proofpoint

CYBER SECURITY SUMMIT

EMAIL FRAUD DEFENSE:
How To Fight The Next Generation of Targeted BEC Attacks

Brian Westnedge

bwestnedge@proofpoint.com

November 8, 2017

THE BUSINESS PROBLEM

BUSINESS EMAIL COMPROMISE (BEC) & CONSUMER PHISHING

We Authenticate Everything We Need To Trust…

	Authenticated?
Network Access	☑
Applications	☑
Endpoints	☑
Transactions	☑
Physical Access	☑
Email	✗

…Except Email

Email is Insecure by Definition

Network Working Group
Request for Comments: 2821
Obsoletes: 821, 974, 1869
Updates: 1123
Category: Standards Track

J. Klensin, Editor
AT&T Laboratories
April 2001

Simple Mail Transfer Protocol

7.1 Mail Security and Spoofing

SMTP mail is inherently insecure in that it is feasible for even fairly casual users to negotiate directly with receiving and relaying SMTP servers and create messages that will trick a naive recipient into believing that they came from somewhere else. Constructing such a message so that the "spoofed" behavior cannot be detected by an expert is somewhat more difficult, but not sufficiently so as to be a deterrent to someone who is determined and knowledgeable…

https://www.ietf.org/rfc/rfc2821.txt

Business Email Compromise / Impostor Email

Tue 2/23/2016 6:46 PM

Wage Review

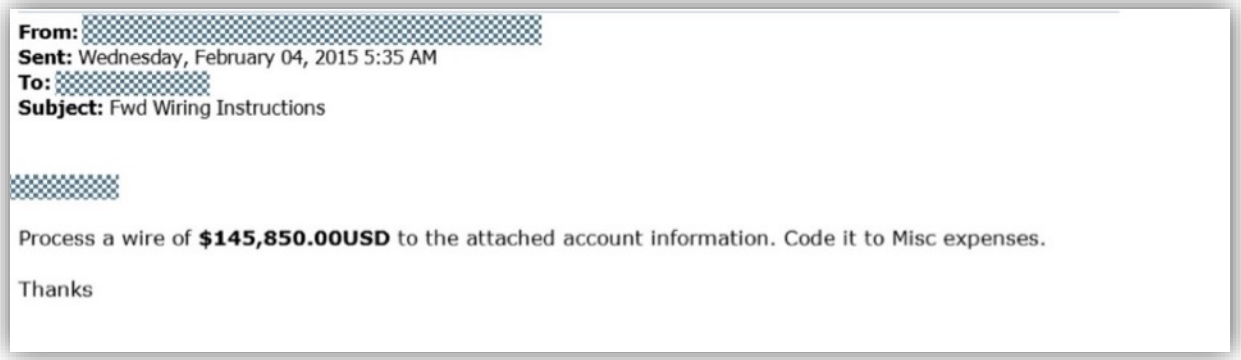
To

Retention Policy 270 Days Inbox Folder Retention (9 months) Expires 11/19/2016

Hello

Kindly send me the w2s for all employees in the company for the 2015 tax year for review. Thank you.

Regards,



From:
Sent: Wednesday, February 04, 2015 5:35 AM
To:
Subject: Fwd Wiring Instructions

Process a wire of **$145,850.00USD** to the attached account information. Code it to Misc expenses.

Thanks

Company Acquisition

I´ve just had some news from our attorneys confirming that we are in the final stages of completing a very important acquisition for the company. Having been privately negotiating this acquisition for a number of months it´s great news we are finally so close to closing.

I will need you to make a wire payment today in the form of a deposit for the acquisiton.

Use this email as my full approval for this and any additional wires that may be required over coming days.

It´s been agreed that, at this stage, the acquisition needs to remain private, so I have arranged for the lead attorney, Mark Curtis, to contact you directly. He will work with you to ensure we have everything completed in line with the terms agreed.

You will need to give him your full attention and provide him with all relevant information he requires for due dilligence.

