Modern Email Security

fredrik@storedsafe.com

Fredrik Söderblom

XPD AB

15 years of audits in the US and Europe

A Swedish start-up

AB StoredSafe

Agenda

Motivation

Mitigations

Future

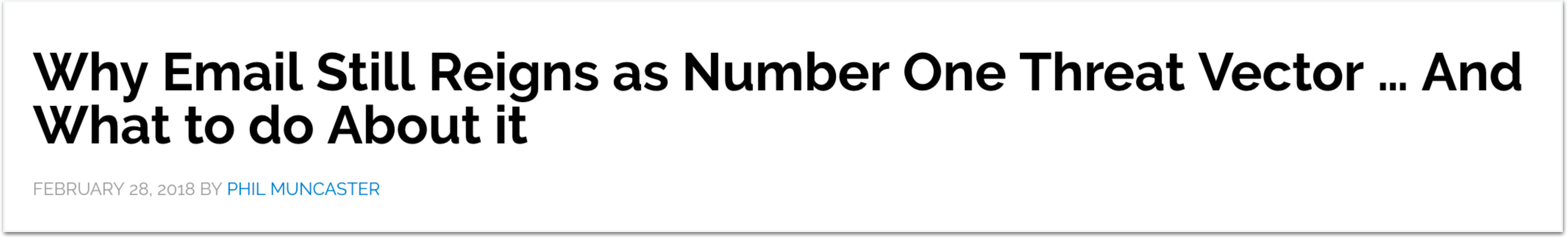
Action Plan

Why is this of any use at all, it’s just mail. Right?

“With over 100 billion corporate emails exchanged each day, it’s no wonder that email remains a major threat vector.”

“With over **100 billion** corporate emails exchanged each day, it’s no wonder that email remains a major threat vector.”

It’s just mail. Right?

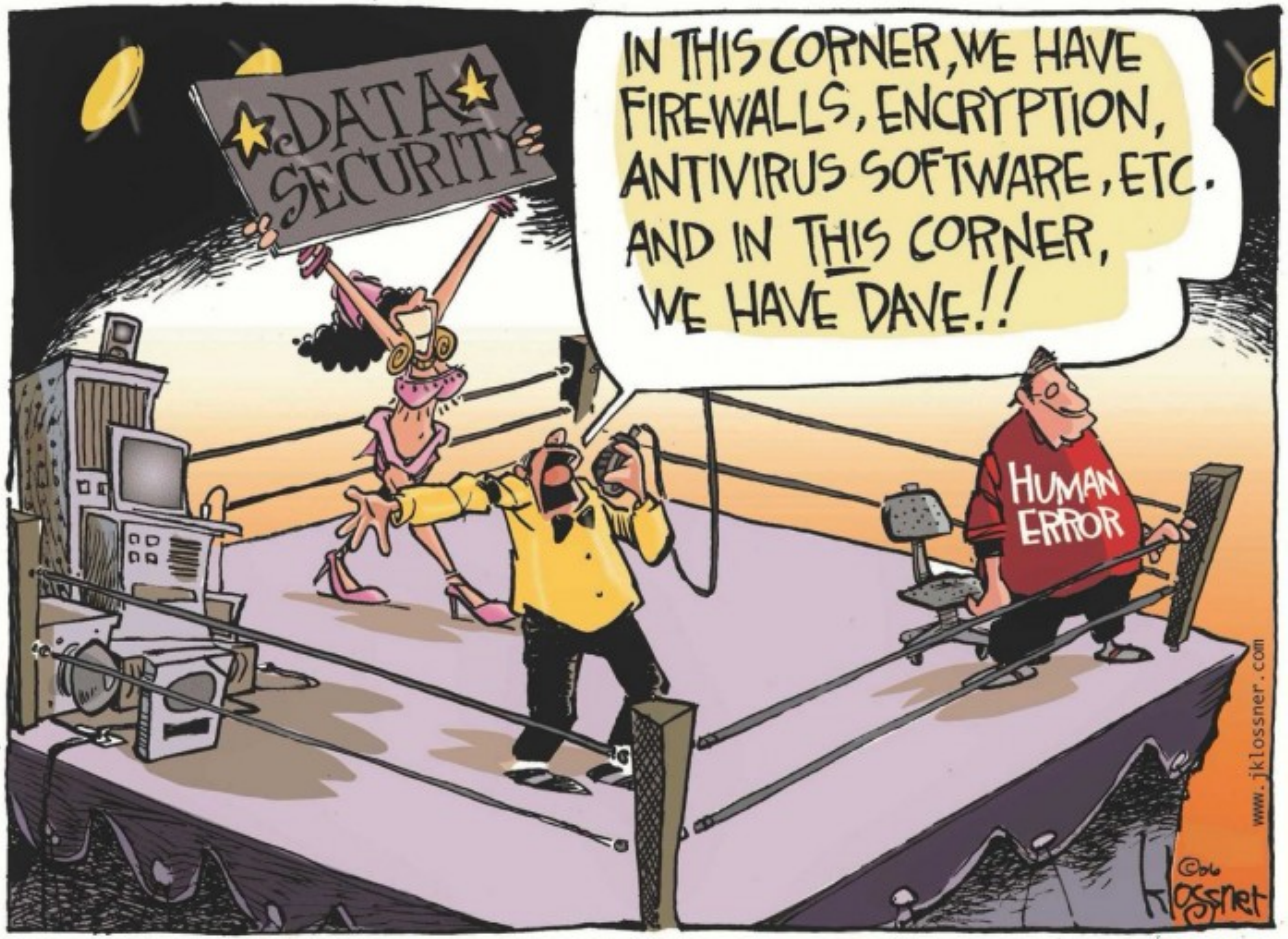


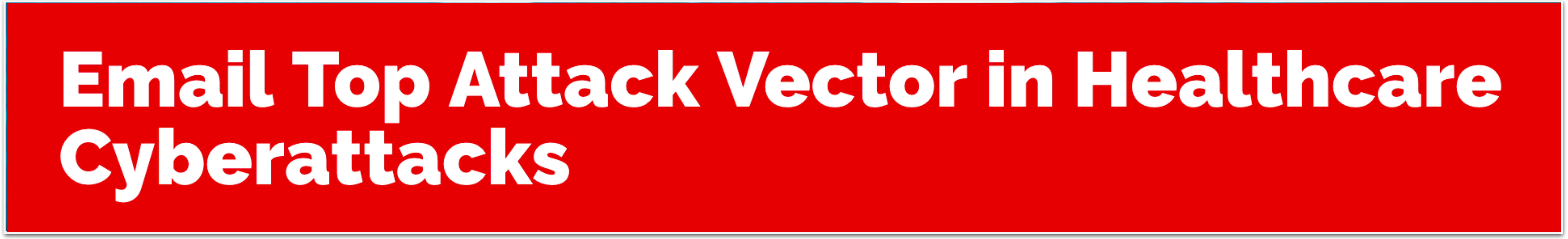
Why Email Still Reigns as Number One Threat Vector … And What to do About it

FEBRUARY 28, 2018 BY PHIL MUNCASTER

1 NOV 2018 NEWS

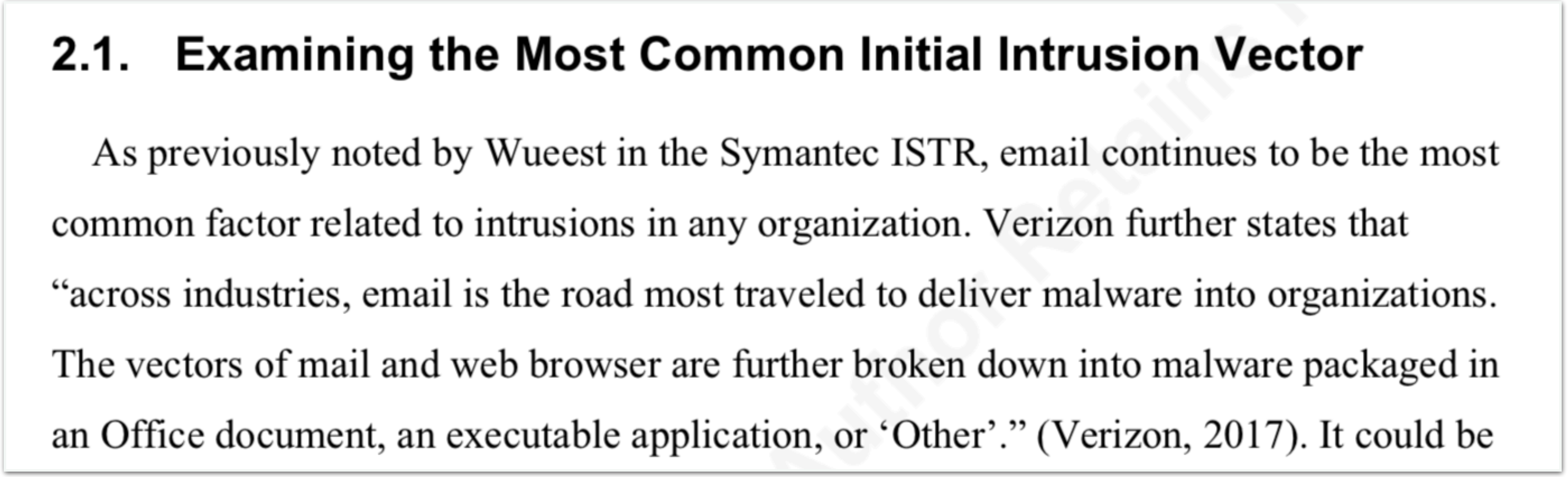
Email a Top Attack Vector, Users Can't ID a Fake


DATA SECURITY
IN THIS CORNER, WE HAVE FIREWALLS, ENCRYPTION, ANTIVIRUS SOFTWARE, ETC. AND IN THIS CORNER, WE HAVE DAVE!!
HUMAN ERROR
www.jklossner.com
©06 Lossner



