



Preventing Unauthorized Email Spoofing with DMARC

January 24, 2016

About Your Speaker

- Founding Team Member at Agari
- Assisted Microsoft & FBI with B54 Citadel botnet takedown (2013)
- Previous Roles:
 - CTO of Brandmail Solutions
 - CTO of Concurro
 - CTO of 365 Media
 - Director, Strategic Projects, SAP
 - Applications Consultant, Oracle



John Wilson
Field CTO, Agari

About Agari

Agari's Mission:

Eliminate email as a vector for Cyber Crime

Founded in 2009, Agari provides systems and services to help companies take back control of their email channel.

Agari's 100+ clients include:

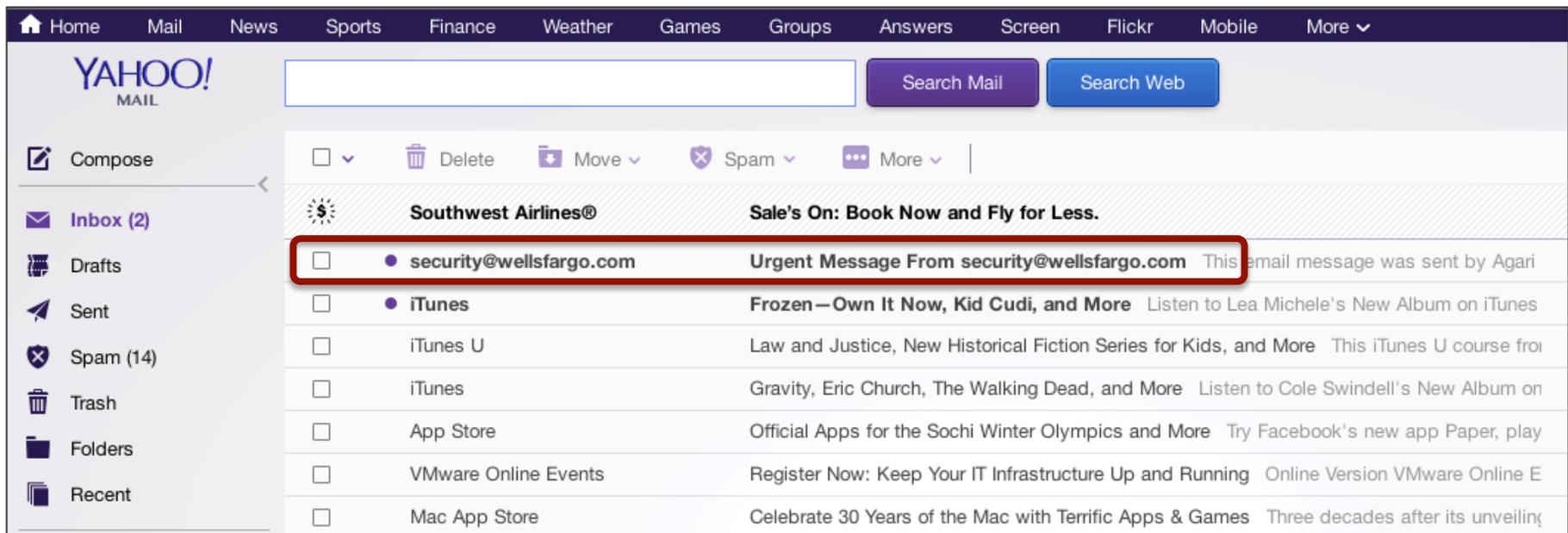
- 4 of the top 5 US banks
- 3 of the top 5 UK banks
- 4 of the top 5 social networks

Agenda

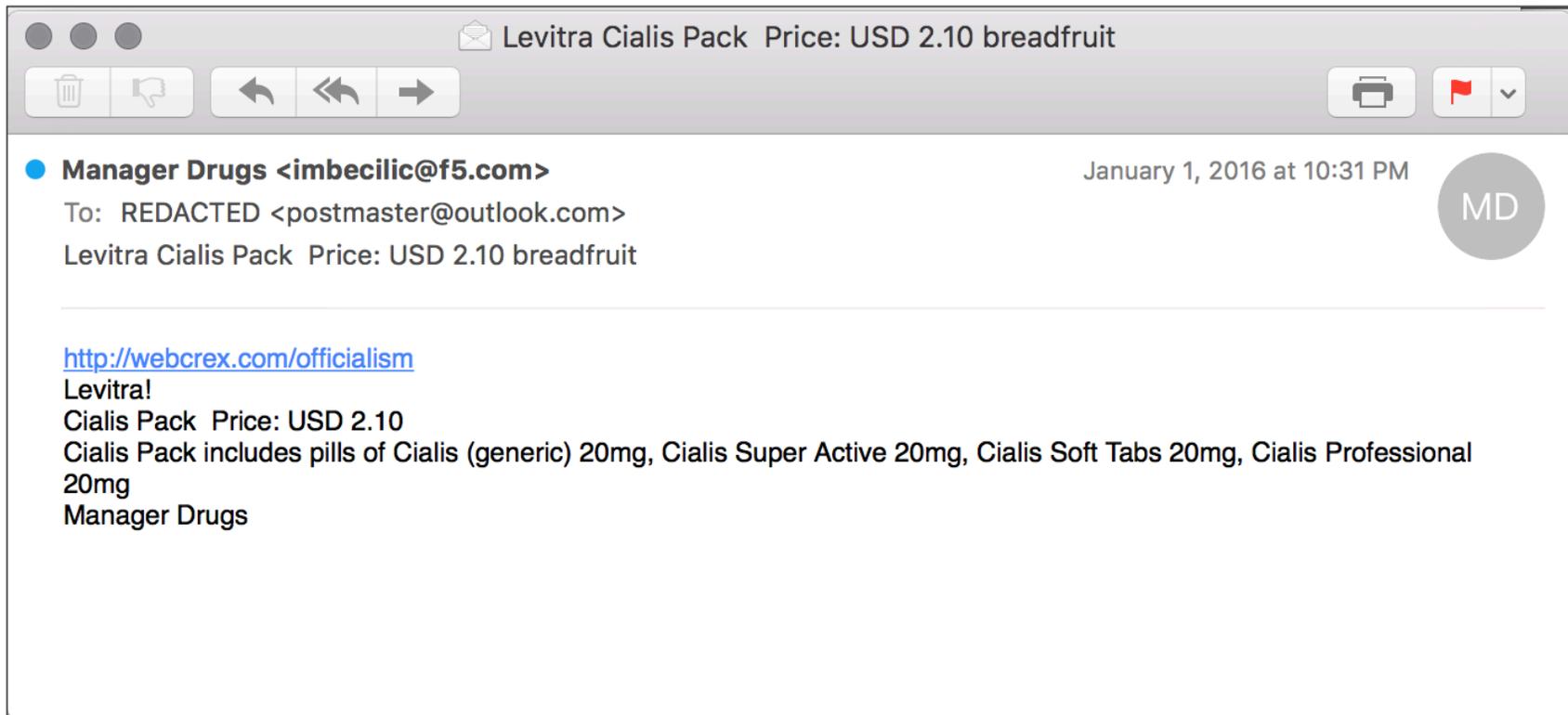
- Why cybercriminals love email
- Previous attempts to solve this problem
- The current best solution
- Technical details of SPF, DKIM, and DMARC
- Open source tools
- Edge cases and solutions
- Estimating DMARC adoption with Ashley Madison data

Email's Fundamental Flaw

- Email has no built-in authentication
- Spoofing an email address is a trivial effort – no hacking required



Fraud Example #1: Pharma Spam



Fraud Example #1: Pharma Spam

Levitra Cialis Pack Price: USD 2.10 breadfruit

Manager Drugs <imbecilic@f5.com>
To: REDACTED <postmaster@outlook.com>
Levitra Cialis Pack Price: USD 2.10 breadfruit

<http://webcrex.com/officialism>

Levitra!
Cialis Pack Price: USD 2.10
Cialis Pack includes pills of Cialis (generic) 20mg
Manager Drugs

CANADIAN Health&Care Mall

ALL PRODUCTS | ABOUT US | HOW TO ORDER | TESTIMONIALS | FAQ | CONTACTS

HAPPY COLUMBUS DAY! SAVE ON EVENT! CIALIS + VIAGRA
ORDER NOW \$74.95

Healthcare Online

USD GBP CAD EUR AUD CHF

MEN'S HEALTH

- Viagra *
- Cialis *
- Cialis + Viagra Powerpack *
- Cialis Super Active+ *
- Viagra Super Active+ *
- Generic Levitra *
- Viagra Super P-Force *
- Viagra Professional *
- Cialis Professional *
- Cialis Soft Tabs *
- Viagra Soft Tabs *
- Priligy (Dapoxetine) *
- Kamagra *
- Kamagra Oral Jelly *
- Avana (Avanafil) *
- Super Avana (Avanafil & Dapoxetine) *
- Kamagra Soft *
- Cialis Super Force *

[View all products](#)

Most Popular Products

Viagra as low as \$0.89 \$0.80
Generic Viagra is used to treat male Impotence also known as Erectile Dysfunction. Also, it has been approved by US FDA for treating pulmonary arterial hypertension.
[More Info](#) **Order now**

Cialis as low as \$1.22 \$1.10
Generic Cialis is used to treat erection problems in men. It is the only drug which is not only fast acting (works in 30 minutes) but is also known to be effective for as long as 36 hours, thus enabling you to choose the moment that is just right for you as well as your partner. Millions of men have benefited from Cialis as it works effectively in mild, moderate or severe Erectile Dysfunction.
[More Info](#) **Order now**