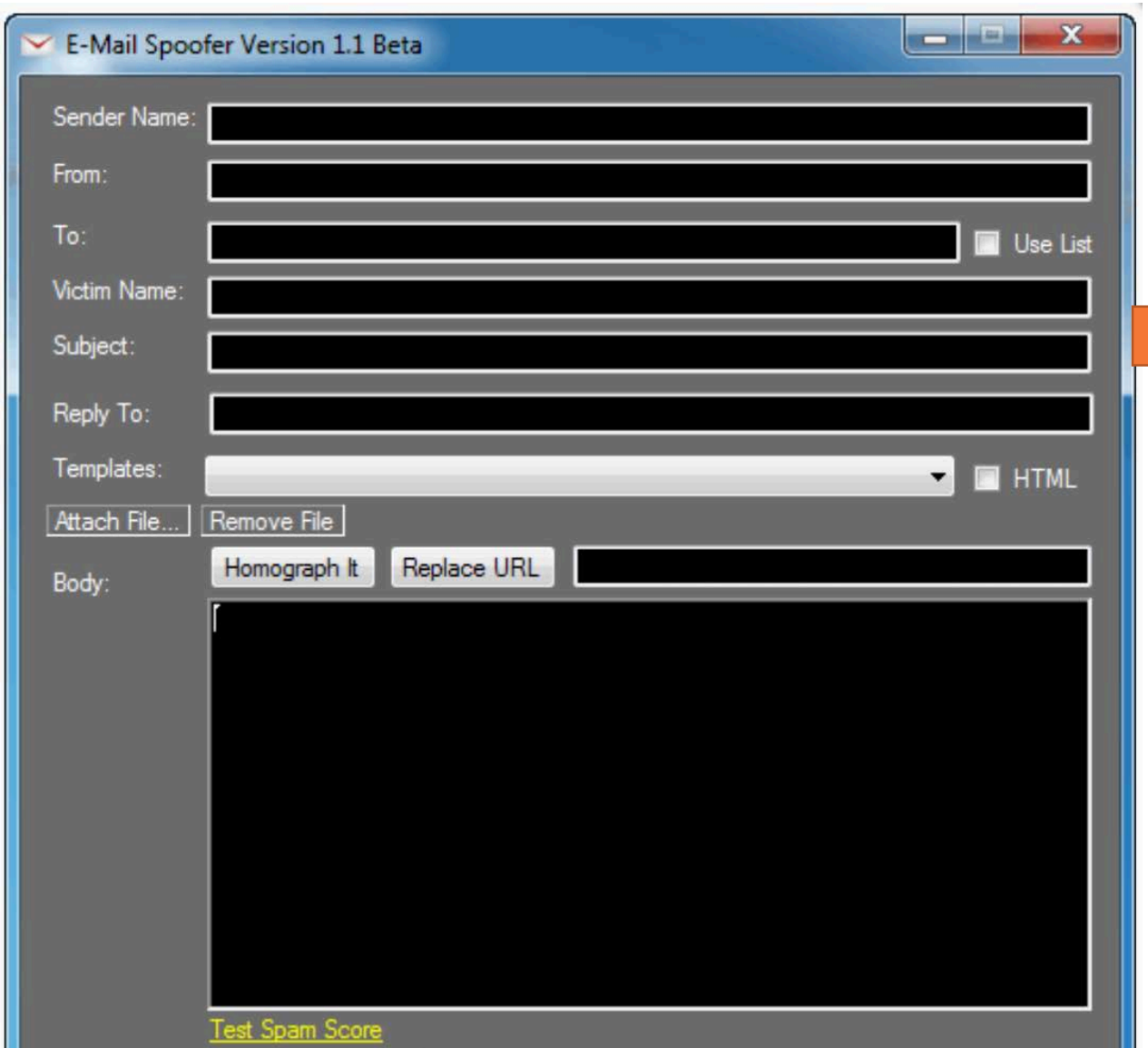
As things stand the plan is to announce the acquisition in the coming days, which is why I need you to make the deposit payment as soon as possible.

If you have any questions relay them directly to Mark as he will be updating me on progress.

Once you´ve read this email, let me know and I´ll have Mark get in touch right away.

Regards,

The Easiest (and Most Lucrative) Attack Going



From: CEO<ceo@acme.com>
Subject: Are you at your desk? I'm locked out
Date: Oct 5, 2016 7:17 PM PDT
To: CEO Admin<EA@acme.com>

From: Partner <partnerexec@partner.com>
Subject: Big new order – please ship ASAP
Date: Oct 9, 2016 8:07 AM PDT
To: order admin<oa@acme.com>

From: AR <AR@acme.com>
Subject: New Wiring Instructions
Date: Oct 2, 2016 4:37 PM CDT
To: AP <AP@partner.com>

Hi Sam,
We've changed banks. Our new wiring instructions

Source: FBI

A Board-Level Business Risk

$100M

Stolen By One Person Spoofing Trusted Business Partners

(United States Department of Justice)

$5.3B

Reported Losses to BEC Email Fraud Across 40,203 Victims

(FBI)

2/3

Of All Impostor Emails Are Domain-spoofing Attacks

(Proofpoint research)

150%

YoY Increase Of Consumer Phishing Campaigns

(APWG)

Traditional Security Solutions Have Limitations

> “The secure email gateway market is experiencing renewed interest due largely to an increase in targeted phishing attacks. Vendors are responding with URL link protection and attachment sandboxing, but have not addressed social engineering attacks with no payload.”

Gartner®

Peter Firstbrook, Research VP
Neil Wynne, Sr research Analyst

Source: Gartner Magic Quadrant for Secure Email Gateways

Why Haven’t Organizations Fixed This Already?