Email Top Attack Vector in Healthcare Cyberattacks

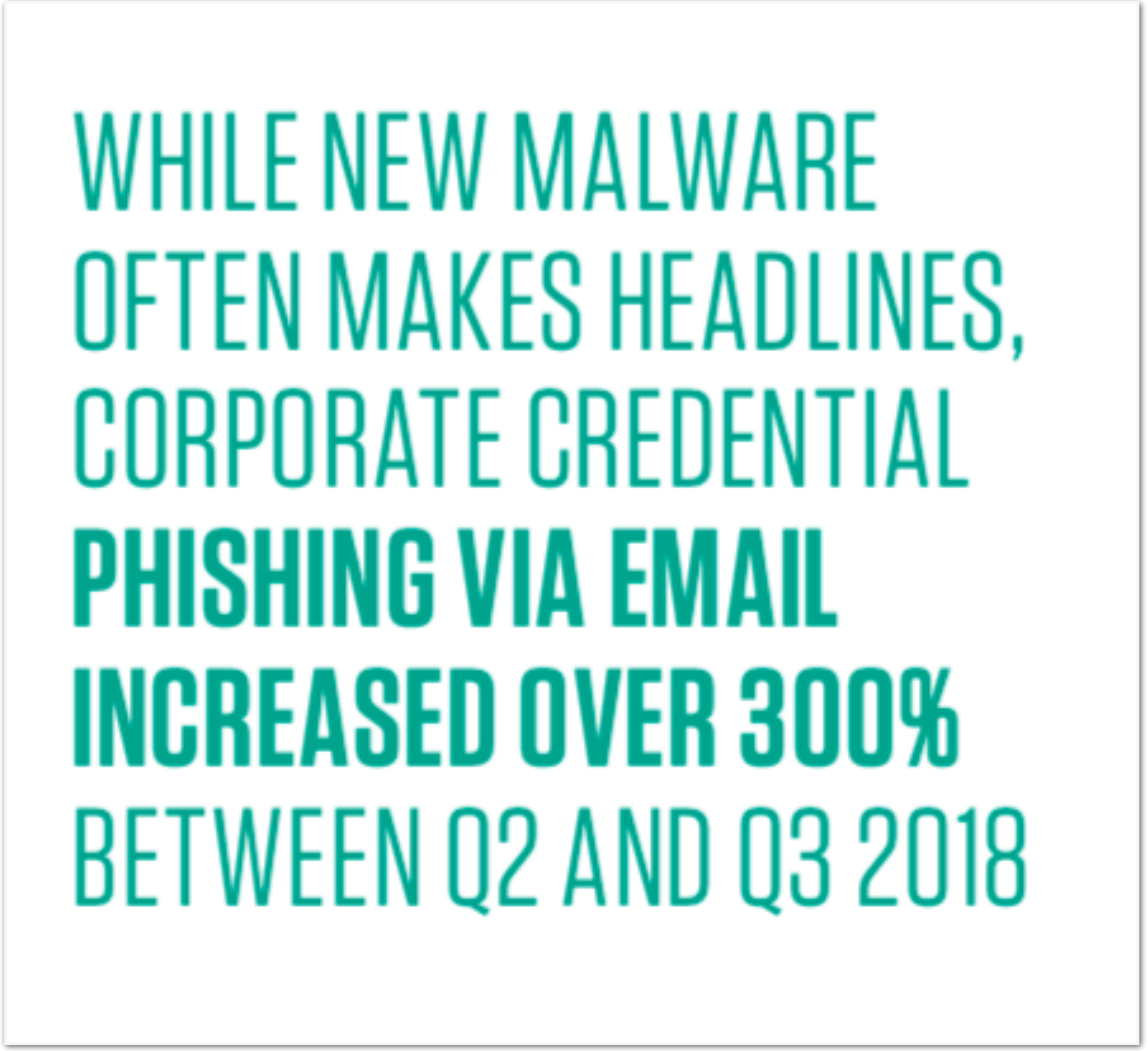
Source HIPAA Journal



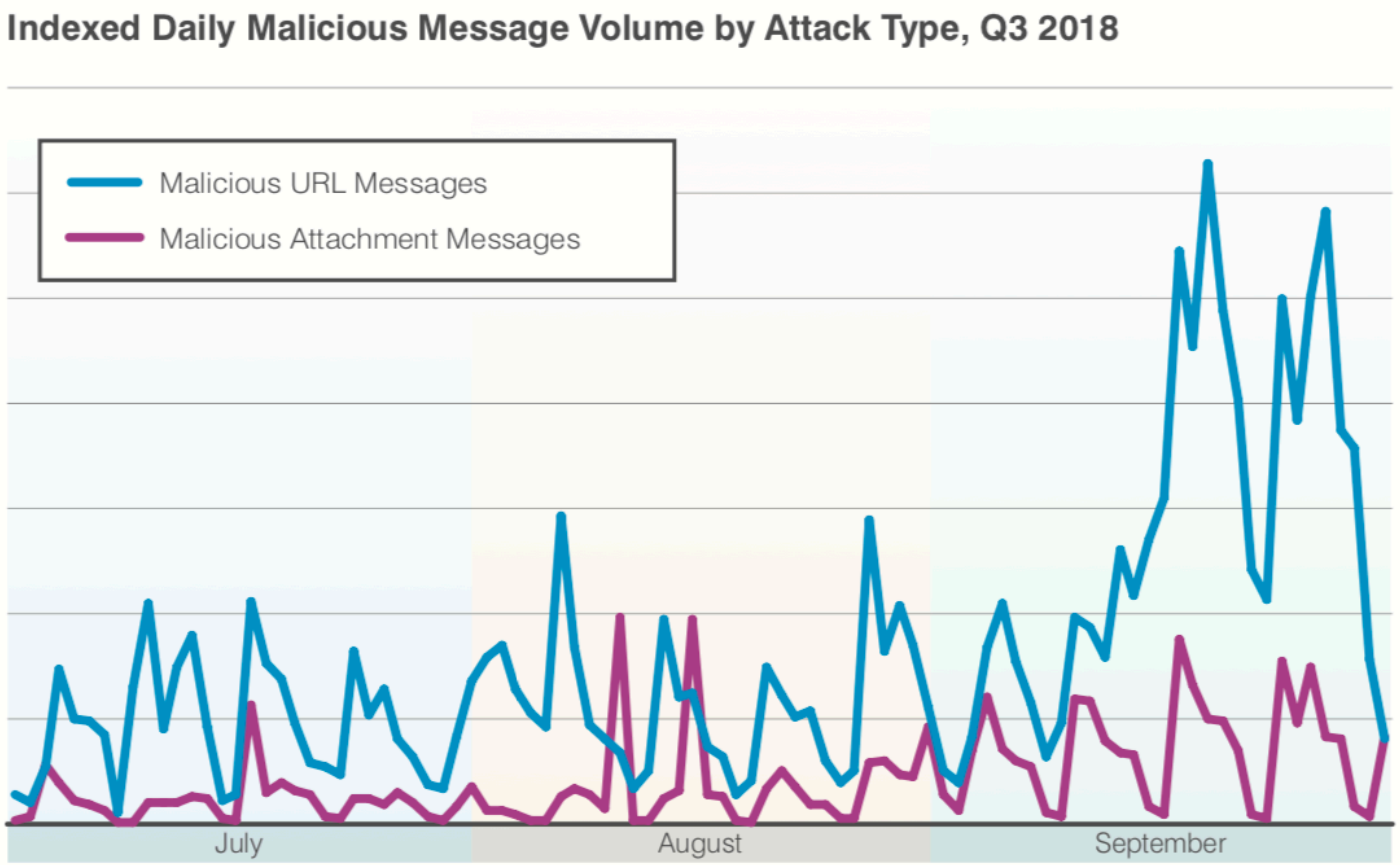
2.1. Examining the Most Common Initial Intrusion Vector

As previously noted by Wueest in the Symantec ISTR, email continues to be the most common factor related to intrusions in any organization. Verizon further states that “across industries, email is the road most traveled to deliver malware into organizations. The vectors of mail and web browser are further broken down into malware packaged in an Office document, an executable application, or ‘Other’.” (Verizon, 2017). It could be

Source SANS



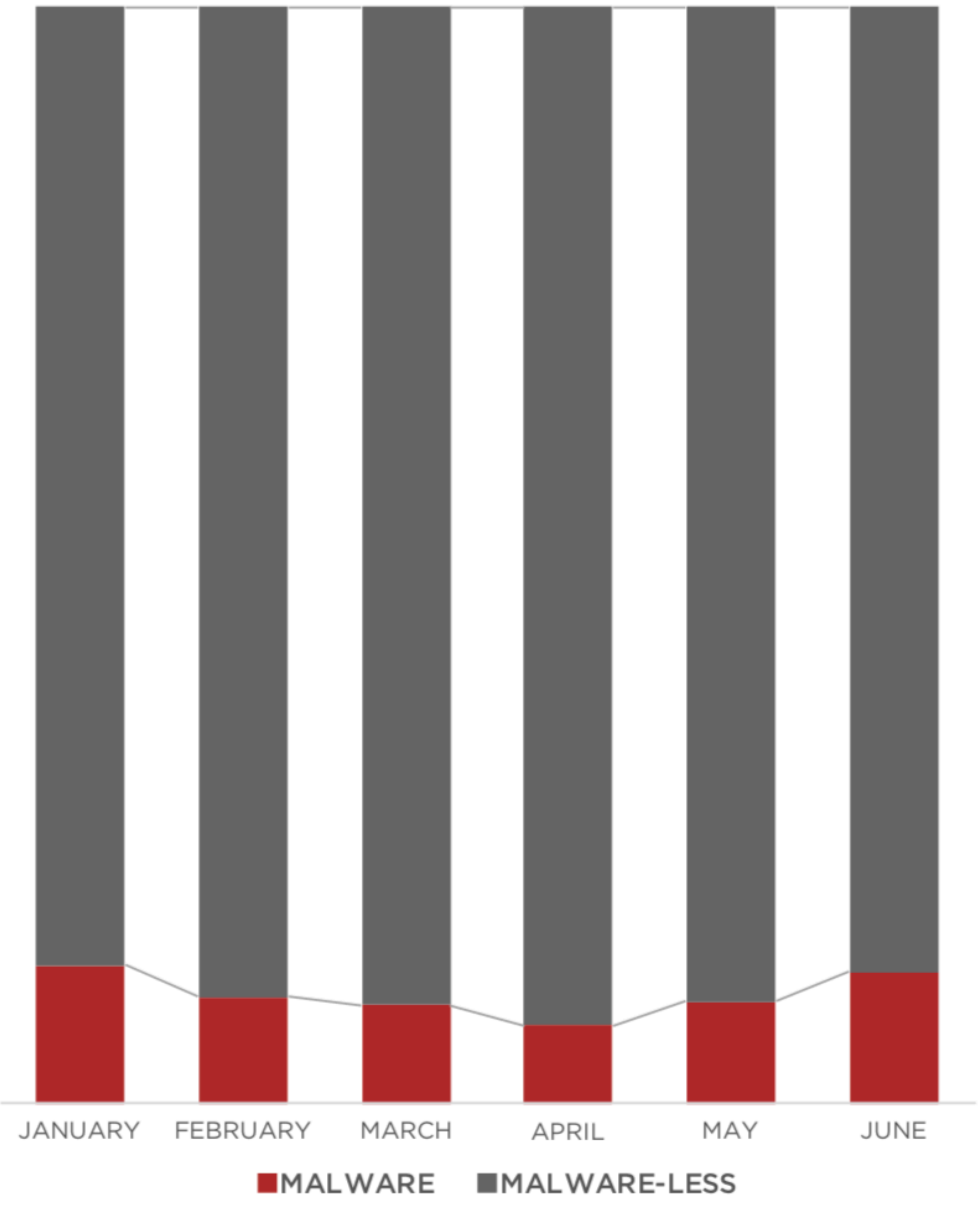
WHILE NEW MALWARE OFTEN MAKES HEADLINES, CORPORATE CREDENTIAL **PHISHING VIA EMAIL INCREASED OVER 300%** BETWEEN Q2 AND Q3 2018