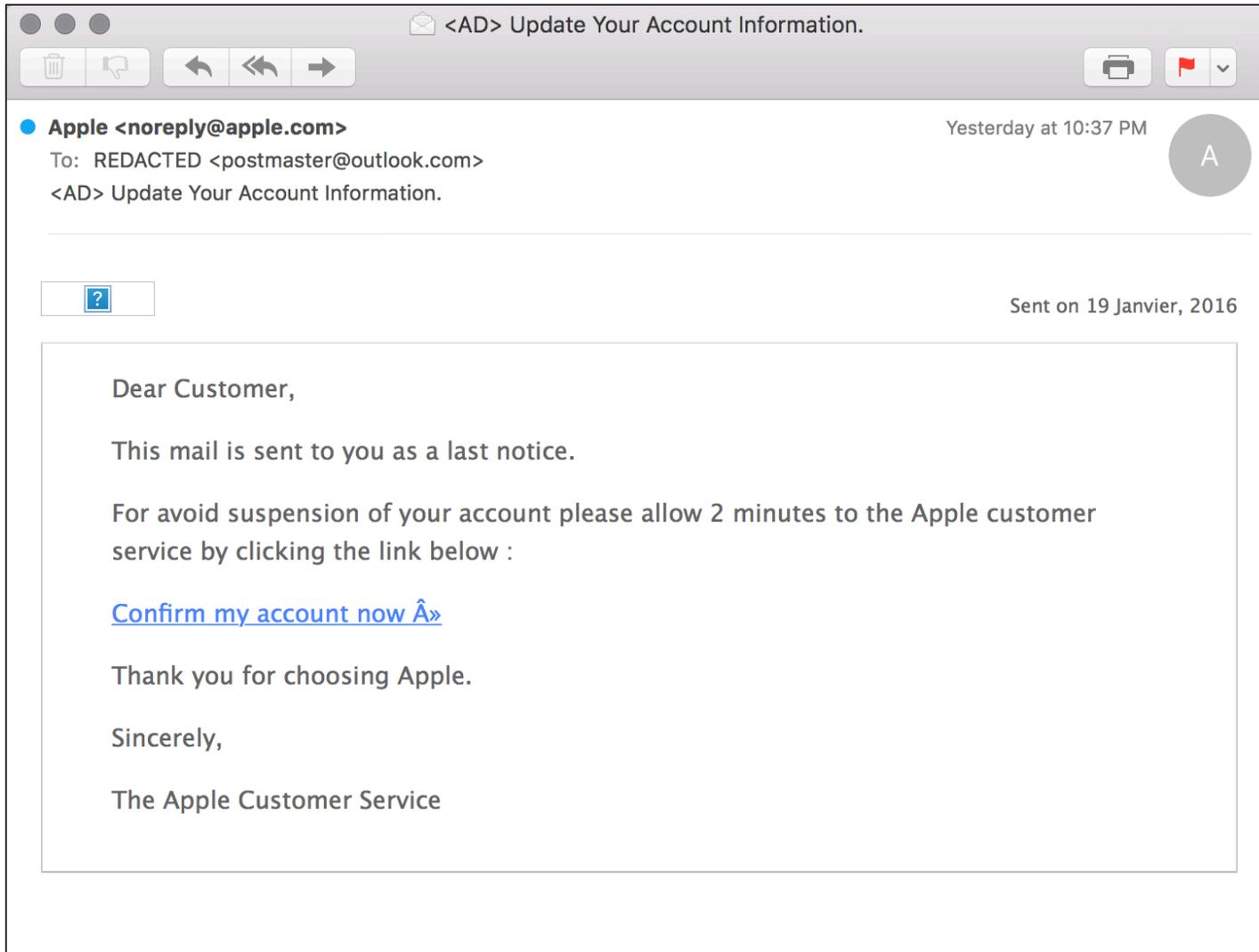
Cialis + Viagra Powerpack special price
Cialis + Viagra Powerpack is a powerful combination of drugs used for treating erectile dysfunction, more commonly known as impotence. Since becoming available, both Cialis and Viagra have been the prime treatment for erectile dysfunction. Effective and quick-acting, Cialis and Viagra provide restored and enhanced ability for sexual intercourse.
[More Info](#) **Order now**