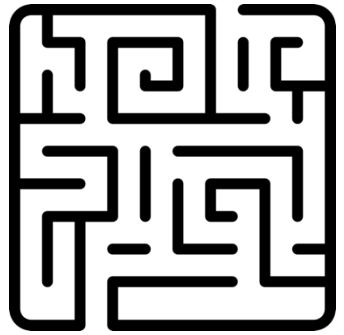
Protocols Aren’t Solutions

- SPF/DKIM can’t protect customers or partners
- DMARC hard to execute, no intelligence to classify senders

High Risk of Blocking Legitimate Email

- Implementing authentication badly will block legitimate email
- Email always has exceptions, impossible to fully automate

It’s Hard



- Spoofing: normal, critical business practice
- Requires deep intelligence and expertise to tell good from bad

Authentication Specifics

Authentication: Policy-Based Protection

SPF

(Sender Policy Framework)

BENEFITS

- Specify who can send email on behalf of a domain
- List IPs of authorized senders in a DNS record
- If IP sending email isn't listed in SPF record, the message fails SPF authentication

DKIM

(DomainKeys Identified Mail)

- Transmit a message in a way that can be verified by the email provider
- Digitally sign emails from specified domain
- Verification made possible through cryptographic authentication within digital signature of email

Authentication: Policy-Based Protection

SPF

(Sender Policy Framework)

FAILINGS

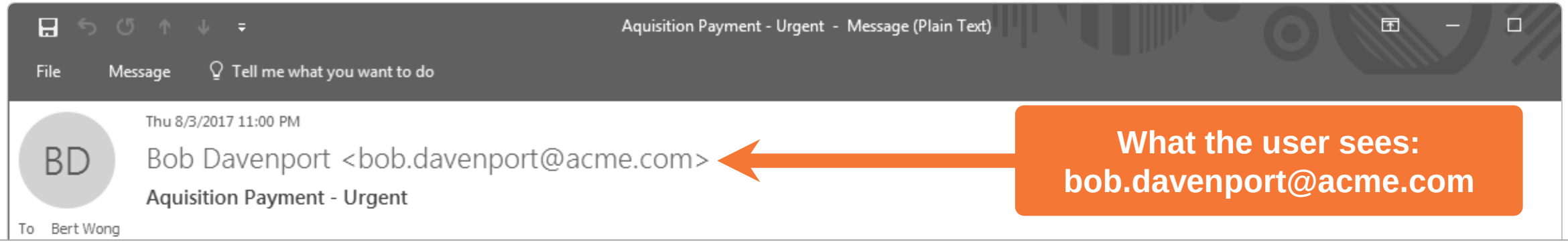
- Just because a message fails SPF doesn't mean it will always be blocked from the inbox
- SPF breaks when a message is forwarded
- SPF does nothing to protect you against spoofing of the display name of the "header from" address

DKIM

(DomainKeys Identified Mail)

- DKIM adoption is spotty meaning that the absence of a DKIM signature does not necessarily indicate the email is fraudulent
- DKIM alone is not a universally reliable way of authenticating the identity of a sender
- DKIM does nothing to prevent the spoofing of the visible Header From domain

SPF and DKIM are Ineffective Against Fraud



What the user sees:
bob.davenport@acme.com

```
Delivered-To: bert.wong@acme.com
Received: by 10.79.114.17 with SMTP id n17csp15
        Mon, 1 Aug 2016 02:31:07 -0700 (PDT)
X-Received: by 10.25.39.85 with SMTP id n82mr85
        Mon, 01 Aug 2016 02:31:07 -0700 (PDT)
Return-Path: blackhat@phisher.com>
Received: from mail-lf0-x22f.google.com (mail-l
        by mx.google.com with ESMTPS id y195si1
        for <bert.wong@acme.com>
        (version=TLS1_2 cipher=ECDHE-RSA-AES128
        Mon, 01 Aug 2016 02:31:06 -0700 (PDT)
Received-SPF: pass (google.com: domain of black
Authentication-Results: mx.google.com;
       dkim=pass header.i=@phisher.com;
       spf=pass  domain of  blackhat@phisher.com>
```

The actual sender:
blackhat@phisher.com

Passes SPF & DKIM

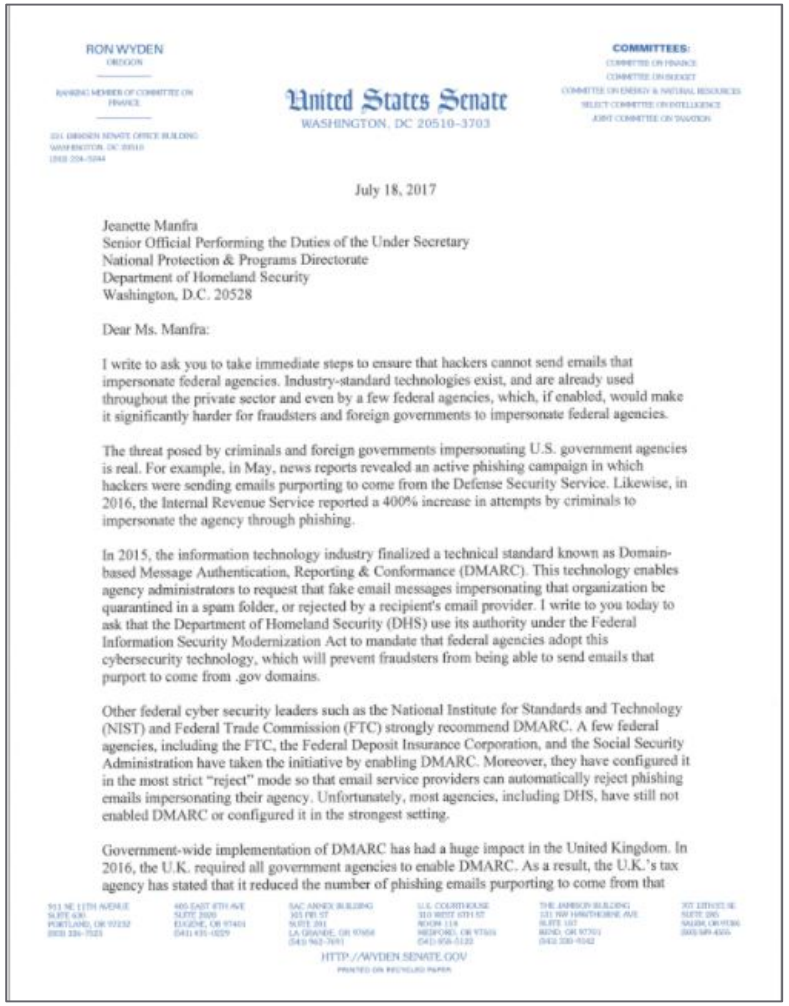
Enter DMARC!

