36px;padding-left:8px;padd
x;min-width:88px;font-size:14px;font-weight:400;color:#ffffff;b
```



MAR 19

http://myaccount.google.com-securitysettingpage.tk/security/signinoptions/password?e=am9obi5wb2Rlc3RhQGdtYWlsLmNvbQ%3D%3D&fn=Sm9obiBQb2Rlc3Rh&n=Sm9obg%3D%3D&img=Ly9saDQuZ29vZ2xldXNlcmNvbnRlbnQuY29tLy1RZVlPbHJkVGp2WS9BQUFB...

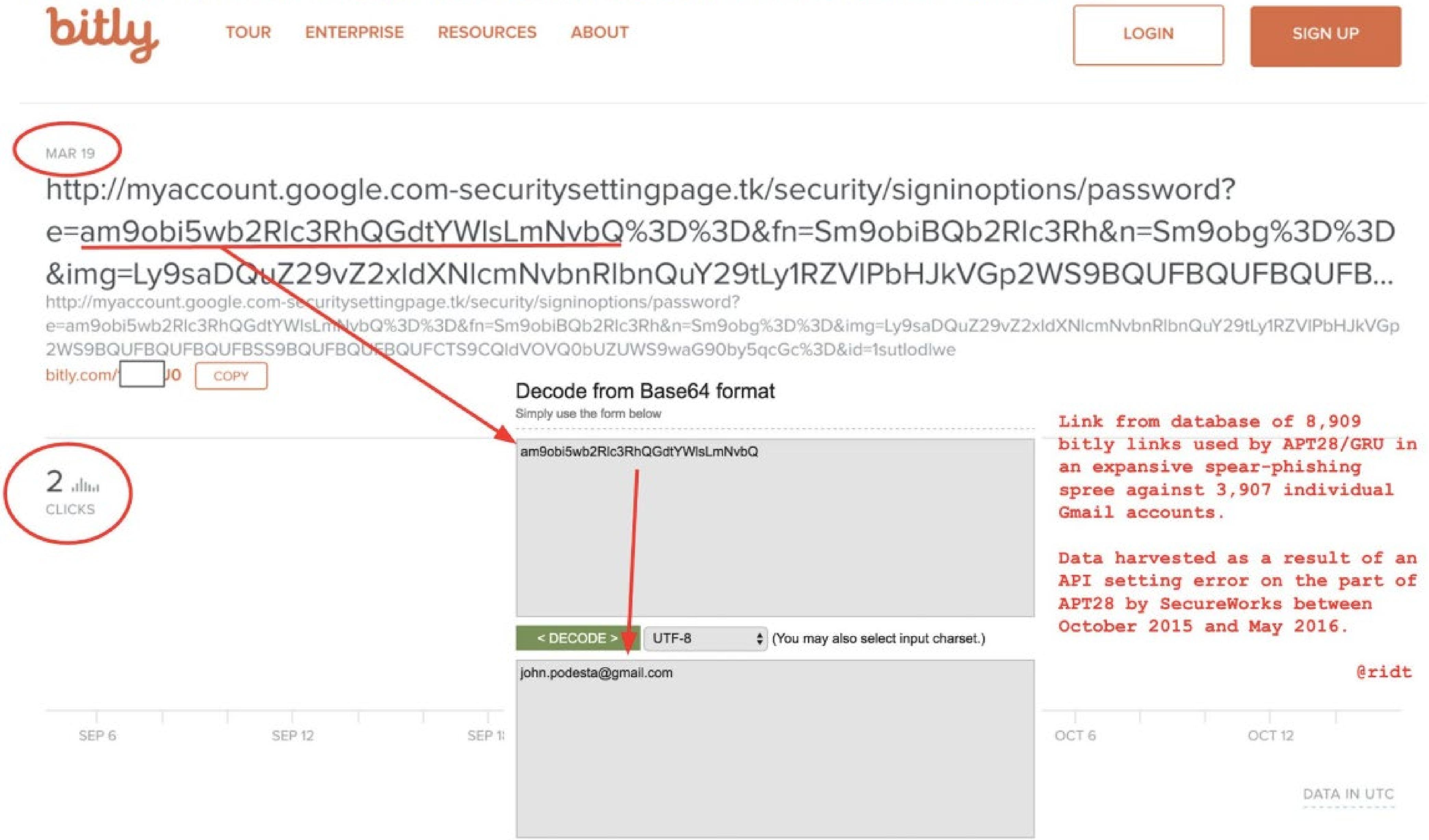
http://myaccount.google.com-securitysettingpage.tk/security/signinoptions/password?e=am9obi5wb2Rlc3RhQGdtYWlsLmNvbQ%3D%3D&fn=Sm9obiBQb2Rlc3Rh&n=Sm9obg%3D%3D&img=Ly9saDQuZ29vZ2xldXNlcmNvbnRlbnQuY29tLy1RZVlPbHJkVGp2WS9BQUFBQUFBQUFBSS9BQUFBQUFBQUFCTS9CQldVOVQ0bUZUWS9waG90by5qcGc%3D&id=1sutlodlwe

bitly.com/[redacted] COPY

2 CLICKS

© https://hotforsecurity.bitdefender.com/blog/this-is-the-email-that-hacked-hillary-clintons-campaign-chief-17039.html

How APT28/FANCYBEAR/GRU breached John Podesta's account



MAR 19

http://myaccount.google.com-securitysettingpage.tk/security/signinoptions/password?e=am9obi5wb2Rlc3RhQGdtYWlsLmNvbQ%3D%3D&fn=Sm9obiBQb2Rlc3Rh&n=Sm9obg%3D%3D&img=Ly9saDQuZ29vZ2xldXNlcmNvbnRlbnQuY29tLy1RZVlPbHJkVGp2WS9BQUFBQUFBQUFB...

http://myaccount.google.com-securitysettingpage.tk/security/signinoptions/password?e=am9obi5wb2Rlc3RhQGdtYWlsLmNvbQ%3D%3D&fn=Sm9obiBQb2Rlc3Rh&n=Sm9obg%3D%3D&img=Ly9saDQuZ29vZ2xldXNlcmNvbnRlbnQuY29tLy1RZVlPbHJkVGp2WS9BQUFBQUFBQUFBSS9BQUFBQUFBQUFCTS9CQldVOVQ0bUZUWS9waG90by5qcGc%3D&id=1sutlodlwe

bitly.com/[redacted]J0 COPY

2 CLICKS

SEP 6 SEP 12 SEP 1 OCT 6 OCT 12

DATA IN UTC

Decode from Base64 format

Simply use the form below

am9obi5wb2Rlc3RhQGdtYWlsLmNvbQ

< DECODE > UTF-8 (You may also select input charset.)

