

CSE508 Network Security

11/16/2017 **Spam and Phishing**

Michalis Polychronakis

Stony Brook University

SPAM



*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, ...

Fraudulent activities: likes, retweets, clicks, app store rankings, fake reviews, ...



Spam lifecycle

Gathering addresses

Valid, active 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

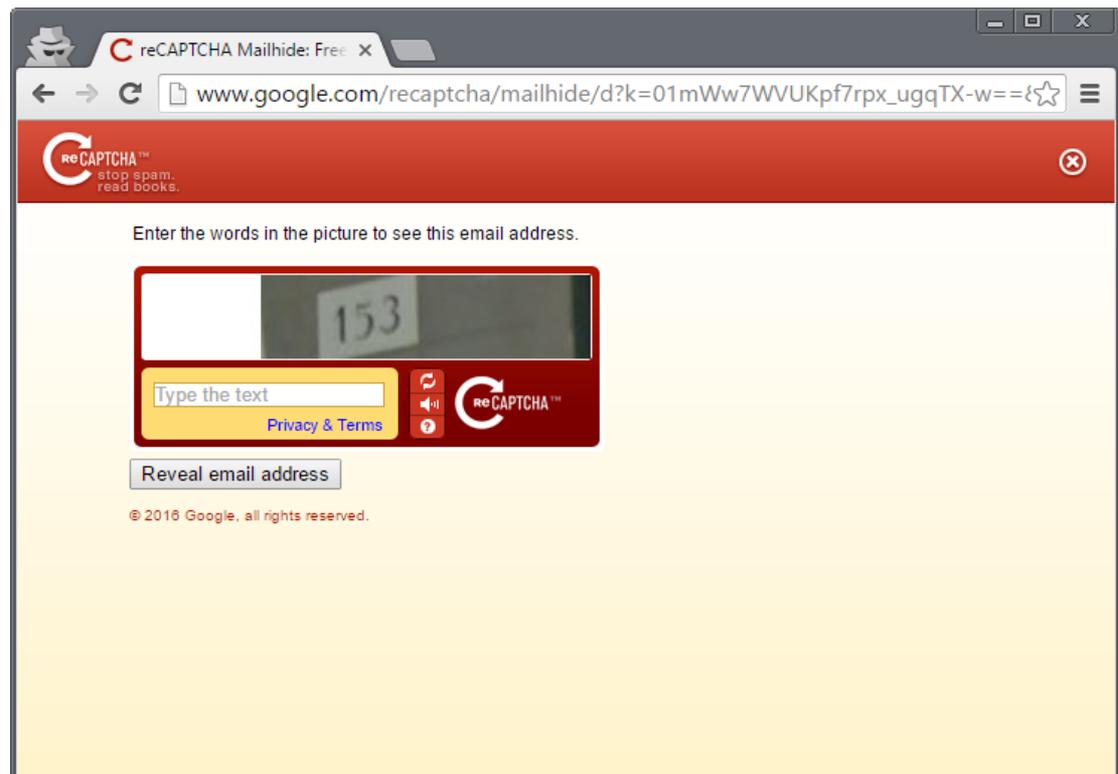
Keep it safe from address harvesting

Munging: username [at] example.com

Image instead of text

CAPTCHAs

...