Cialis Super Active+ as low as \$2.22 \$2.00

Your Cart:
Items: 0 | Total: \$0.00

Search

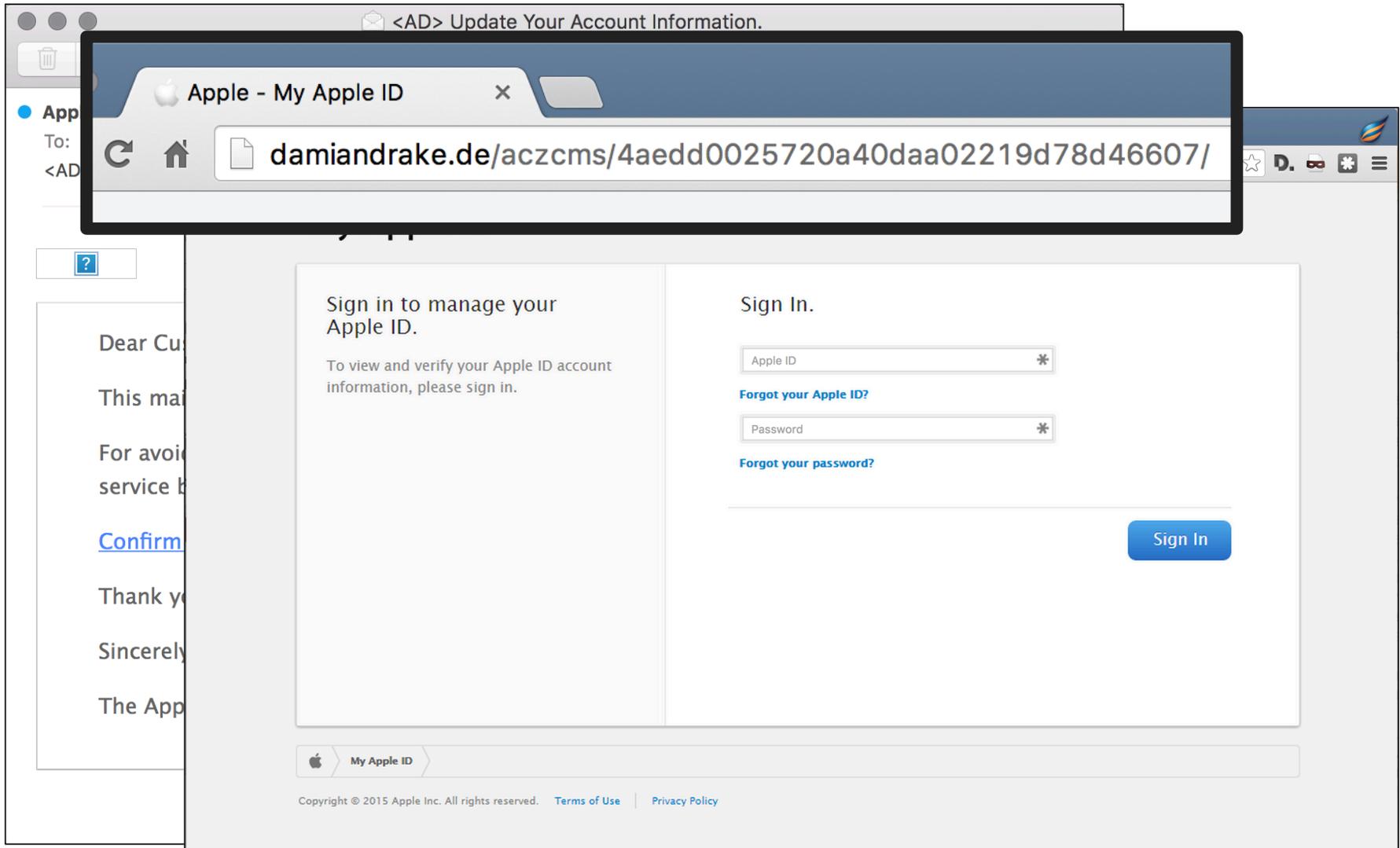
Fraud Example #2: Phishing



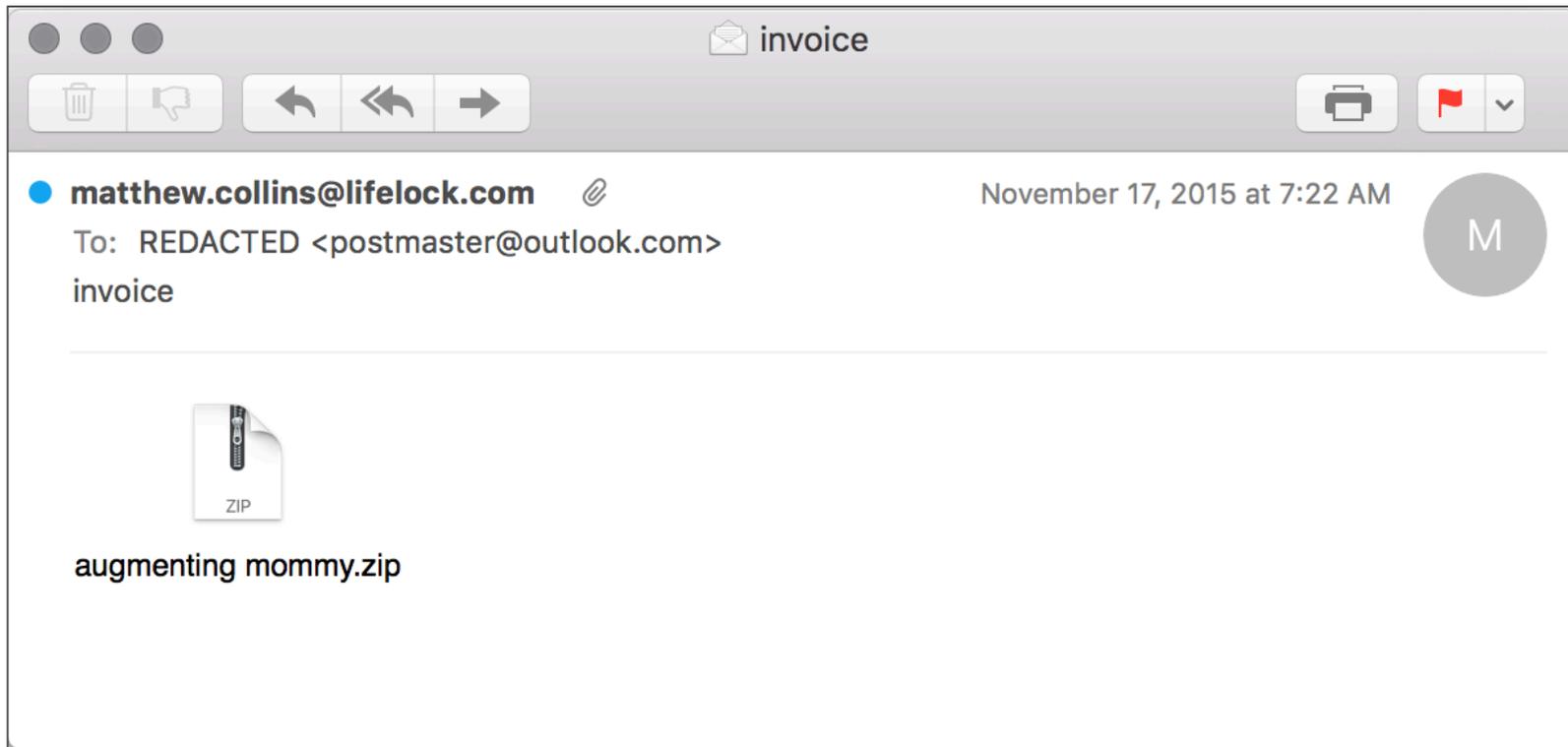
Fraud Example #2: Phishing

The image shows a phishing attempt. On the left, an email from 'Apple <noreply>' is partially visible, with the subject '<AD> Update Your Account Information.' The email body contains a 'Confirm' link. On the right, a browser window displays a fake sign-in page for 'My Apple ID'. The page title is 'My Apple ID' and the URL is 'damiandrake.de/aczcms/4aedd0025720a40daa02219d78d46607/'. The page content includes a sign-in form with fields for 'Apple ID' and 'Password', both marked with an asterisk. There are links for 'Forgot your Apple ID?' and 'Forgot your password?'. A blue 'Sign In' button is at the bottom right. The footer of the page includes the Apple logo, 'My Apple ID', and copyright information: 'Copyright © 2015 Apple Inc. All rights reserved. Terms of Use | Privacy Policy'. The browser's address bar shows a 'PROTECTED' status.

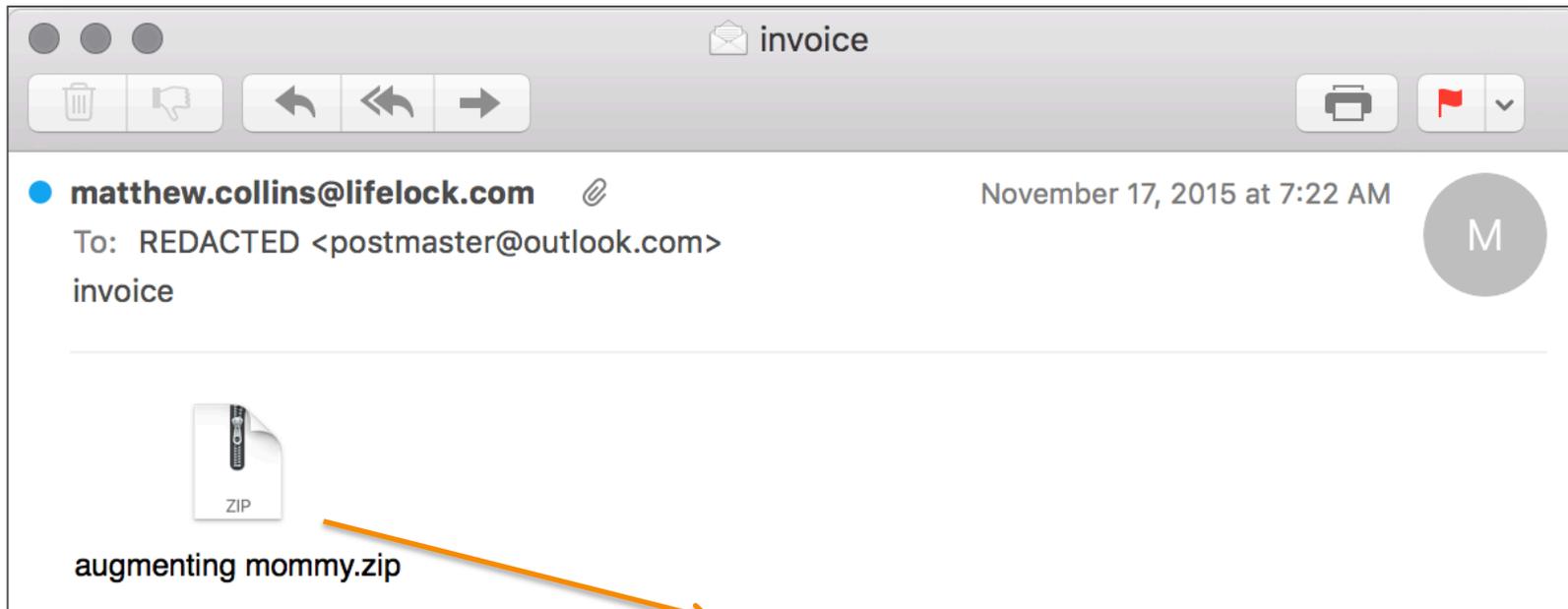
Fraud Example #2: Phishing



Fraud Example #3: Malware



Fraud Example #3: Malware



SHA256: d800579892050fb9f7d3b81b643380b84015ceec19c59501769b5e3c045aa104

File name: augmenting mommy.zip

Detection ratio: 43 / 55

Analysis date: 2016-01-05 23:40:02 UTC (1 minute ago)



Previous Attempts to Fix Email

There have been numerous attempts to reduce/eliminate unauthorized email spoofing.

These Include:

1. Sender Policy Framework (SPF)
2. SenderID
3. DomainKeys
4. DomainKeys Identified Mail (DKIM)
5. Author Domain Signing Practices (ADSP)
6. Visual Trust Indicators: Brandmail, GoodMail, Iconix, Google Gold Key
7. Domain-Based Message Authentication, Reporting, and Conformance (DMARC)

Visual Trust Indicators

home | contact us

Because a **BRAND** is much more than a trademark, It's a **TRUSTMARK!**

about partners product tech info center contact **how to get started**

Welcome to Brandmail Solutions, Europe's leading email authentication and email ID solutions provider. At Brandmail, we work with both ISP's and Sending Brands to provide the most robust and scalable preventative anti-phishing solution on the market. Based on Domain Keys and DKIM, the Brandmail solution is easy to enable and requires no proprietary technology for Email Senders.

Our system is now deployed across a network of over 25million active mailboxes in Europe. Leading brands utilizing our technology include:

OTTO **Weltbild** **Postbank** **facebook**

The Brandmail Solutions Experience

Typical	Branded & Secured
<p>Inbox</p> <p>From Subject</p> <p>Dave Jones Get your en...</p> <p>Quinn Direct Your instan...</p> <p>Bob Howard Important n...</p> <p>Mary Smith Dinner Thu...</p> <p>Free prescriptions Free medic...</p> <p>TGA RE: support...</p> <p>Irish Jobs Latest news</p> <p>News Magazine Top stories</p> <p>San Petersen Party invita...</p> <p>Susan Smith Haven't ask...</p> <p>MyHome in Account sta...</p> <p>Payrol, Inc. Urgent notic...</p> <p>News Magazine Top stories</p>	<p>From</p> <p>Dave Jones</p> <p>QUINNdirect</p> <p>Amir Shervan</p> <p>Mary Smith</p> <p>Free prescriptions</p> <p>Bob Howard Important notice</p> <p>Mary Smith Dinner Thursday</p> <p>Free prescriptions Free medication online</p> <p>Irish Jobs Latest news</p> <p>News Magazine Top stories this week</p> <p>San Petersen Party invitation</p>

SECURE BRAND STAMP

Sender: **QUINNdirect**
 Sender Address: info@quinn-insurance.com

Message verified as authentic and secure by Brandmail Solutions

- Patented Technology
- 100% Secure
- Inbox Branding
- Guaranteed Delivery
- Eliminate Phishing
- No Plug-in Required
- DKIM + DomainKeys

Secure Communications and Measurable Brand Impressions

And the current winners are...

There have been numerous attempts to reduce/eliminate unauthorized email spoofing.