Indexed Daily Malicious Message Volume by Attack Type, Q3 2018

Figure 1: Indexed daily attack type trend, July-September 2018

Source Proofpoint



90%

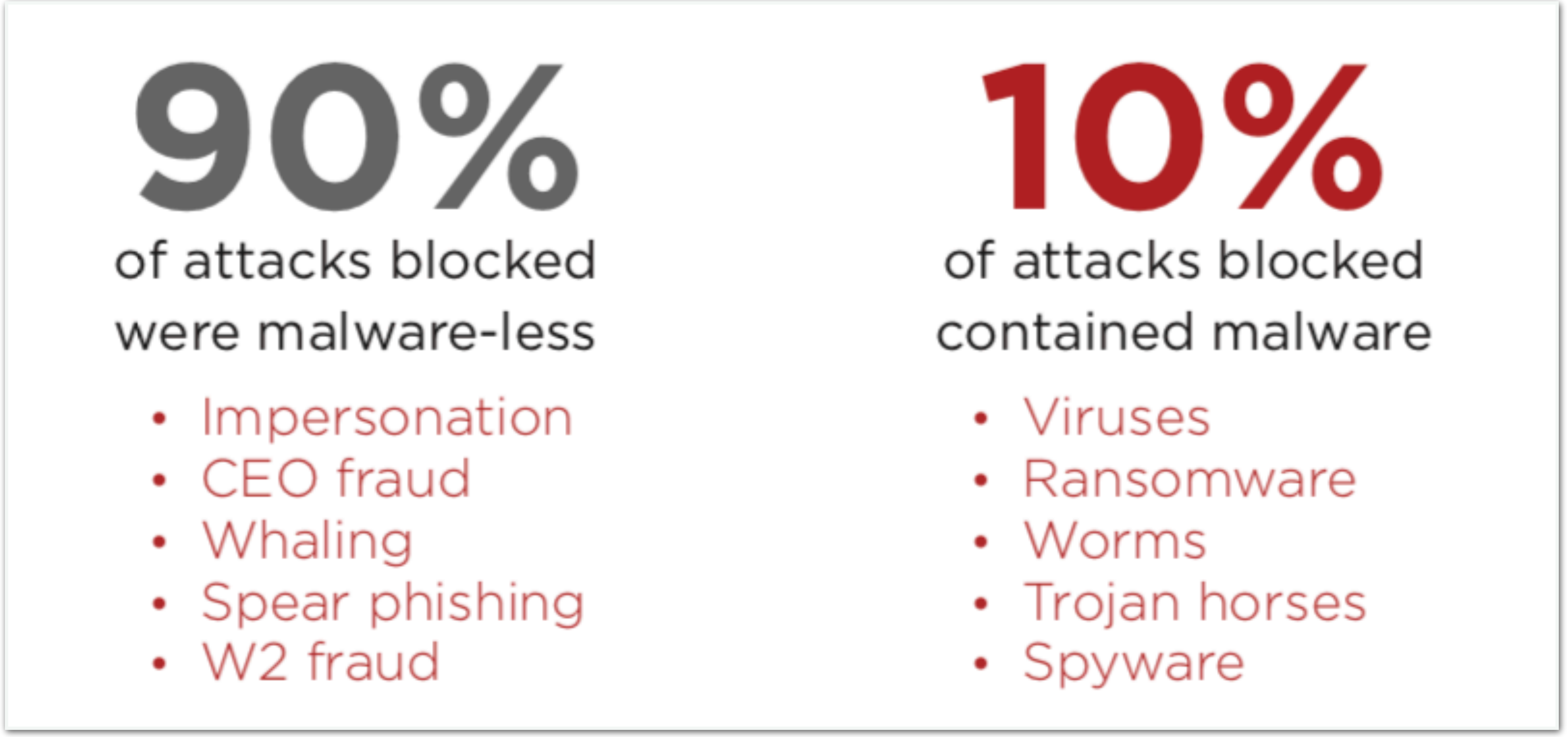
of attacks blocked were malware-less

- Impersonation
- CEO fraud
- Whaling
- Spear phishing
- W2 fraud

10%

of attacks blocked contained malware

- Viruses
- Ransomware
- Worms
- Trojan horses
- Spyware



90%

of attacks blocked were malware-less

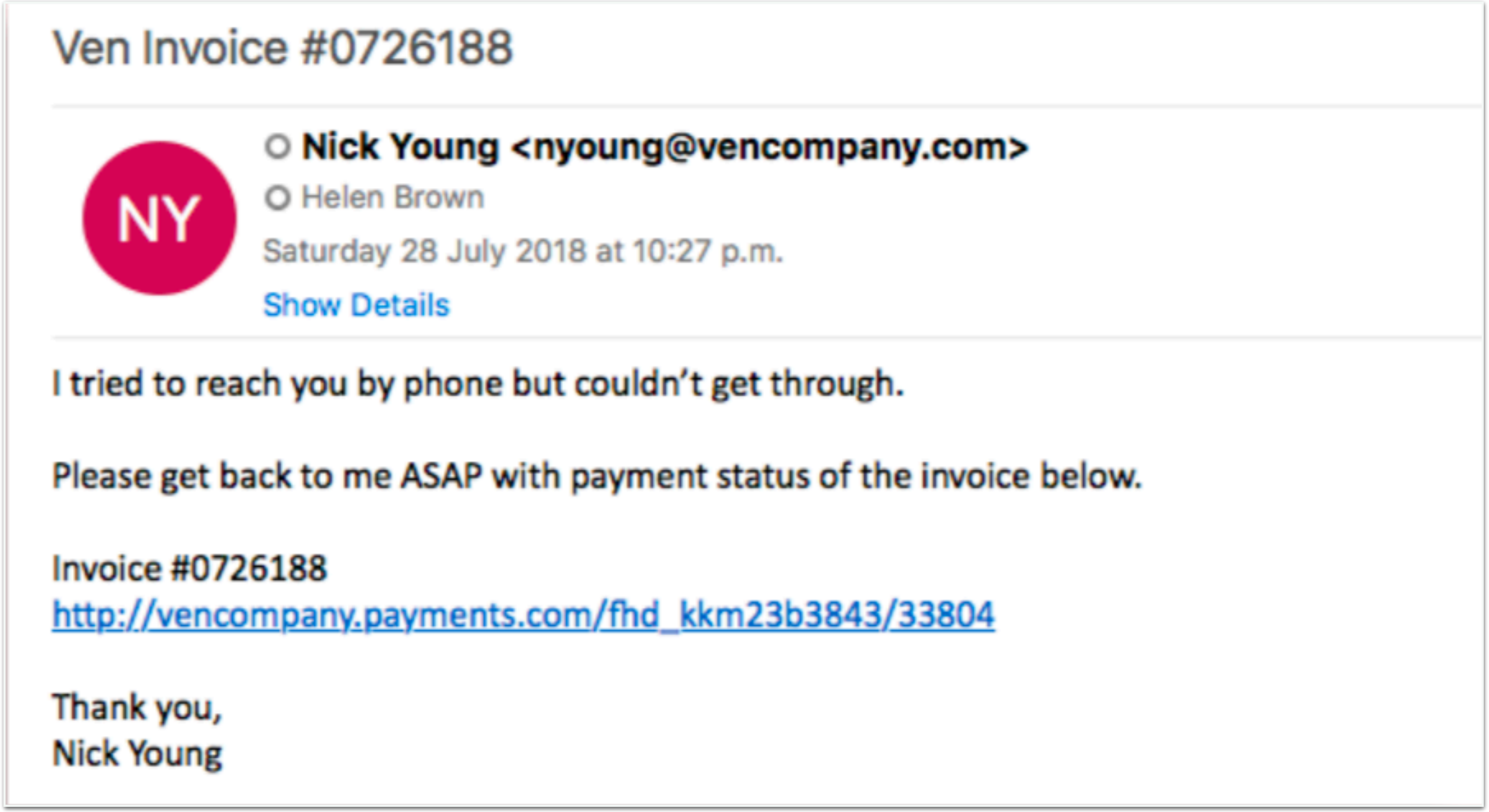
- Impersonation
- CEO fraud
- Whaling
- Spear phishing
- W2 fraud

10%

of attacks blocked contained malware

- Viruses
- Ransomware
- Worms
- Trojan horses
- Spyware

Source Fireeye



Ven Invoice #0726188

○ **Nick Young <nyoung@vencompany.com>**

○ Helen Brown

Saturday 28 July 2018 at 10:27 p.m.

I tried to reach you by phone but couldn't get through.

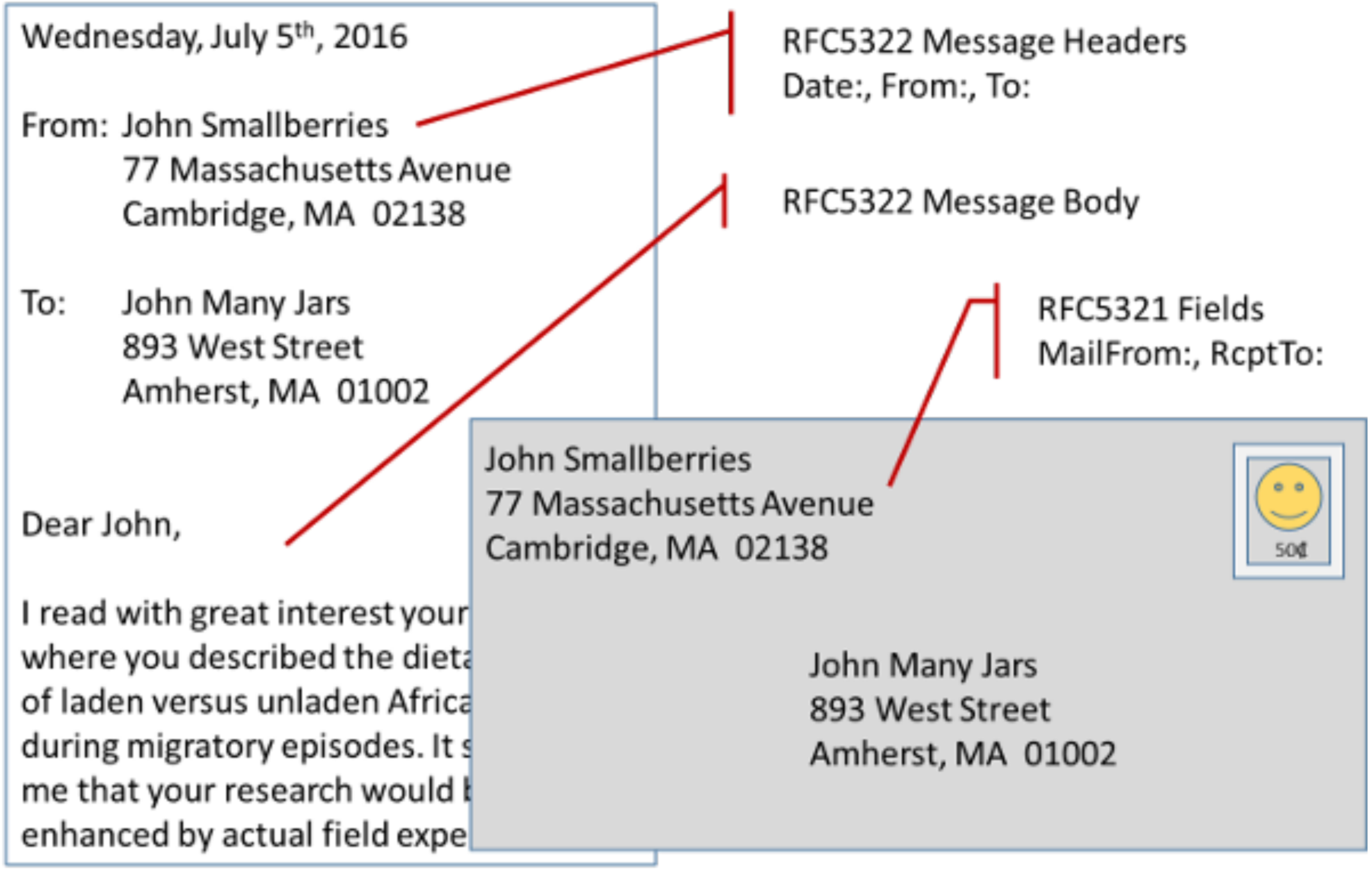
Please get back to me ASAP with payment status of the invoice below.

Invoice #0726188
http://vencompany.payments.com/fhd_kkm23b3843/33804

Thank you,
Nick Young

Source Fireeye

(Mitigations)



Wednesday, July 5th, 2016

From: John Smallberries
77 Massachusetts Avenue
Cambridge, MA 02138

To: John Many Jars
893 West Street
Amherst, MA 01002

Dear John,

I read with great interest your
where you described the dieta
of laden versus unladen Africa
during migratory episodes. It s
me that your research would b
enhanced by actual field expe

RFC5322 Message Headers
Date:, From:, To:

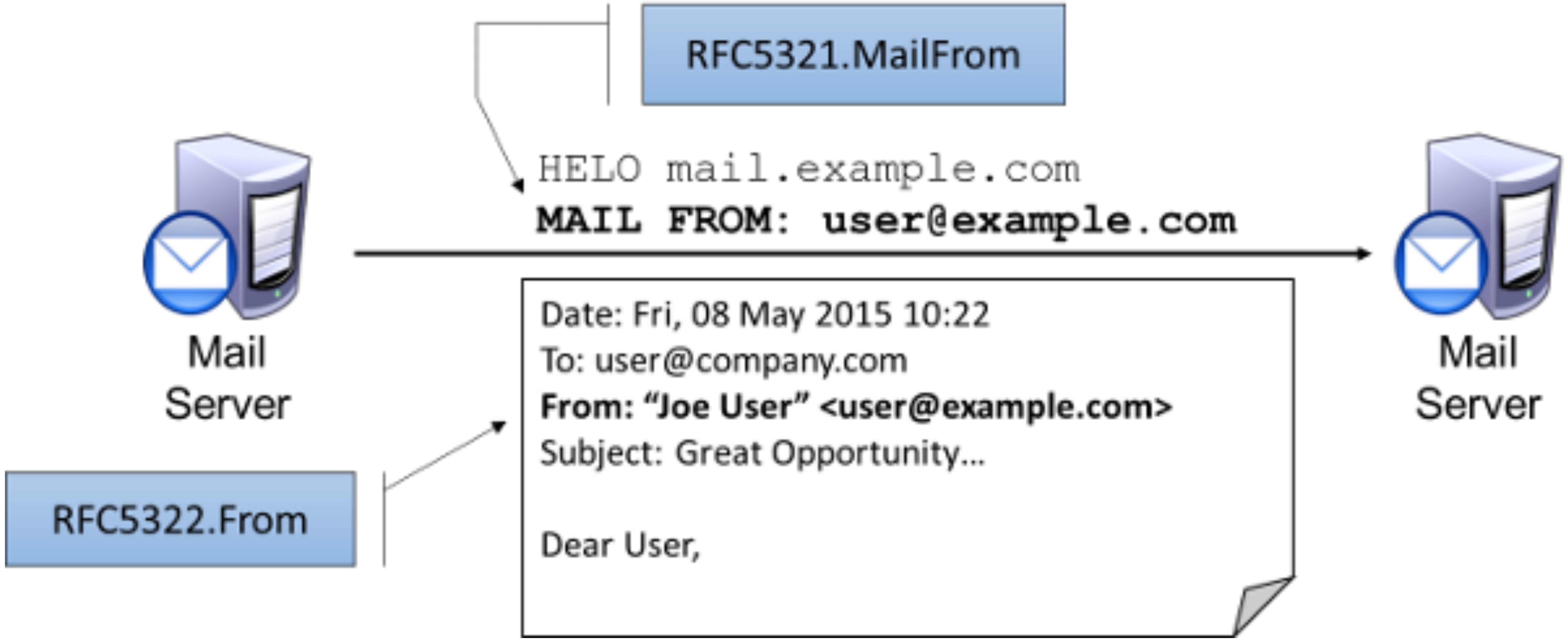
RFC5322 Message Body

RFC5321 Fields
MailFrom:, RcptTo:

John Smallberries
77 Massachusetts Avenue
Cambridge, MA 02138

John Many Jars
893 West Street
Amherst, MA 01002

Source dmarc.org



RFC5321.MailFrom

```
HELO mail.example.com
MAIL FROM: user@example.com
```

Date: Fri, 08 May 2015 10:22
To: user@company.com
From: “Joe User” <user@example.com>
Subject: Great Opportunity…

Dear User,

RFC5322.From

Source dmarc.org

STARTTLS

SPF

DKIM

DMARC

DNSSEC

DANE

CAA

Lets start by examining two problems - at the same time

```
$ nc -v smtp.corp.com 25
Connection to smtp.corp.com port 25 [tcp/smtp] succeeded!
220 smtp.corp.com ESMTP
```

```
$ nc -v smtp.corp.com 25
Connection to smtp.corp.com port 25 [tcp/smtp] succeeded!
220 smtp.corp.com ESMTP
EHLO evildoer.com
```

```
$ nc -v smtp.corp.com 25
Connection to smtp.corp.com port 25 [tcp/smtp] succeeded!
220 smtp.corp.com ESMTP
EHLO evildoer.com
250-smtp.corp.com
250-STARTTLS
250-ENHANCEDSTATUSCODES
250-8BITMIME
250-DSN
```

```
$ nc -v smtp.corp.com 25
Connection to smtp.corp.com port 25 [tcp/smtp] succeeded!
220 smtp.corp.com ESMTP
EHLO evildoer.com
250-smtp.corp.com
250-STARTTLS
250-ENHANCEDSTATUSCODES
250-8BITMIME
250-DSN
MAIL FROM: <bogus@evildoer.com>
```