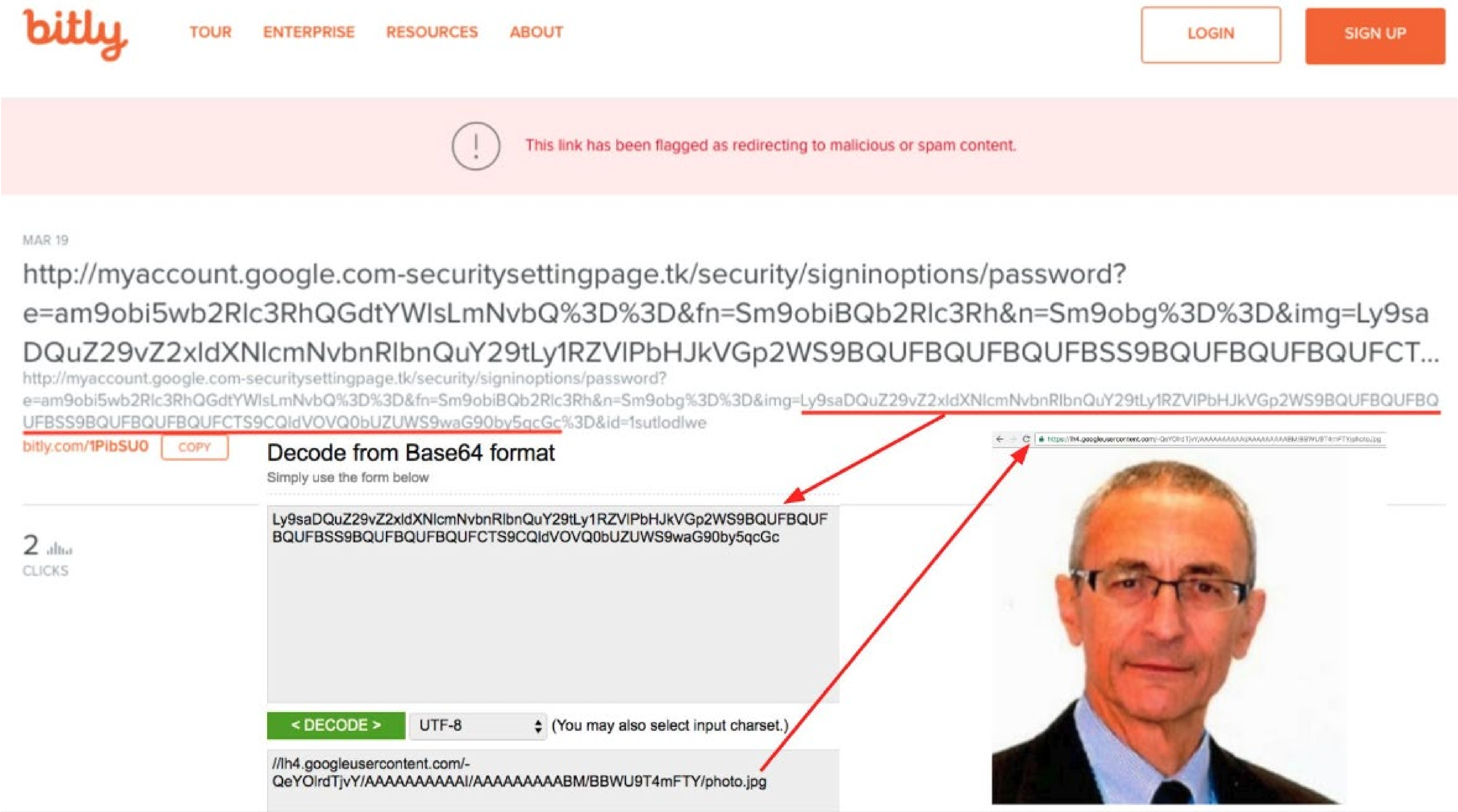
john.podesta@gmail.com

Link from database of 8,909 bitly links used by APT28/GRU in an expansive spear-phishing spree against 3,907 individual Gmail accounts.

Data harvested as a result of an API setting error on the part of APT28 by SecureWorks between October 2015 and May 2016.

@ridt

© Thomas Rid - https://twitter.com/RidT/status/789097977352691712



This link has been flagged as redirecting to malicious or spam content.

MAR 19

http://myaccount.google.com-securitysettingpage.tk/security/signinoptions/password?e=am9obi5wb2Rlc3RhQGdtYWlsLmNvbQ%3D%3D&fn=Sm9obiBQb2Rlc3Rh&n=Sm9obg%3D%3D&img=Ly9saDQuZ29vZ2xldXNlcmNvbnRlbnQuY29tLy1RZVlPbHJkVGp2WS9BQUFBQUFBQUFBSS9BQUFBQUFBQUFCT...

http://myaccount.google.com-securitysettingpage.tk/security/signinoptions/password?e=am9obi5wb2Rlc3RhQGdtYWlsLmNvbQ%3D%3D&fn=Sm9obiBQb2Rlc3Rh&n=Sm9obg%3D%3D&img=Ly9saDQuZ29vZ2xldXNlcmNvbnRlbnQuY29tLy1RZVlPbHJkVGp2WS9BQUFBQUFBQUFBSS9BQUFBQUFBQUFCTS9CQldVOVQ0bUZUWS9waG90by5qcGc%3D&id=1sutlodlwe

bitly.com/1PibSU0 COPY

2 CLICKS

Decode from Base64 format

Simply use the form below

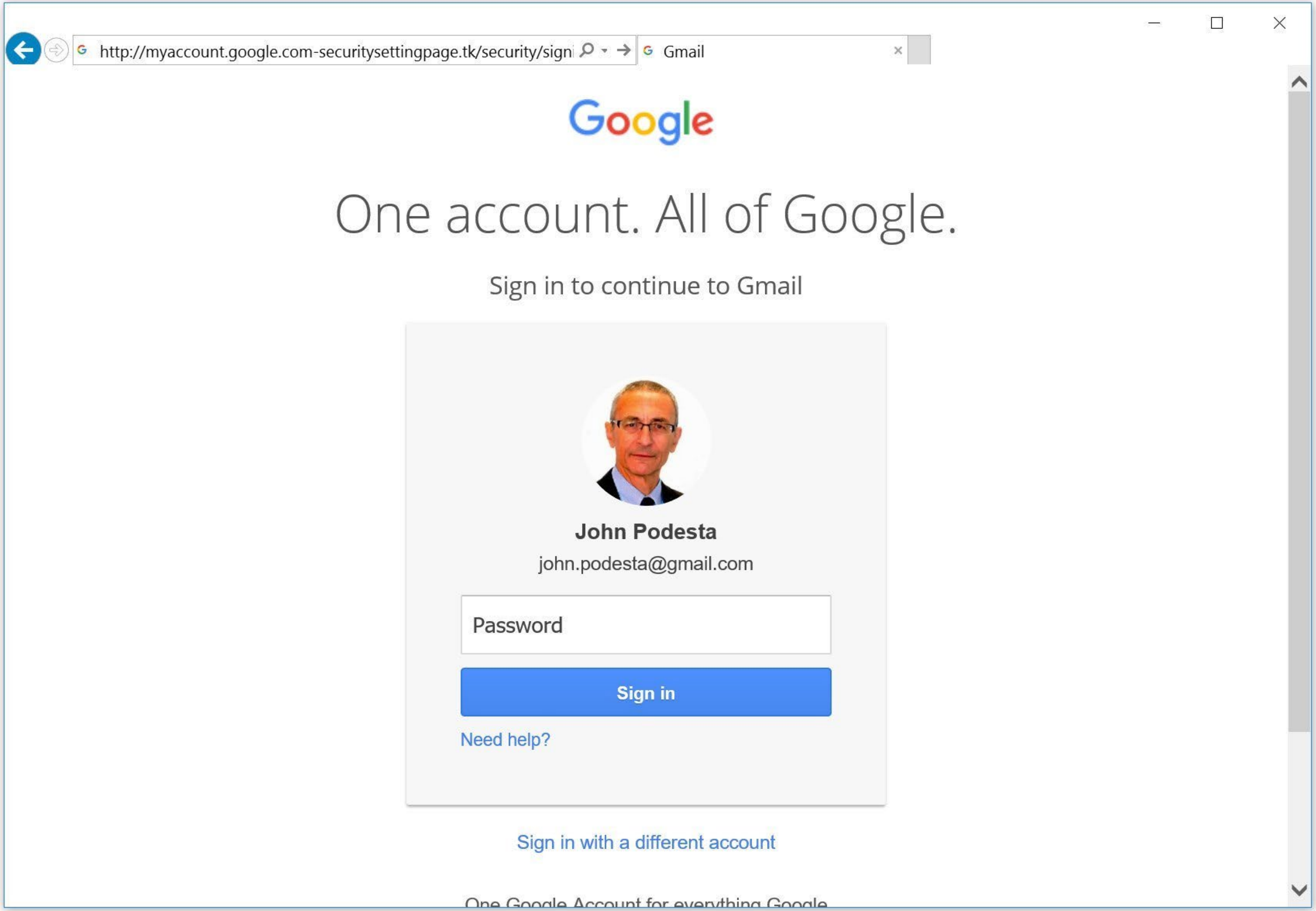
```
Ly9saDQuZ29vZ2xldXNlcmNvbnRlbnQuY29tLy1RZVlPbHJkVGp2WS9BQUFBQUFBQUFBSS9BQUFBQUFBQUFCTS9CQldVOVQ0bUZUWS9waG90by5qcGc
```

< DECODE > UTF-8 (You may also select input charset.)