These Include:

1. **Sender Policy Framework (SPF)**
2. SenderID
3. DomainKeys
4. **DomainKeys Identified Mail (DKIM)**
5. Author Domain Signing Practices (ADSP)
6. Visual Trust Indicators: Brandmail, GoodMail, Iconix, Google Gold Key
7. **Domain-Based Message Authentication, Reporting, and Conformance (DMARC)**

Relevant Standards

RFC 5321: Simple Mail Transport Protocol (SMTP)

RFC 5322: Internet Message Format

RFC 7372: Sender Policy Framework v1 (SPF)

RFC 6376: DomainKeys Identified Mail (DKIM) Signatures

RFC 7489: Domain-based Message Authentication, Reporting, and Conformance (DMARC)

DRAFT: Authenticated Received Chain (ARC)

Authenticated Email with DMARC

DMARC

- Visibility
- Policy
- Alignment
- Scalable

SPF

- Authenticates Envelope
- Breaks due to relaying
- Must Understand Ecosystem
- Receivers don't honor policy model

DKIM

- Survives Relaying
- Authenticates the Signing domain
- Must Understand Ecosystem
- Nobody adopted policy model (ADSP)

SMTP

- Moves email around the Internet
- No Authentication

SMTP in Action

SERVER

CLIENT

```
220 mta1257.mail.bf1.yahoo.com ESMTP ready
250 mta1257.mail.bf1.yahoo.com
250 sender <test@test.com> ok
250 recipient <johnmwilson3@yahoo.com> ok
354 go ahead

                Subject: SMTP Demo
                Message-Id: <159@agari.com>
                From: test@test.com

                This is a test message.
                .
quit
```

A Question of Identity

helo sherlock-poc-00.qa.agari.com

mail from: <test@test.com>

rcpt to: johnmwilson3@yahoo.com

data

DKIM-Signature: v=1; d=agari.com; s=s1024; h=...

Subject: SMTP Demo

Message-Id: <160@agari.com>

From: test@example.com

This is a test message.

.

quit

A Question of Identity

helo sherlock-poc-00.qa.agari.com ¹ HELO Domain

mail from: <test@test.com>

rcpt to: johnmwilson3@yahoo.com

data

DKIM-Signature: v=1; d=agari.com; s=s1024; h=...

Subject: SMTP Demo

Message-Id: <160@agari.com>

From: test@example.com

This is a test message.

.

quit

A Question of Identity

helo sherlock-poc-00.qa.agari.com ¹ HELO Domain

mail from: <test@test.com> ² Envelope Domain

rcpt to: johnmwilson3@yahoo.com

data

DKIM-Signature: v=1; d=agari.com; s=s1024; h=...

Subject: SMTP Demo

Message-Id: <160@agari.com>

From: test@example.com

This is a test message.

.

quit

A Question of Identity

```
helo sherlock-poc-00.qa.agari.com 1 HELO Domain
mail from: <test@test.com> 2 Envelope Domain
rcpt to: johnmwilson3@yahoo.com
data
DKIM-Signature: v=1; d=agari.com; s=s1024; h=... 3 Signing Domain
Subject: SMTP Demo
Message-Id: <160@agari.com>
From: test@example.com

This is a test message.
.
quit
```

A Question of Identity

```
helo sherlock-poc-00.qa.agari.com 1 HELO Domain
mail from: <test@test.com> 2 Envelope Domain
rcpt to: johnmwilson3@yahoo.com
data
DKIM-Signature: v=1; d=agari.com; s=s1024; h=... 3 Signing Domain
Subject: SMTP Demo
Message-Id: <160@agari.com>
From: test@example.com 4 From Header Domain

This is a test message.
.
quit
```

Sender Policy Framework (SPF)

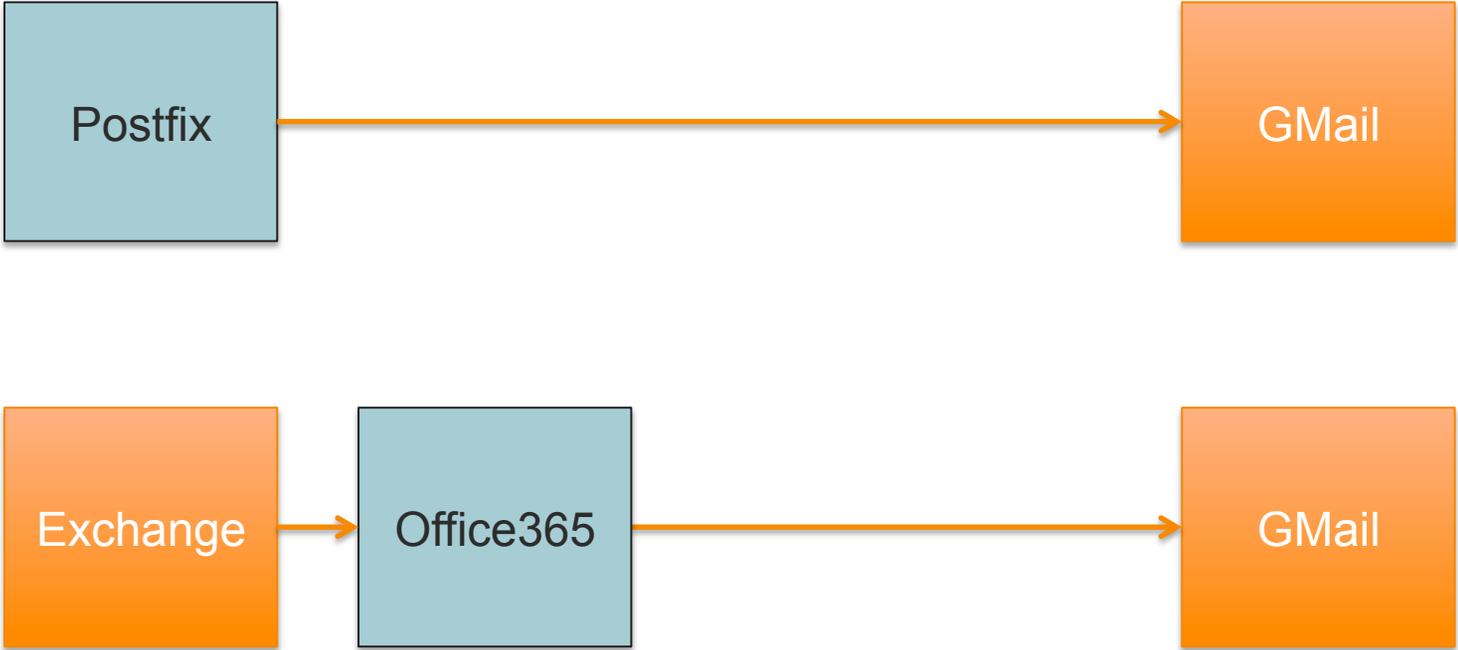
```
$ dig apple.com TXT +short  
"v=spf1 ip4:17.0.0.0/8 -all"
```

```
$ dig paypal.com TXT +short  
"v=spf1 include:pp._spf.paypal.com  
include:3ph1._spf.paypal.com  
include:3ph2._spf.paypal.com  
include:3ph3._spf.paypal.com  
include:3ph4._spf.paypal.com  
include:c._spf.ebay.com ~all"
```

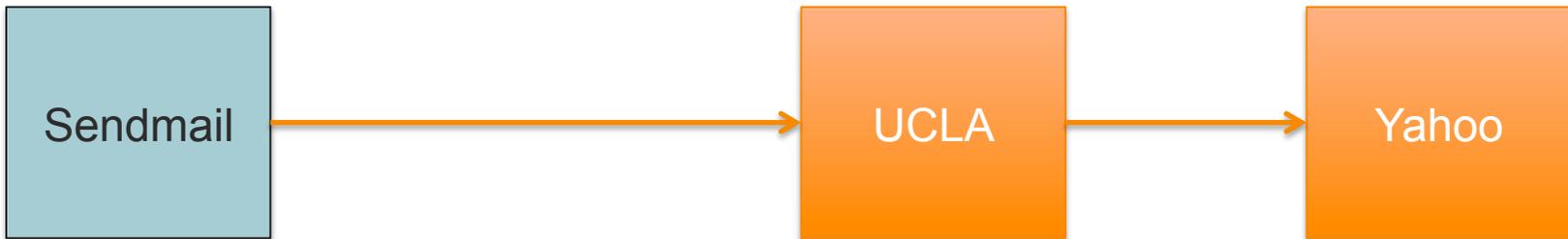
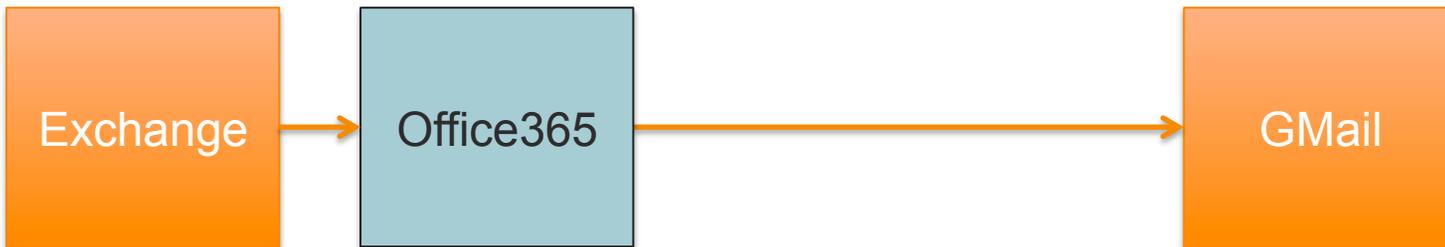
Some Possible Mail Flows