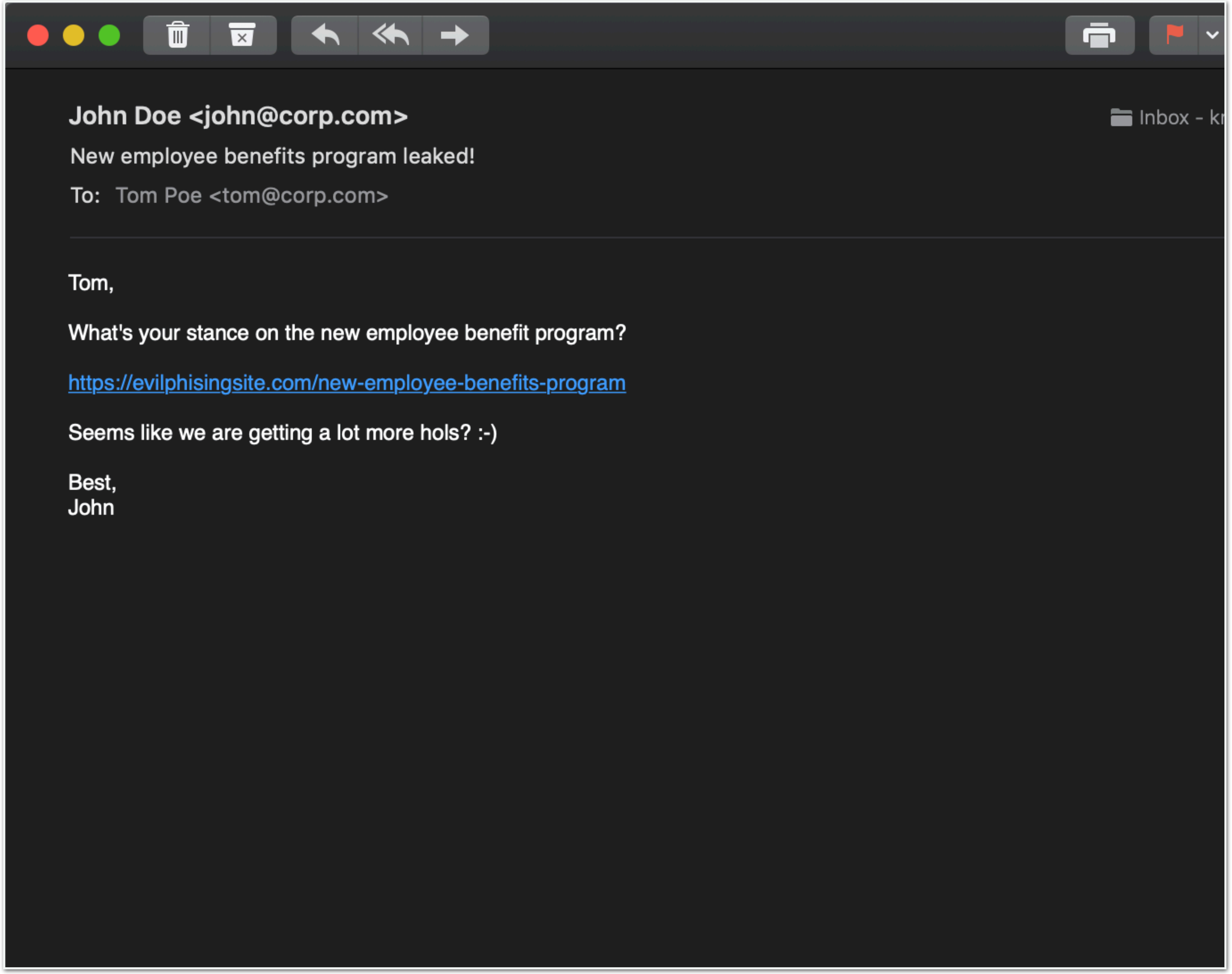
```
$ nc -v smtp.corp.com 25
Connection to smtp.corp.com port 25 [tcp/smtp] succeeded!
220 smtp.corp.com ESMTP
EHLO evildoer.com
250-smtp.corp.com
250-STARTTLS
250-ENHANCEDSTATUSCODES
250-8BITMIME
250-DSN
MAIL FROM: <bogus@evildoer.com>
250 2.1.0 Ok
RCPT TO: <tom@corp.com>
```

```
$ nc -v smtp.corp.com 25
Connection to smtp.corp.com port 25 [tcp/smtp] succeeded!
220 smtp.corp.com ESMTP
EHLO evildoer.com
250-smtp.corp.com
250-STARTTLS
250-ENHANCEDSTATUSCODES
250-8BITMIME
250-DSN
MAIL FROM: <bogus@evildoer.com>
250 2.1.0 Ok
RCPT TO: <tom@corp.com>
250 2.1.5 Ok
DATA
354 End data with <CR><LF>.<CR><LF>
```

```
$ nc -v smtp.corp.com 25
Connection to smtp.corp.com port 25 [tcp/smtp] succeeded!
220 smtp.corp.com ESMTP
EHLO evildoer.com
250-smtp.corp.com
250-STARTTLS
250-ENHANCEDSTATUSCODES
250-8BITMIME
250-DSN
MAIL FROM: <bogus@evildoer.com>
250 2.1.0 Ok
RCPT TO: <tom@corp.com>
250 2.1.5 Ok
DATA
354 End data with <CR><LF>.<CR><LF>
From: "John Doe" <john@corp.com>
To: "Tom Poe" <tom@corp.com>
Subject: New employee benefits program leaked!

Tom,

What's your stance on the new employee benefit program?

https://evilphisingsite.com/new-employee-benefits-program

Seems like we are getting a lot more hols? :-)

Best,
John
.
```

```
$ nc -v smtp.corp.com 25
Connection to smtp.corp.com port 25 [tcp/smtp] succeeded!
220 smtp.corp.com ESMTP
EHLO evildoer.com
250-smtp.corp.com
250-STARTTLS
250-ENHANCEDSTATUSCODES
250-8BITMIME
250-DSN
MAIL FROM: <bogus@evildoer.com>
250 2.1.0 Ok
RCPT TO: <tom@corp.com>
250 2.1.5 Ok
DATA
354 End data with <CR><LF>.<CR><LF>
From: "John Doe" <john@corp.com>
To: "Tom Poe" <tom@corp.com>
Subject: New employee benefits program leaked!

Tom,

What's your stance on the new employee benefit program?

https://evilphisingsite.com/new-employee-benefits-program

Seems like we are getting a lot more hols? :-)

Best,
John
.
250 2.0.0 Ok: queued as 43E9220439
QUIT
221 2.0.0 Bye
```

```
$ nc -v smtp.corp.com 25
Connection to smtp.corp.com port 25 [tcp/smtp] succeeded!
220 smtp.corp.com ESMTP
EHLO evildoer.com
250-smtp.corp.com
250-STARTTLS
250-ENHANCEDSTATUSCODES
250-8BITMIME
250-DSN
MAIL FROM: <bogus@evildoer.com>
250 2.1.0 Ok
RCPT TO: <tom@corp.com>
250 2.1.5 Ok
DATA
354 End data with <CR><LF>.<CR><LF>
From: "John Doe" <john@corp.com>
To: "Tom Poe" <tom@corp.com>
Subject: New employee benefits program leaked!

Tom,

What's your stance on the new employee benefit program?

https://evilphisingsite.com/new-employee-benefits-program

Seems like we are getting a lot more hols? :-)

Best,
John
.
250 2.0.0 Ok: queued as 43E9220439
QUIT
221 2.0.0 Bye
```



John Doe <john@corp.com>

New employee benefits program leaked!

To: Tom Poe <tom@corp.com>

Tom,

What's your stance on the new employee benefit program?

https://evilphisingsite.com/new-employee-benefits-program

Seems like we are getting a lot more hols? :-)

Best,
John

STARTTLS to the rescue

```
$ nc -v smtp.corp.com 25
Connection to smtp.corp.com port 25 [tcp/smtp] succeeded!
220 smtp.corp.com ESMTP
EHLO evildoer.com
250-smtp.corp.com
250-STARTTLS
250-ENHANCEDSTATUSCODES
250-8BITMIME
250-DSN
```

```
$ nc -v smtp.corp.com 25
Connection to smtp.corp.com port 25 [tcp/smtp] succeeded!
220 smtp.corp.com ESMTP
EHLO evildoer.com
250-smtp.corp.com
250-STARTTLS
250-ENHANCEDSTATUSCODES
250-8BITMIME
250-DSN
STARTTLS
220 2.0.0 Ready to start TLS
```

```
$ nc -v smtp.corp.com 25
Connection to smtp.corp.com port 25 [tcp/smtp] succeeded!
220 smtp.corp.com ESMTP
EHLO evildoer.com
250-smtp.corp.com
250-STARTTLS
250-ENHANCEDSTATUSCODES
250-8BITMIME
250-DSN
STARTTLS
220 2.0.0 Ready to start TLS
owMC4zNCAvU3lzdGVtL0xpYnJhcnkvRnJhbWV3b3Jrcy9RdWlja0xvb
2suZnJhbWV3b3JrL1ZlcnNpb25zL0EvUmVzb3VyY2VzL3F1aWNrbG9v
a2QuYXBwL0NvbnRlbnRzL1hQQ1NlcnZpY2VzL1F1aWNrTG9va1NhdGV
sbGl0ZS54cGMvQ29udGVudHMvTWFjT1MvUXVpY2tMb29rU2F0ZWxsaX
RlCiAgNTAxIDI0NjM1ICAgICAxICAgMCAxMTo1MVBNID8/ICAgICAgI
CAgMDowNy42MSAvU3lzdGVtL0xpYnJhcnkvQ29yZVNlcnZpY2VzL1Jl
cG9ydENyYXNoIGFnZW50CiAgNTAxIDI0NjY0ICAgICAxICAgMCAxMTo
1M1BNID8/ICAgICAgICAgMDowMC4yOSAvU3lzdGVtL0xpYnJhcnkvRn
JhbWV3b3Jrcy9BZGRyZXNzQm9vay5mcmFtZXdvcmsvVmVyc2lvbnMvQ
S9IZWxwZXJzL0FkZHJlc3NCb29rU291cmNlU3luYy5hcHAvQ29udGVu
dHMvTWFjT1MvQWRkcmVzc0Jvb2tTb3VyY2VTeW5jCiAgNTAxIDI0NjY
1ICAgICAxICAgMCAxMTo1M1BNID8/ICAgICAgICAgMDowMC4wOSAvTG
licmFyeS9BcHBsaWNhdGlvbiBTdXBwb3J0L0dQR1Rvb2xzL0dQR1N1a
XRlX1VwZGF0ZXIuYXBwL0NvbnRlbnRzL01hY09TL0dQR1N1aXRlX1Vw
ZGF0ZXIKICA1MDEgIDQ5ODUgICA4NTEgICAwIEZyaTA0UE0gdHR5czA
wNSAgICAwOjAwLjA5IC9BcHBsaWNhdGlvbnMvaVRlcm0uYXBwL0Nvbn
RlbnRzL01hY09TL2lUZXJtMiAtLXNlcnZlciBsb2dpbiAtZnAgZnJzb
wogICAgMCAgNDk4NiAgNDk4NSAgIDAgRnJpMDRQTSB0dHlzMDA1ICAg
IDA6MDAuMDQgbG9naW4gLWZwIGZyc28KICA1MDEgIDQ5ODcgIDQ5ODY
cmVTZXJ2aWNlcy5mcmFtZXdvcmsvRnJhbWV3b3Jrcy9NZXRhZGF0YS5
mcmFtZXdvcmsvVmVyc2lvbnMvQS9TdXBwb3J0L21kd29ya2VyX3NoYX
JlZCAtcyBtZHdvcmtlciAtYyBNRFNJbXBvcnRlcldvcmtlciAtbSBjb
DEgICAwIDExOjQyUE0gPz8gICAgICAgICAwOjAyLjU5IC9TeXN0ZW0v
```

```
$ nc -v smtp.corp.com 25
Connection to smtp.corp.com port 25 [tcp/smtp] succeeded!
220 smtp.corp.com ESMTP
EHLO evildoer.com
250-smtp.corp.com
250-STARTTLS
250-ENHANCEDSTATUSCODES
250-8BITMIME
250-DSN
STARTTLS
220 2.0.0 Ready to start TLS
```

```
owMC4zNCAvU3lzdGVtL0xpYnJhcnkvRnJhbWV3b3Jrcy9RdWlja0xvb
2suZnJhbWV3b3JrL1ZlcnNpb25zL0EvUmVzb3VyY2VzL3F1aWNrbG9v
a2QuYXBwL0NvbnRlbnRzL1hQQ1NlcnZpY2VzL1F1aWNrTG9va1NhdGV
sbGl0ZS54cGMvQ29udGVudHMvTWFjT1MvUXVpY2tMb29rU2F0ZWxsaX
RlCiAgNTAxIDI0NjM1ICAgICAxICAgMCAxMTo1MVBNID8/ICAgICAgI
CAgMDowNy42MSAvU3lzdGVtL0xpYnJhcnkvQ29yZVNlcnZpY2VzL1Jl
cG9ydENyYXNoIGFnZW50CiAgNTAxIDI0NjY0ICAgICAxICAgMCAxMTo
1M1BNID8/ICAgICAgICAgMDowMC4yOSAvU3lzdGVtL0xpYnJhcnkvRn
JhbWV3b3Jrcy9BZGRyZXNzQm9vay5mcmFtZXdvcmsvVmVyc2lvbnMvQ
S9IZWxwZXJzL0FkZHJlc3NCb29rU291cmNlU3luYy5hcHAvQ29udGVu
dHMvTWFjT1MvQWRkcmVzc0Jvb2tTb3VyY2VTeW5jCiAgNTAxIDI0NjY
1ICAgICAxICAgMCAxMTo1M1BNID8/ICAgICAgICAgMDowMC4wOSAvTG
licmFyeS9BcHBsaWNhdGlvbiBTdXBwb3J0L0dQR1Rvb2xzL0dQR1N1a
XRlX1VwZGF0ZXIuYXBwL0NvbnRlbnRzL01hY09TL0dQR1N1aXRlX1Vw
ZGF0ZXIKICA1MDEgIDQ5ODUgICA4NTEgICAwIEZyaTA0UE0gdHR5czA
wNSAgICAwOjAwLjA5IC9BcHBsaWNhdGlvbnMvaVRlcm0uYXBwL0Nvbn
RlbnRzL01hY09TL2lUZXJtMiAtLXNlcnZlciBsb2dpbiAtZnAgZnJzb
wogICAgMCAgNDk4NiAgNDk4NSAgIDAgRnJpMDRQTSB0dHlzMDA1ICAg
IDA6MDAuMDQgbG9naW4gLWZwIGZyc28KICA1MDEgIDQ5ODcgIDQ5ODY
cmVTZXJ2aWNlcy5mcmFtZXdvcmsvRnJhbWV3b3Jrcy9NZXRhZGF0YS5
mcmFtZXdvcmsvVmVyc2lvbnMvQS9TdXBwb3J0L21kd29ya2VyX3NoYX
JlZCAtcyBtZHdvcmtlciAtYyBNRFNJbXBvcnRlcldvcmtlciAtbSBjb
DEgICAwIDExOjQyUE0gPz8gICAgICAgICAwOjAyLjU5IC9TeXN0ZW0v
```

