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 \(\rightarrow\) easily blocked

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

Beyond email
   \textit{Fraudulent messages}: Facebook, Twitter, Yelp, Amazon, online comments, forum messages, Apple/Google Store, …
   \textit{Fraudulent activities}: likes, retweets, clicks, app store rankings, fake reviews, …
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
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@gra, 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
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

Important update on Chrome Supervised Users

Hi Michelle,

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.
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, …
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 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/K5PZCV8atl6a1Dvg=;
b=Nch9yEorgibAjkh90ukDL6SU0FYn70qP6AMSWFfpLO+W3iroMoVdKIjKk8Cv6Gc1TW ...

mikepo@styx:~> dig 20161025._domainkey.1e100.net TXT
;; ANSWER SECTION:
20161025._domainkey.1e100.net. 21599 IN TXT "k=rsa; p=MIIBIjANBgkqhkiG9w0BAQEFAAOCQ8AMIIBCgKCAQEAnOv6+Txyz+5Ec7mT719QQtOj6g2MjpErYUGVrRGGc7f5rmE..."
**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

1. **Author Composes & Sends Email**
2. **Sending Mail Server Inserts DKIM Header**
3. **Email Sent to Receiver**

**IP Blocklists, Reputation, Rate Limits, etc.:**
- **Standard Validation Tests**
- **Anti-Spam Filters, etc.:**

**Validate and Apply Sender DMARC Policy**
- Retrieve **Verified DKIM Domains**
- Retrieve "Envelope From" via SPF
- **Apply Appropriate DMARC Policy**

**Standard Processing**
- **Passed**
- **Quarantine**
- **Failure Report sent to Sender**

**Update the periodic Aggregate Report to be sent to Sender**

[http://dmarc.org/overview/](http://dmarc.org/overview/)
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 it.
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…
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


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
https://accounts.google.com/no-phish.com
Address Obfuscation

Homographs, internationalized domain names (IDN), punycode


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


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” (2012)

MuddyWater (2018)

Social engineering to enable macros

Decoy document images according to the target’s country

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: XXXXXXXXXXXXXX

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

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

Member of XXXXXXXXX Department,

PLEASE CHANGE YOUR XXXXXXX PASSWORD!

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

To change your XXXXXXX password:
http://XXXXXXXXX.XXX  -> forgot your password -> follow the instructions
More training of users to click on things…
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

Are you available?

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

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

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

This report describes “Phish For The Future,” an advanced persistent spear phishing 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 spear phishing 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

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.

CHANGE PASSWORD

Best,
The Gmail Team
Gmail’s filters didn’t catch it…

> *From:* Google  
| <no-reply@accou  
nts.gmail.com>  
> *Date:* March 19, 2016 at 4:34:30 AM EDT.  
> *To:* john.po  
de@desta.com  
> *Subject:* S...me...ne has you r passw...rd*.  
> S...me...ne has your passw...rd.  
> Hi John..>
Sensibly, Podesta forwarded the email, asking what to do.

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

http://myaccount.google.com/securitysettingpage.tk/security/signioptions/password?e=am9obi5w5w22Rlc3RhQGdTyWLSmNvbQ%3D%3D&f=n=Sm9obiBQb2Rlc3Rh&n=Sm9obg%3D%3D&img=Ly9saDQuZ29vZ2xlLXMlNvbmlnRlbQuY29tLy1RZVI/PhHJkVgp2WS9BQFBU...
How APT28/FANCYBEAR/GRU breached John Podesta’s account