```
//lh4.googleusercontent.com/-QeYOlrdTjvY/AAAAAAAAAAI/AAAAAAAAABM/BBWU9T4mFTY/photo.jpg
```

https://lh4.googleusercontent.com/-QeYOlrdTjvY/AAAAAAAAAAI/AAAAAAAAABM/BBWU9T4mFTY/photo.jpg

© Thomas Rid - https://twitter.com/RidT/status/789097977352691712



http://myaccount.google.com-securitysettingpage.tk/security/signi

One account. All of Google.

Sign in to continue to Gmail

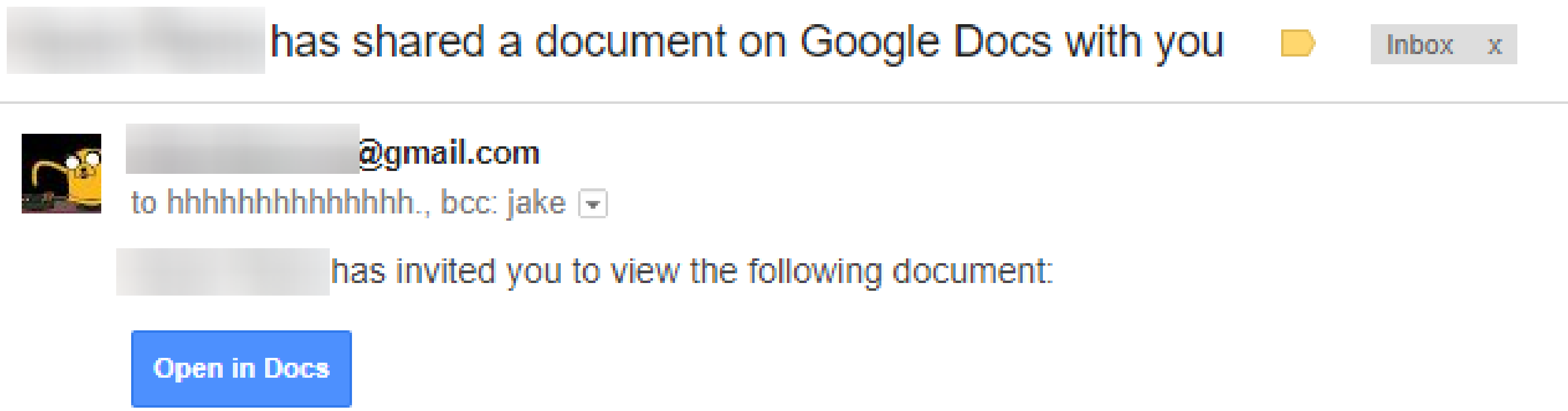
John Podesta

john.podesta@gmail.com

One Google Account for everything Google

Recent Google Docs Phishing Campaign

1) Fake "Google doc has been shared with you" email



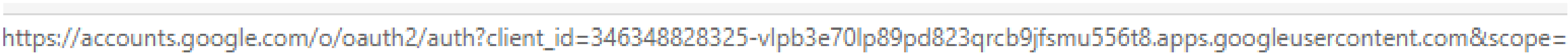
[redacted] has shared a document on Google Docs with you

[redacted]@gmail.com

to hhhhhhhhhhhhhh., bcc: jake

[redacted] has invited you to view the following document:

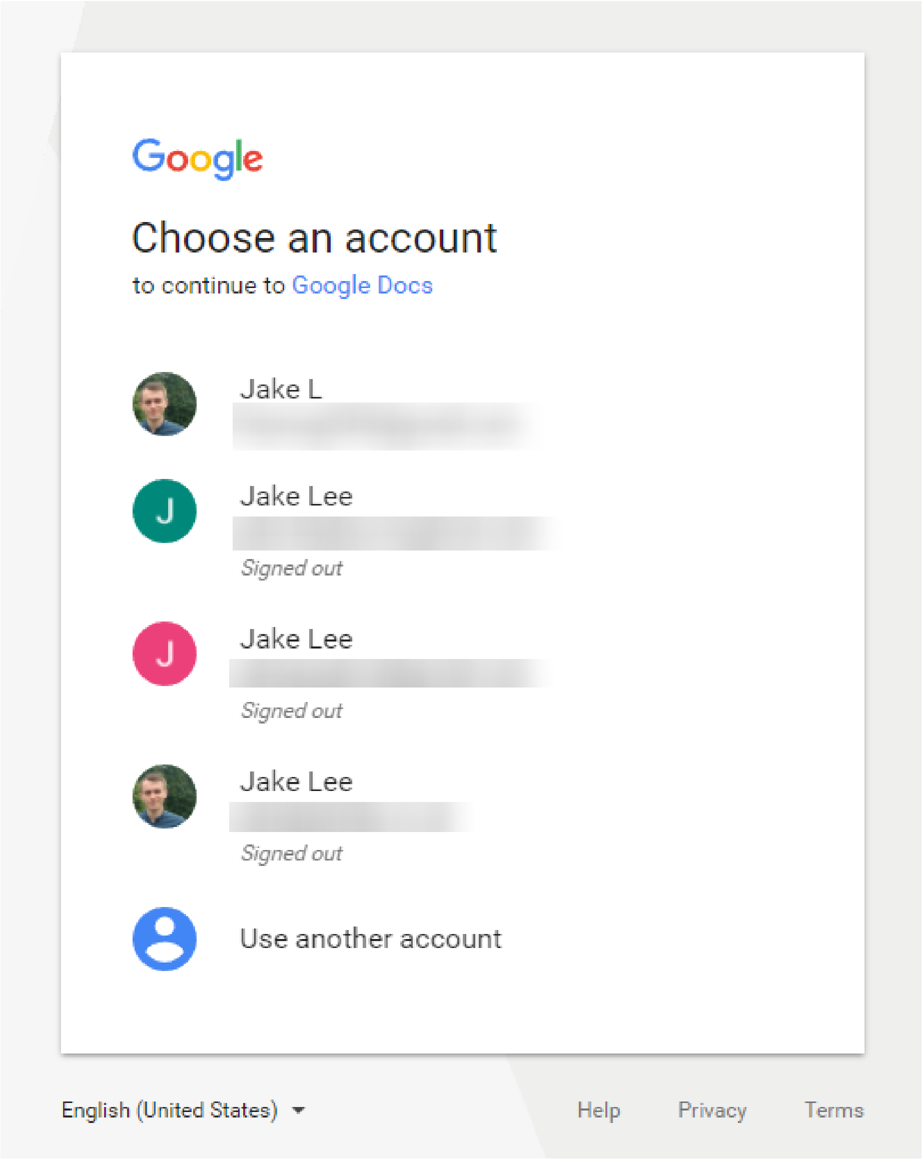
2) Button's URL looks legit



https://accounts.google.com/o/oauth2/auth?client_id=346348828325-vlpb3e70lp89pd823qrcb9jfsmu556t8.apps.googleusercontent.com&scope=

© JakeSteam - https://www.reddit.com/r/google/comments/692cr4/new_google_docs_phishing_scam_almost_undetectable/

3) Real Google account selection prompt