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, Viagra

- 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

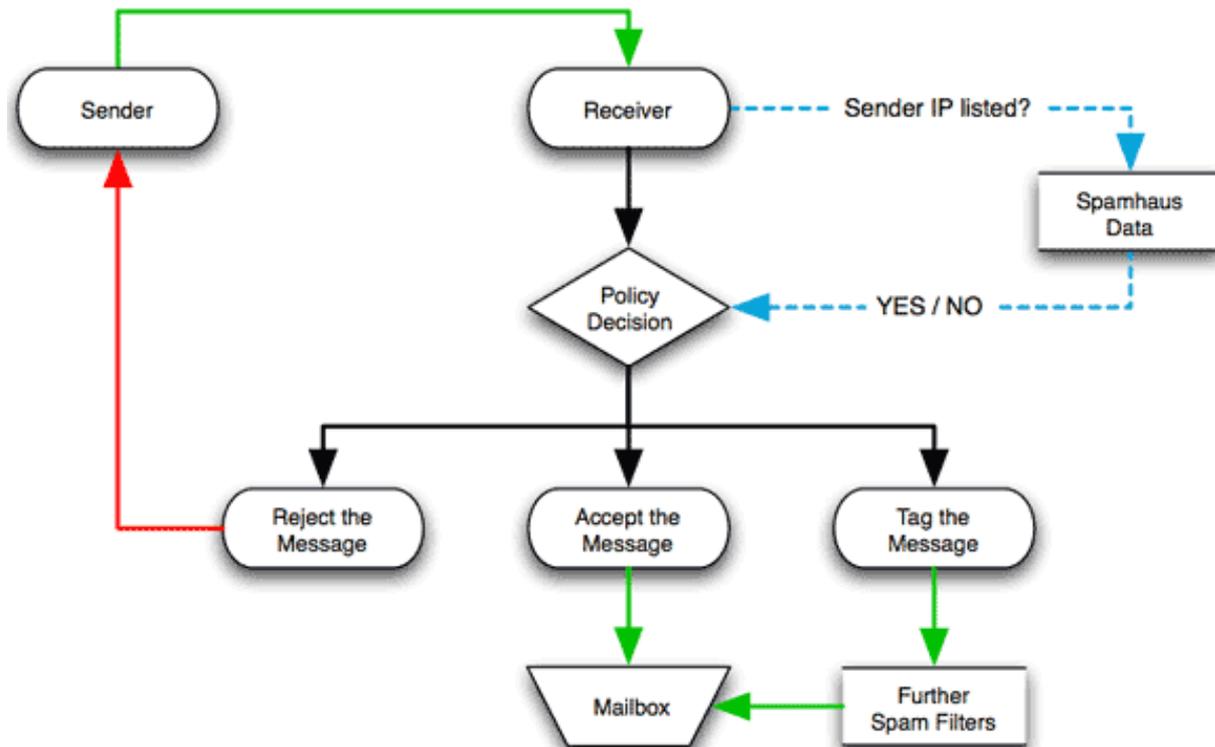
Important program update from MileagePlus.

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

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



False positives, IP addresses change hands, ...

Blocklist Removal Center - X

← → ↻ <https://www.spamhaus.org/lookup/> ☆ ☰

SPAMHAUS

THE SPAMHAUS PROJECT

Home SBL XBL PBL DBL DROP ROKSO

Blocklist Removal Center About Spamhaus | FAQs | News Blog

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.

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.

Associated Documents

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

© 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 addresses of the domain(s) provided in the HELO and MAIL FROM commands