Some Possible Mail Flows



Some Possible Mail Flows



SPF Issues

1. Breaks due to Relaying/Auto-Forwarding
2. Mailing Lists
3. Authenticates the Envelope Domain (MAIL FROM)
4. 10-lookup limit
5. DNS: TCP Failover
6. Don't forget your NDRs and OOOs! (HELO fallback)

DomainKeys Identified Mail (DKIM)

```
DKIM-Signature: v=1; a=rsa-sha256; q=dns/txt; c=relaxed/relaxed;  
t=1452797764;  
s=m1; d=mktdns.com; i=@mktdns.com;  
h=Date:From:To:Subject:MIME-Version:Content-Type;  
bh=RRSNK9HgZTD19RkhqzAz6BCwQwOgMkeqlYhpQlNcBe0=;  
b=M3uhaNzDRcdjyb7W47U1AJFxNfEaxWQUtumTPg+ZDbpFI tSiRTvq5IisZNM+1N8D  
KUk162WTTU5AR6Uza8P+Gx+E1+EDzvI67+K2hfwCMiJxGy+A2VyNzvyn3KPVL7QWmdx  
b8QGgwm2CD5MmpiGoof5fv42IL1fFIG+ghVyW4i4=
```

```
$ dig m1._domainkey.mktdns.com TXT +short  
"v=DKIM1\;k=rsa  
\;p=MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCrXrxjXj4Tyz0zoKUw3mlg  
+zRZG3i6fkWmcqB9+/HSZdxUmStLhq5EKWQuXZfHZ6QsRUq/  
ZKbP6lOCXUPyY5k1lFBkjjbv2qP1iL/5lOWcRMDKsaJxtDHXxXHtkjgEgWM8Xyes/  
LEkQ5HlPQN+89DUeAJGf1lgTa6rk1Gxzch0lQIDAQAB"
```

DomainKeys Identified Mail (DKIM)

```
DKIM-Signature: v=1; a=rsa-sha256; q=dns/txt; c=relaxed/relaxed;  
t=1452797764;
```

```
s=m1; d=mktdns.com; i=@mktdns.com;
```

```
n=Date:From:To:Subject:MIME-Version:Content-Type;
```

```
bh=RRSNK9HgZTD19RkhqzAz6BCwQwOgMkeq1YhpQ1NcBe0=;
```

```
b=M3uhaNzDRcdjyb7W47U1AJFxFxEaxWQUtumTPg+ZDbpFItSiRTvq5IisZNM+1N8D  
KUxl62WTTU5AR6Uza8P+Gx+E1+EDzvI67+K2hfwCMiJxGy+A2VyNzvyn3KPVL7QWmdx  
b8QGgwm2CD5MmpiGoof5fv42IL1fFIG+ghVyW4i4=
```

```
$ dig m1._domainkey.mktdns.com TXT +short
```

```
"v=DKIM1;k=rsa
```

```
\;p=MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCrXrxjXj4Tyz0zoKUw3mlg
```

```
+zRZG3i6fkWmcqB9+/HSZdxUmStLhq5EKWQuXZfHZ6QsRUq/
```

```
ZKbP6lOCXUPyY5k1lFBkjbbv2qP1iL/5lOWcRMDKsaJxtDHXxXHtkjgEgWM8Xyes/
```

```
LEkQ5HlPQN+89DUeAJGf1lgTa6rk1Gxzch0lQIDAQAB"
```

DomainKeys Identified Mail (DKIM)

```
DKIM-Signature: v=1; a=rsa-sha256; q=dns/txt; c=relaxed/relaxed;  
t=1452797764;
```

```
s=m1; d=mktDNS.com; i=@mktDNS.com;
```

```
n=Date:From:To:Subject:MIME-Version:Content-Type;
```

```
bh=RRSNK9HgZTD19RkhqzAz6BCwQwOgMkeq1YhpQ1NcBe0=;
```

```
b=M3uhaNzDRcdjyb7W47U1AJFxNfEaxWQUtumTPg+ZDbpFI tSiRTvq5IisZNM+1N8D  
KUk162WTTU5AR6Uza8P+Gx+E1+EDzvI67+K2hfwCMiJxGy+A2VyNzvyn3KPVL7QWmdx  
b8QGgwm2CD5Mmpiooof5fv42IL1fFIG+ghVyW4i4=
```

```
$ dig m1 _domainkey.mktDNS.com TXT +short
```

```
"v=DKIM1\;k=rsa
```

```
\;p=MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCrXrxjXj4Tyz0zoKUw3mlg
```

```
+zRZG3i6fkWmcqB9+/HSZdxUmStLhq5EKWQuXZfHZ6QsRUq/
```

```
ZKbP6lOCXUPyY5k1lFBkjjbv2qP1iL/5lOWcRMDKsaJxtDHXxXHtkjgEgWM8Xyes/
```

```
LEkQ5HlPQN+89DUeAJGf1lgTa6rk1Gxzch0lQIDAQAB"
```

DomainKeys Identified Mail (DKIM)

```
DKIM-Signature: v=1; a=rsa-sha256; q=dns/txt; c=relaxed/relaxed;  
t=1452797764;
```

```
s=m1; d=mktdns.com; i=@mktdns.com;
```

```
n=Date:From:To:Subject:MIME-Version:Content-Type;
```

```
bh=RRSNK9HgZTD19RkhqzAz6BCwQwOgMkeq1YhpQlNcBe0=;
```

```
b=M3uhaNzDRcdjyb7W47U1AJFxFNfEaxWQUtumTPg+ZDbpFItSiRTvq5IisZNM+1N8D  
KUk162WTTU5AR6Uza8P+Gx+E1+EDzvI67+K2hfwCMiJxGy+A2VyNzvyn3KPVL7QWmdx  
b8QGgwm2CD5Mmpiooof5fv42ILlfFIG+ghVyW4i4=
```

```
$ dig m1._domainkey.mktdns.com TXT +short
```

```
"v=DKIM1;k=rsa
```

```
\;p=MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCrXrxjXj4Tyz0zoKUw3mlg
```

```
+zRZG3i6fkWmcqB9+/HSZdxUmStLhq5EKWQuXZfHZ6QsRUq/
```

```
ZKbP6lOCXUPyY5k1lFBkjjbv2qP1iL/5lOWcRMDKsaJxtDHXxXHtkjgEgWM8Xyes/
```

```
LEkQ5HlPQN+89DUeAJGf1lgTa6rk1Gxzch0lQIDAQAB"
```

DKIM Issues

1. Benign Message Modifications
2. Mailing Lists
3. Authenticates Signing Identity (DKIM d=)
4. Replay Attack
5. Key Size

DMARC

```
$ dig _dmarc.twitter.com TXT +short
```

```
"v=DMARC1; p=reject; rua=mailto:d@rua.agari.com; ruf=mailto:d@ruf.agari.com; fo=1"
```

v=DMARC1 Record applies to version 1 of the DMARC specification

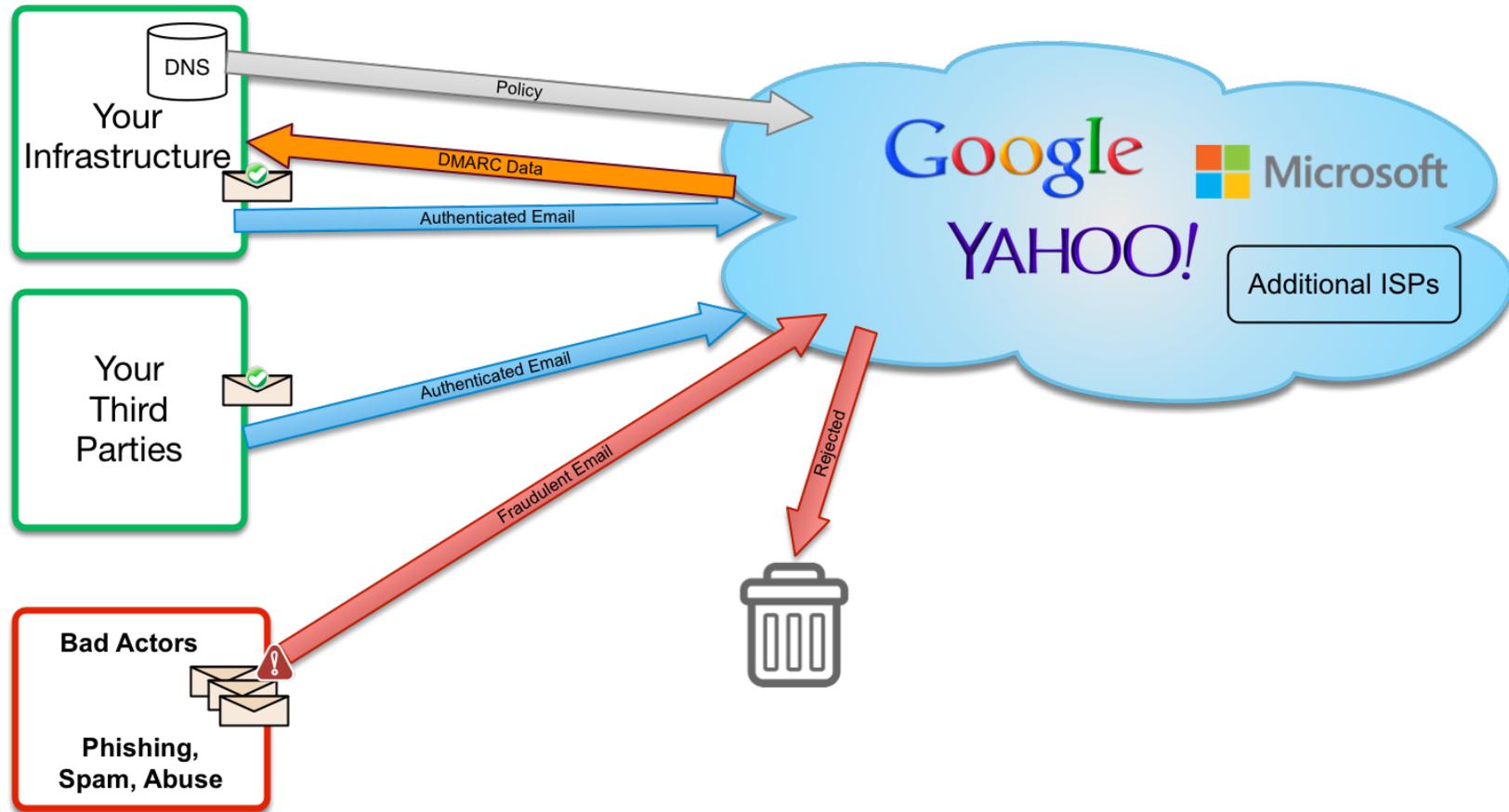
p=reject Domain owner wishes to have failing messages blocked by receivers