Gain insights
into the email threat landscape to identify threats against employees, partners and customers.

Quarantine or reject
messages that fail authentication via an explicit policy setting – fraudulent messages are blocked before they hit the inbox.

Reclaim control
of the email channel by authenticating legitimate traffic coming from domains you own.

A Letter from Senator Ron Wyden



RON WYDEN
OREGON

COMMITTEES:

United States Senate
WASHINGTON, DC 20510-3703

July 18, 2017

Jeanette Manfra
Senior Official Performing the Duties of the Under Secretary
National Protection & Programs Directorate
Department of Homeland Security
Washington, D.C. 20528

Dear Ms. Manfra:

I write to ask you to take immediate steps to ensure that hackers cannot send emails that impersonate federal agencies. Industry-standard technologies exist, and are already used throughout the private sector and even by a few federal agencies, which, if enabled, would make it significantly harder for fraudsters and foreign governments to impersonate federal agencies.

The threat posed by criminals and foreign governments impersonating U.S. government agencies is real. For example, in May, news reports revealed an active phishing campaign in which hackers were sending emails purporting to come from the Defense Security Service. Likewise, in 2016, the Internal Revenue Service reported a 400% increase in attempts by criminals to impersonate the agency through phishing.

In 2015, the information technology industry finalized a technical standard known as Domain-based Message Authentication, Reporting & Conformance (DMARC). This technology enables agency administrators to request that fake email messages impersonating that organization be quarantined in a spam folder, or rejected by a recipient's email provider. I write to you today to ask that the Department of Homeland Security (DHS) use its authority under the Federal Information Security Modernization Act to mandate that federal agencies adopt this cybersecurity technology, which will prevent fraudsters from being able to send emails that purport to come from .gov domains.

Other federal cyber security leaders such as the National Institute for Standards and Technology (NIST) and Federal Trade Commission (FTC) strongly recommend DMARC. A few federal agencies, including the FTC, the Federal Deposit Insurance Corporation, and the Social Security Administration have taken the initiative by enabling DMARC. Moreover, they have configured it in the most strict "reject" mode so that email service providers can automatically reject phishing emails impersonating their agency. Unfortunately, most agencies, including DHS, have still not enabled DMARC or configured it in the strongest setting.

Government-wide implementation of DMARC has had a huge impact in the United Kingdom. In 2016, the U.K. required all government agencies to enable DMARC. As a result, the U.K.'s tax agency has stated that it reduced the number of phishing emails purporting to come from that

HTTP://WYDEN.SENATE.GOV

"STARTTLS encryption and anti-phishing technologies like DMARC are two cheap, effective ways to secure email from being intercepted or impersonated by bad guys"

"It's my hope that private sector companies move quickly to upgrade their own email security."

DHS BOD 18-01: Enhancing Email And Web Security

DHS objective	Enable	Disable
Better protect users from phishing attacks spoofing agency identities	• DMARC	
Minimize spam	• SPF • DMARC	
Ensure the integrity and confidentiality of internet-delivered data	• HTTPS • HSTS • HSTS browser preload	• SSLv2 • SSLv3 • 3DES • RC4 ciphers

DMARC Secures Legitimate Domains

> **Setting a DMARC policy of "reject" provides the strongest protection against spoofed email**, ensuring that unauthenticated messages are rejected at the mail server, even before delivery. Additionally, DMARC reports provide a mechanism for an agency to be made aware of the source of an apparent forgery, information that they wouldn't normally receive otherwise.

Department of Homeland Security
Binding Operational Directive 18-01

> "We're rapidly moving toward a world where all email is authenticated...If your domain doesn't protect itself with DMARC, you will be increasingly likely to see your messages sent directly to a spam folder or even rejected."