Helps to block spam at its 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+SEc7mT719QQtOj6g  
2MjpErYUGVrRGGc7f5rmE1cRP1lhwx8PVoH0iuRzyok7IqjvAub9kk9fBoE9u ...
```

SPF + DKIM = DMARC

Domain-based Message Authentication, Reporting & Conformance (DMARC)

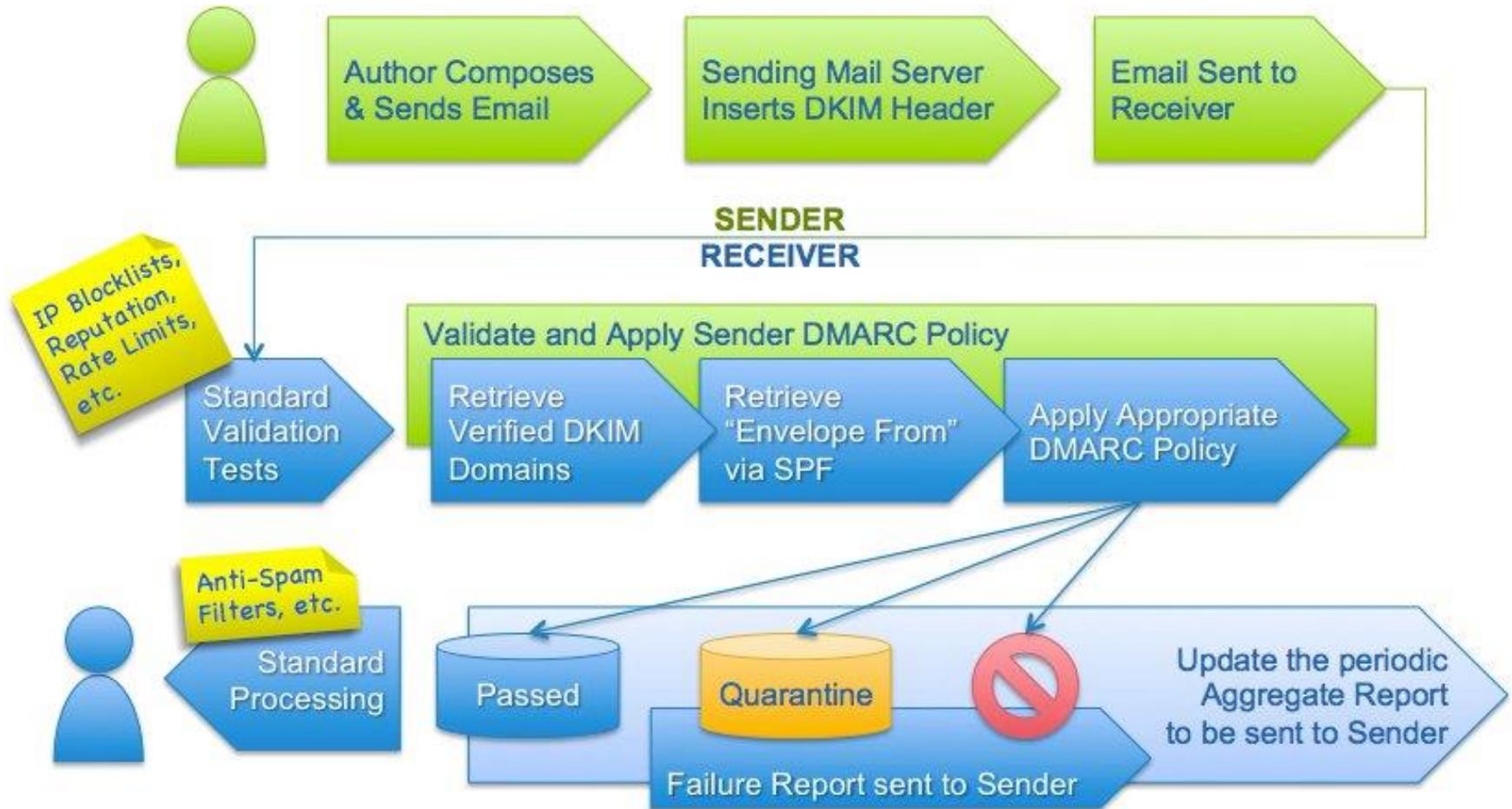
Standardizes how email receivers perform email authentication using SPF and DKIM

Tells receivers what to do if neither of those authentication methods passes – such 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





Covering the global threat landscape

Blog

Bulletin

VB100

VBSpam

VBWeb

Consulting

Conference

Resource

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

site

Bl

VB
aw
yoGo
CN
cerVir
an
VBVol
cal
esp
forVB
pro
anPa
mo

Olc

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, ...)

Besides spam, we also care about phishing...

Phishing

Spoofer emails pointing to spoofed webpages

Financial institutions, cloud services, and other targets

Asking for credentials, credit card numbers, and other sensitive information

“Your Fedex package information”

“Your account has been suspended”

“Your credit card statement”

Spear phishing

Enticing messages that appear to come from well-known individuals or businesses

May even come from real friends/acquaintances through compromised accounts (!)