Google

Choose an account

to continue to Google Docs

Jake L
[redacted]

Jake Lee
[redacted]
Signed out

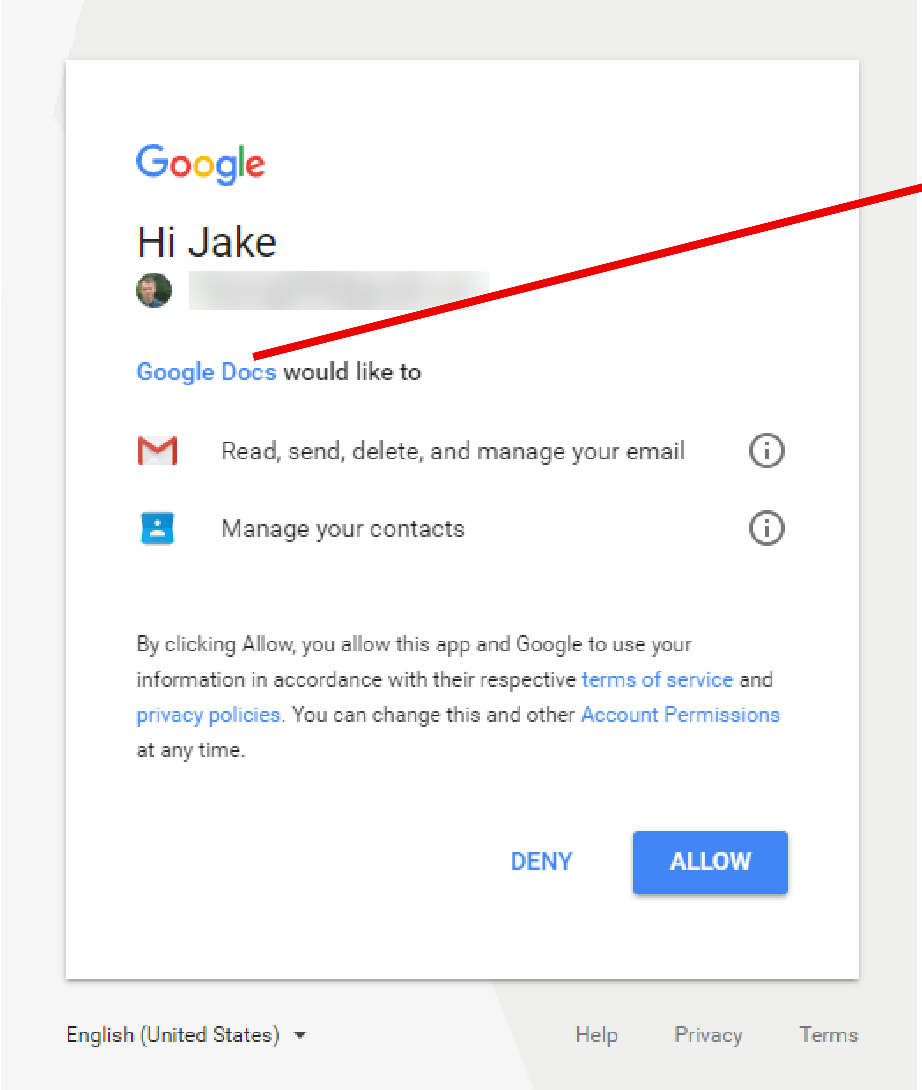
Jake Lee
[redacted]
Signed out

Jake Lee
[redacted]
Signed out

Use another account

© JakeSteam - https://www.reddit.com/r/google/comments/692cr4/new_google_docs_phishing_scam_almost_undetectable/

4) *"Google Docs would like to…"*



Google

Hi Jake

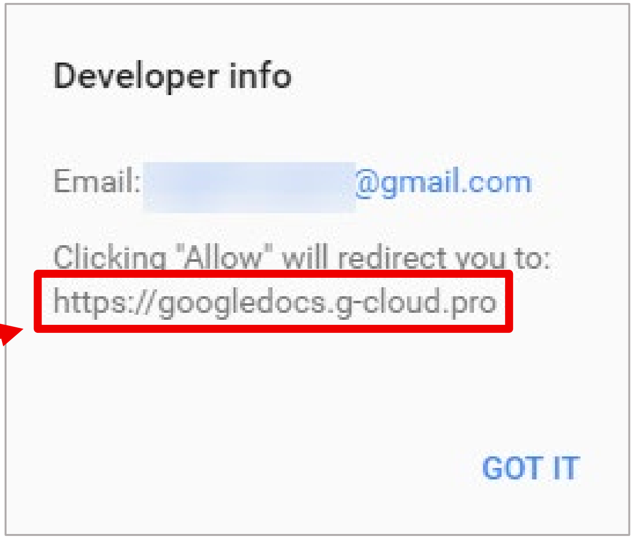
[redacted]

Google Docs would like to

Read, send, delete, and manage your email

Manage your contacts

By clicking Allow, you allow this app and Google to use your information in accordance with their respective terms of service and privacy policies. You can change this and other Account Permissions at any time.



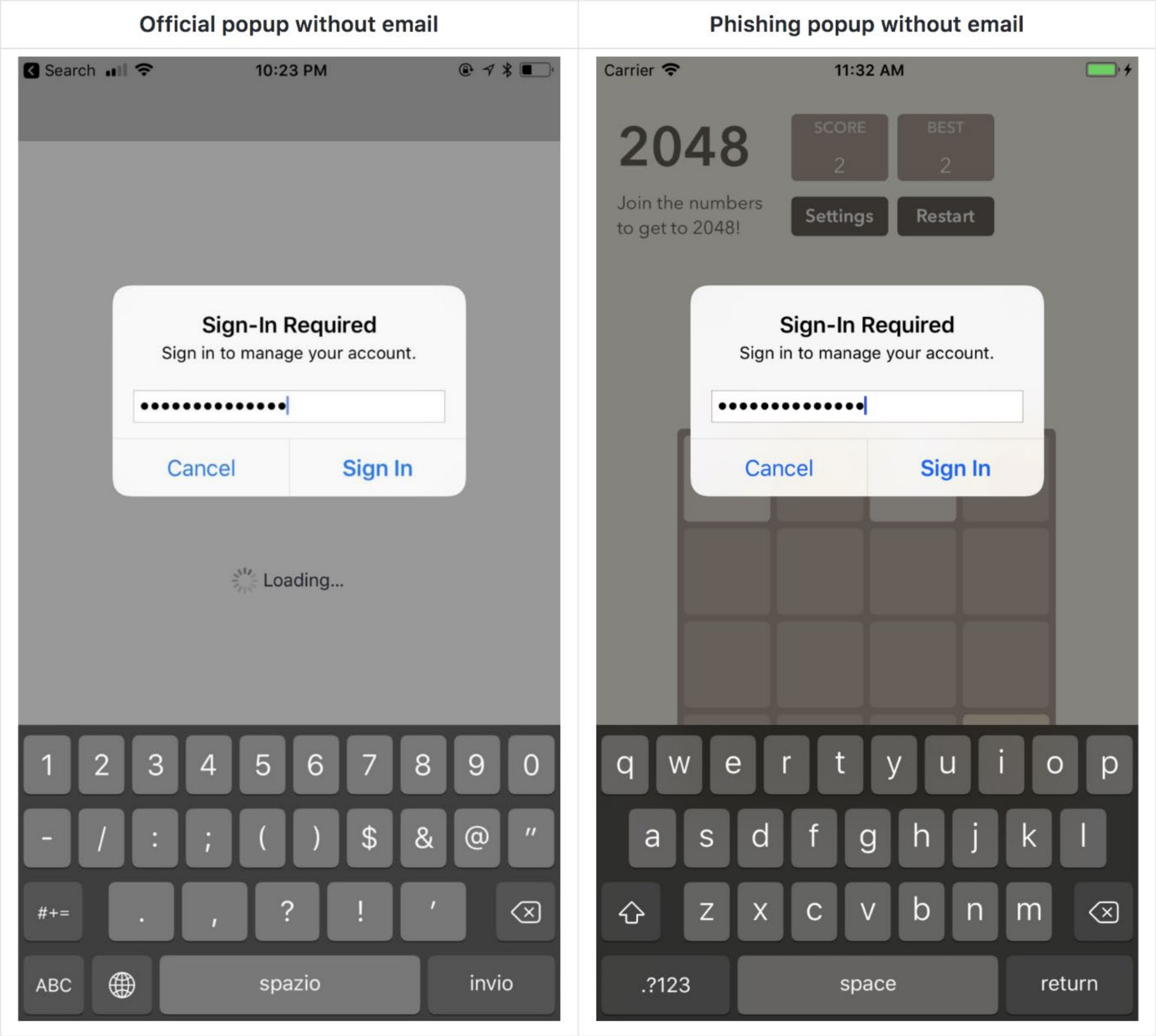
Developer info

Email: [redacted]@gmail.com

Clicking "Allow" will redirect you to:
https://googledocs.g-cloud.pro

© JakeSteam - https://www.reddit.com/r/google/comments/692cr4/new_google_docs_phishing_scam_almost_undetectable/

Phishing beyond email



Official popup without email

Sign-In Required
Sign in to manage your account.