rua=mailto:d@rua.agari.com Receivers should send summary data to d@rua.agari.com

ruf=mailto:d@ruf.agari.com Receivers should send forensic data to d@ruf.agari.com

fo=1 Domain owner would like forensic reports for messages failing 1 or more protocols

DMARC Data Flow



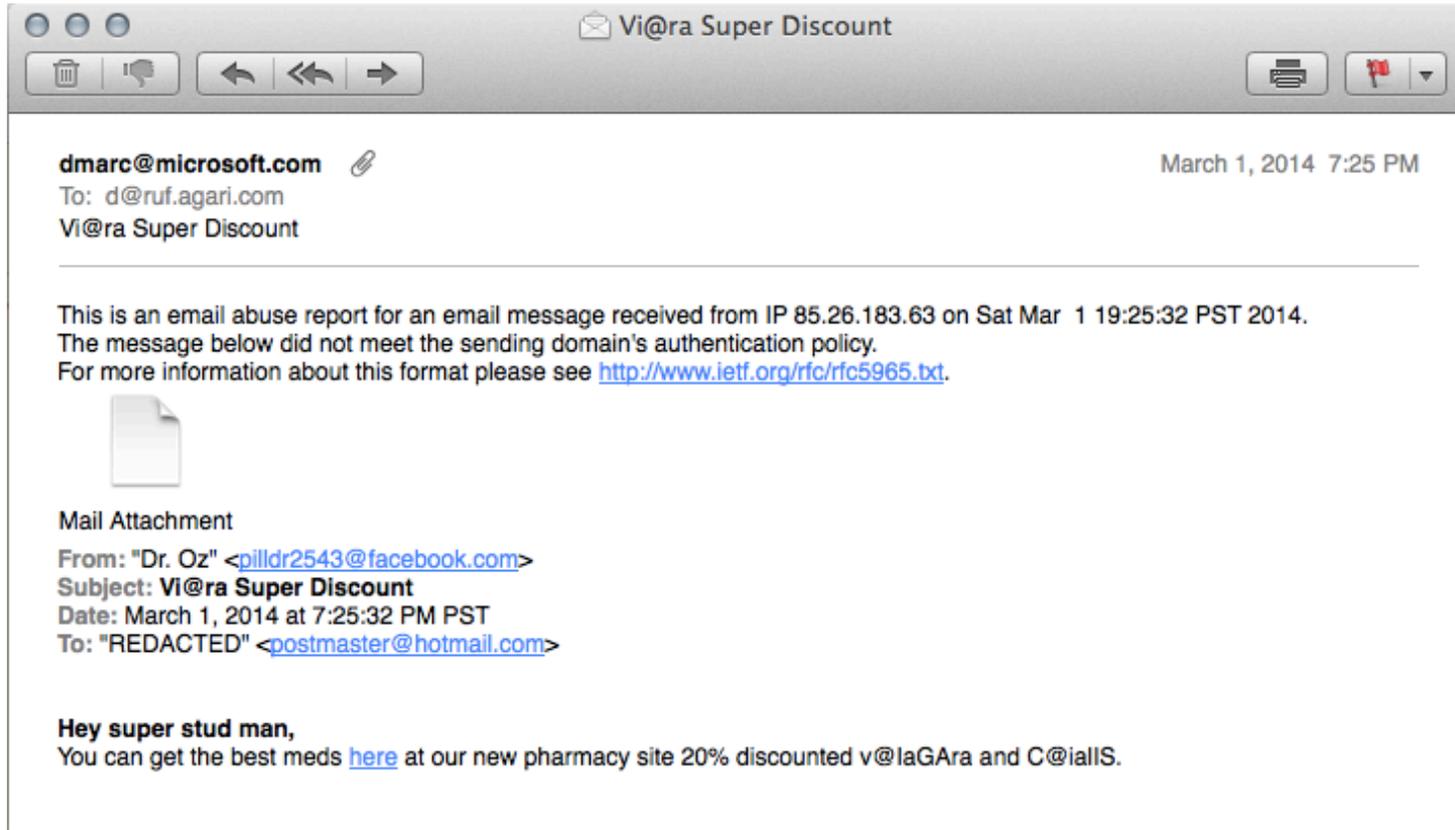
DMARC XML Aggregate Data Example

```
<?xml version="1.0"?>
<feedback>
  <report_metadata>
    <org_name>Yahoo! Inc.</org_name>
    <email>postmaster@dmARC.ya
    <report_id>1393150703.9760
    <date_range>
      <begin>1393027200</begin>
      <end>1393113599</end>
    </date_range>
  </report_metadata>
  <policy_published>
    <domain>alertsp.chase.com</domain>
    <adkim>r</adkim>
    <aspf>r</aspf>
    <p>reject</p>
    <pct>100</pct>
  </policy_published>
```

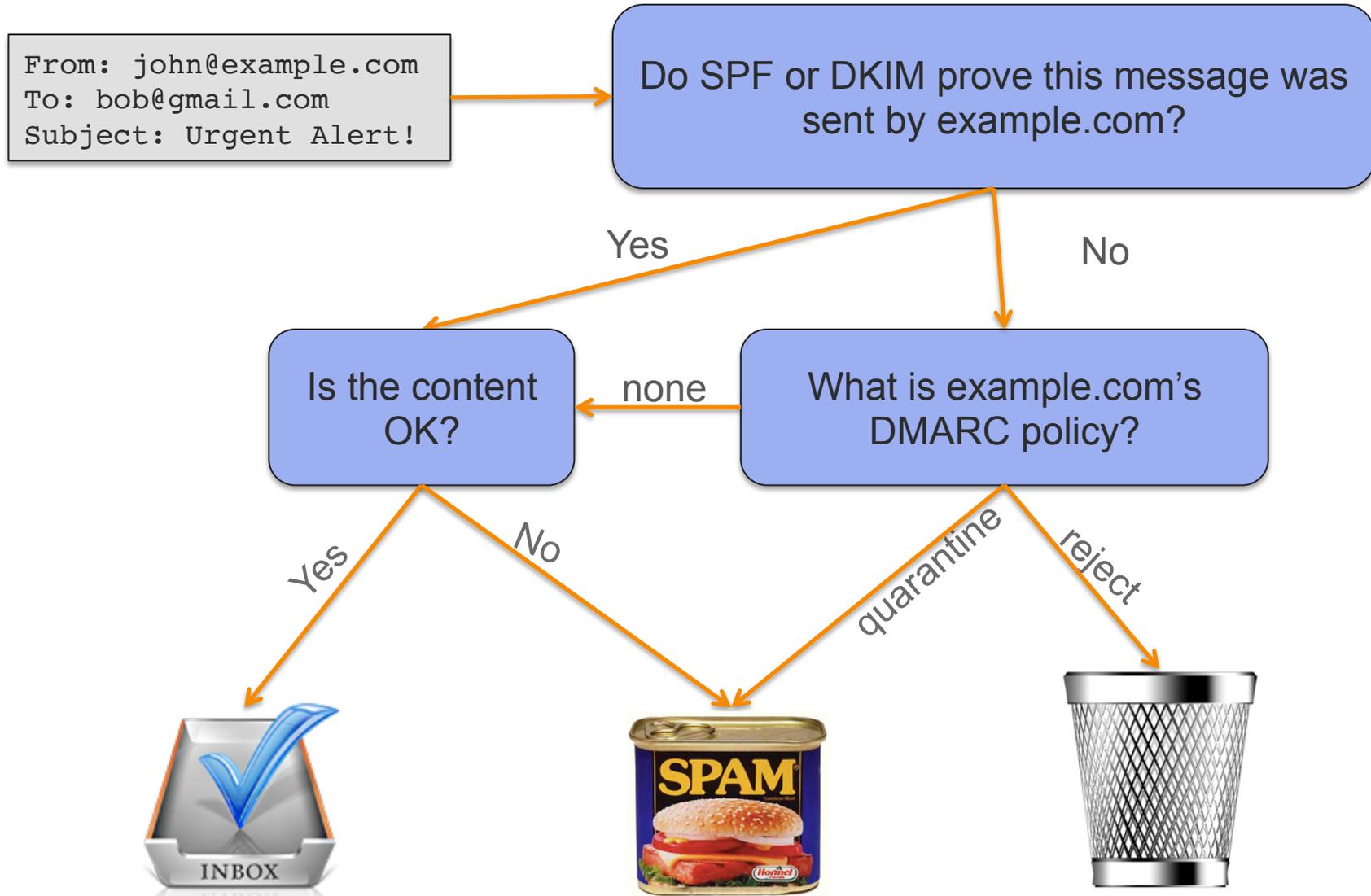
```
<record>
  <row>
    <source_ip>106.10.149.115</source_ip>
    <count>1</count>
    <policy_evaluated>
      <disposition>none</disposition>
      <dkim>pass</dkim>
      <spf>fail</spf>
    </policy_evaluated>
  </row>
  <identifiers>
    <header_from>alertsp.chase.com</header_from>
  </identifiers>
  <auth_results>
    <dkim>
      <domain>alertsp.chase.com</domain>
      <result>pass</result>
    </dkim>
    <spf>
      <domain>alertsp.chase.com</domain>
      <result>fail</result>
    </spf>
  </auth_results>
</record>
```