John Rae-Grant
Product Manager

DMARC Record

v=DMARC1; **p=none;** fo=1; rua=mailto:dmarc_rua@emaildefense.proofpoint.com; ruf=mailto:dmarc_ruf@emaildefense.proofpoint.com

- ‘p=none’ – No policy given – for reporting purposes only
- ‘p=quarantine’ – Instructs receiving MTA to junk messages that fail SPF/DKIM/Alignment
- ‘p=reject’ – Instructs receiving MTA to block/reject messages that fail SPF/DKIM/Alignment

Full DMARC Implementation

Visibility

Understand who is sending email using your domain

Identify & Authorize

Approve legitimate email senders

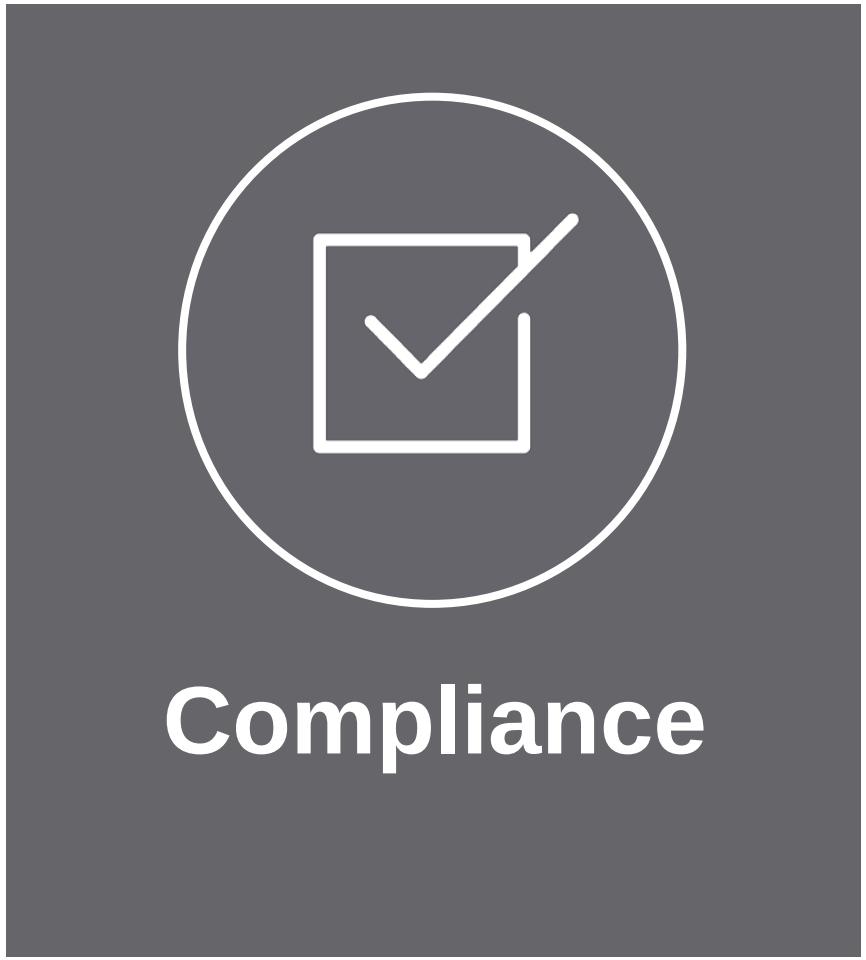
Block fraudulent email

Protect employees, partners and customers

DMARC Provides Visibility

- Monitor ALL emails (inbound and outbound) from your domains and those of third parties
- Accurately distinguish between legitimate emails and fraudulent
- Identify and authorize legitimate senders
- Domain discovery

DMARC Ensures Authentication Compliance



- Identify gaps in current SPF/DKIM configurations
- Understand the reasons behind each SPF/DKIM authentication failure
- Reduce risk to legitimate email

