BCNET 2019

Protect your Email - How to use DMARC, SPF and DKIM as a 3-punch combo

Presenting BCNET's Use Case

By Alex Doradea-Cabrera and Rossilyne Tan

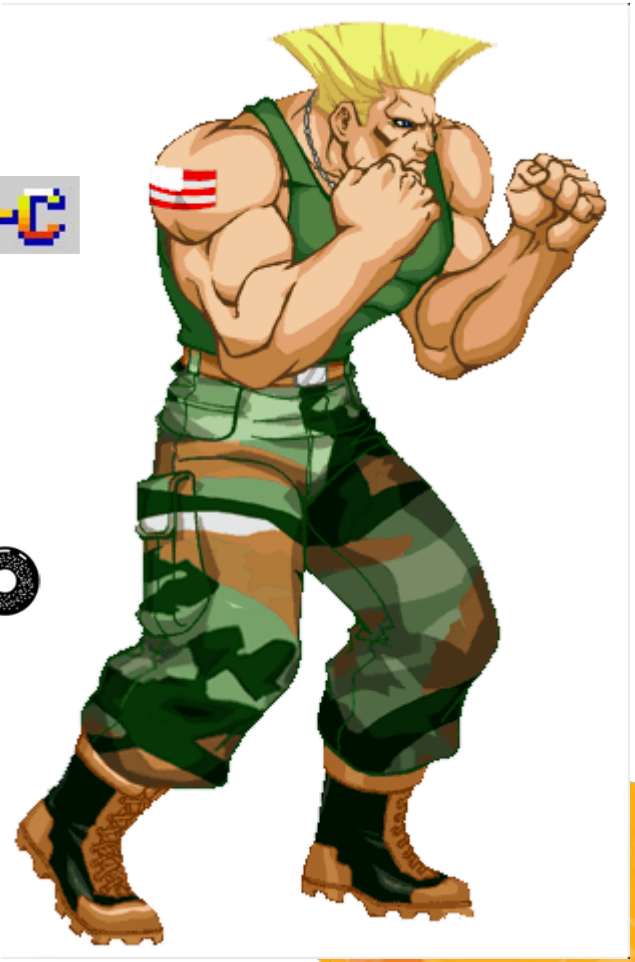
#BCNET2019

IMAGE SOURCE: https://freepngimg.com

Speaker Stats

Name	ROSS ILYNE TAN
Power	😴😴😴😴😴
Style	💇💇💇💇
Attack	⬆➡+P+K
Likes	🎮🎮🎮

Name	ALEX D-C
Power	☕☕☕
Style	🧢🧢🧢
Attack	↙➡↻+K
Likes	🍩🍩🍩🍩🍩



#BCNET2019

BCNET 2019

What is the 3-punch combo?
How it works?
Did it work?
What's next?
Q&A

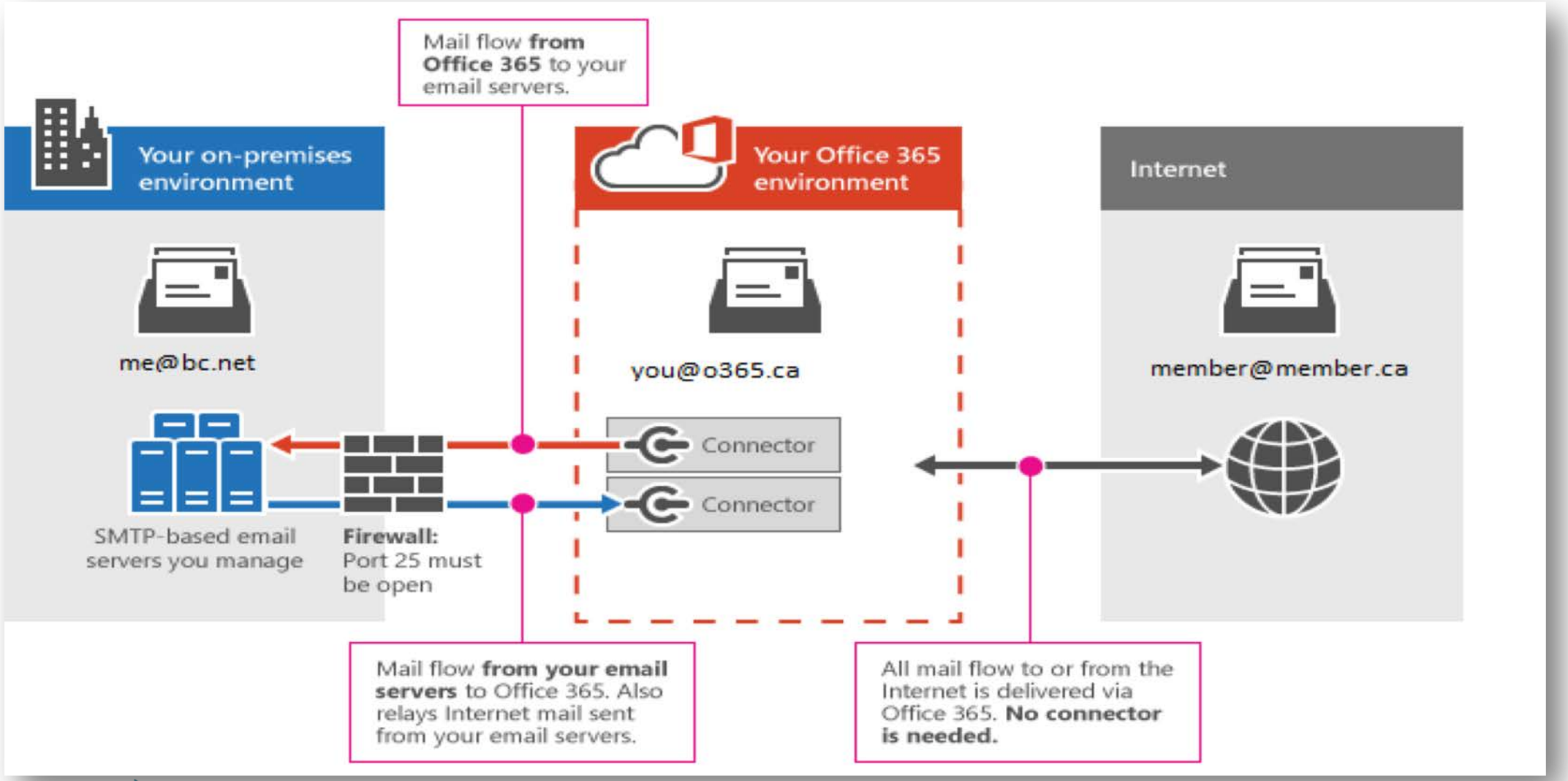
#BCNET2019

BCNET 2019

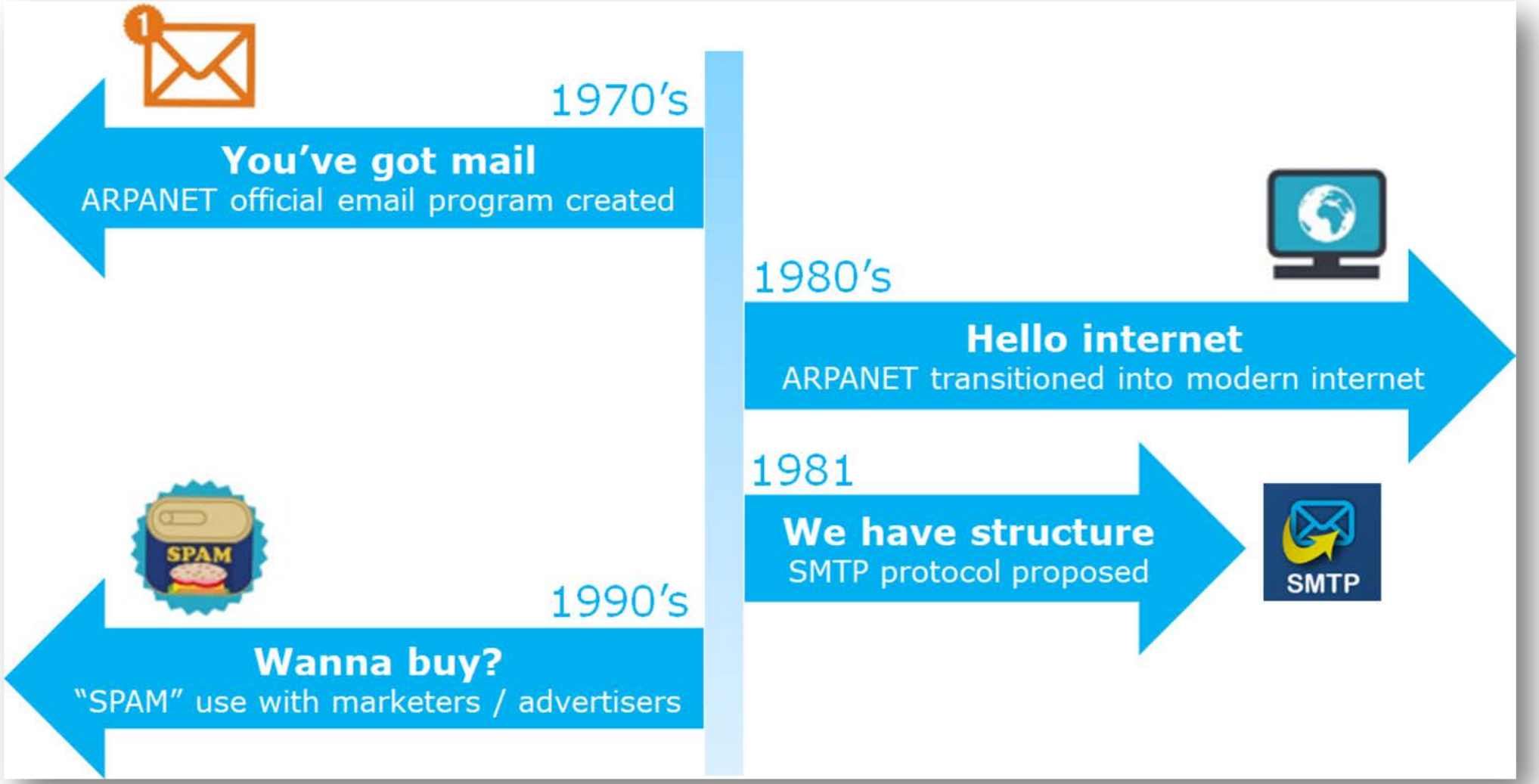
Email Security

What is available for us to use today?