Cancel | Sign In

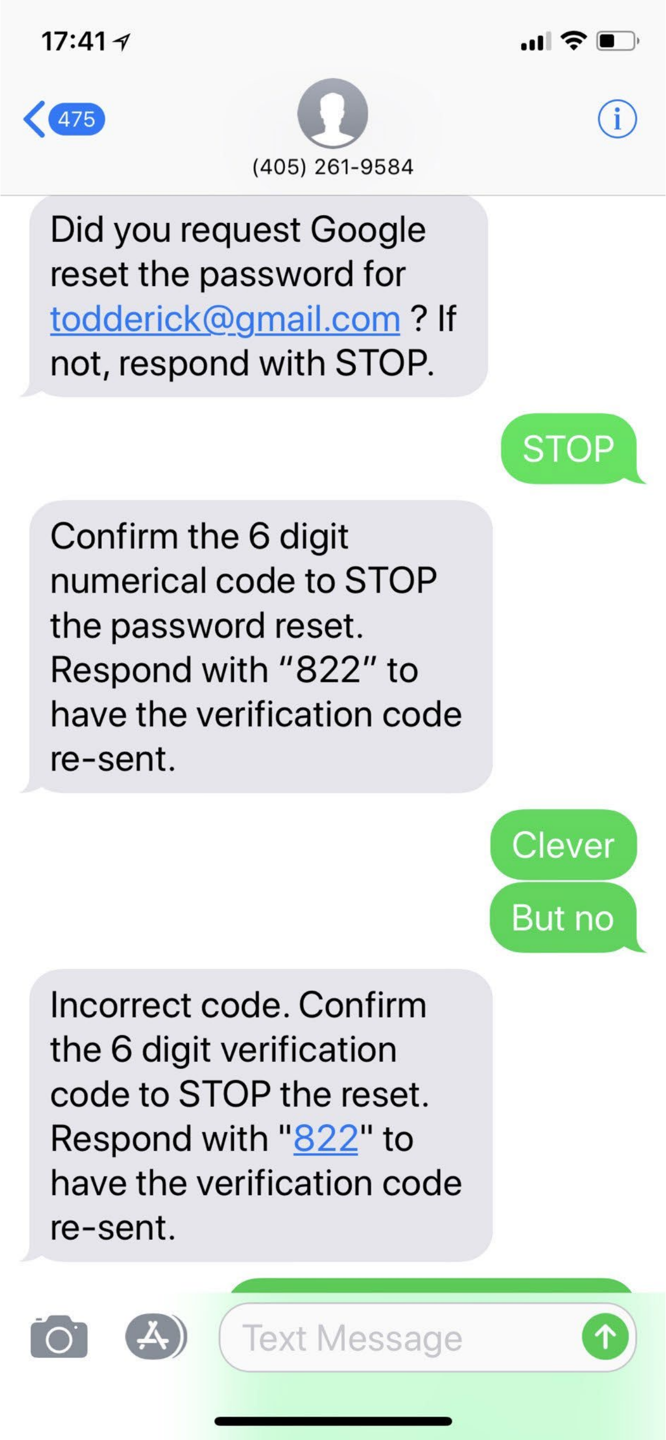
Loading...

Phishing popup without email

Sign-In Required
Sign in to manage your account.

Cancel | Sign In

© Felix Krause - https://krausefx.com/blog/ios-privacy-stealpassword-easily-get-the-users-apple-id-password-just-by-asking



Did you request Google reset the password for todderick@gmail.com ? If not, respond with STOP.

STOP

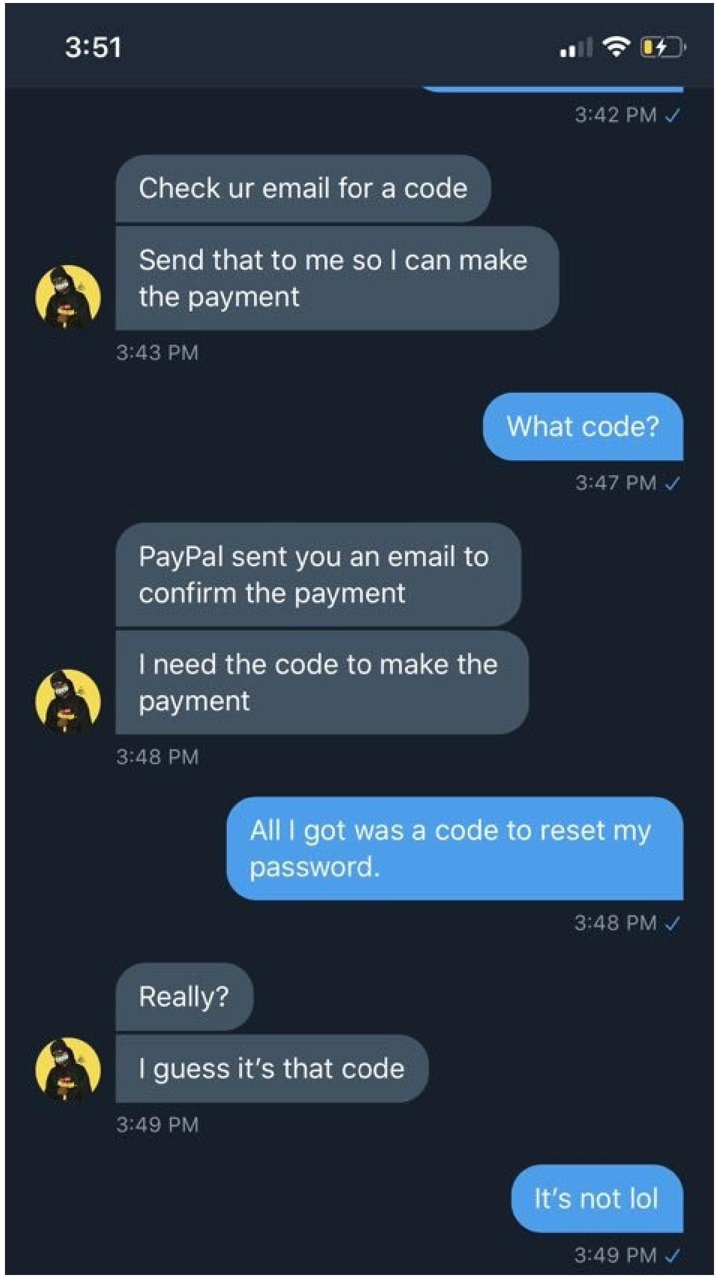
Confirm the 6 digit numerical code to STOP the password reset. Respond with “822” to have the verification code re-sent.