STARTTLS took care of the encryption problem (sort of, at least)

But why …

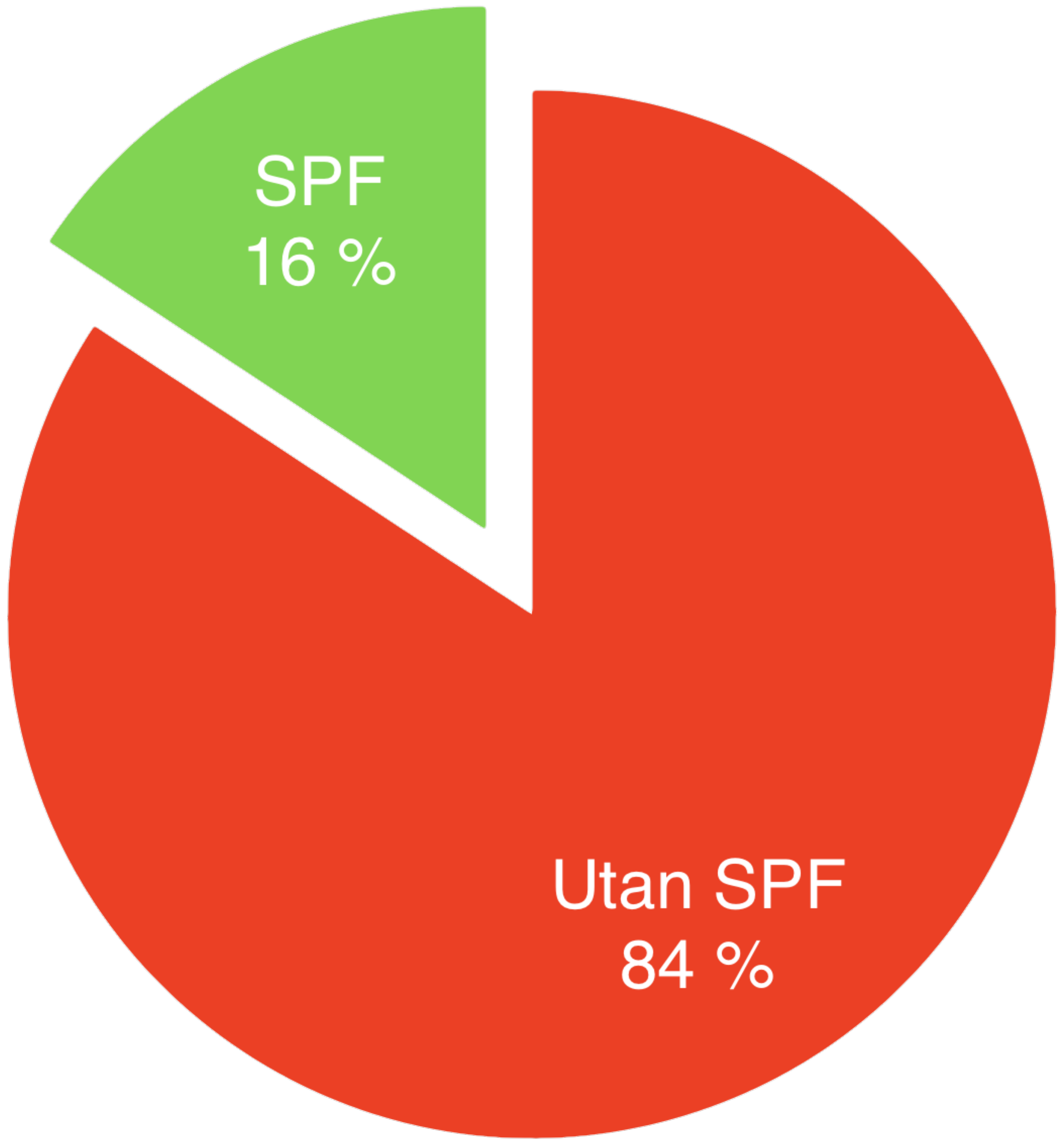
can anyone send email from any domain?

SPF to the rescue

SPF policy published in DNS

```
$ dig evildoer.com. txt +short
"v=spf1 mx -all”
$ dig evildoer.com. mx +short
10 smtp.evildoer.com.
$ dig smtp.evildoer.com. a +short
1.2.3.4
```

SPF i .se



Source dagrs.se

6%

But why …

can anyone forge email from my address?

DKIM to the rescue

```
DKIM-Signature: v=1; a=rsa-sha256; c=simple/simple;
   d=corp.com; s=jan2018;
   h=mime-version:content-type:x-originating-ip:
    message-id:date:thread-index:thread-topic:
    subject:to:from:received;
   bh=2z+pihDQfpV2Fi02GBwCo7yD2Jmm3q6OiGWBVImh7BY=;
.
.
From: “John Doe” <john@corp.com>
.
```

```
DKIM-Signature: v=1; a=rsa-sha256; c=simple/simple;
   d=corp.com; s=jan2018;
   h=mime-version:content-type:x-originating-ip:
    message-id:date:thread-index:thread-topic:
    subject:to:from:received;
   bh=2z+pihDQfpV2Fi02GBwCo7yD2Jmm3q6OiGWBVImh7BY=;
.
.
From: “John Doe” <john@corp.com>
.
```

DKIM public key stored in DNS

```
DKIM-Signature: v=1; a=rsa-sha256; c=simple/simple;
  d=corp.com; s=jan2018;
  h=mime-version:

$ dig jan2018._domainkey.corp.com. txt +short
"v=DKIM1; k=rsa; p=MIGfMA0GCSqGSIb3DQEBAQUAA4GNADC…
aEkTqlc+T1wIDAQAB”
```

Issues?

```
$ nc -v smtp.corp.com 25
Connection to smtp.corp.com port 25 [tcp/smtp] succeeded!
220 smtp.corp.com ESMTP
EHLO evildoer.com
250-smtp.corp.com
250-STARTTLS
250-ENHANCEDSTATUSCODES
250-8BITMIME
250-DSN
MAIL FROM: <bogus@evildoer.com>
250 2.1.0 Ok
RCPT TO: <tom@corp.com>
250 2.1.5 Ok
DATA
354 End data with <CR><LF>.<CR><LF>
From: "John Doe" <john@corp.com>
To: "Tom Poe" <tom@corp.com>
Subject: New employee benefits program leaked!

Tom,

What's your stance on the new employee benefit program?

https://evilphisingsite.com/new-employee-benefits-program

Seems like we are getting a lot more hols? :-)

Best,
John
.
```

RFC5321.MailFrom

RFC5322.From

```
$ nc -v smtp.corp.com 25
Connection to smtp.corp.com port 25 [tcp/smtp] succeeded!
220 smtp.corp.com ESMTP
EHLO evildoer.com
250-smtp.corp.com
250-STARTTLS
250-ENHANCEDSTATUSCODES
250-8BITMIME
250-DSN
MAIL FROM: <bogus@evildoer.com>
250 2.1.0 Ok
RCPT TO: <tom@corp.com>
250 2.1.5 Ok
DATA
354 End data with <CR><LF>.<CR><LF>
From: "John Doe" <john@corp.com>
To: "Tom Poe" <tom@corp.com>
Subject: New employee benefits program leaked!

Tom,

What's your stance on the new employee benefit program?

https://evilphisingsite.com/new-employee-benefits-program

Seems like we are getting a lot more hols? :-)

Best,
John
.
```

SPF only restricts this

```
$ nc -v smtp.corp.com 25
Connection to smtp.corp.com port 25 [tcp/smtp] succeeded!
220 smtp.corp.com ESMTP
EHLO evildoer.com
250-smtp.corp.com
250-STARTTLS
250-ENHANCEDSTATUSCODES
250-8BITMIME
250-DSN
MAIL FROM: <bogus@evildoer.com>
250 2.1.0 Ok
RCPT TO: <tom@corp.com>
250 2.1.5 Ok
DATA
354 End data with <CR><LF>.<CR><LF>
From: "John Doe" <john@corp.com>
To: "Tom Poe" <tom@corp.com>
Subject: New employee benefits program leaked!

Tom,

What's your stance on the new employee benefit program?

https://evilphisingsite.com/new-employee-benefits-program

Seems like we are getting a lot more hols? :-)

Best,
John
.
```

DKIM only verifies this

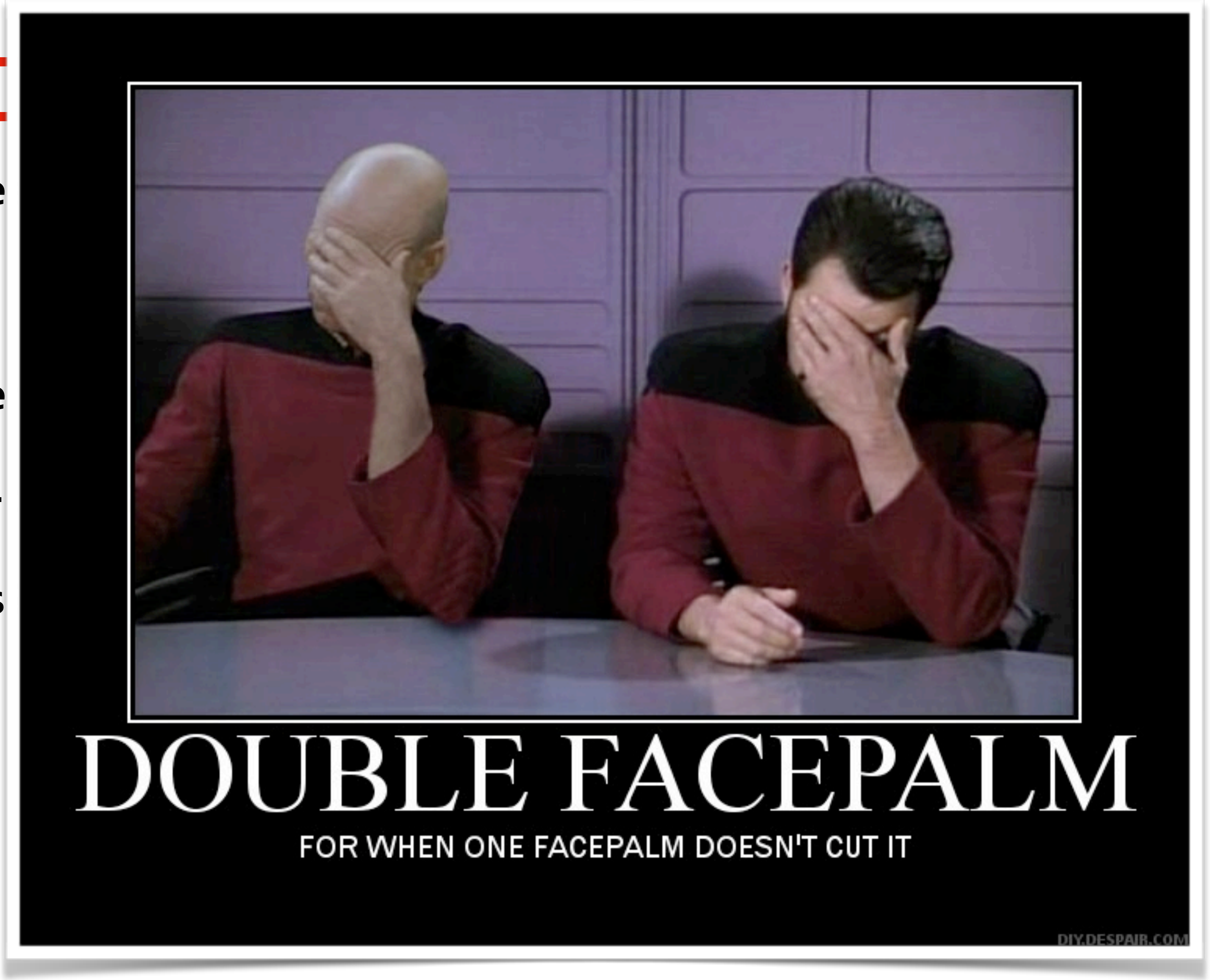
```
$ nc -v smtp.corp.com 25
Connection to smtp.corp.com port 25 [tcp/smtp] succeeded!
220 smtp.corp.com ESMTP
EHLO evildoer.com
250-smtp.corp.com
250-STARTTLS
250-ENHANCEDSTATUSCODES
250-8BITMIME
250-DSN
MAIL FROM: <bogus@evildoer.com>
250 2.1.0 Ok
RCPT TO: <tom@corp.com>
250 2.1.5 Ok
DATA
354 End data with <CR><LF>.<CR><LF>
From: "John Doe" <john@corp.com>
To: "Tom Poe" <tom@corp.com>
Subject: New employee benefits program leaked!

Tom,

What's your stance on the new employee benefit program?

https://evilphisingsite.com/new-employee-benefits-program

Seems like we are getting a lot more hols? :-)

Best,
John
.
```