Basics of Email



Email History



Types of Attacks

Phishing
Spoofing
Impersonation
Malware/adware (Virus, Ransomware, Trojans)
Email Marketers / Spammers
Malicious attachments
Malicious URLs
Browser exploits

Available Defenses

Secure Encryption

Secure Email Server

Anti Spam Filters

Black-Listed URLs & Spam Block Lists

Phishing Campaigns

SIEM or Internal Monitoring Tools

AI or Machine Learning

#BCNET2019

BCNET 2019

BCNET's Past Email Threat Landscape

Using Office 365 since April 2016

Phishing/Spoofing Attacks

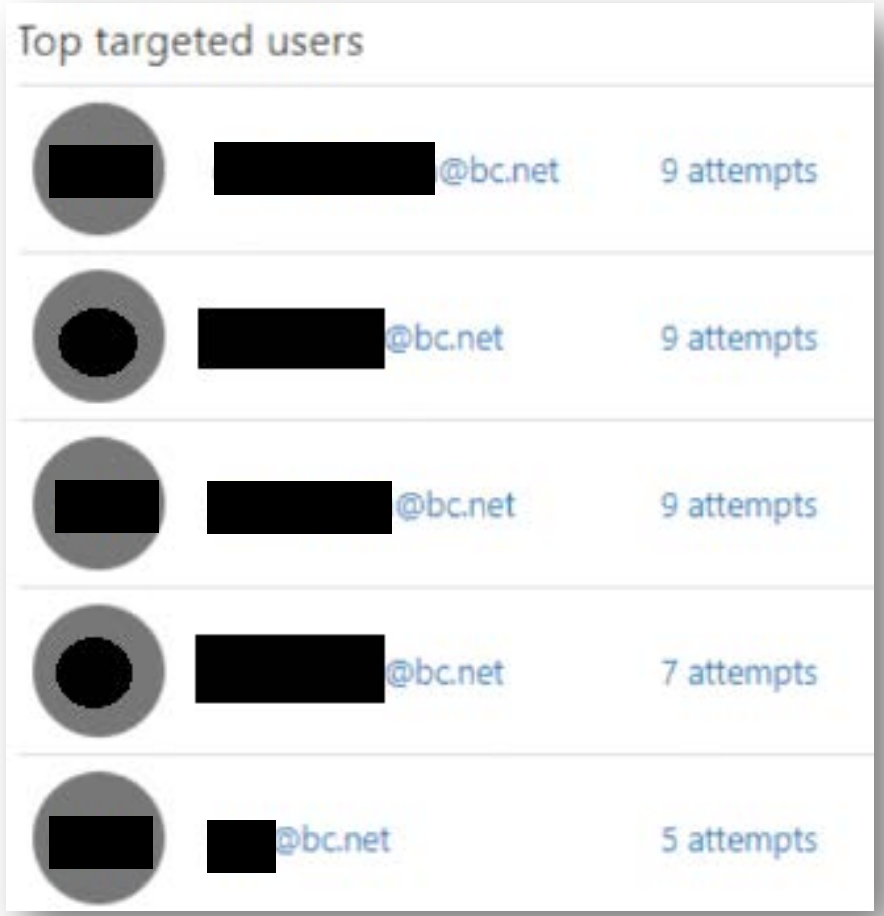
From: [redacted]
Sent: Tuesday, August 14, 2018 4:12 PM
To: [redacted]
Subject: High Priority

Can you run a task for me ASAP? P.S I am in a meeting at the moment can't take calls. Just reply.

Regards.

Sent from iPad

Daily Email Statistics



#BCNET2019

BCNET 2019

DMARC, DKIM, and SPF

What do these mean?

SPF

Sender **P**olicy **F**ramework

DKIM

Domain **K**eys **I**dentified **M**ail

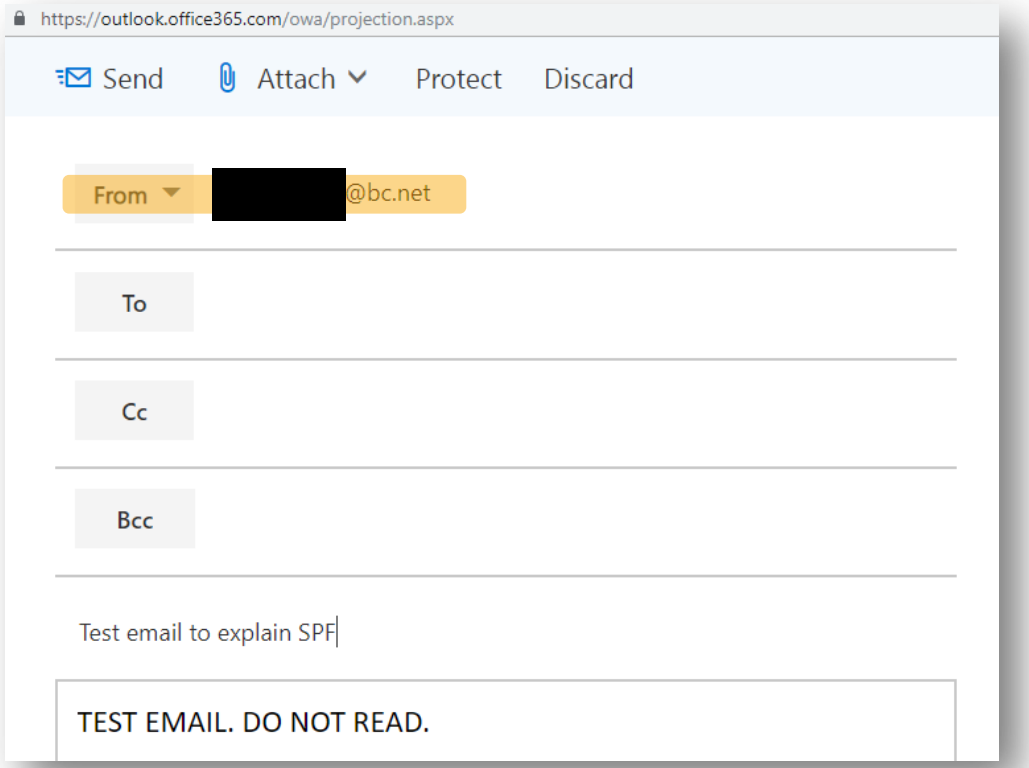
DMARC

Domain-based **M**essage **A**uthentication, **R**eporting & **C**onformance

SPF

Sender Policy Framework

"It's not about stopping spam; it's about controlling and stopping attempted sender forgeries."



Exchange Online

Type	Priority	Host name	Points to address or value
MX	0	@	[redacted]
TXT	-	@	v=spf1 include:spf.protection.outlook.com -all
CNAME	-	autodiscover	[redacted]

DKIM

Domain Keys Identified Mail

"You're authenticating with 100% certainty both the sender and the message with a TXT record."

X *This is a legitimate email*

Sign Here

DMARC

Domain-based **M**essage **A**uthentication, **R**eporting, & **C**onformance

"It applies clear instructions for the message receiver to follow if an email does not pass SPF or DKIM authentication—for instance, reject, junk it, or do nothing.

#BCNET2019

BCNET 2019

DMARC DKIM SPF

How do these three work together?