Clever

But no

Incorrect code. Confirm the 6 digit verification code to STOP the reset. Respond with "822" to have the verification code re-sent.

© https://twitter.com/_thp/status/980215525862203392



3:42 PM ✓

Check ur email for a code

Send that to me so I can make the payment

3:43 PM

What code?

3:47 PM ✓

PayPal sent you an email to confirm the payment

I need the code to make the payment

3:48 PM

All I got was a code to reset my password.

3:48 PM ✓

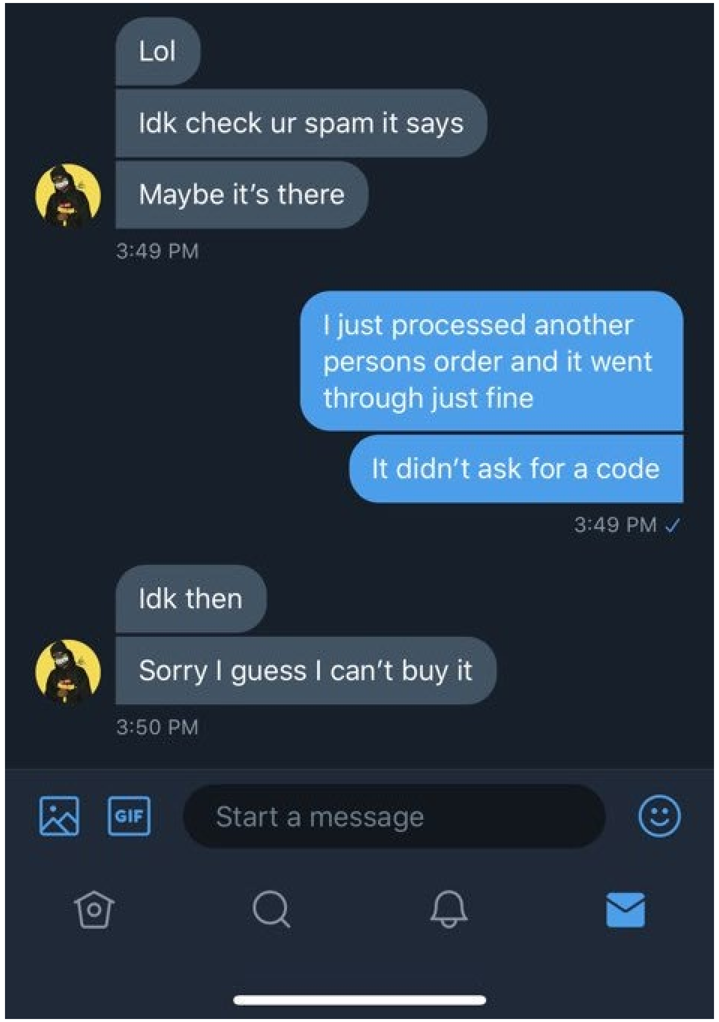
Really?

I guess it's that code

3:49 PM

It's not lol

3:49 PM ✓



Lol

Idk check ur spam it says

Maybe it's there

3:49 PM

I just processed another persons order and it went through just fine

It didn't ask for a code

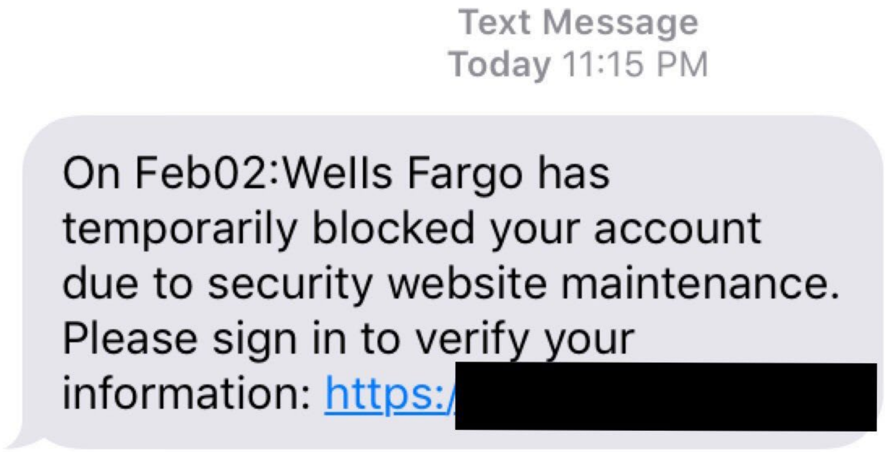
3:49 PM ✓

Idk then

Sorry I guess I can't buy it

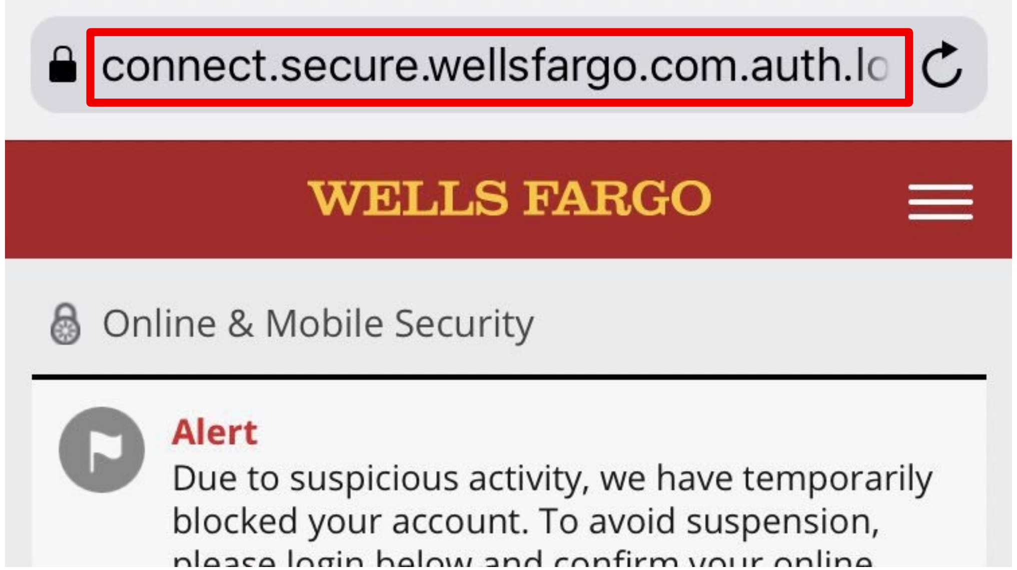
3:50 PM

© https://twitter.com/lilblackjxss/status/1075863331477561345



Text Message
Today 11:15 PM

On Feb02:Wells Fargo has temporarily blocked your account due to security website maintenance. Please sign in to verify your information: https:/[redacted]



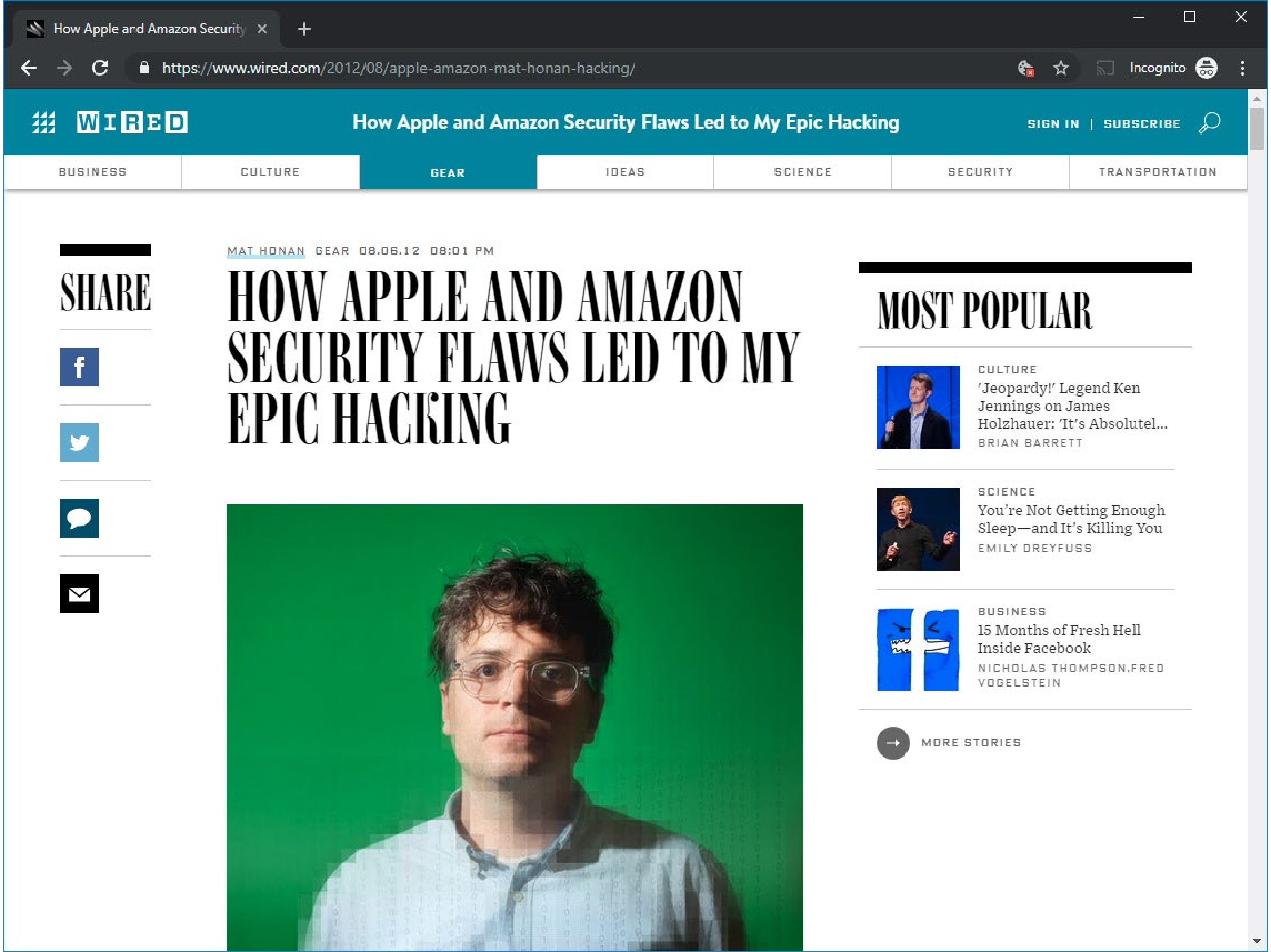
connect.secure.wellsfargo.com.auth.lo

Online & Mobile Security

Alert

Due to suspicious activity, we have temporarily blocked your account. To avoid suspension, please login below and confirm your online

© https://twitter.com/SwiftOnSecurity/status/1091933620749721601



How Apple and Amazon Security Flaws Led to My Epic Hacking

MAT HONAN GEAR 08.06.12 08:01 PM

HOW APPLE AND AMAZON SECURITY FLAWS LED TO MY EPIC HACKING

MOST POPULAR

CULTURE
'Jeopardy!' Legend Ken Jennings on James Holzhauer: 'It's Absolutel...
BRIAN BARRETT

SCIENCE
You're Not Getting Enough Sleep—and It's Killing You
EMILY DREYFUSS

BUSINESS
15 Months of Fresh Hell Inside Facebook
NICHOLAS THOMPSON,FRED VOGELSTEIN

- Google, Twitter, AppleID accounts compromised within one hour
  - Attacker remotely erased (!) all data on iPhone, iPad, and MacBook
  - Lost photos of his daughter that were not saved anywhere else ;-(