Address Obfuscation

Misspelled/similar domain names

From: info@paypa1.com <http://www.citybank.com>

Misleading <A> tags

<http://www.attacker.com>

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

Homographs, internationalized domain names (IDN), punycode

<http://ebay.com> (<http://xn--eby-7cd.com/>) – Cyrillic “a” vs. Latin “a”

Most browsers display IDNs only for the system’s configured language

Punycode 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

Hide the actual destination URL

Recent phishing message targeting SBU users

From: **SBU Team** <ebrahle2@kent.edu>

Date: Tue, Feb 2, 2016 at 8:42 PM

Subject: cyber security

To: XXXXXXXXXXXXX

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

Legitimate message from an IT department

From: XXXXXXXXXXXX

Date: XXXXXXXXXXXX

Subject: Important! You must change your XXXXXXXX password

To: XXXXXXXXXXXXXXXX

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

Member of XXXXXXXXXXXX Department,

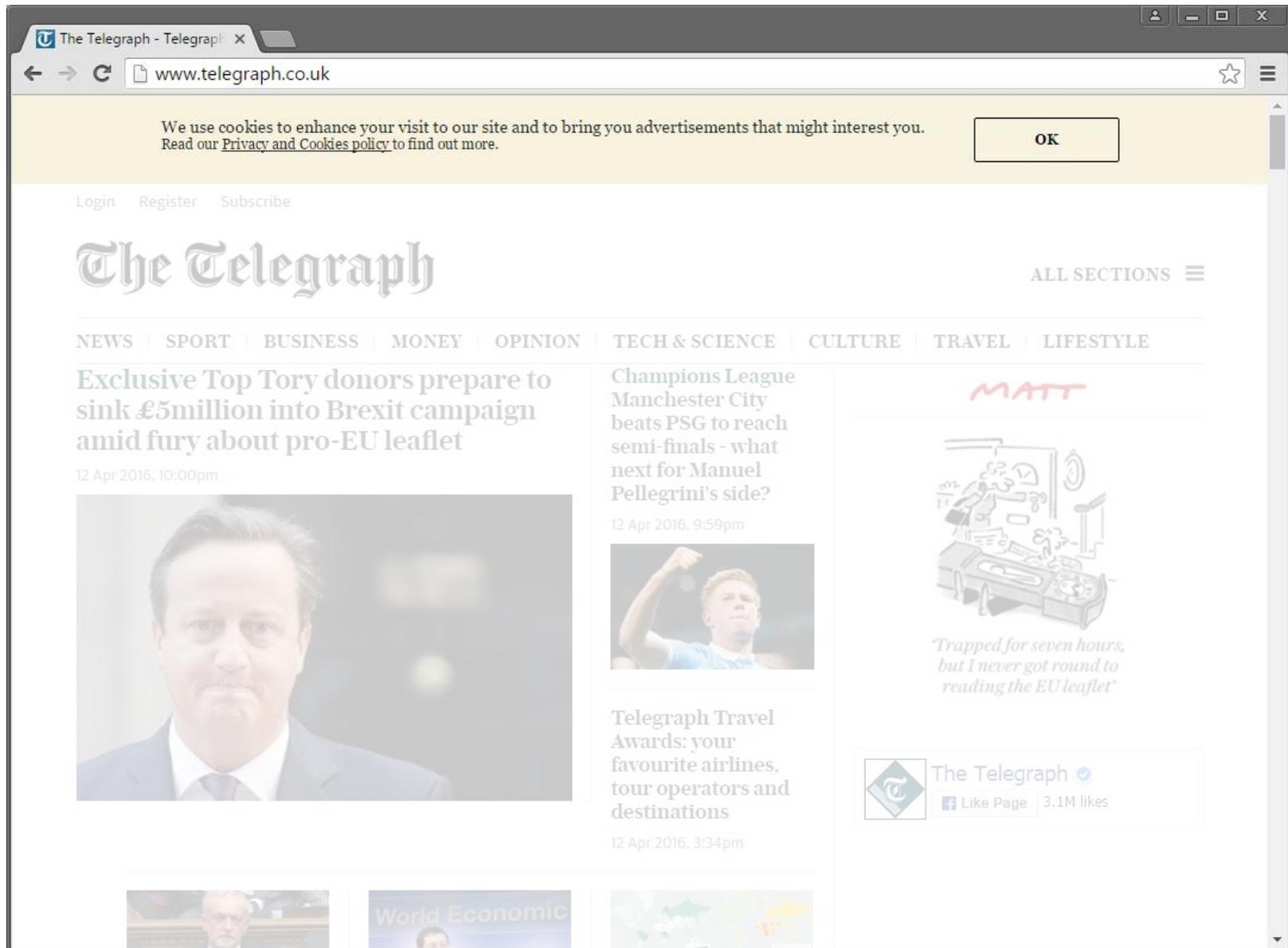
PLEASE CHANGE YOUR XXXXXXXX PASSWORD!

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

To change your XXXXXXXX password:

<http://XXXXXXXXXXXX.XXX> -> forgot your password -> follow the instructions

More training of users to click on things...