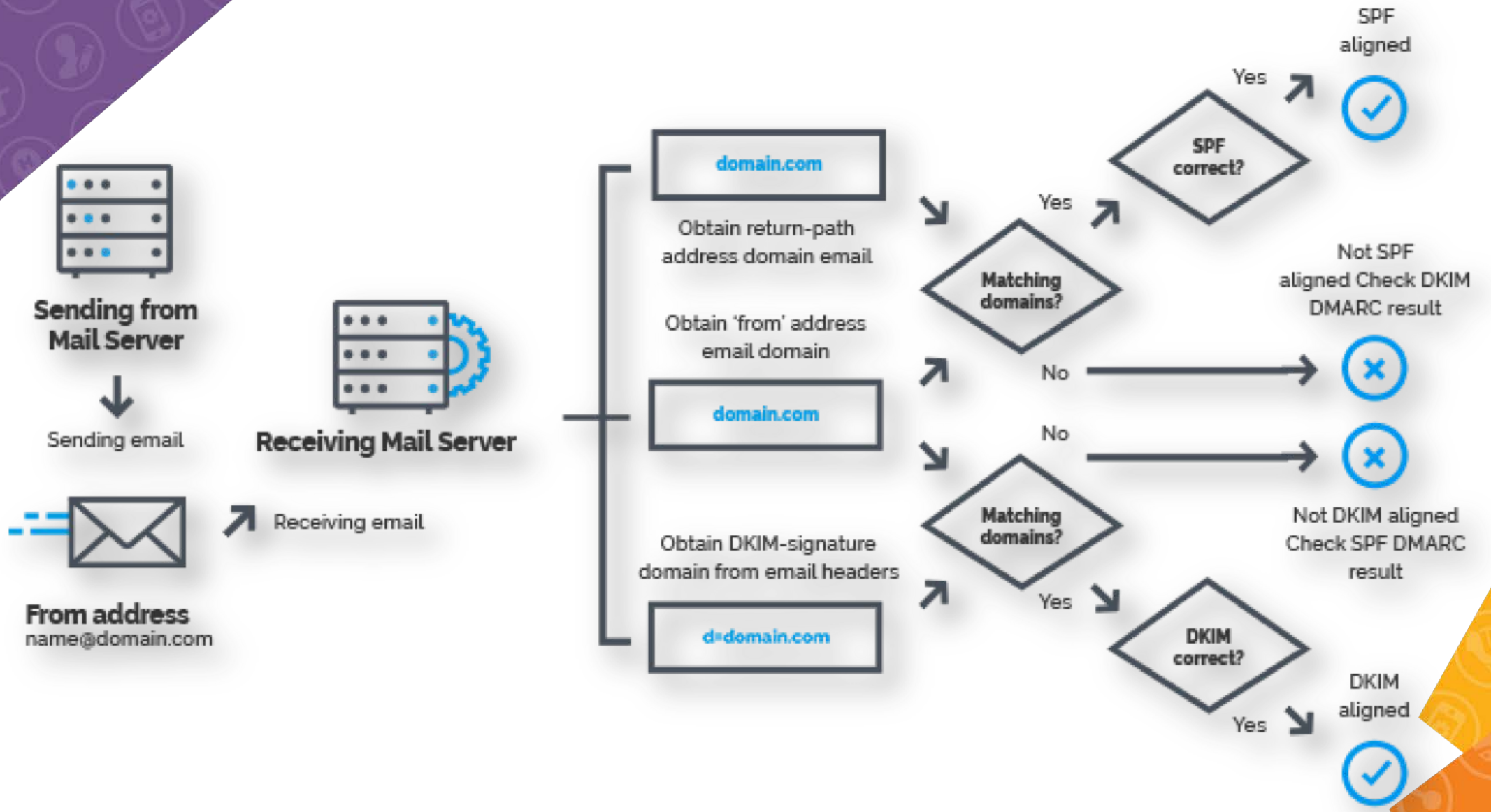


IMAGE SOURCE: https://www.dmarcanalyzer.com/dmarc/

#BCNET2019

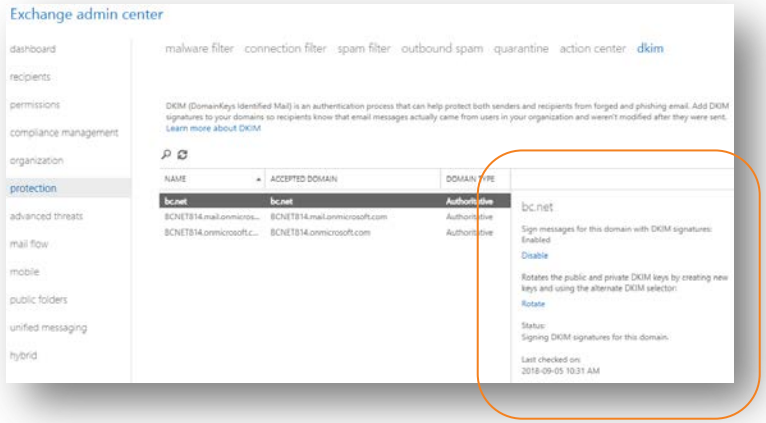
BCNET 2019

Implementation Process in Office 365

DKIM, SPF…

DKIM Setup

Office 365's Exchange Admin Center



bc.net

Sign messages for this domain with DKIM signatures:
Enabled

Disable

Rotates the public and private DKIM keys by creating new keys and using the alternate DKIM selector:

Rotate

Status:
Signing DKIM signatures for this domain.

SPF Setup

Exchange Online

Type	Priority	Host name	Points to address or value
MX	0	@	[redacted]
TXT	-	@	v=spf1 include:spf.protection.outlook.com -all
CNAME	-	autodiscover	[redacted]