Why Authentication Fails: Partner Limitations

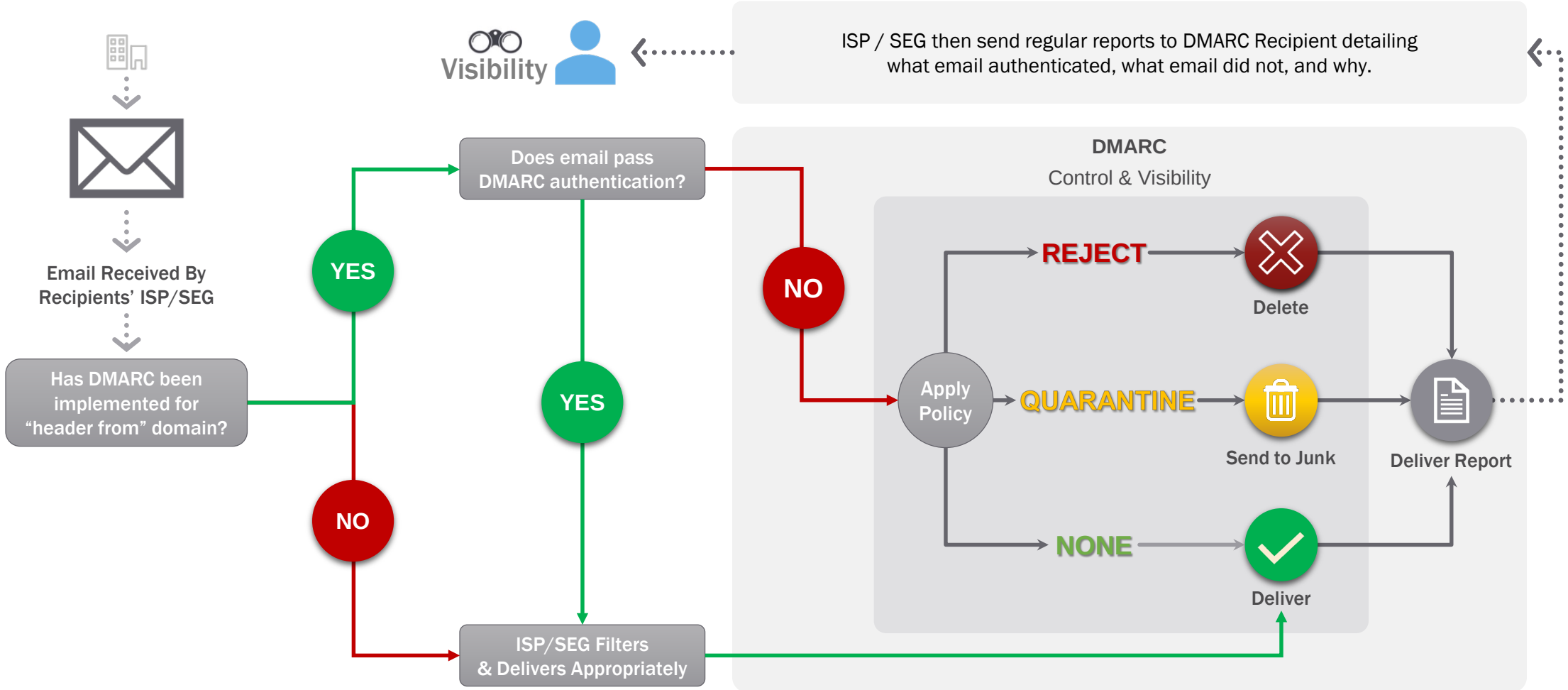
Third Party	Authentication Challenges
Office 365	Tenant ID configuration, SPF include management, reporting
Google Apps	False positives from calendar invites (SPF misalignment)
Symantec.cloud	Cannot sign DKIM, cannot report
salesforce	Bounce management reporting Mfrom issue
zendesk	Laborious process to get authentication correct
MANDRILL	Double signing leading to intermittent DKIM failure, Mfrom issues
MailChimp	Deliberate SPF misconfiguration, do not understand authentication
SendGrid	Double DKIM signing leading to intermittent DKIM pass rate

DMARC Eliminates Domain Spoofing

- Block BEC/impostor emails before they reach your employees
- Block Phishing/BEC emails before they reach your partners
- Block Phishing emails before they reach your consumers

DMARC In Action

How DMARC Works



DMARC Policy Settings:

NONE: Entire email ecosystem is monitored to map out legitimate traffic.

QUARANTINE: Messages that fail DMARC move to the spam folder.

REJECT: Messages that fail DMARC do not get delivered at all.

Domain Detail: hmrc.gov.uk

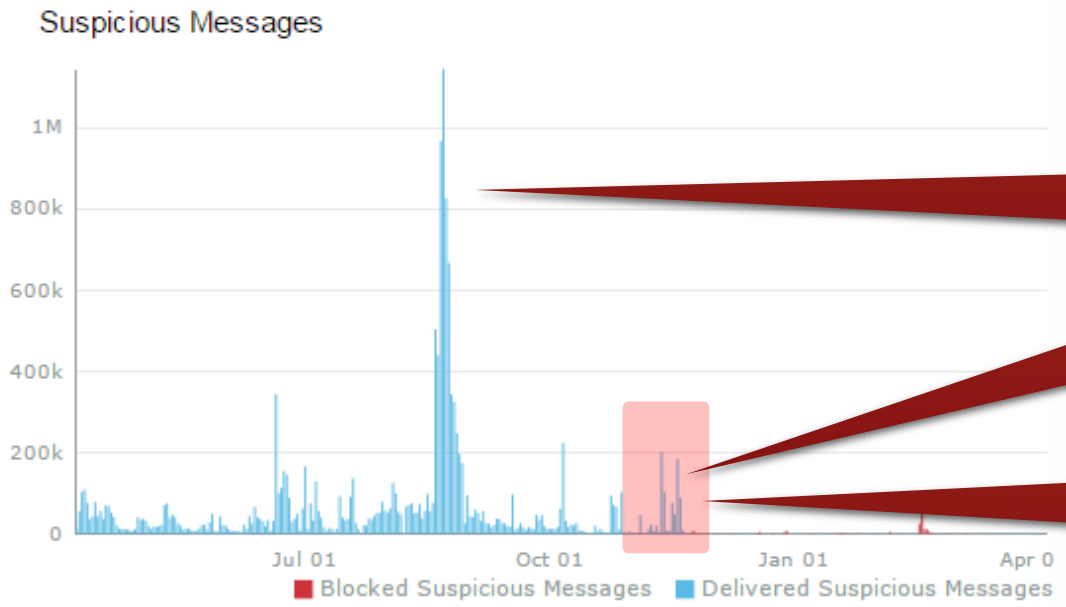
04/06/2016 - 04/06/2017

1 issue detected

Legitimate Messages

Overview | Suspicious Activity | Authentication Failures | Forwarding Authentication Failures | No Problems