The screenshot shows the homepage of The Telegraph website in a browser window. The browser's address bar displays 'www.telegraph.co.uk'. A yellow cookie consent banner is at the top, with an 'OK' button. Below the banner, there are links for 'Login', 'Register', and 'Subscribe'. The main header features the 'The Telegraph' logo in a large, stylized font, and a navigation menu with 'ALL SECTIONS' and a hamburger menu icon. A secondary navigation bar lists various news categories: NEWS, SPORT, BUSINESS, MONEY, OPINION, TECH & SCIENCE, CULTURE, TRAVEL, and LIFESTYLE. The main content area is divided into three columns. The left column features a large article titled 'Exclusive Top Tory donors prepare to sink £5million into Brexit campaign amid fury about pro-EU leaflet', dated '12 Apr 2016, 10:00pm', with a portrait of David Cameron. The middle column has an article titled 'Champions League Manchester City beats PSG to reach semi-finals - what next for Manuel Pellegrini's side?', dated '12 Apr 2016, 9:59pm', with a photo of a player. The right column contains a cartoon illustration of a man at a desk with the name 'MATT' written above it, and a quote: 'Trapped for seven hours, but I never got round to reading the EU leaflet'. Below the cartoon is a Facebook widget for 'The Telegraph' with '3.1M likes'. At the bottom, there are three small preview cards for other articles, including one titled 'World Economic'.