- 4:33pm – call to AppleCare
  - Caller reported that he couldn’t get into their `me.com` email
  - The caller couldn’t answer the security questions
  - Apparently, this happens quite often…
- Apple representative asked an alternative set of questions
  - **Billing address**
  - **Last four digits of credit card**
- The hackers had to find just those two pieces of information…

Step 0: Reconnaissance

Twitter account ➔ personal website ➔ personal Gmail address

Google’s account password recovery page ➔ no 2FA was used ➔ page showed that reset confirmation has been sent to `m••••n@me.com` (`me.com` == Apple’s free email)

`m••••n@me.com` is the backup email address ➔ becomes attackers’ **primary target**

Step 1: Find billing address

Whois search on website’s domain

Step 2: Find last four digits of credit card on Apple account

Call Amazon: *“please add a new credit card to my account”* ➔ Amazon asked for: name, e-mail address, billing address

Call Amazon (again): *“I’ve lost access to my account”* ➔ provide name, billing address, (newly added) credit card number ➔ Amazon allows you to add a new email to the account ➔ password reset ➔ view all ccards on file (last four digits – *good enough!*)

What else went wrong

No two-factor authentication

This was in 2012, awareness about 2FA was not that high

Daisy-chained accounts: Amazon → Apple ID → Gmail → Twitter

Same username across accounts

`mhonan@gmail.com`, `mhonan@me.com`, `mhonan@wired.com`

Find My Mac enabled for laptop

Perhaps not as useful as Find My Phone (phones are more likely to get lost)

Remote hard drive wipe → system asks to create a four-digit recovery PIN

If wipe is initiated by attacker, there's no way for the victim to know the PIN

No regular backups

Phishing Countermeasures

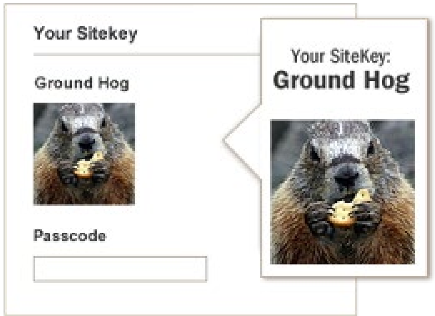
Stop confusing users! Organizations should not include links in emails

User education

- Don’t trust links in emails – type the address in your browser
- (analogous to: don’t trust phone calls that ask for your info – ***always hang up and call the number at the back of your card***)