SPF only restricts this

DKIM only verifies this

```
$ nc -v smtp.corp.com 25
Connection to smtp.corp.com port 25 [tcp/smtp] succeeded!
220 smtp.corp.com ESMTP
EHLO evildoer.com
250-smtp.corp.com
250-STARTTLS
250-ENHANCEDSTATUSCODES
250-8BITMIME
250-DSN
MAIL FROM: <bogus@evildoer.com>
250 2.1.0 Ok
RCPT TO: <tom@corp.com>
250 2.1.5 Ok
DATA
354 End data with <CR><LF>.<CR><LF>
From: "John Doe" <john@corp.com>
To: "Tom Poe" <tom@corp.com>
Subject: New employee benefits program le

Tom,

What's your stance on the new employee be

https://evilphisingsite.com/new-employee-

Seems like we are getting a lot more hols

Best,
John
.
```

Here be dragons



DMARC to the rescue

DMARC checks SPF result

✓

DMARC checks DKIM result

✓

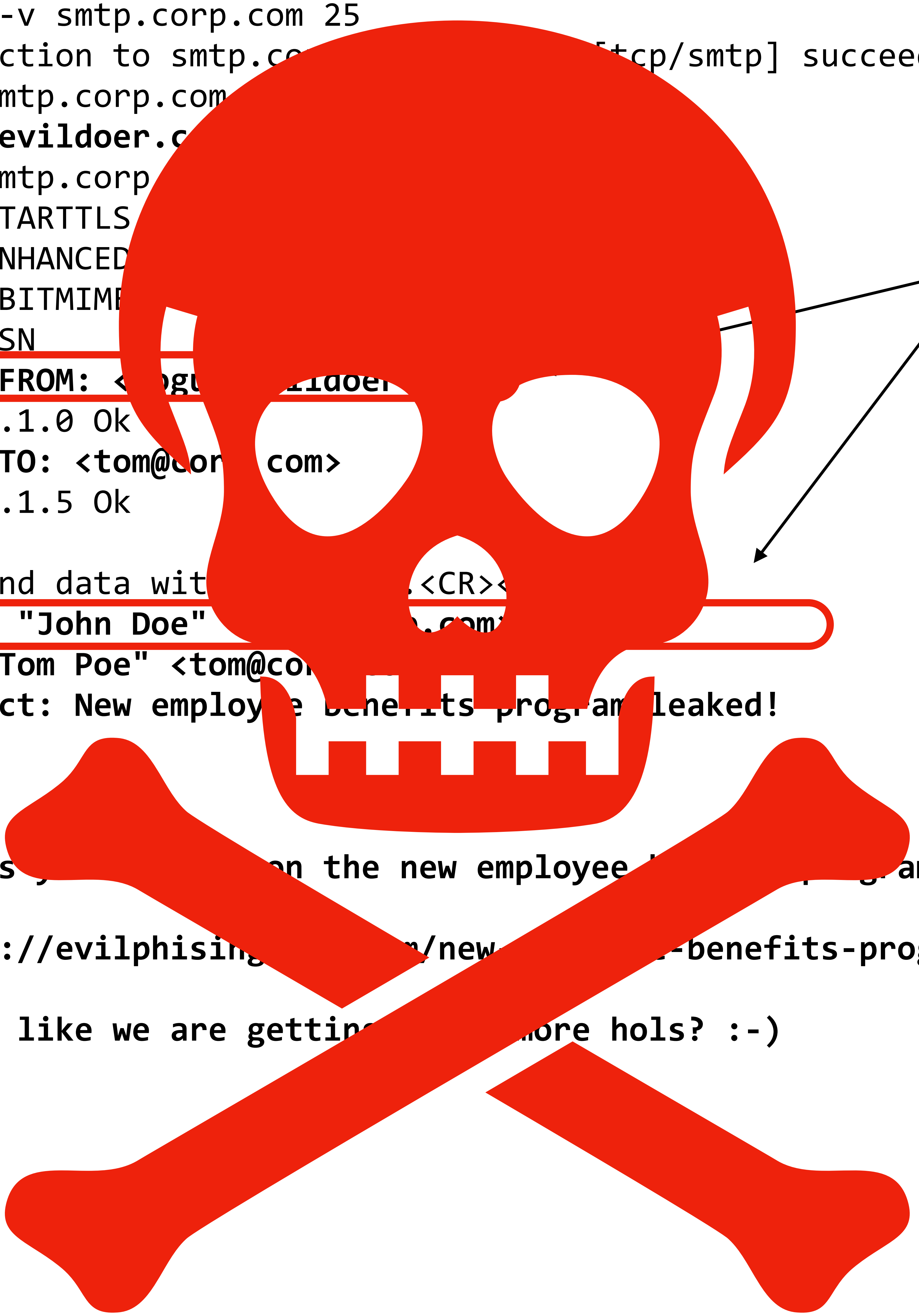
DMARC compares both From

✓

```
$ nc -v smtp.corp.com 25
Connection to smtp.corp.com port 25 [tcp/smtp] succeeded!
220 smtp.corp.com ESMTP
EHLO evildoer.com
250-smtp.corp.com
250-STARTTLS
250-ENHANCEDSTATUSCODES
250-8BITMIME
250-DSN
MAIL FROM: <bogus@evildoer.com>
250 2.1.0 Ok
RCPT TO: <tom@corp.com>
250 2.1.5 Ok
DATA
354 End data with <CR><LF>.<CR><LF>
From: "John Doe" <john@corp.com>
To: "Tom Poe" <tom@corp.com>
Subject: New employee benefits program leaked!

Tom,

What's your stance on the new employee benefit program?

https://evilphisingsite.com/new-employee-benefits-program

Seems like we are getting a lot more hols? :-)

Best,
John
.
```

DMARC
looks for a match

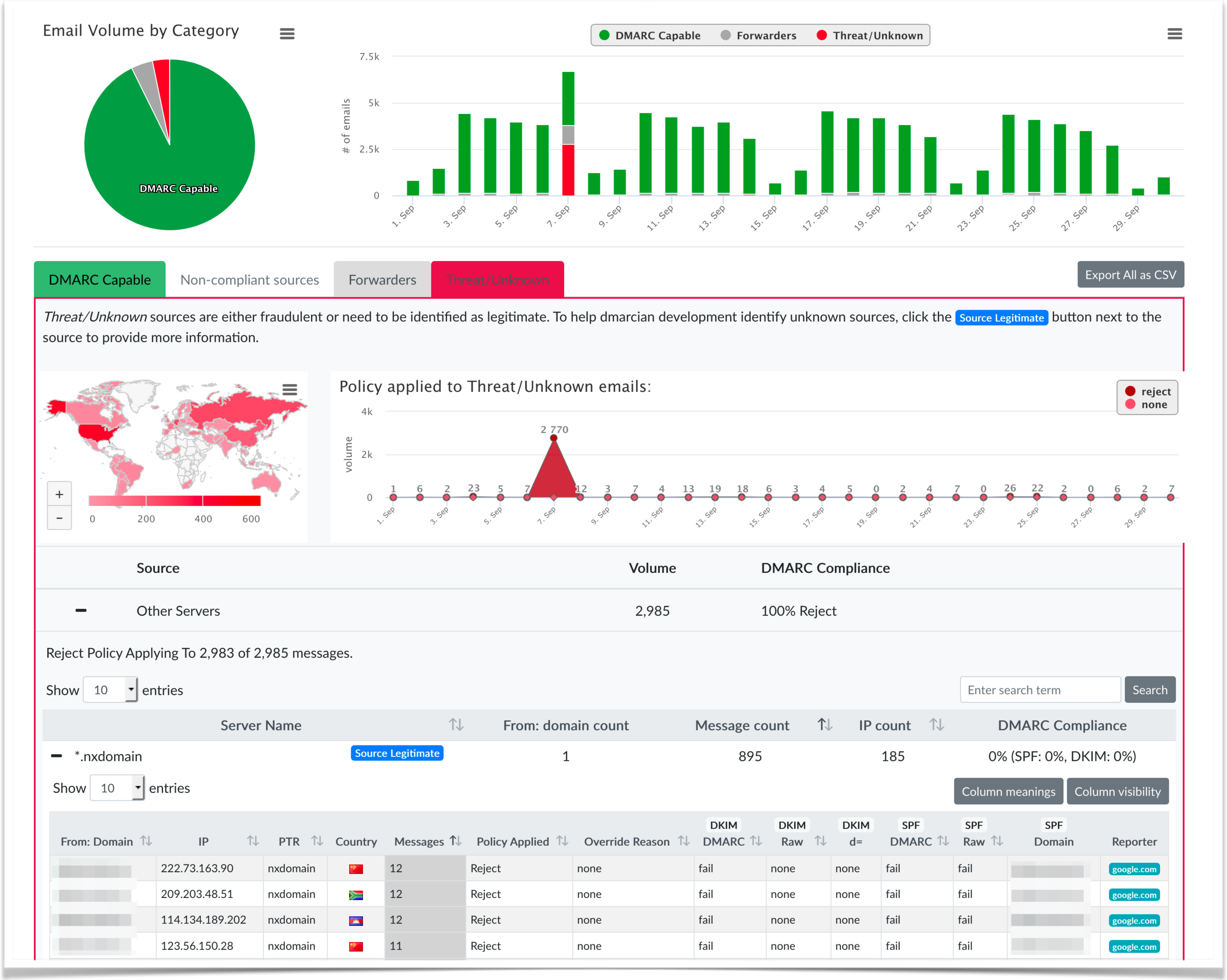
```
$ nc -v smtp.corp.com 25
Connection to smtp.co                  tcp/smtp] succeeded!
220 smtp.corp.com
EHLO evildoer.c
250-smtp.corp
250-STARTTLS
250-ENHANCED
250-8BITMIM
250-DSN
MAIL FROM: < ogu    ildoer
250 2.1.0 Ok
RCPT TO: <tom@cor   com>
250 2.1.5 Ok
DATA
354 End data wit          .<CR><
From: "John Doe"          .com>
To: "Tom Poe" <tom@co
Subject: New employ e benefits program leaked!

Tom,

What's y        n the new employee           am?

https://evilphising        /new        -benefits-program

Seems like we are gettin       more hols? :-)

Best,
John
.
```



DMARC looks for a match

DMARC, the snitch.

```
$ dig _dmarc.xpd.se. txt +short
"v=DMARC1; p=reject; rua=mailto:56756f0475@rep.dmarcanalyzer.com;
ruf=mailto:56756f0475@for.dmarcanalyzer.com; fo=1;"
```



DMARC Capable | Non-compliant sources | Forwarders | Threat/Unknown

Export All as CSV

Threat/Unknown sources are either fraudulent or need to be identified as legitimate. To help dmarcian development identify unknown sources, click the Source Legitimate button next to the source to provide more information.

	Source	Volume	DMARC Compliance
−	Other Servers	2,985	100% Reject

Reject Policy Applying To 2,983 of 2,985 messages.

Show 10 entries

Enter search term Search

	Server Name		From: domain count	Message count	IP count	DMARC Compliance
−	*.nxdomain	Source Legitimate	1	895	185	0% (SPF: 0%, DKIM: 0%)

Show 10 entries

Column meanings | Column visibility

From: Domain	IP	PTR	Country	Messages	Policy Applied	Override Reason	DKIM DMARC	DKIM Raw	DKIM d=	SPF DMARC	SPF Raw	SPF Domain	Reporter
[redacted]	222.73.163.90	nxdomain	🇨🇳	12	Reject	none	fail	none	none	fail	fail	[redacted]	google.com
[redacted]	209.203.48.51	nxdomain	🇿🇦	12	Reject	none	fail	none	none	fail	fail	[redacted]	google.com
[redacted]	114.134.189.202	nxdomain	🇰🇭	12	Reject	none	fail	none	none	fail	fail	[redacted]	google.com
[redacted]	123.56.150.28	nxdomain	🇨🇳	11	Reject	none	fail	none	none	fail	fail	[redacted]	google.com

DMARC bridges the gap between SPF and DKIM

DMARC gives you insight on use

DMARC gives you insight on abuse

Might give you a heads-up

SPF/DKIM/DMARC Recommendations

Move third party senders to a subdomain - marketing.domain.cc

Ensure a clean SPF on apex - domain.cc

Setup DMARC reporting and monitor it

Do a phased roll-out of DMARC - none, quarantine and reject

On quarantine and reject do each phase (1%, 50%, 100%) for two weeks

Trust Issues?