Step 1 of 2

Obtain SPF Data

Office 365

Step 2 of 2

Input SPF Data

Infoblox

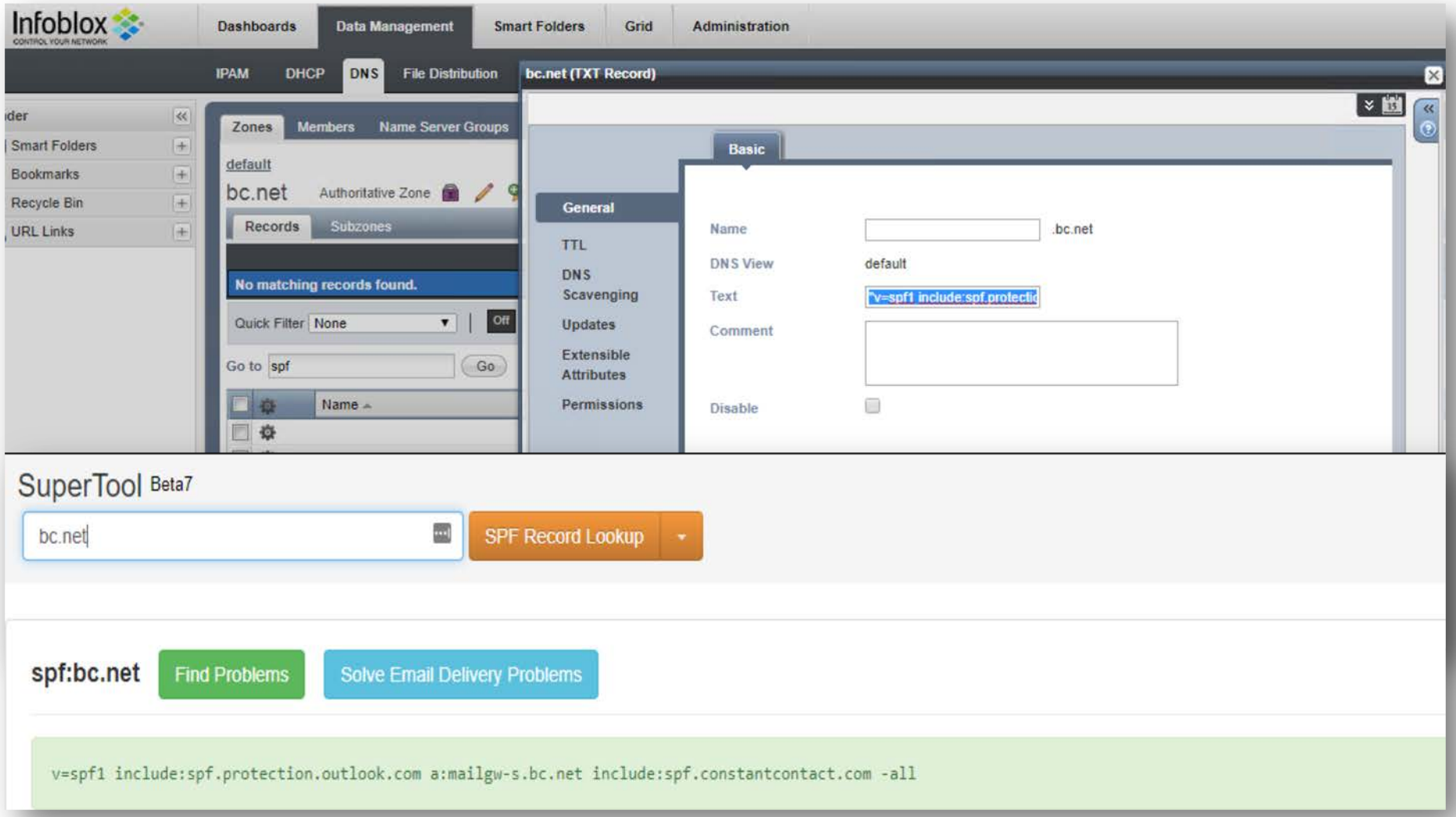
#BCNET2019

BCNET 2019

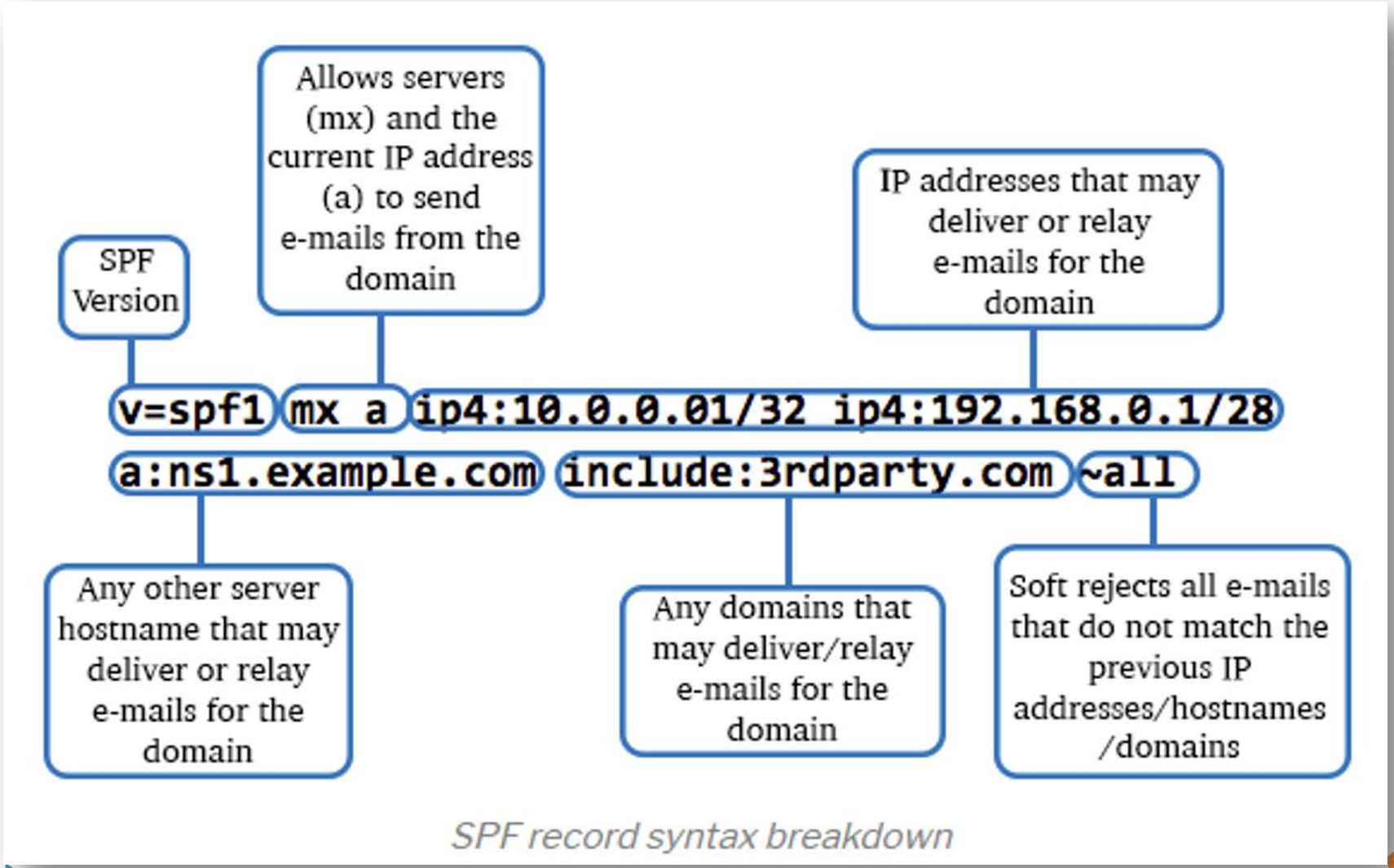
Implementation in Infoblox/DNS

…SPF, and DMARC

SPF TxT Record Creation



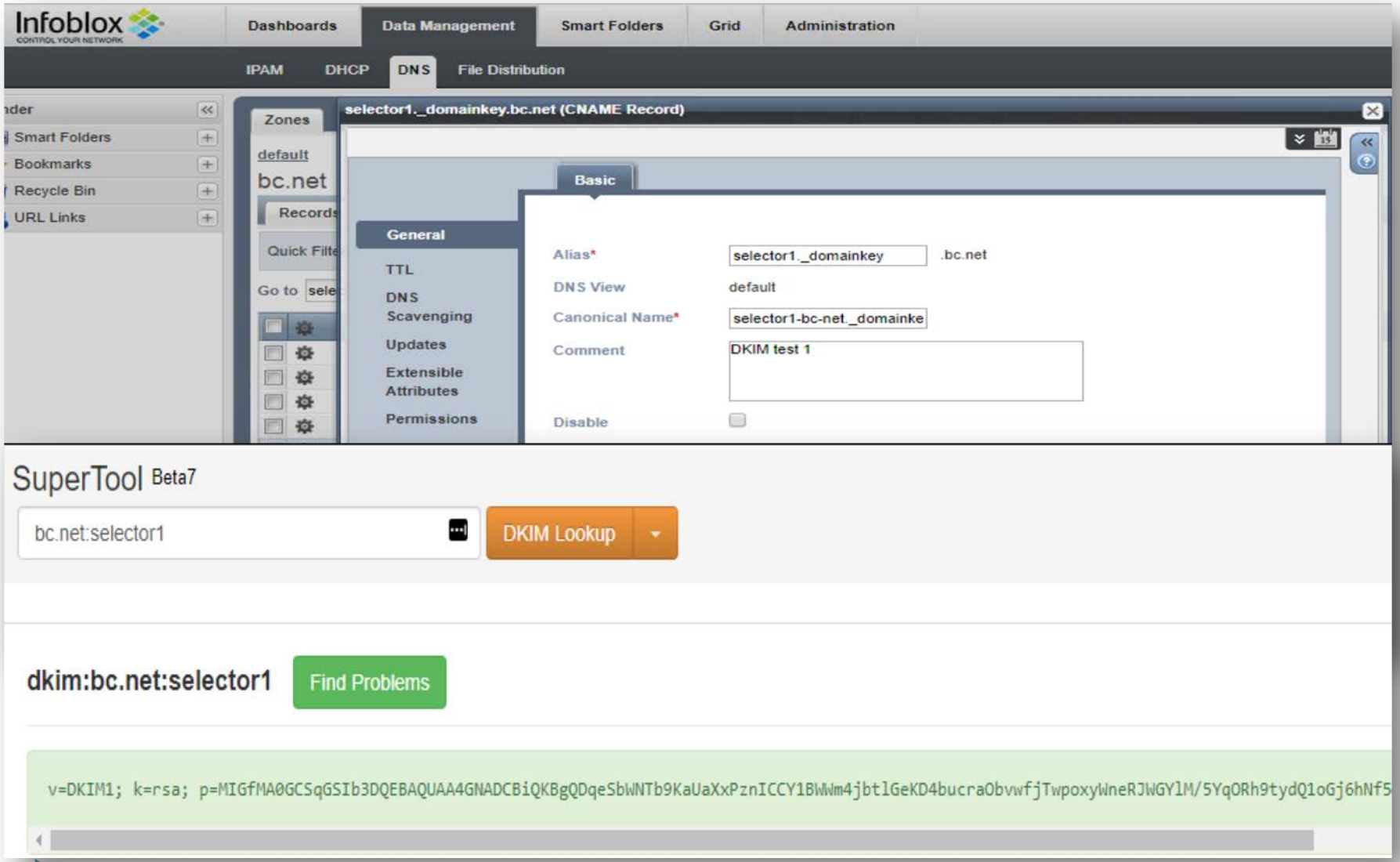
SPF Tags



SPF record syntax breakdown

IMAGE SOURCE: www.pair.com

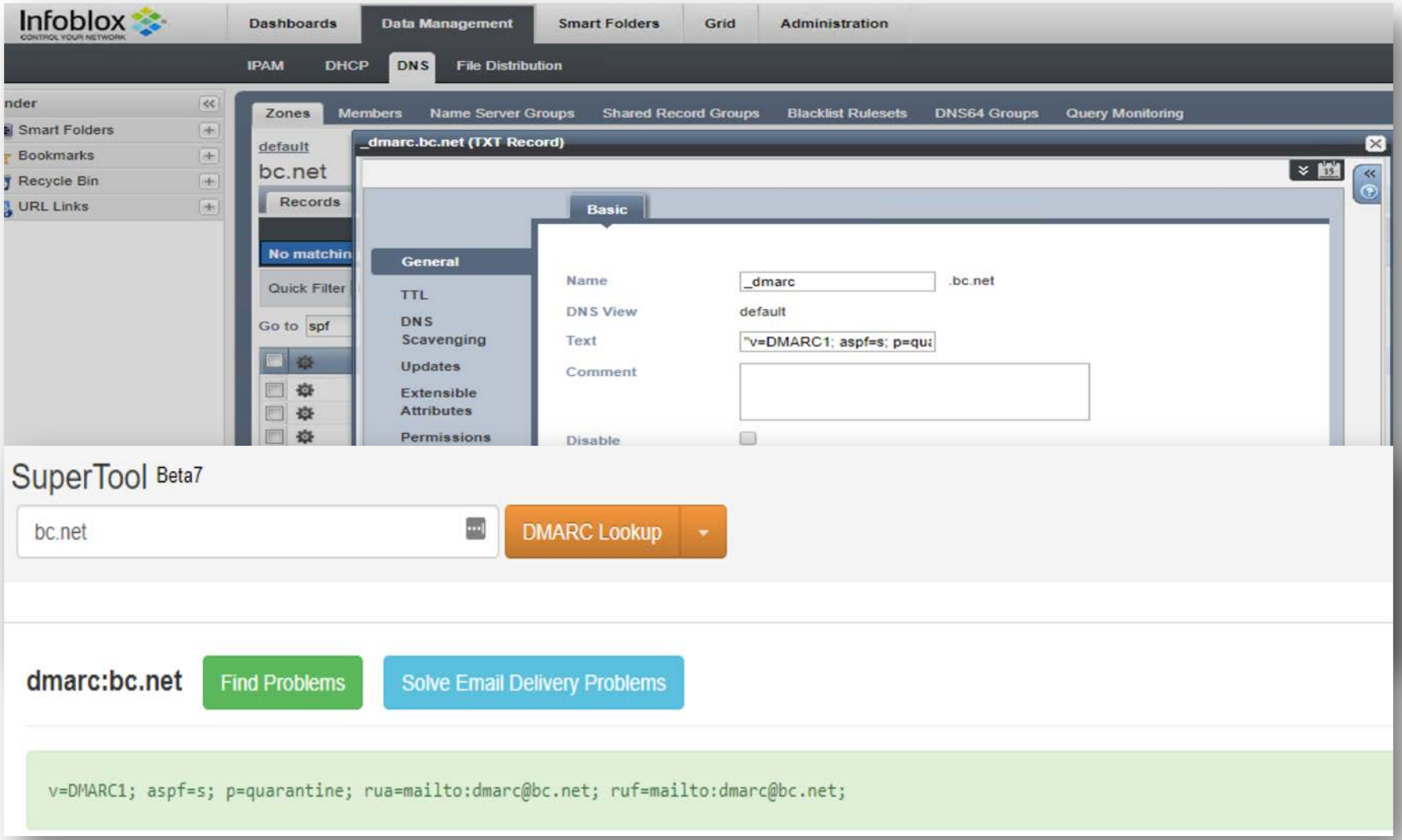
DKIM Selector File Creation



DKIM Tags

Tag	TagValue	Name	Description
v	DKIM1	Version	The DKIM record version.
k	rsa	Key type	The type of the key used by tag (p).
p	MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQDqeSbWNTb9KaUaXxPznICCY1BWWm4jbtlGeKD4bucraObvwfjTwpoxyWneRJWGYlM/5YqORh9tydQ1oGj6hNf5/Q+jeghR3Y0Yn/hgghYAKy4vb5TXjDRI7ekyelbgKL6GK0a+49Og+jv+f1k/NabLcM3qjihqoWZdte1lvYWxSQIDAQAB	Public Key	Public-key data. The syntax and semantics of this tag value before being encoded in base64 are defined by the (k) tag.
n	1024,1487262932,1	Notes	Notes that might be of interest.

DMARC TxT Record Creation



DMARC Tags

Tag Name	Purpose	Sample
v	Protocol version	v=DMARC1
pct	Percentage of messages subjected to filtering	pct=20
ruf	Reporting URI for forensic reports	ruf=mailto:authfail@example.com
rua	Reporting URI of aggregate reports	rua=mailto:aggrep@example.com
p	Policy for organizational domain	p=quarantine
sp	Policy for subdomains of the OD	sp=reject
adkim	Alignment mode for DKIM	adkim=s
aspf	Alignment mode for SPF	aspf=r