DMARC Forensic Feedback Example

Full Message Example (hotmail.com, outlook.com, etc.):



Typical DMARC Policy Enforcement Flow



DMARC Policy Enforcement in Action

```
telnet> Trying 66.196.118.35...
Connected to mta6.am0.yahoodns.net.
Escape character is '^]'.
220 mta1312.mail.bf1.yahoo.com ESMTP ready
HELO foon.paul.sf.agari.com
250 mta1312.mail.bf1.yahoo.com

MAIL FROM: <security@chase.com>
250 sender <security@chase.com> ok

RCPT TO: <johnmwilson3@yahoo.com>
250 recipient <johnmwilson3@yahoo.com> ok

DATA
354 go ahead
Message-Id: <1393480824.24.agari1393480824@foon.paul.sf.agari.com>
Date: Wed, 26 Feb 2014 22:00:24 -0800
Subject: Urgent Message From security@chase.com
From: security@chase.com
To: johnmwilson3@yahoo.com

This email message was sent by Agari to demonstrate just
how easy it is to spoof an email address.

This message was sent to johnmwilson3@yahoo.com.

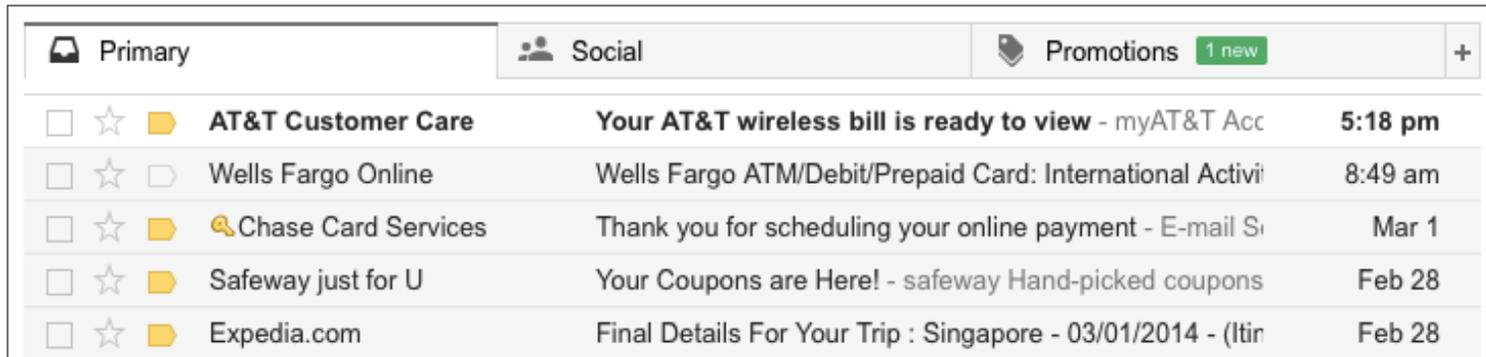
554 5.7.9 Message not accepted for policy reasons. See http://postmaster.yahoo.com/errors/postmaster-28.html
Connection closed by foreign host.
```

Limitations

- DMARC does not solve the “Friendly From” Problem:

From: PayPal Security <paypay2182@hotmail.com>

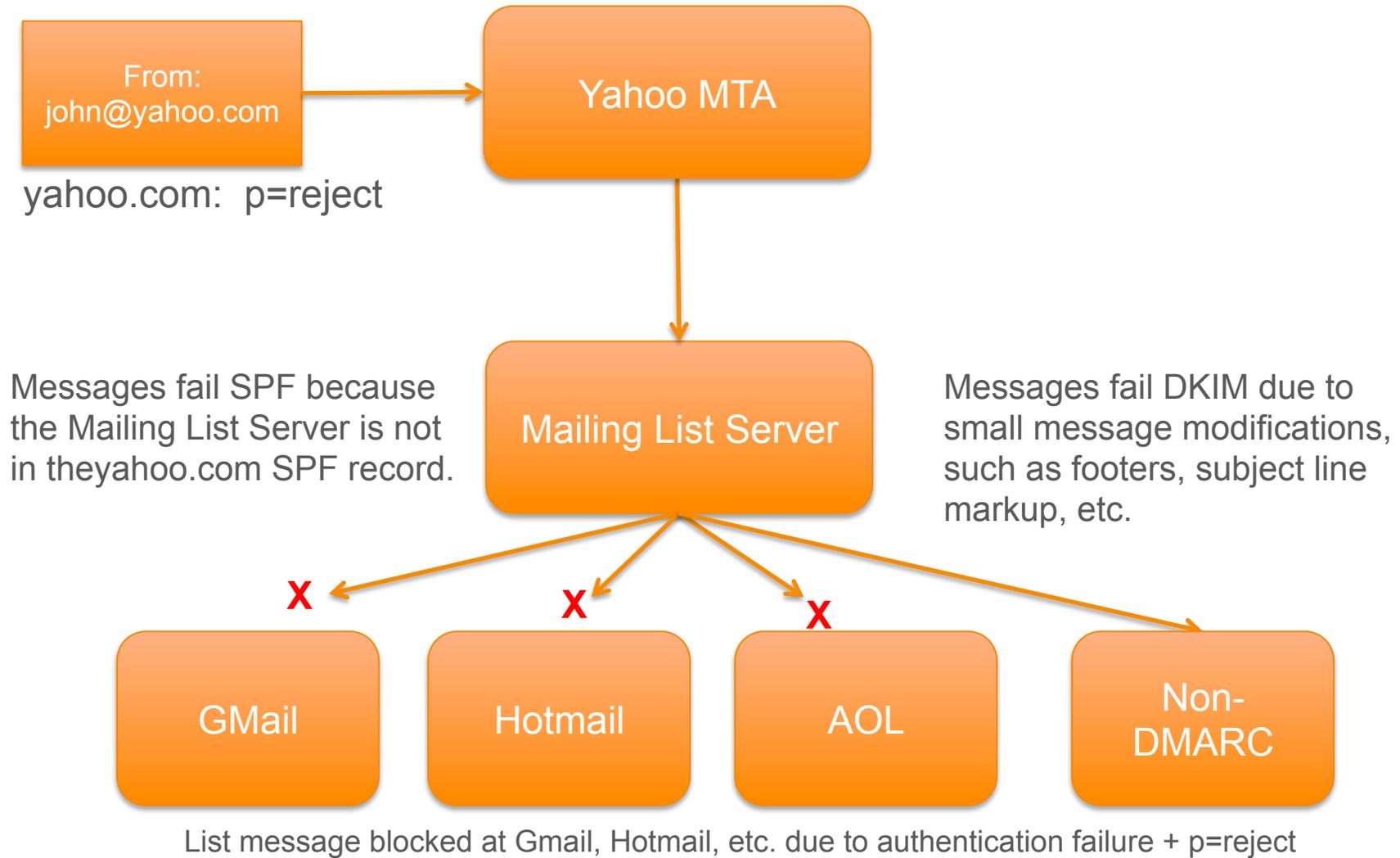
- Inbox differentiation may help here



Primary	Social	Promotions	1 new	+
<input type="checkbox"/> <input type="star"/> <input type="folder"/>	AT&T Customer Care	Your AT&T wireless bill is ready to view - myAT&T Acc	5:18 pm	
<input type="checkbox"/> <input type="star"/> <input type="folder"/>	Wells Fargo Online	Wells Fargo ATM/Debit/Prepaid Card: International Activi	8:49 am	
<input type="checkbox"/> <input type="star"/> <input type="folder"/>	<input type="magnifying-glass"/> Chase Card Services	Thank you for scheduling your online payment - E-mail S	Mar 1	
<input type="checkbox"/> <input type="star"/> <input type="folder"/>	Safeway just for U	Your Coupons are Here! - safeway Hand-picked coupons	Feb 28	
<input type="checkbox"/> <input type="star"/> <input type="folder"/>	Expedia.com	Final Details For Your Trip : Singapore - 03/01/2014 - (Itir	Feb 28	

- If your mail provider doesn't support DMARC, the bad stuff still gets through
 - This is an ever-decreasing pool
 - Herd Immunity

Controversy: Mailing Lists



But wait it gets worse...

The Mailing List Server sees a bunch of SMTP 5xx errors due to yahoo.com's DMARC p=reject policy.

The Mailing List Server automatically removes members from the mailing list after N messages that user bounce. To the Mailing List Server, DMARC rejections look no different than “mailbox full” or “no such user” errors.

After a couple of Yahoo users post to a mailing list, most of the mailing list users get unsubscribed since the yahoo.com messages were undeliverable to anybody at Gmail, Hotmail, Yahoo, AOL, Comcast, etc.