DigiNotar
Internet Trust Services

Trust Issues?

DigiNotar
Internet Trust Services

Symantec

Trust Issues?

DigiNotar
Internet Trust Services

Symantec

Trust Issues?

COMODO

Meet DANE (TLSA)

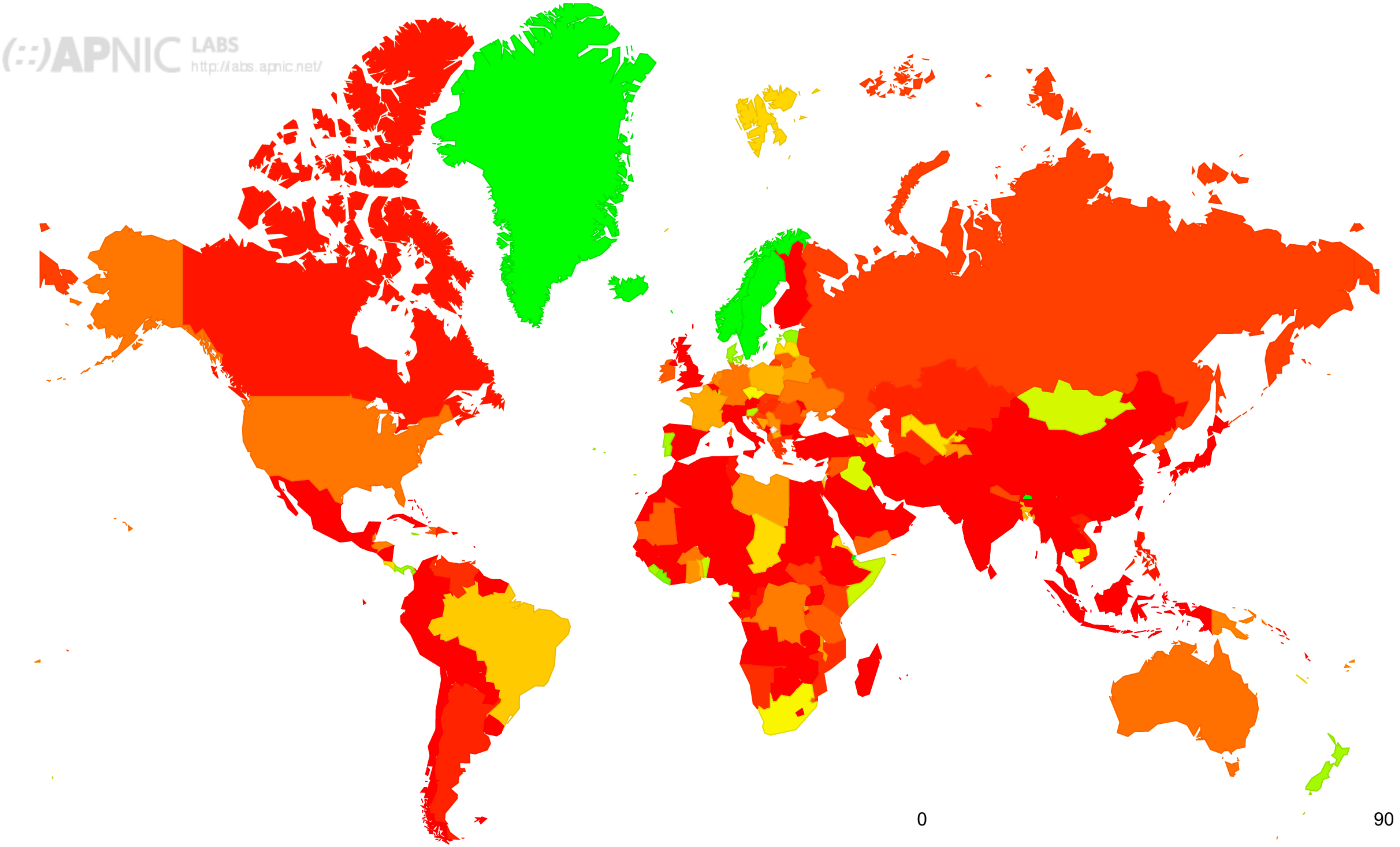
```
$ dig _25._tcp.xpd.se. tlsa
_25._tcp.xpd.se.  3600  IN TLSA  3 1 1
DE88D250D2B461DBFBD8B5C776482C7FFB12655108F5AAB340B59234
45805AD4
```

CAA

```
$ dig storedsafe.com. caa
storedsafe.com.      86400 IN CAA   0 issue "geotrust.com"
storedsafe.com.      86400 IN CAA   0 issue "letsencrypt.org"
storedsafe.com.      86400 IN CAA   0 iodef "mailto:security@storedsafe.com"
storedsafe.com.      86400 IN CAA   0 issue "digicert.com"
```

DNSSEC

DNSSEC Validation Rate by country (%)



The Future
NEXT EXIT

MTA-STS

TLS-RPT

REQUIRETLS

ARC

MTA-STS

```
$ dig _mta-sts.xpd.se. txt
_mta-sts.xpd.se. 300   IN TXT   "v=STSv1; id=20180630;"
```

```
$ curl https://mta-sts.xpd.se/.well-known/mta-sts.txt
version: STSv1
mode: testing
mx: smtp.xpd.se
max_age: 86400
```

TLS-RPT

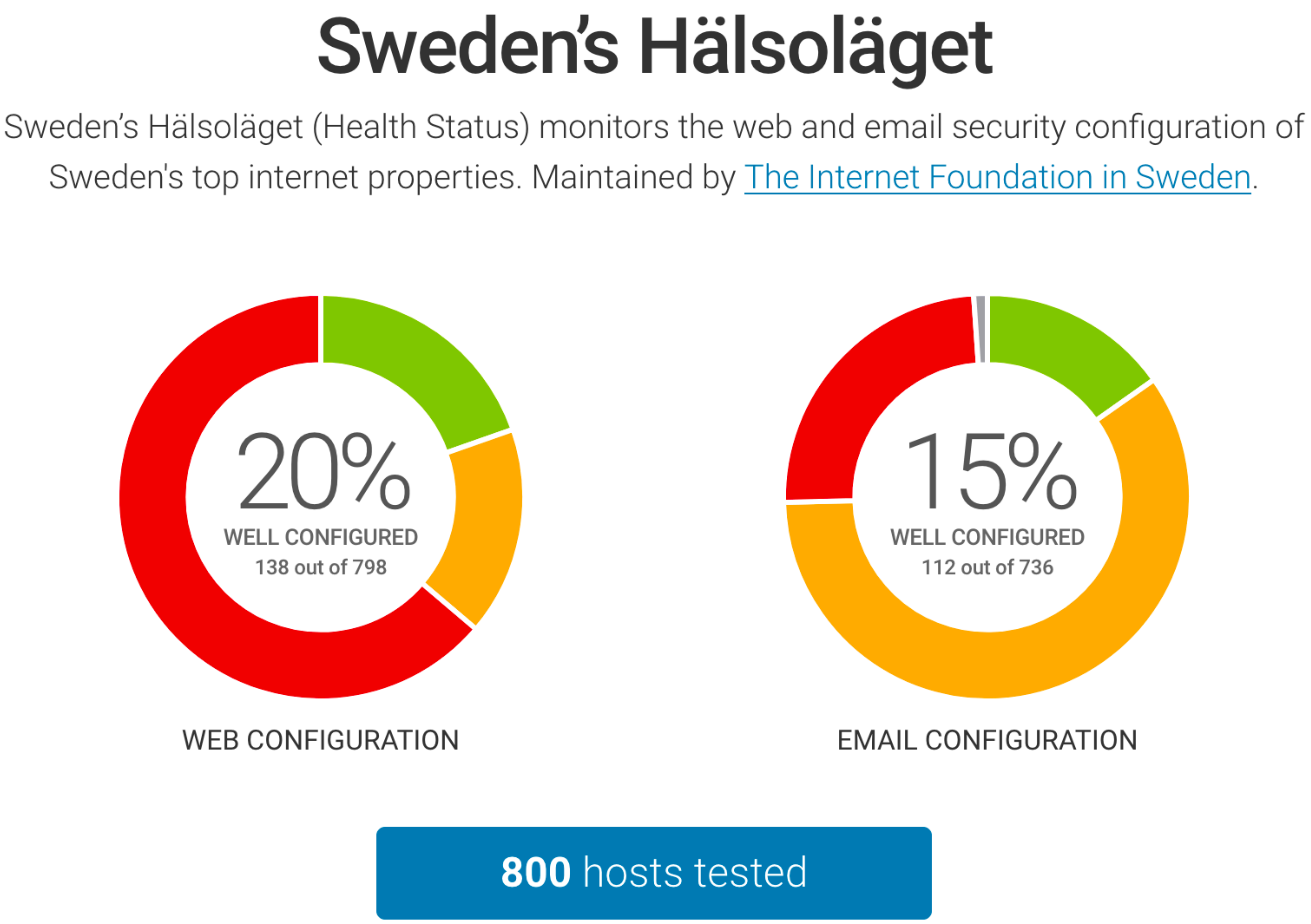
```
$ dig _smtp._tls.xpd.se. txt
_smtp._tls.xpd.se. 3600  IN TXT"v=TLSRPTv1; rua=mailto:mta-sts@xpd.se"
```

REQUIRETLS

```
$ openssl s_client -starttls smtp -connect smtp.corp.com:25
250 DSN
EHLO example.com
250-smtp.corp.com
250-ENHANCEDSTATUSCODES
250-AUTH PLAIN LOGIN
250-DSN
250-REQUIRETLS
MAIL FROM:<user@example.com> REQUIRETLS
250 2.1.0 Ok
```

ARC

State of the nation



Sweden’s Hälsoläget

Sweden’s Hälsoläget (Health Status) monitors the web and email security configuration of Sweden's top internet properties. Maintained by The Internet Foundation in Sweden.