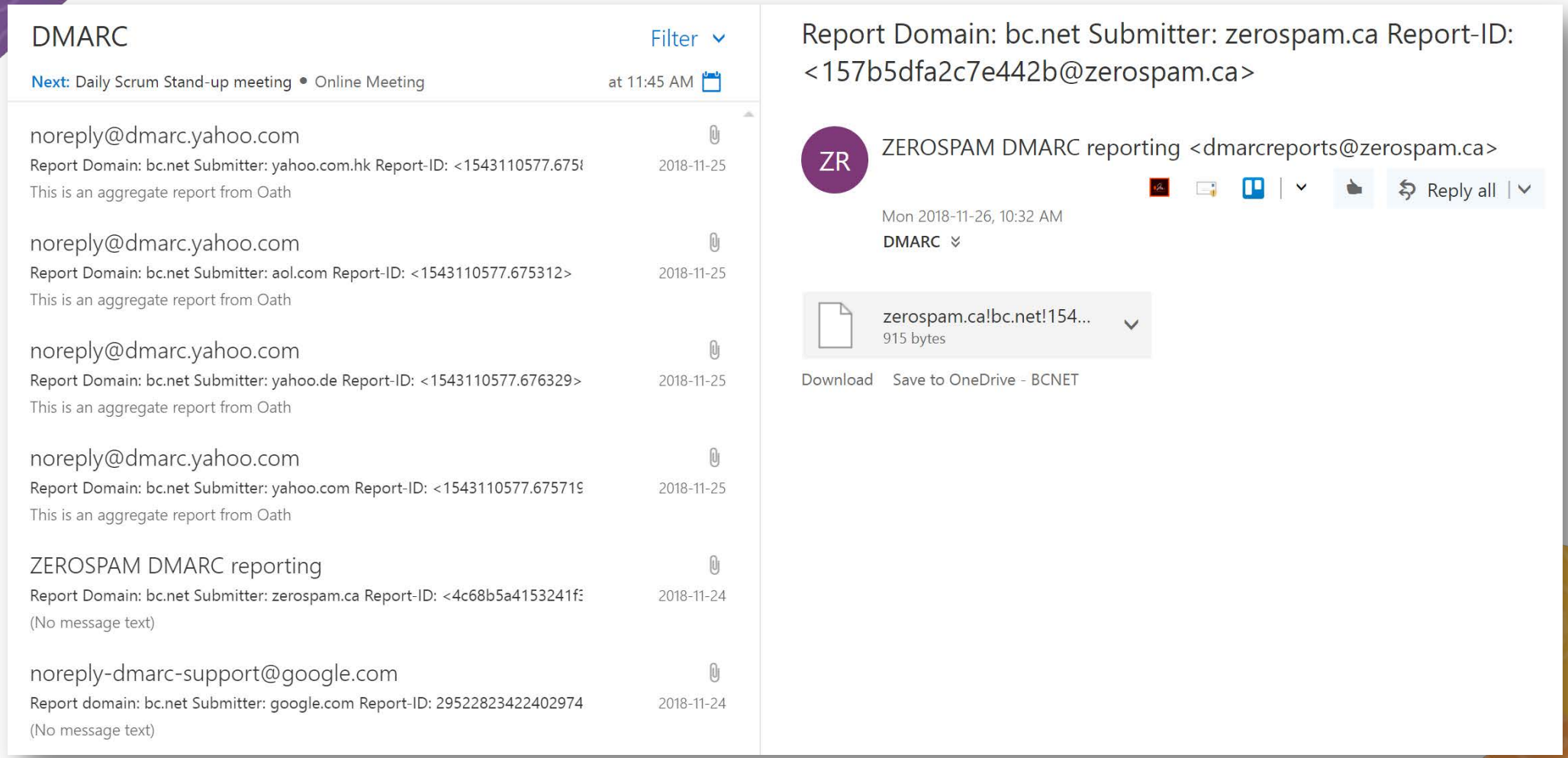
#BCNET2019

BCNET 2019

BCNET's Current Email Threat Landscape

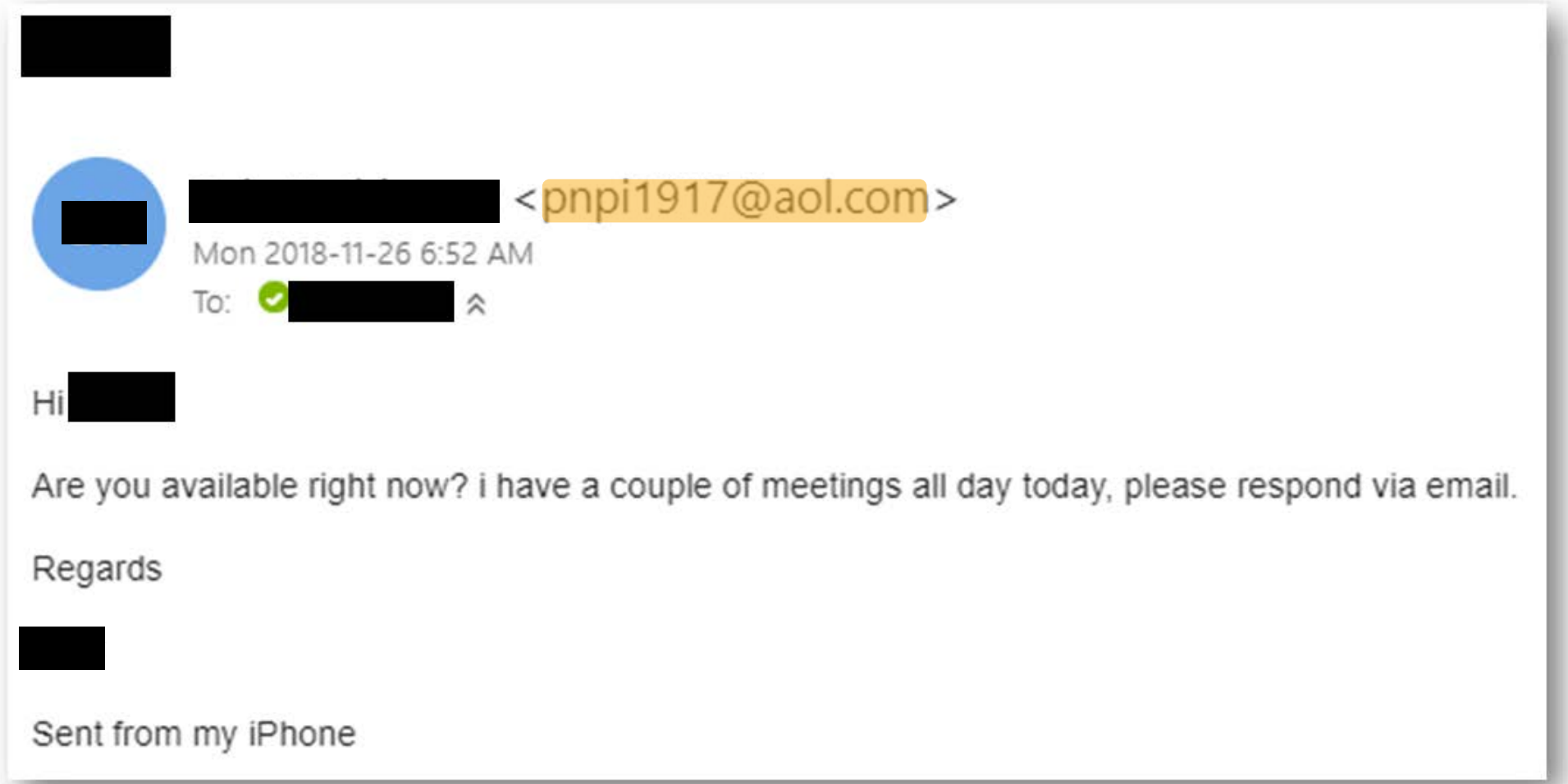
Since activating DMARC, DKIM, & SPF back in November 2018

Sample DMARC Reports



Sample Impersonation Attack

Desktop View


[redacted]

[redacted] <pnpi1917@aol.com>

Mon 2018-11-26 6:52 AM

To: [redacted]

Hi [redacted]

Are you available right now? i have a couple of meetings all day today, please respond via email.