Hide Charts



Spikes to well over 1 Million / day

Let's Look Closer At Where The Blue Bars Stop In November

Regular daily volume of ~200k emails abusing the HMRC domain

Messages Category	Messages Reported	DMARC Failures	Blocked Messages	% Blocked
Suspicious Activity	**14,603,360**	**14,601,078**	**155,898**	**1.07%**

Domain Detail: hmrc.gov.uk

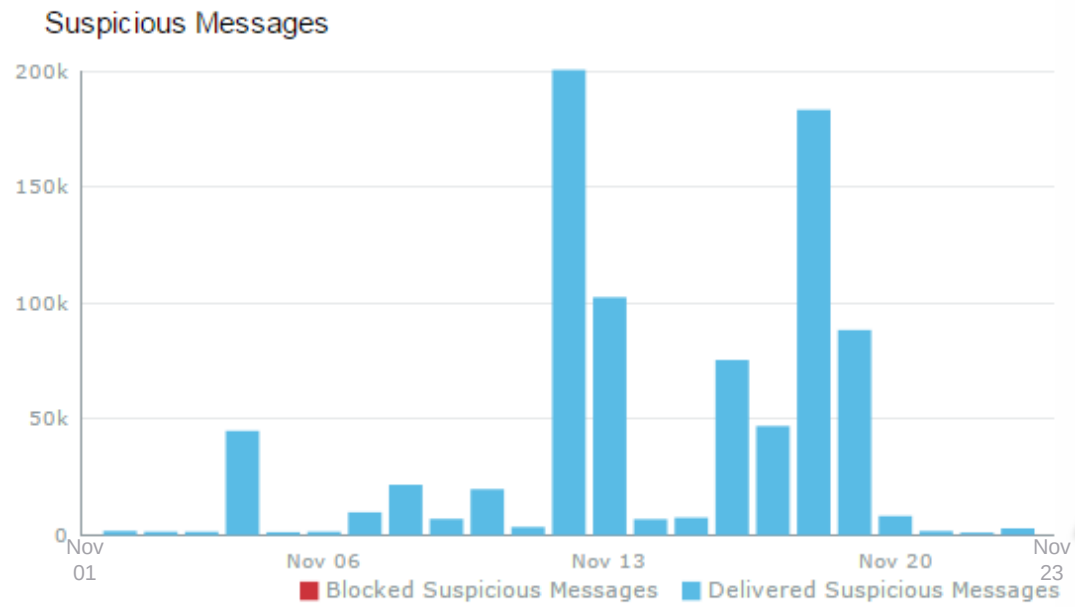
11/01/2016 - 11/23/2016

1 issue detected

Legitimate Messages

Overview | Suspicious Activity | Authentication Failures | Forwarding Authentication Failures | No Problems

Hide Charts



DMARC Reject Policy Implemented Nov 24th

All Fraudulent Messages Being Delivered

Messages Category	Messages Reported	DMARC Failures	Blocked Messages	% Blocked
Suspicious Activity	**840,638**	**840,638**	**156**	**0.02%**

Domain Detail: hmrc.gov.uk

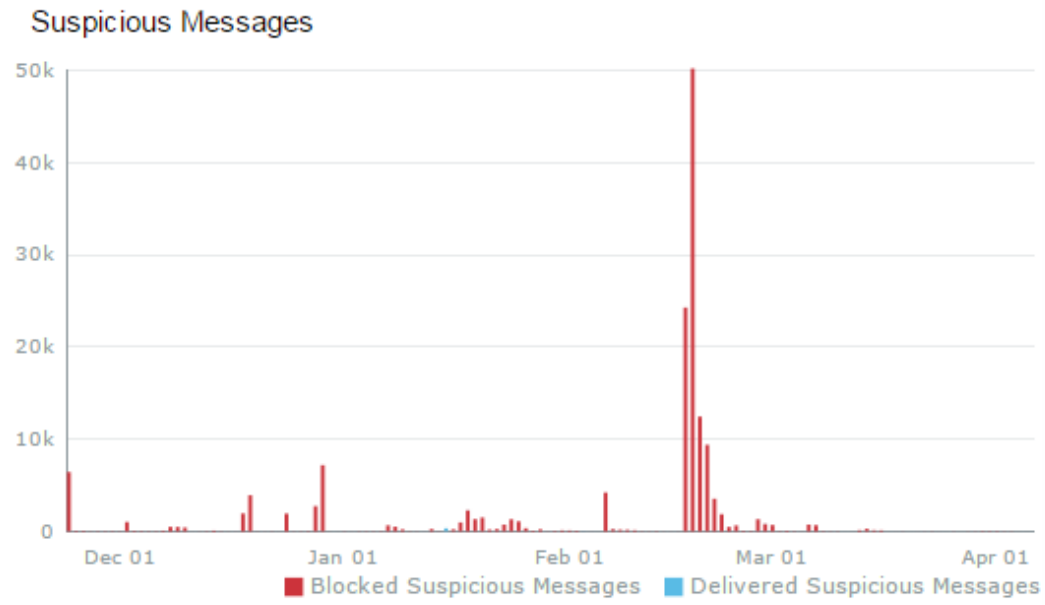
11/24/2016 - 04/06/2017

1 issue detected

Legitimate Messages

Overview | Suspicious Activity | Authentication Failures | Forwarding Authentication Failures | No Problems