Options to deal with Mailing Lists

1. List Participant:

Post using an address that doesn't implement a strong DMARC policy

Pros: No need to change mailing list software.

Cons: This is getting more and more difficult! How am I supposed to know my webmail provider just implemented DMARC p=reject?!?

2. List Operator:

Send list messages "From:" the list itself, rather than the originator. Add a Reply-To: header with the originator's email address.

Pros: Keeps the mail flowing, even when the sending address has a p=reject policy.

Cons: Changes the semantics of Reply vs. Reply-All. Requires the List Operator to cooperate. Not all mailing list software can support this.

Mailman: <http://wiki.list.org/DEV/DMARC>

Options to deal with Mailing Lists (2)

3. List Operator:

Status Quo, except don't auto-unsubscribe for DMARC rejections.

Pros: Avoids having the whole list get unsubscribed due to a couple of p=reject messages.

Cons: Some users won't be able to post to the list anymore. Different receivers use different SMTP error codes to denote DMARC rejections.

4. Receiver:

Detect mailing list traffic and override DMARC reject for list-originated traffic.

Pros: No change necessary on part of poster or list operator.

Cons: Opens a loophole for fraud. Anybody can spoof a message from user@paypal.com to the list, circumventing paypal.com's DMARC policy.

Options to deal with Mailing Lists (3)

5. List Operator, Receiver:

Implement ARC (Authenticated Received Chain).

Pros: Lets DMARC play well with mailing lists without sacrificing security.

Cons: Requires the list operator AND the receiver to implement ARC.

<http://arc-spec.org/> - Authenticated Received Chain specification

Open Source Tools

OpenDKIM

← → ↻ www.opendkim.org

OpenDKIM

[Download](#) [Documentation](#) [Bug/Feature Tracking](#) [Mailing lists](#) [Community](#) [Services](#) [Donate](#) [Links](#) [License](#)

OpenDKIM

OpenDKIM is a community effort to develop and maintain a C library for producing DKIM-aware applications and an open source milter for providing DKIM service.

The project started from a code fork of version 2.8.3 of the open source [dkim-milter](#) package developed and maintained by [Sendmail, Inc.](#)

OpenDKIM is an open source implementation of the DKIM (Domain Keys Identified Mail) sender authentication system proposed by the E-mail Signing Technology Group (ESTG), now standardized by the IETF ([RFC6376](#)). It also includes implementations of the [RFC5617](#) Vouch By Reference (VBR, [RFC5518](#)) proposed standard and the experimental Authorized Third Party Signatures protocol (ATPS, [RFC6541](#)).

- C library + milter
- Performs DKIM signing and DKIM signature validation

Open Source SPF Tools

← → ↻ www.openspf.org/Implementations

[Home](#) | [Sitemap](#) | [Recent Changes](#) | [Login](#)

Sender Policy Framework Implementations

There are several SPF [libraries](#) available. Many [mail servers](#) support SPF natively. Most popular mail servers also have [extensions](#) or [unofficial patches](#) available. The SPF project does not endorse any of the software listed below unless noted otherwise. We have not checked all of the software for fitness for any purpose. Please report SPF-supporting software to the [spf-discuss mailing list](#) or by [contacting us directly](#).

Libraries

Name	Type	Author(s)	Contact	Test Suite releases passed
libspf2	C	Shevek, Wayne Schlitt	spf-devel	?
RMSPF	C (Windows)	Roger Moser	Roger Moser	?
Mail::SPF	Perl	Julian Mehnle, Shevek	Julian Mehnle	2008.08: since 2.006 2007.05: since 2.004
pyspf	Python	Stuart Gathman, Scott Kitterman, Terence Way	see Python Package Index	RFC 7208: since 2.0.9 2008.08: since 2.0.5 2007.05: since 2.0.4
jSPF	Java	Stefano Bagnara, Norman Maurer	see website	2007.05: since 0.9.6
InterPC.SPF	.NET	Eddy Minet	InterPC.SPF Forum	2007.05: since 1.1

libspf2

← → ↻ www.libspf2.org

libspf2 - SPF Library - Home

SPF | SRS

Navigation

- > Home
- > Status
- > Download
- > Documentation
- > Support
- > FAQ

Welcome

libspf2 implements the Sender Policy Framework, a part of the SPF/SRS protocol. It is used by Exim, Zmailer and MS Exchange to check SPF records and make sure that the email is not forged, commonly used by spammers, scammers and email viruses/worms.

News

June 10th, 2013: libspf2 version 1.2.10 has been released, and is available [here](#).

November 4th, 2008: libspf2 version 1.2.9 has been released, and is available [here](#). It fixes an envelope sender, amongst other issues. An update is recommended.

OpenDMARC

← → ↻ www.trusteddomain.org/opendmarc/

OpenDMARC

OpenDMARC is a free open source software implementation of the DMARC specification. You can browse the source code, download the latest released version or view the release trackers [here](#).

This work is part of an initiative of [The Trusted Domain Project](#) has been sponsored by TrustSphere, Cloudmark, Sendmail, NLNet, American Greetings, Google and others. [View the project here](#).

Documentation

- [Package README](#)
- [libopendmarc](#)
- [opendmarc README](#)
- [opendmarc\(8\)](#)
- [opendmarc.conf\(5\)](#)
- [reports README](#)
- [opendmarc-import\(8\)](#)
- [opendmarc-reports\(8\)](#)

- Implemented as a milter (mail filter)
- Performs DMARC verification and reporting
- Uses MySQL to store data between reporting intervals

DMARC Adoption

DMARC Adoption – Consumer Mailbox Providers

85% of US, 60% world-wide consumer mailboxes today and growing

Provider	Mailboxes	Data	Enforcement	Msg Level
Yahoo!	320 Million	✓	✓	✓*
AT&T (via Yahoo)	8 Million	✓	✓	✓*
Rogers Communications (via Yahoo)	10 Million	✓	✓	✓*
Verizon (via Yahoo)	6 Million	✓	✓	✓*
Xtra, SBC, Ameritech, and additional Y! partners	20 Million	✓	✓	✓*
Google (Including 4.6M Apps Domains)	425 Million	✓	✓	
Microsoft (Hotmail, Live.com, Outlook.com, MSN)	380 Million	✓	✓	✓
AOL	50 Million	✓	✓	
Comcast	20 Million	✓	✓	
NetEase (163.com, 126.com, yeah.net)	510 Million	✓	✓	✓**
xs4all.nl	1 Million	✓	✓	
Mail.ru	300 Million	✓	✓	
Yandex	200 Million		✓	
LinkedIn	-	✓	✓	✓
Facebook	800 Million		✓	
iCloud	15 Million	2016	2016	

* URLs only; via private channel

** Full body available upon request

* Via Private Channel

DMARC Adoption – Business Mailbox Providers

Open Source	Status
Sendmail (via OpenDMARC)	production
Postfix (via OpenDMARC)	production
qmail (via qsmtpd and OpenDMARC)	production
Commercial	Status
Google Apps	production
Cisco/IronPort	production
Proofpoint	production (limited, no reporting)
Symantec Cloud	production (no reporting)
Message Systems (via OpenDMARC)	production
Office 365	production (quarantine only, no reporting)
Alt-N Mdaemon	production

Estimating Receiver Adoption

1. Start with a list of email addresses
2. Look up the MX host for each
3. See if that host is known to support DMARC
4. Tally everything up

For #1 I will use the Ashley Madison breach dataset



Doing the MX Lookups

```
$ dig gmail.com mx +short
```

```
40 alt4.gmail-smtp-in.1.google.com.  
20 alt2.gmail-smtp-in.1.google.com.  
5 gmail-smtp-in.1.google.com.  
30 alt3.gmail-smtp-in.1.google.com.  
10 alt1.gmail-smtp-in.1.google.com.
```



```
$ dig netflix.com mx +short
```

```
1 aspmx.1.google.com.  
10 aspmx2.googlemail.com.  
10 aspmx3.googlemail.com.  
5 alt1.aspmx.1.google.com.  
5 alt2.aspmx.1.google.com.
```



```
$ dig ucla.edu mx +short
```

```
10 mx-ucb2.smtp.ucla.edu.  
10 mx-asm2.smtp.ucla.edu.  
10 mx-csb1.smtp.ucla.edu.  
5 mx.smtp.ucla.edu.  
10 mx-csb2.smtp.ucla.edu.  
10 mx-ucb1.smtp.ucla.edu.  
99 v4.smtp.ucla.edu.
```



DMARC Coverage by Country - Results

Country	Estimated Coverage
Venezuela	96.9%
Mexico	95.5%
USA	90.7%
New Zealand	89.1%
Canada	88.5%
Brazil	87.8%
Australia	86.7%
UK	86.4%
France	77.1%
Germany	42.0%
Japan	38.7%

Resources

<http://dmarc.org> - Everything about DMARC including the specification

<http://dkim.org> - Everything about DKIM

<http://www.openspf.org/> - Everything you need to know about SPF

<http://www.libspf2.org/> - An open-source library to do SPF

<https://www.agari.com/resources/> - Agari technical and marketing documents, videos, whitepapers, etc.

<http://www.stevejenkins.com/blog/2015/03/installing-opendmarc-rpm-via-yum-with-postfix-or-sendmail-for-rhel-centos-fedora/> - Step-by-step “how-to” to install and run opendmarc

<http://wiki.list.org/DEV/DMARC> - How to make Mailman play well with DMARC

<http://arc-spec.org/> - Authenticated Received Chain specification

<https://github.com/linkedin/lafayette> - Project to ingest, store, index, and search ARF data

Thank You!