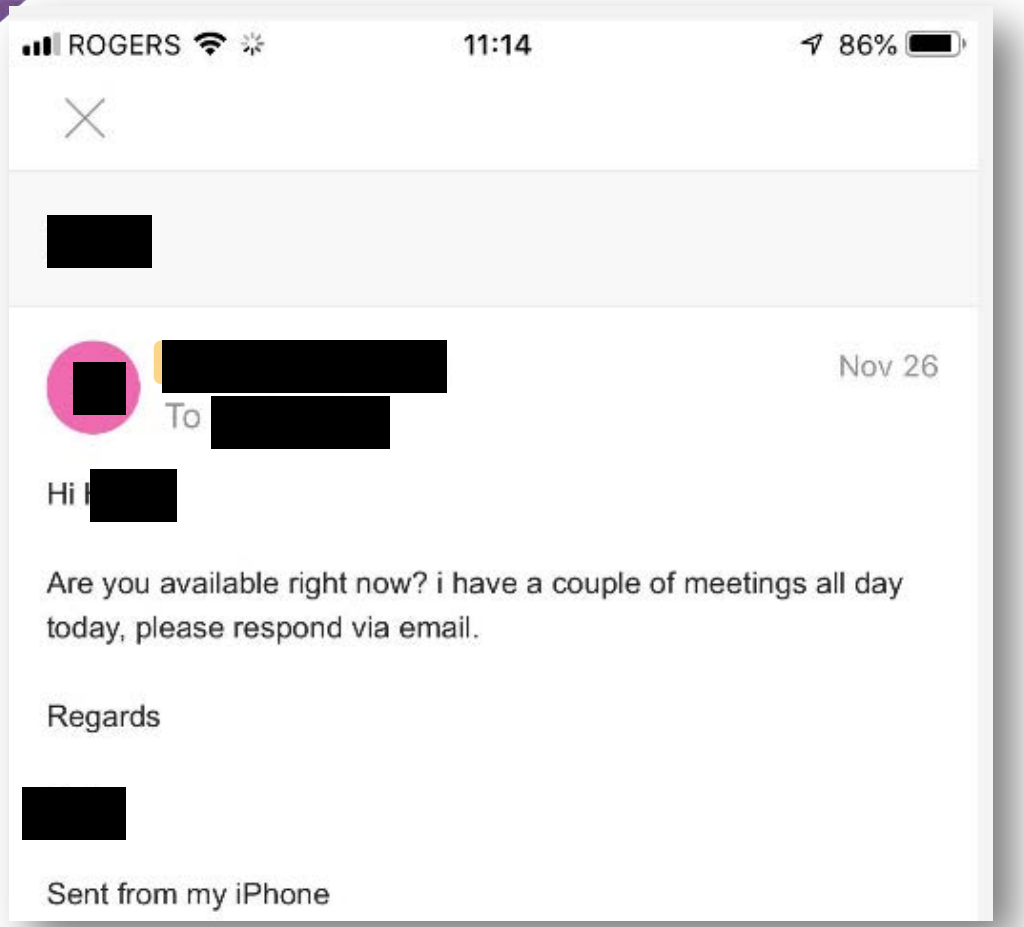
Regards

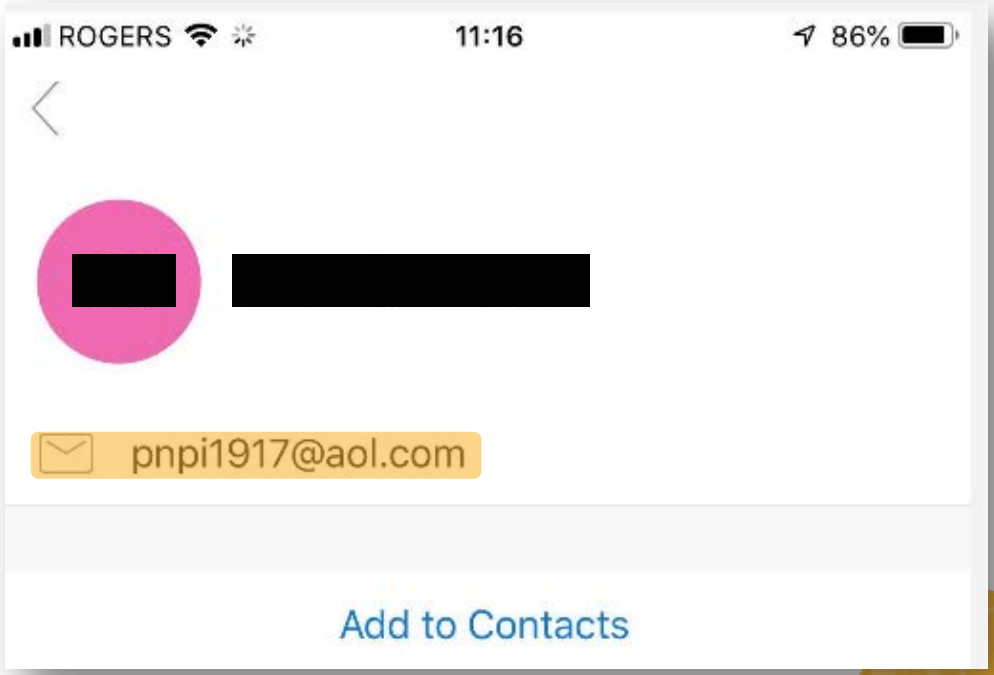
[redacted]

Sent from my iPhone

Sample Impersonation Attack

Smartphone App View





Email Screenshot

Sample Impersonation Attack

```
Authentication-Results: spf=pass (sender IP is 74.6.128.34)
 smtp.mailfrom=aol.com; bc.net; dkim=pass (signature was verified)
 header.d=aol.com;bc.net; dmarc=pass action=none
 header.from=aol.com;compauth=pass reason=100
Received-SPF: Pass (protection.outlook.com: domain of aol.com designates
 74.6.128.34 as permitted sender) receiver=protection.outlook.com;
 client-ip=74.6.128.34; helo=sonic304-11.consmr.mail.bf2.yahoo.com;
Received: from sonic304-11.consmr.mail.bf2.yahoo.com (74.6.128.34) by
 TO1CAN01FT005.mail.protection.outlook.com (10.152.122.116) with Microsoft
 SMTP Server (version=TLS1_2, cipher=TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384) id
 15.20.1339.10 via Frontend Transport; Mon, 26 Nov 2018 14:52:38 +0000
DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed;
d=aol.com; s=a2048; t=1543243957; bh=Jc20qtGxVBdNUzRhjUOItZfk8ntVZ+YSxZSlkpkqZr8=;
h=Date:From:To:Subject:References:From:Subject;
b=FJiqSafVUp+6PZ6TwwpgyH1sYwyPcc7Re+bk9dqlqg5r9gt
Received: from sonic.gate.mail.ne1.yahoo.com by sonic304.consmr.mail.bf2.yahoo.com
Mon, 26 Nov 2018 14:52:37 +0000
Date: Mon, 26 Nov 2018 14:52:33 +0000 (UTC)
From: [redacted] <pnpi1917@aol.com>
To: [redacted]@bc.net
Message-ID: <356869847.6175662.1543243953962@mail.yahoo.com>
Subject: [redacted]
```

spf = **pass**

dkim = **pass**

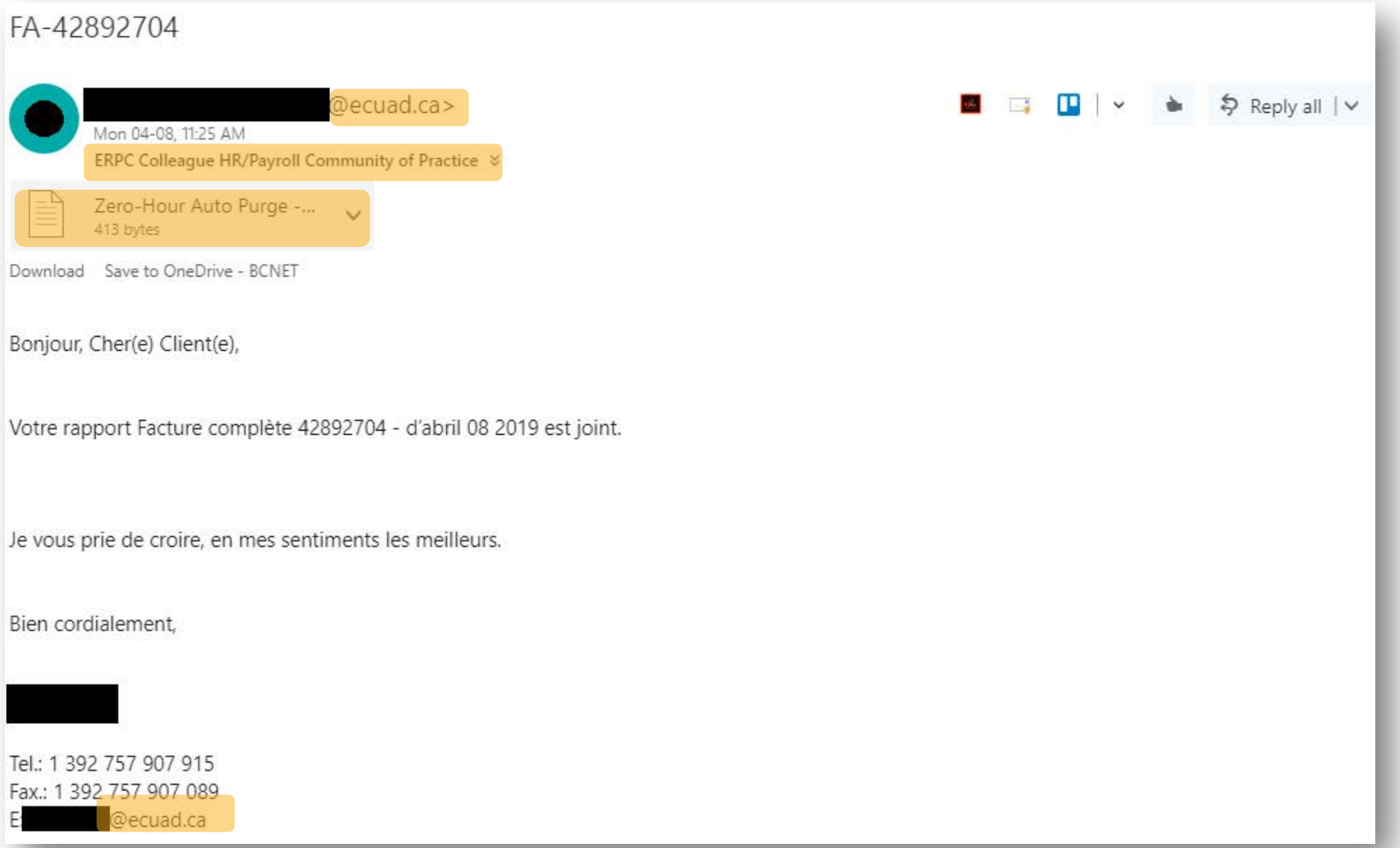
dmarc = **pass**

action = **none**

Name of spoofed sender

pnpi1917@aol.com

Sample Spoofed External *DL Member



*DL stands for "Distribution List" a.k.a. "Mailing List" or "Listserv"