Phishing Countermeasures

Stop confusing users

Institutions shouldn't 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 call the number at the back of your card)

Augmenting password logins

Two-step login: show user-specific information before prompting for the password

Probably too inconvenient

Anti-phishing filters, tools, ...

U2F tokens!



Spear Phishing

Well-prepared, personalized, convincing messages targeted to particular individuals

Seemingly coming from trusted colleagues (may come from real colleagues if their accounts have been compromised)

Personalized for their target: 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 credentials stealing

Many recent incidents



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.

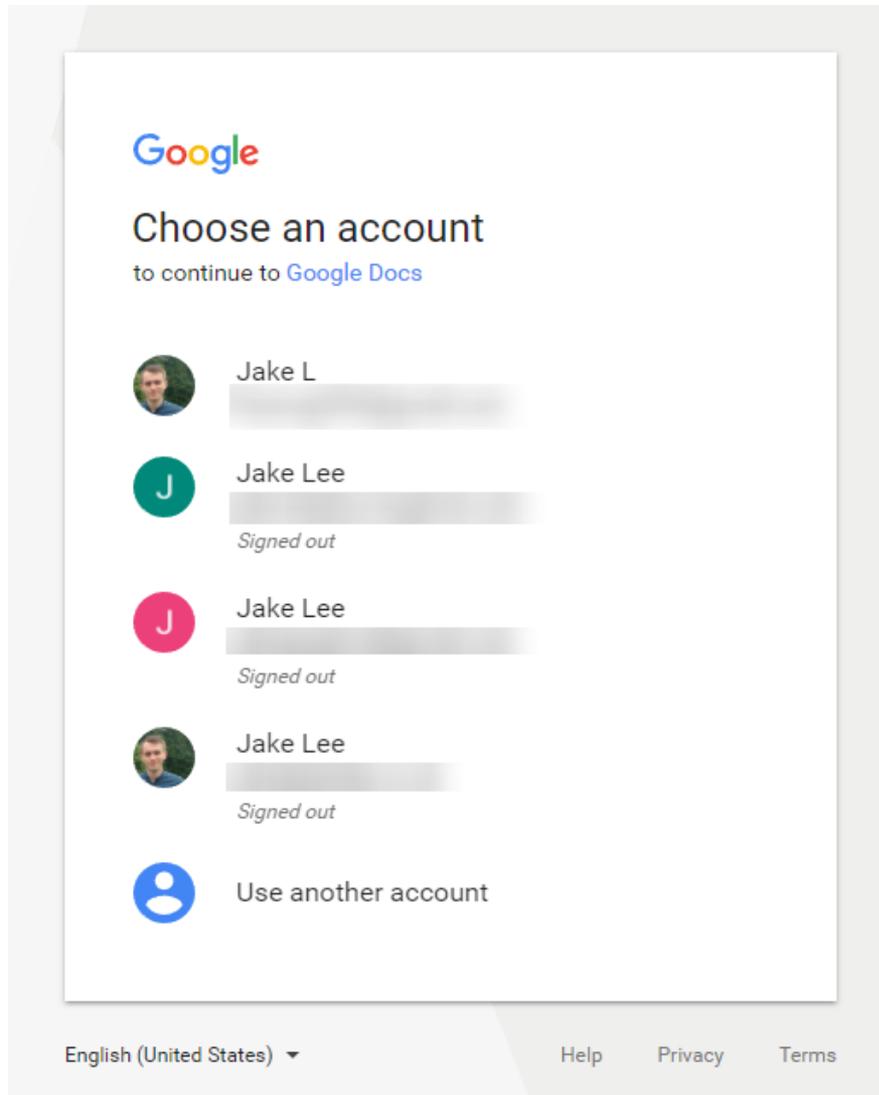
Another attack pretended to be from a target's husband, sharing family photos; the email was forged to include the husband's name.

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.

3) Real Google account selection prompt



4) "Google Docs would like to..."