Augmenting password logins

- Two-step login: show user-specific information before prompting for the password
- Too inconvenient, easy to fool/ignore → not used anymore



Your Sitekey

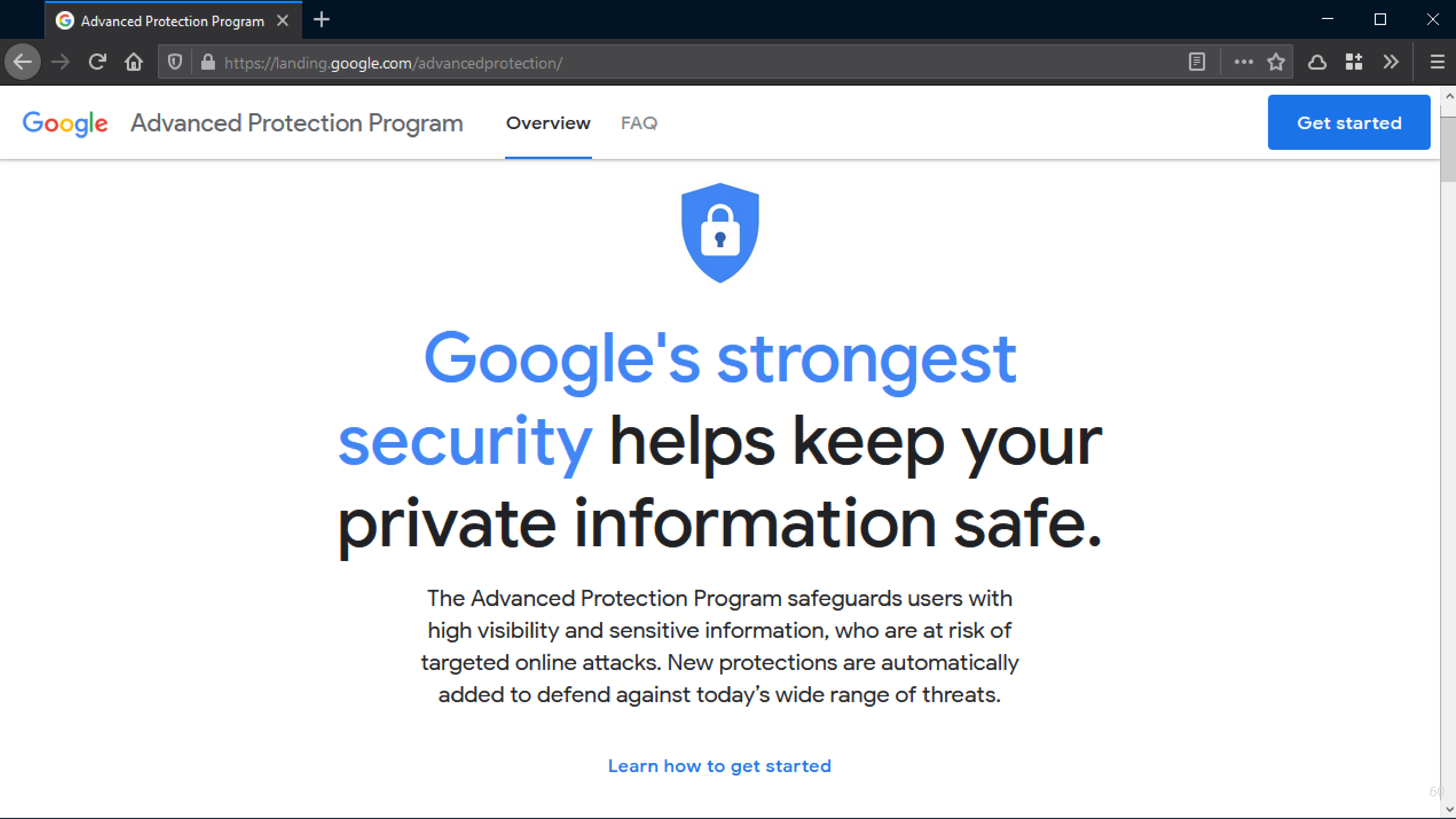
Ground Hog

Passcode

Your SiteKey: Ground Hog

Anti-phishing filters, detection tools, …

~~2-factor authentication~~ → **U2F tokens**


Advanced Protection Program
https://landing.google.com/advancedprotection/
Google
Advanced Protection Program
Overview
FAQ
Get started

Google's strongest security helps keep your private information safe.

The Advanced Protection Program safeguards users with high visibility and sensitive information, who are at risk of targeted online attacks. New protections are automatically added to defend against today's wide range of threats.

Learn how to get started

Maybe rethink email altogether?

Signal

Secure messaging apps offer many benefits

- True end-to-end encryption: the provider cannot read message content
- User-friendly verification of contacts' identities
- Forward secrecy: past communications remain secure even if private keys are stolen
- *No spam!* Only approved contacts can send messages

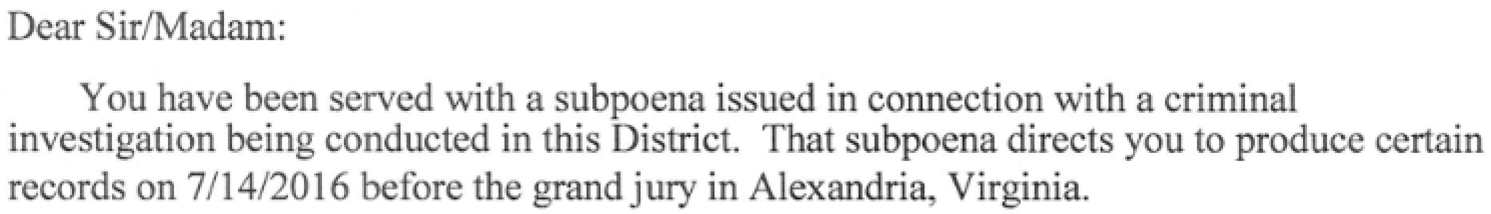
Best option: **Signal**

- Double Ratchet Algorithm (precursor: OTR protocol)
- Good alternatives (but closed-source): WhatsApp (uses Signal protocol), iMessage

Metadata is still there!

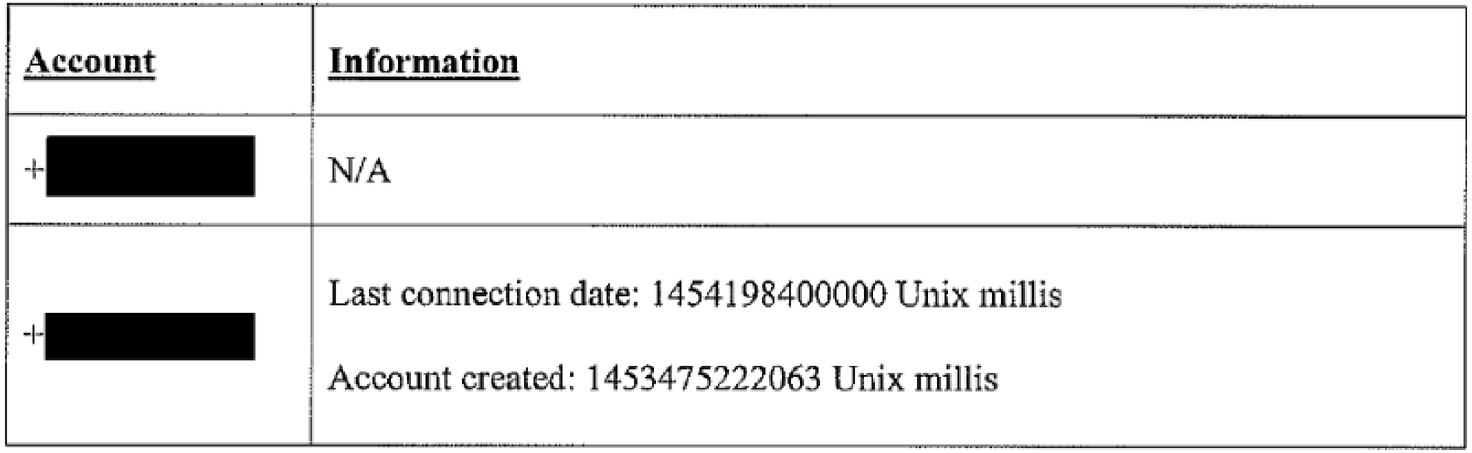
- Signal is actively trying to minimize it

Grand jury subpoena for Signal user data (2016)



Dear Sir/Madam:

You have been served with a subpoena issued in connection with a criminal investigation being conducted in this District. That subpoena directs you to produce certain records on 7/14/2016 before the grand jury in Alexandria, Virginia.



Account	**Information**
+[redacted]	N/A
+[redacted]	Last connection date: 1454198400000 Unix millis Account created: 1453475222063 Unix millis

https://signal.org/bigbrother/eastern-virginia-grand-jury/