Sample Spoofed External *DL Member

spf = **pass**

dkim = **fail**

dmarc = **fail**

action = **none**

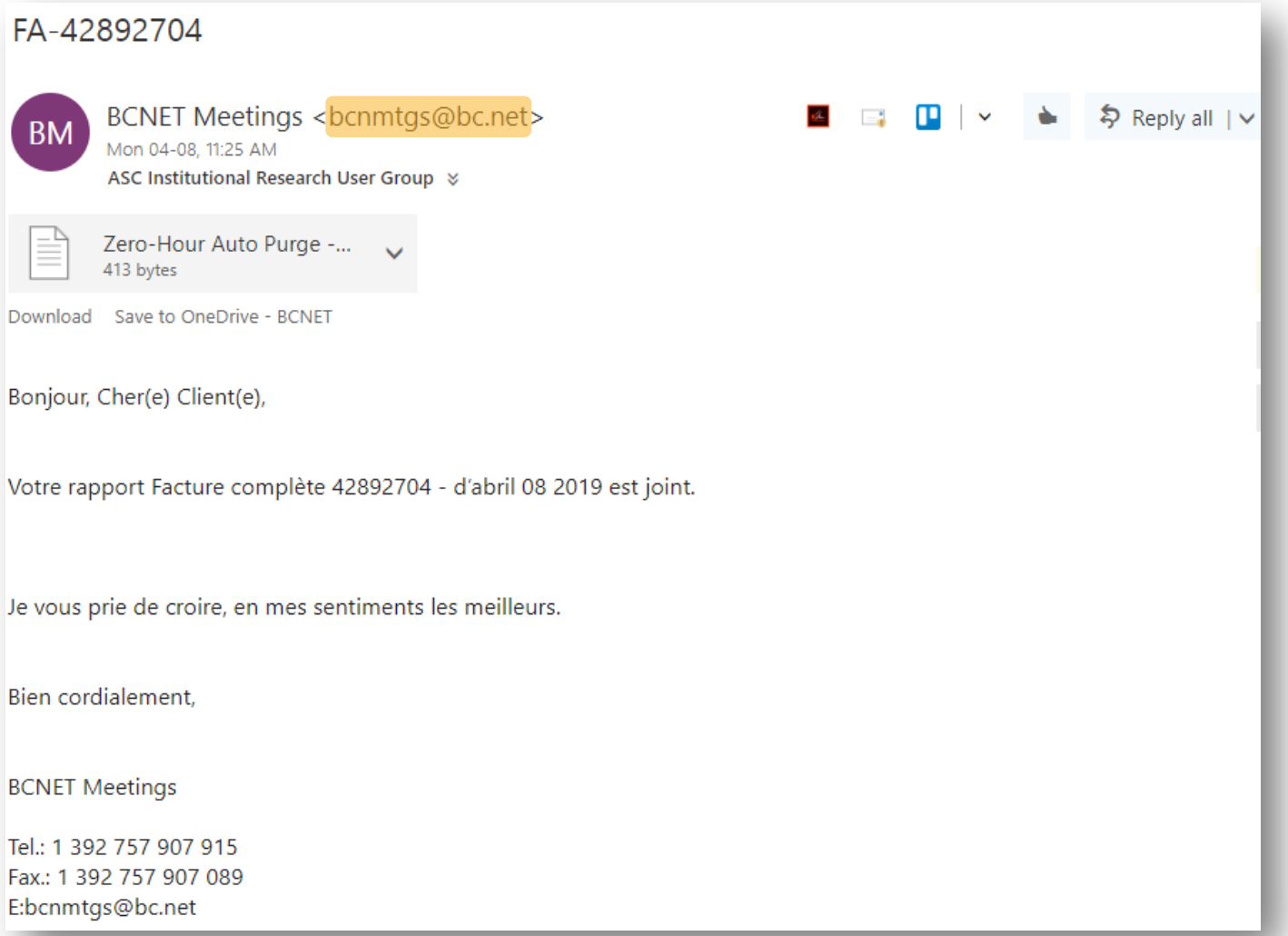
howard.chen@fourpointslax.com

###@ecuad.ca

asc-hrpug@bc.net

```
Authentication-Results: spf=pass (sender IP is 199.66.225.3)
 smtp.mailfrom=fourpointslax.com; bc.net; dkim=fail (no key for signature)
 header.d=fourpointslax.com;bc.net; dmarc=fail action=none
 header.from=ecuad.ca;
Received-SPF: Pass (protection.outlook.com: domain of fourpointslax.com
 designates 199.66.225.3 as permitted sender) receiver=protection.outlook.com;
 client-ip=199.66.225.3; helo=web11.globalit.com;
Received: from web11.globalit.com (199.66.225.3) by
 QB1CAN01FT011.mail.protection.outlook.com (10.152.120.129) with Microsoft
 SMTP Server (version=TLS1_2, cipher=TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384) id
 15.20.1771.16 via Frontend Transport; Mon, 8 Apr 2019 18:24:53 +0000
DKIM-Signature: v=1; a=rsa-sha256; q=dns/txt; c=relaxed/relaxed;
        d=fourpointslax.com; s=default; h=Content-Type:MIME-Version:Subject:To:From:
        Date:Sender:Reply-To:Message-ID:Cc:Content-Transfer-Encoding:Content-ID:
        Content-Description:Resent-Date:Resent-From:Resent-Sender:Resent-To:Resent-Cc
        :Resent-Message-ID:In-Reply-To:References:List-Id:List-Help:List-Unsubscribe:
        List-Subscribe:List-Post:List-Owner:List-Archive;
Received: from [185.144.64.86] (port=54049)
        by web11.globalit.com with esmtpsa (TLSv1.2:ECDHE-RSA-AES256-GCM-SHA384:256)
        (Exim 4.91)
        (envelope-from <howard.chen@fourpointslax.com>)
        id 1hDYwt-0001Lg-Hp
        for asc-hrpug@bc.net; Mon, 08 Apr 2019 11:24:52 -0700
Date: Mon, 08 Apr 2019 22:54:50 +0330
From: [redacted]@ecuad.ca> <howard.chen@fourpointslax.com>
To: asc-hrpug@bc.net
Subject: FA-42892704
```

Sample Spoofed Internal DL Member



FA-42892704

BM

BCNET Meetings <bcnmtgs@bc.net>

Mon 04-08, 11:25 AM

ASC Institutional Research User Group

Reply all

Zero-Hour Auto Purge -...
413 bytes

Download Save to OneDrive - BCNET

Bonjour, Cher(e) Client(e),

Votre rapport Facture complète 42892704 - d'abril 08 2019 est joint.

Je vous prie de croire, en mes sentiments les meilleurs.

Bien cordialement,

BCNET Meetings

Tel.: 1 392 757 907 915
Fax.: 1 392 757 907 089
E:bcnmtgs@bc.net

Sample Spoofed Internal DL Member

spf = **pass**

dkim = **fail**

dmarc = **fail**

action = **quarantine**

bcnmtgs@bc.net

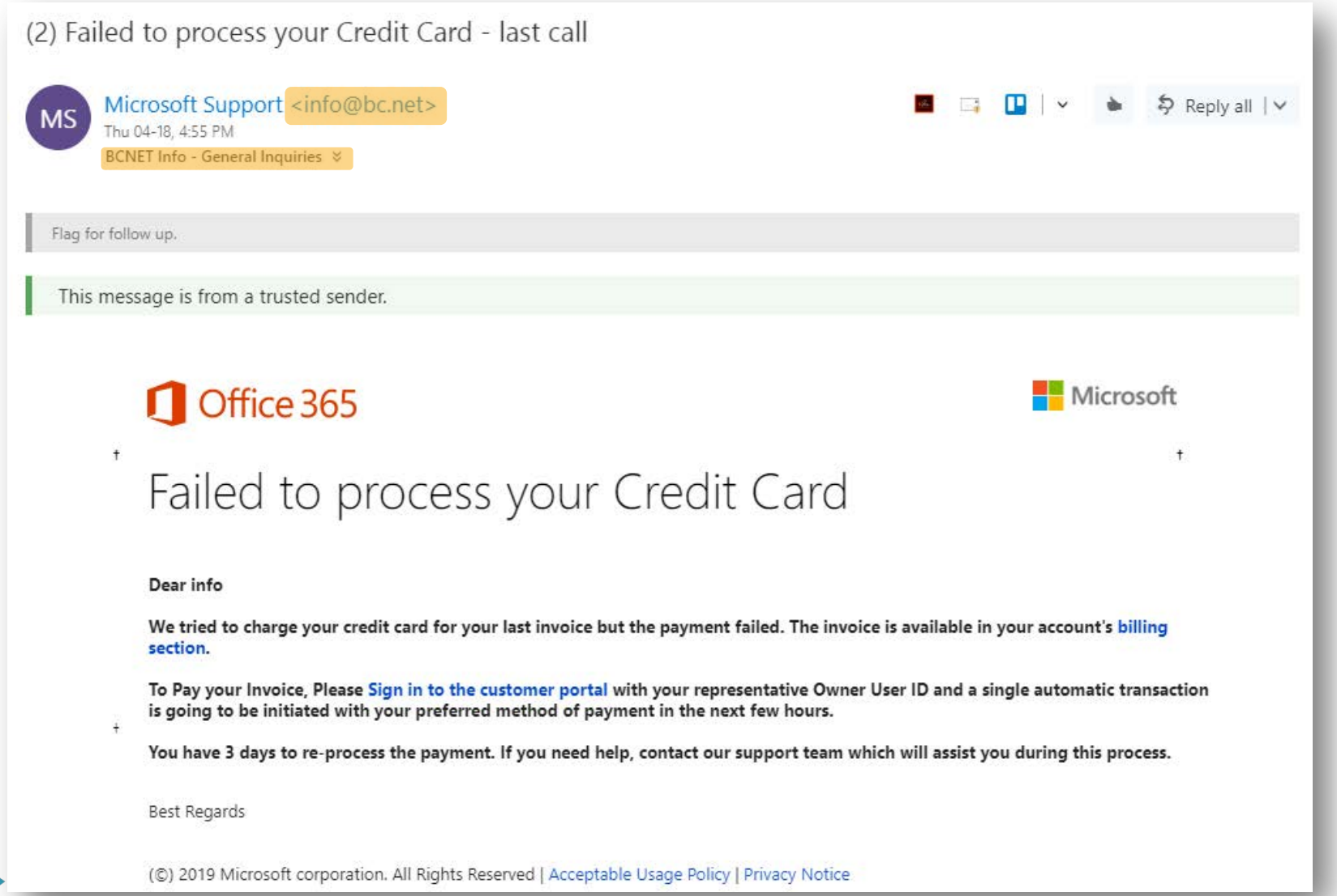
```
Authentication-Results: spf=pass (sender IP is 199.66.225.3)
 smtp.mailfrom=fourpointslax.com; bc.net; dkim=fail (no key for signature)
 header.d=fourpointslax.com;bc.net; dmarc=fail action=quarantine
 header.from=bc.net;
Received-SPF: Pass (protection.outlook.com: domain of fourpointslax.com
 designates 199.66.225.3 as permitted sender) receiver=protection.outlook.com;
 client-ip=199.66.225.3; helo=web11.globalit.com;
Received: from web11.globalit.com (199.66.225.3) by
 QB1CAN01FT008.mail.protection.outlook.com (10.152.120.88) with Microsoft SMTP
 Server (version=TLS1_2, cipher=TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384) id
 15.20.1771.16 via Frontend Transport; Mon, 8 Apr 2019 18:24:51 +0000
DKIM-Signature: v=1; a=rsa-sha256; q=dns/txt; c=relaxed/relaxed;
        d=fourpointslax.com; s=default; h=Content-Type:MIME-Version:Subject:To:From:
        Date:Sender:Reply-To:Message-ID:Cc:Content-Transfer-Encoding:Content-ID:
        Content-Description:Resent-Date:Resent-From:Resent-Sender:Resent-To:Resent-Cc
        :Resent-Message-ID:In-Reply-To:References:List-Id:List-Help:List-Unsubscribe:
        List-Subscribe:List-Post:List-Owner:List-Archive;
        bh=9wYaFQ1CcfIvBbR6fcqkkyKZVpeJ2ne80eo2b8wcXEY=; b=PLQAixrukY/qvoNvVVAPMi+Tti
        N39LVluM4gXd1p/mTnOXlB14n7q7iyeikwTPyLvrpyJjScCw9x8Gfenb0kW6Wo0RUKghs27EQcks+
        pzJfTxucWscoYsMLS1Qxasb/Qu4jWswL9wDLVnM+3Z5L/uNGDe2fJ8nBlDPkbyG70wNvBQRKGdSsO
        hCeGYgUehlFT56WrUImUhT+cAa2A8JRi4mmggX/QxuFKqu1B7QM+TZErbKqFxHeShcJoTjG1agF9t
        ugGHRkmSIJXMOHDIkNNkMZnh98wYovhrHo6n8YlpDGb947CdS5J5Eiv6poo2nPCUbtAR9+6a2xYGw
        t28drALA==;
Received: from [185.144.64.86] (port=54049)
        by web11.globalit.com with esmtpsa (TLSv1.2:ECDHE-RSA-AES256-GCM-SHA384:256)
        (Exim 4.91)
        (envelope-from <howard.chen@fourpointslax.com>)
        id 1hDYwr-0001Lg-0Q
        for asc-ircug@bc.net; Mon, 08 Apr 2019 11:24:49 -0700
Date: Mon, 08 Apr 2019 22:54:48 +0330
From: BCNET Meetings <bcnmtgs@bc.net> <howard.chen@fourpointslax.com>
To: asc-ircug@bc.net
Subject: FA-42892704
```

BCNET 2019

#BCNET2019

Message Header

Sample Filter Rule Intervention



(2) Failed to process your Credit Card - last call

MS

Microsoft Support <info@bc.net>

Thu 04-18, 4:55 PM

BCNET Info - General Inquiries

Reply all

Flag for follow up.