The image shows a Google Docs permission dialog box. At the top, it says "Google" and "Hi Jake". Below that, it says "Google Docs would like to" and lists two permissions: "Read, send, delete, and manage your email" and "Manage your contacts". At the bottom, there are "DENY" and "ALLOW" buttons. A red arrow points from the "ALLOW" button to a "Developer info" popup box. The popup box contains the text "Developer info", "Email: [redacted]@gmail.com", and "Clicking 'Allow' will redirect you to: https://googledocs.g-cloud.pro". The URL is highlighted with a red box. There is also a "GOT IT" button in the popup box.

Google

Hi Jake

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.

DENY ALLOW

Developer info

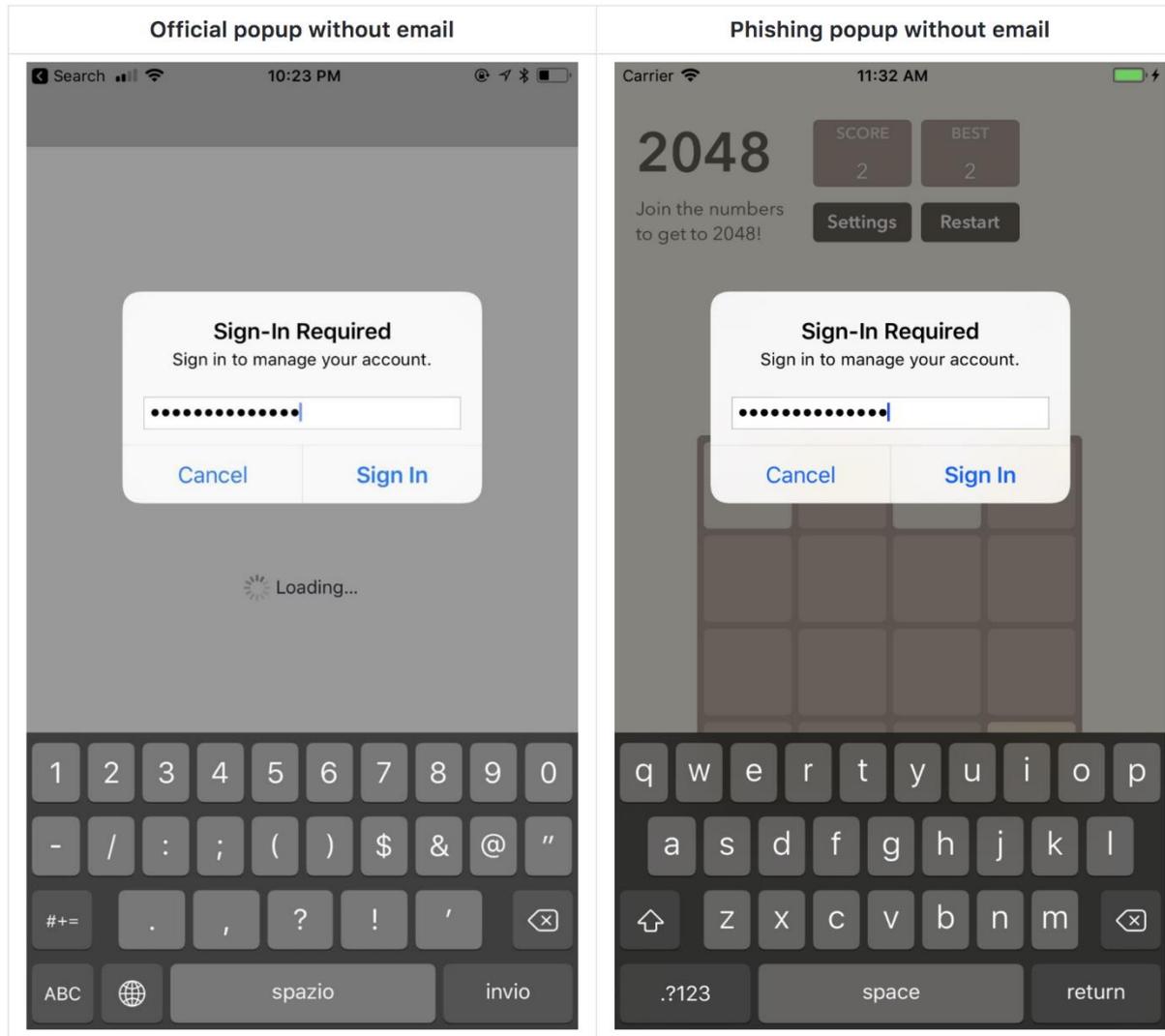
Email: [redacted]@gmail.com

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

GOT IT

English (United States) Help Privacy Terms

Phishing beyond email



Maybe rethink email altogether?

Recent secure messaging apps offer many benefits

True end-to-end encryption: the provider shouldn't be able to read message contents

User-friendly verification of contacts' identities

Forward security: ensure past communications will be secure even if private keys are stolen

Open-source design and implementation, code audits

No spam! Only approved contacts can send messages

Many encouraging efforts

Signal, OTR, Pond, ...

Proprietary, but better than nothing: WhatsApp, iMessage

Metadata is still there!