http://myaccount.google.com-securitysettingpage.tk/security/signinoptions/password?e=am9obi5wb2Rlc3RhQGdtYWlsLmNvbQ%3D%3D&f=Sm9obiBQb2Rlc3Rh&n=Sm9obg%3D%3D&img=Ly9saDQuZ29vZ2xlNcmNbvnRlbnuQ2tLy1RZV1PbHJkVgp2WS9BQUFBQUFBQUFBUFB...
http://myaccount.google.com-securitysettingpage.tk/security/signinoptions/password?e=am9obi5wb2Rlc3RhQGdtYWlsLnVbQ%3D%3D&fn=Sm9obiBQb2Rl&n=Sm9obi3D%3D&img=Ly9saDQuZ29vZ2xlXNlc3NvbnRlbW9yY29tLy1RZVJPbHJkVGp2WS9BQFBUFBQUBQFBUFBQUBQFBUFBQUBQFUC...http://myaccount.google.com-securitysettingpage.tk/security/signinoptions/password?e=am9obi5wb2Rlc3RhQGdtYWlsLnVbQ%3D%3D&fn=Sm9obiBQb2Rl&n=Sm9obi3D%3D&img=Ly9saDQuZ29vZ2xlXNlc3NvbnRlbW9yY29tLy1RZVJPbHJkVGp2WS9BQFBUFBQUBQFBUFBQUBQFBUFBQUBQFUC...

Decode from Base64 format

Simply use the form below

Ly9saDQuZ29vZ2xlXNlc3NvbnRlbW9yY29tLy1RZVJPbHJkVGp2WS9BQFBUFBQUBQFBUFBQUBQFBUFBQUBQFUCBQFBUFBQUBQFBUFBQUBQFBUFBQUBQFUC

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

https://myaccount.google.com/securitysettingpage.tk/security/signinoptions/password?e=am9obi5wb2Rlc3RhQGdtYWlsLnVbQ%3D%3D&fn=Sm9obiBQb2Rl&n=Sm9obi3D%3D&img=Ly9saDQuZ29vZ2xlXNlc3NvbnRlbW9yY29tLy1RZVJPbHJkVGp2WS9BQFBUFBQUBQFBUFBQUBQFBUFBQUBQFUCBQFBUFBQUBQFBUFBQUBQFBUFBQUBQFUCBQFBUFBQUBQFBUFBQUBQFBUFBQUBQFUC

© Thomas Rid - https://twitter.com/RidT/status/789097977352691712
Recent Google Docs Phishing Campaign

1) Fake “Google doc has been shared with you” email

2) Button’s URL looks legit
3) Real Google account selection prompt

![Choose an account prompt](https://www.reddit.com/r/google/comments/692cr4/new_google_docs_phishing_scam_almost_undetectable/)
4) “Google Docs would like to…”

[Image of a Google account permissions screen asking for access to read, send, delete, and manage emails, with a developer info box showing a fake URL: https://googledocs.g-cloud.pro]
Phishing beyond email
Did you request Google reset the password for todderick@gmail.com? If not, respond with STOP.

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

Incorrect code. Confirm the 6 digit verification code to STOP the reset. Respond with "822" to have the verification code re-sent.
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
I just processed another persons order and it went through just fine
It didn’t ask for a code
3:49 PM

Idk then
3:50 PM

Sorry I guess I can’t buy it
3:50 PM
On Feb 02: Wells Fargo has temporarily blocked your account due to security website maintenance. Please sign in to verify your information: https:// connect.secure.wellsfargo.com.auth.lc

Wells Fargo
Online & Mobile Security

Alert
Due to suspicious activity, we have temporarily blocked your account. To avoid suspension, please login below and confirm your online account.
How Apple and Amazon Security Flaws Led to My Epic Hacking

MAT HONAN  GEAR  08.06.12  09:01 PM

HOW APPLE AND AMAZON SECURITY FLAWS LED TO MY EPIC HACKING
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

Anti-phishing filters, detection tools, …

2-factor authentication ➔ U2F tokens
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?

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](https://en.wikipedia.org/wiki/Off-the-Record_Messaging))
- Good alternatives (but closed-source): WhatsApp (uses Signal protocol), iMessage

Metadata is still there!

- Signal is actively trying to minimize it
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.

<table>
<thead>
<tr>
<th>Account</th>
<th>Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>+</td>
<td>N/A</td>
</tr>
<tr>
<td></td>
<td>Last connection date: 1454198400000 Unix millis</td>
</tr>
<tr>
<td></td>
<td>Account created: 1453475222063 Unix millis</td>
</tr>
</tbody>
</table>