This message is from a trusted sender.

Office 365

Microsoft

Failed to process your Credit Card

Dear info

We tried to charge your credit card for your last invoice but the payment failed. The invoice is available in your account's billing section.

To Pay your Invoice, Please Sign in to the customer portal with your representative Owner User ID and a single automatic transaction is going to be initiated with your preferred method of payment in the next few hours.

You have 3 days to re-process the payment. If you need help, contact our support team which will assist you during this process.

Best Regards

(©) 2019 Microsoft corporation. All Rights Reserved | Acceptable Usage Policy | Privacy Notice

Sample Filter Rule Intervention

```
Authentication-Results: spf=none (sender IP is 52.73.13.217)
 smtp.helo=ec2-18-218-156-163.us-east-2.compute.amazonaws.com; bc.net;
 dkim=none (message not signed) header.d=none;bc.net; dmarc=fail
 action=quarantine header.from=bc.net;compauth=fail reason=000
Received-SPF: None (protection.outlook.com:
 ec2-18-218-156-163.us-east-2.compute.amazonaws.com does not designate
 permitted sender hosts)
Received: from ec2-18-218-156-163.us-east-2.compute.amazonaws.com
 (52.73.13.217) by TO1CAN01FT015.mail.protection.outlook.com (10.152.12
 with Microsoft SMTP Server id 15.20.1771.16 via Frontend Transport; Th
 Apr 2019 23:55:02 +0000
Subject: (2) Failed to process your Credit Card - last call
From: Microsoft Support <info@bc.net>
Reply-To: <reply@bbking.club>
To: <info@bc.net>
```

spf = **none**

dkim = **none**

dmarc = **fail**

action = **quarantine**

Microsoft Support

info@bc.net

#BCNET2019

BCNET 2019

Ongoing Mitigation Strategies

How much work is required to combat other threats?

Ongoing Mitigation Strategies

What have we done so far?

- ✓Use DMARC, SPF, & DKIM
- ✓Upgrade to Office 365 A5 License
- ✓Provide Staff Training
  - ✓Regular Phishing Campaigns
  - ✓Quarterly Lunch & Learn
  - ✓Annual Security Awareness Training
- ✓Offer Threat Analysis Assistance

What do we plan to do next?

- ❑Create a dashboard for DMARC reports
- ❑Create actionable items for reports

OpenSource DMARC Analyzers

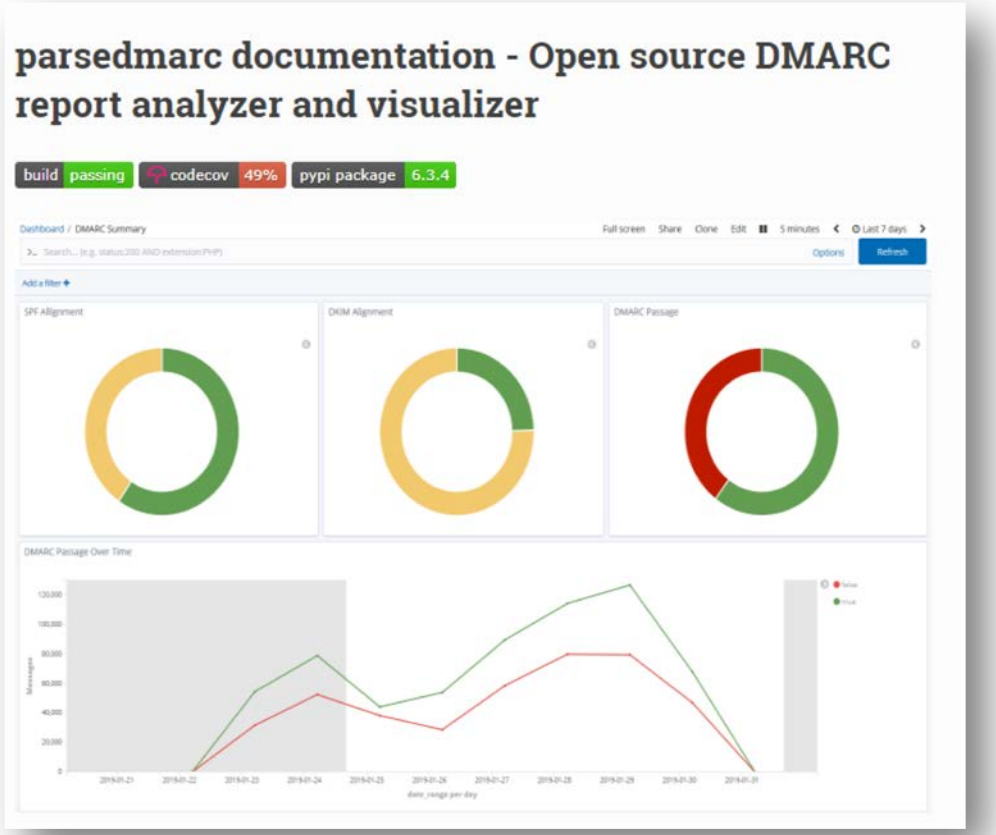


image courtesy of https://domainaware.github.io/parsedmarc/

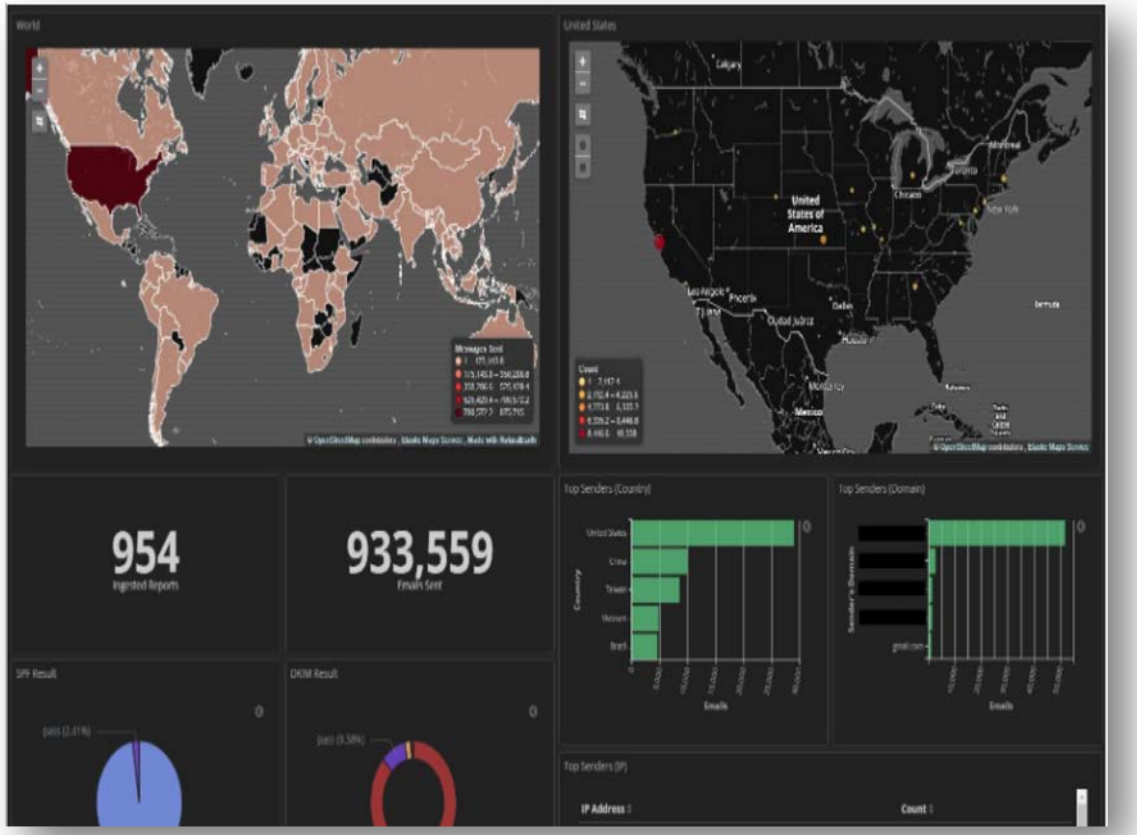


image courtesy of https://github.com/wwalker0307/ElasticMARC

#BCNET2019

BCNET 2019

Q&A

Thank you for joining us this afternoon.

We hope you learned valuable information from BCNET's use case.

Hope to stay in touch!

Alex Doradea-Cabrera
SIEM Systems Administrator
alex.doradea-cabrera@bc.net

Rossilyne Tan
Systems Analyst
rossilyne.tan@bc.net

1. [I]Introduce ourselves
2. Introduce topic/Concepts
    1. [A]Email Security
    2. [R]Past email threat landscape/Risk registry (attackers PV)
3. How it works?
    1. [R]Terminology/Definition (one-line with examples)
    2. [A]How they work together? Mail flow.
4. Implementation
    1. [R]Office 365
    2. [A]Infoblox/DNS
5. Did it work? Current email threat landscape
    1. [A]Outlook makes exceptions
    2. [R]Alias attacks
    3. [R]External email address in DLs
    4. [R] Filter rules intervention
6. Ongoing mitigation strategies
    1. [R]Phishing campaigns
    2. [R]Security awareness trainings (Hugh/Ross)
    3. [A]Data Analytics
7. [IRA]Q&A/Closing Remarks