Hide Charts



Fraudulent Attempts Fallen Dramatically

Fraudulent Messages Being BLOCKED

Messages Category	Messages Reported	DMARC Failures	Blocked Messages	% Blocked
Suspicious Activity	**154,225**	**154,225**	**153,829**	**99.74%**

Leading Companies Fighting Email Fraud

Conclusion

Solving for BEC with Multi-Layered Defense

Granular Policy
& Filtering

Email
Authentication

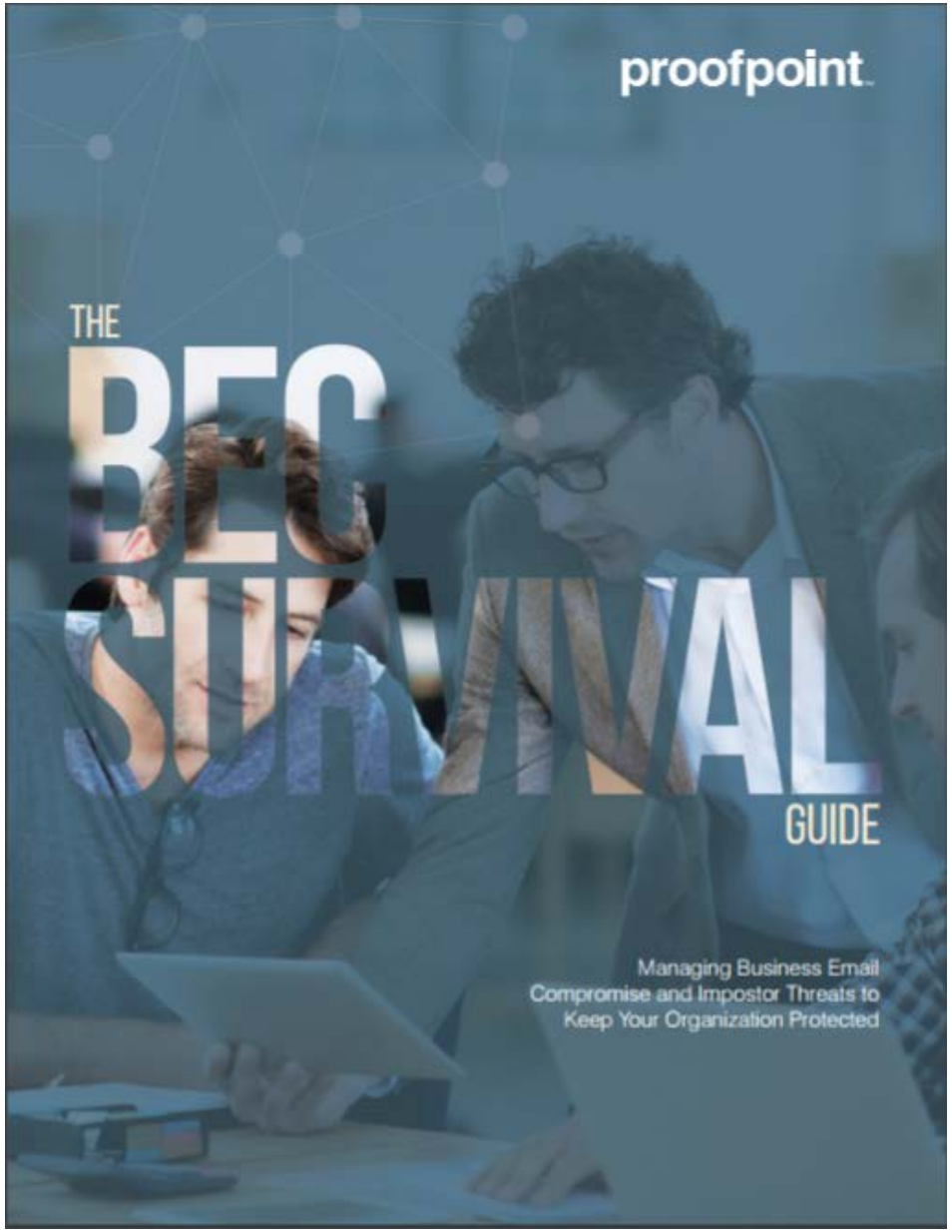
Dynamic Classification
& Analysis

Learn More

The BEC Survival Guide
https://www.proofpoint.com/bec

Check a DMARC Record
https://stopemailfraud.proofpoint.com

Email Fraud Defense
https://www.proofpoint.com/us/products/email-fraud-defense



Thank you!