20%
WELL CONFIGURED
138 out of 798

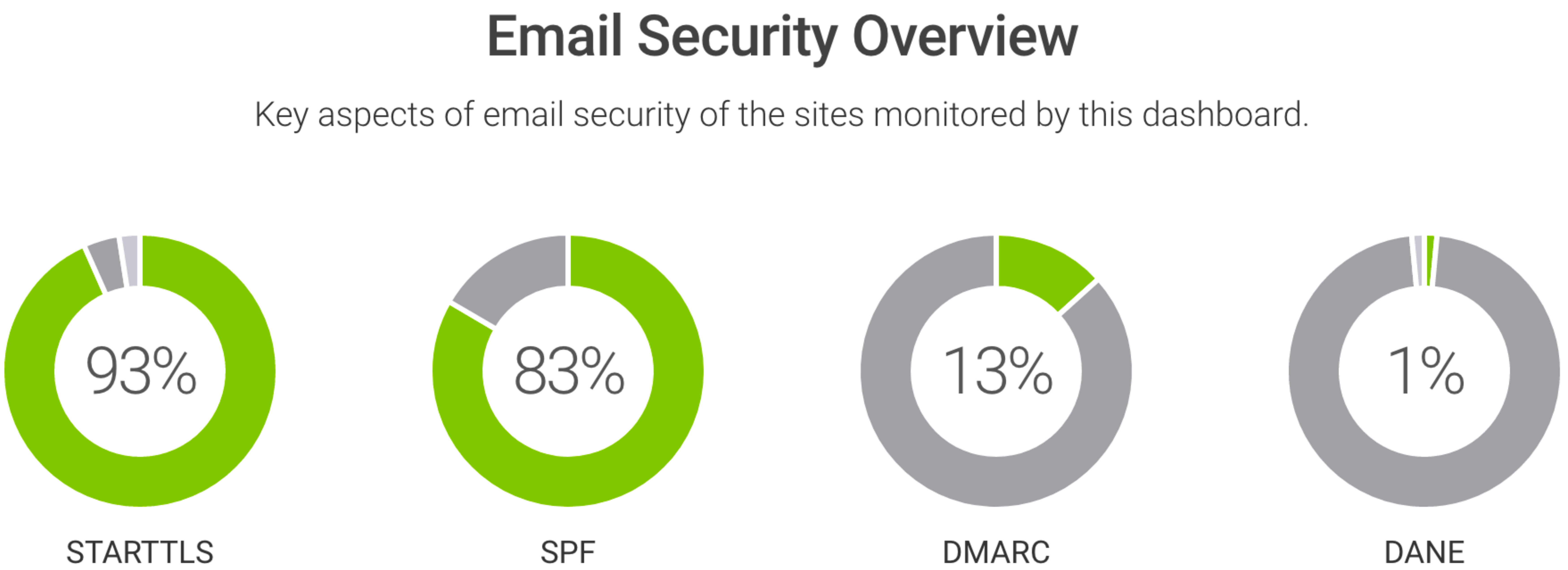
WEB CONFIGURATION

15%
WELL CONFIGURED
112 out of 736

EMAIL CONFIGURATION

800 hosts tested

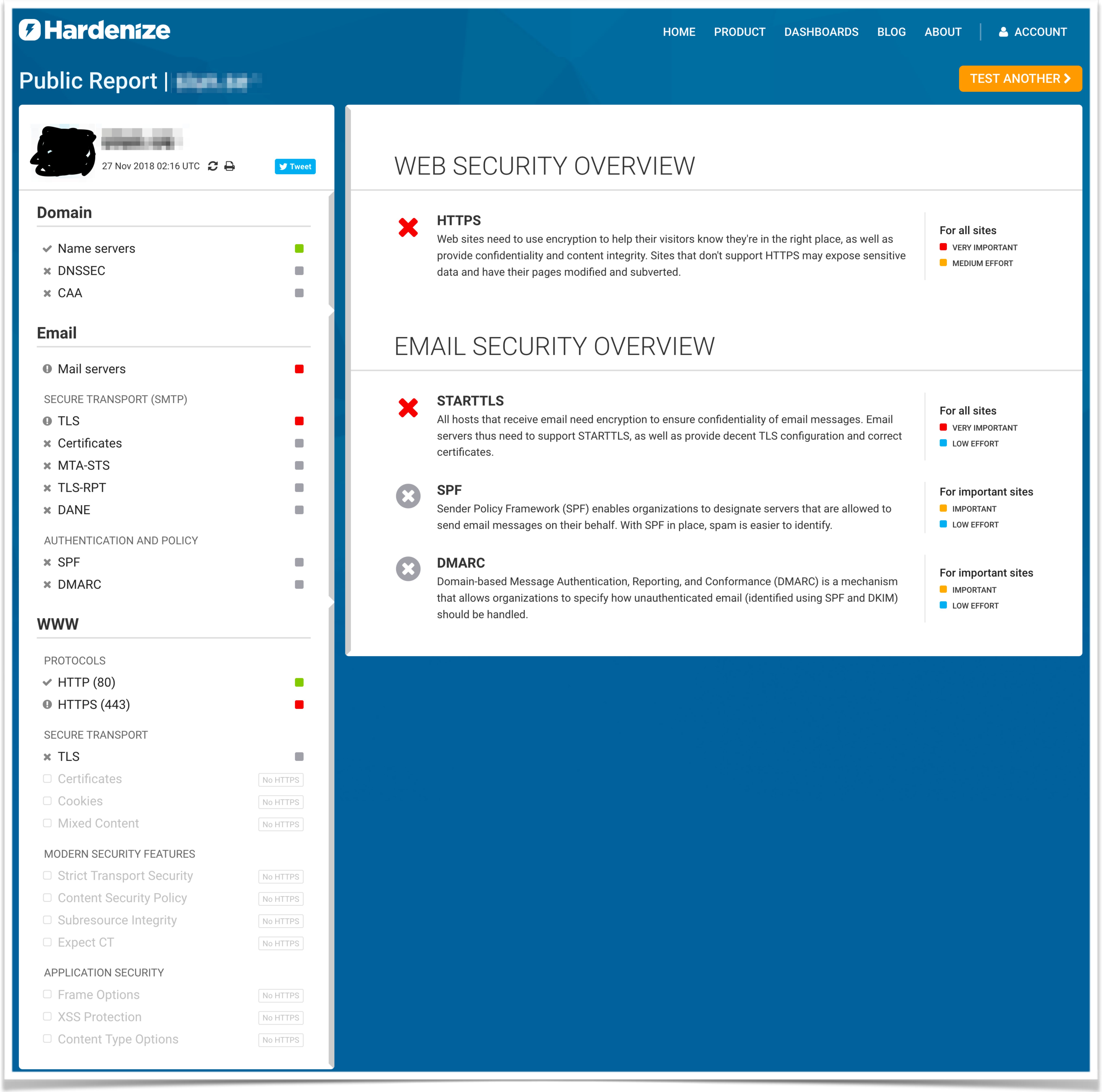
Source hardenize.com



Email Security Overview

Key aspects of email security of the sites monitored by this dashboard.

Source hardenize.com



Public Report | [redacted]

[redacted] [redacted]

27 Nov 2018 02:16 UTC

Domain

- ✓ Name servers 🟩
- ✗ DNSSEC ■
- ✗ CAA ■

Email

- ❗ Mail servers 🟥

SECURE TRANSPORT (SMTP)

- ❗ TLS 🟥
- ✗ Certificates ■
- ✗ MTA-STS ■
- ✗ TLS-RPT ■
- ✗ DANE ■

AUTHENTICATION AND POLICY

- ✗ SPF ■
- ✗ DMARC ■

WWW

PROTOCOLS

- ✓ HTTP (80) 🟩
- ❗ HTTPS (443) 🟥

SECURE TRANSPORT

- ✗ TLS ■
- □ Certificates No HTTPS
- □ Cookies No HTTPS
- □ Mixed Content No HTTPS

MODERN SECURITY FEATURES

- □ Strict Transport Security No HTTPS
- □ Content Security Policy No HTTPS
- □ Subresource Integrity No HTTPS
- □ Expect CT No HTTPS

APPLICATION SECURITY

- □ Frame Options No HTTPS
- □ XSS Protection No HTTPS
- □ Content Type Options No HTTPS

WEB SECURITY OVERVIEW

✗ **HTTPS**

Web sites need to use encryption to help their visitors know they're in the right place, as well as provide confidentiality and content integrity. Sites that don't support HTTPS may expose sensitive data and have their pages modified and subverted.

For all sites
🟥 VERY IMPORTANT
🟧 MEDIUM EFFORT

EMAIL SECURITY OVERVIEW

✗ **STARTTLS**

All hosts that receive email need encryption to ensure confidentiality of email messages. Email servers thus need to support STARTTLS, as well as provide decent TLS configuration and correct certificates.

For all sites
🟥 VERY IMPORTANT
🟦 LOW EFFORT

⊗ **SPF**

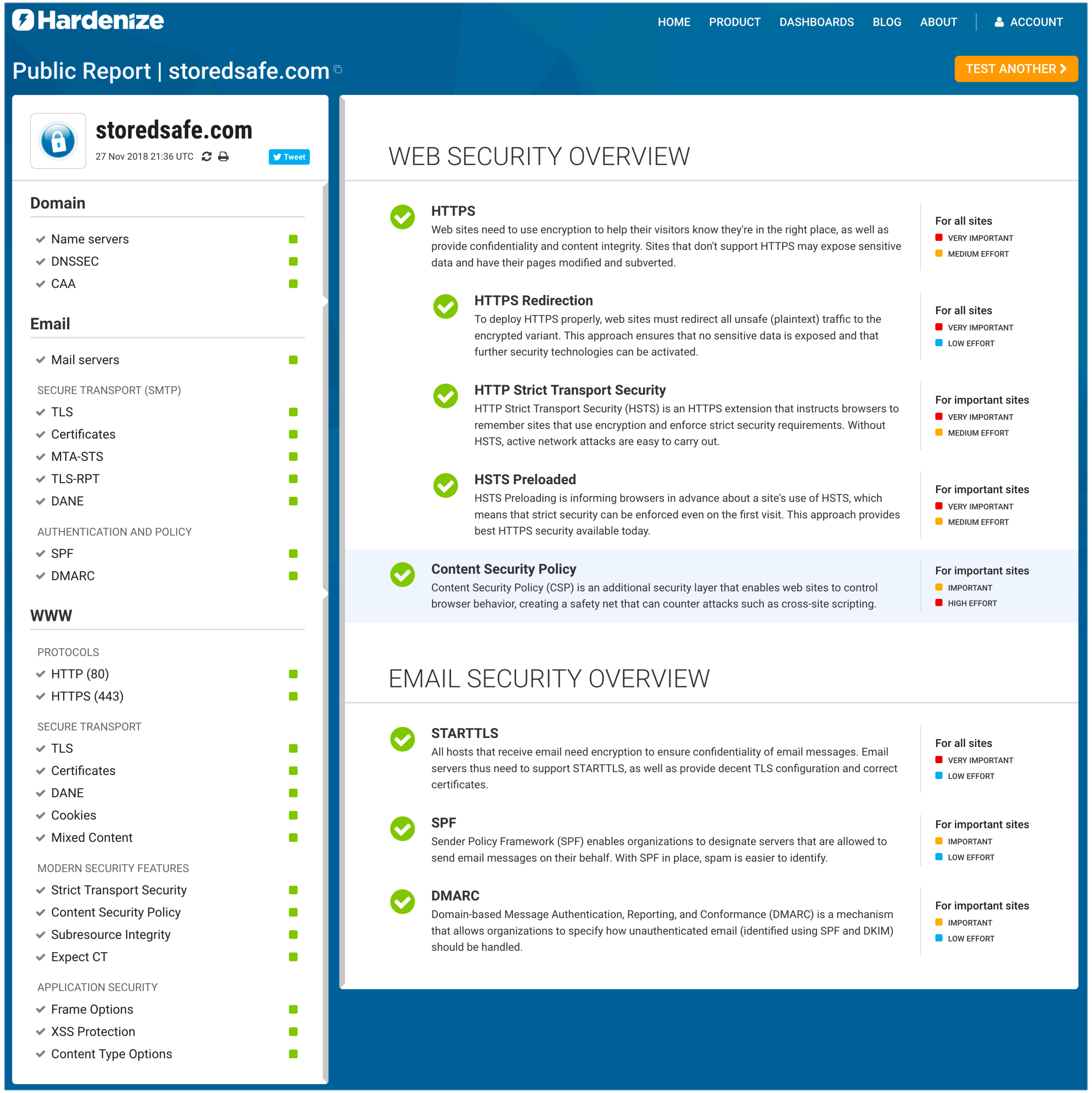
Sender Policy Framework (SPF) enables organizations to designate servers that are allowed to send email messages on their behalf. With SPF in place, spam is easier to identify.

For important sites
🟧 IMPORTANT
🟦 LOW EFFORT

⊗ **DMARC**

Domain-based Message Authentication, Reporting, and Conformance (DMARC) is a mechanism that allows organizations to specify how unauthenticated email (identified using SPF and DKIM) should be handled.

For important sites
🟧 IMPORTANT
🟦 LOW EFFORT



Public Report | storedsafe.com

storedsafe.com

27 Nov 2018 21:36 UTC

Domain

- ✓ Name servers 🟩
- ✓ DNSSEC 🟩
- ✓ CAA 🟩

Email

- ✓ Mail servers 🟩

SECURE TRANSPORT (SMTP)

- ✓ TLS 🟩
- ✓ Certificates 🟩
- ✓ MTA-STS 🟩
- ✓ TLS-RPT 🟩
- ✓ DANE 🟩

AUTHENTICATION AND POLICY

- ✓ SPF 🟩
- ✓ DMARC 🟩

WWW

PROTOCOLS

- ✓ HTTP (80) 🟩
- ✓ HTTPS (443) 🟩

SECURE TRANSPORT

- ✓ TLS 🟩
- ✓ Certificates 🟩
- ✓ DANE 🟩
- ✓ Cookies 🟩
- ✓ Mixed Content 🟩

MODERN SECURITY FEATURES

- ✓ Strict Transport Security 🟩
- ✓ Content Security Policy 🟩
- ✓ Subresource Integrity 🟩
- ✓ Expect CT 🟩

APPLICATION SECURITY

- ✓ Frame Options 🟩
- ✓ XSS Protection 🟩
- ✓ Content Type Options 🟩

WEB SECURITY OVERVIEW

HTTPS

Web sites need to use encryption to help their visitors know they're in the right place, as well as provide confidentiality and content integrity. Sites that don't support HTTPS may expose sensitive data and have their pages modified and subverted.

For all sites
🟥 VERY IMPORTANT
🟧 MEDIUM EFFORT

HTTPS Redirection

To deploy HTTPS properly, web sites must redirect all unsafe (plaintext) traffic to the encrypted variant. This approach ensures that no sensitive data is exposed and that further security technologies can be activated.

For all sites
🟥 VERY IMPORTANT
🟦 LOW EFFORT

HTTP Strict Transport Security

HTTP Strict Transport Security (HSTS) is an HTTPS extension that instructs browsers to remember sites that use encryption and enforce strict security requirements. Without HSTS, active network attacks are easy to carry out.

For important sites
🟥 VERY IMPORTANT
🟧 MEDIUM EFFORT

HSTS Preloaded

HSTS Preloading is informing browsers in advance about a site's use of HSTS, which means that strict security can be enforced even on the first visit. This approach provides best HTTPS security available today.

For important sites
🟥 VERY IMPORTANT
🟧 MEDIUM EFFORT

Content Security Policy

Content Security Policy (CSP) is an additional security layer that enables web sites to control browser behavior, creating a safety net that can counter attacks such as cross-site scripting.

For important sites
🟧 IMPORTANT
🟥 HIGH EFFORT

EMAIL SECURITY OVERVIEW

STARTTLS

All hosts that receive email need encryption to ensure confidentiality of email messages. Email servers thus need to support STARTTLS, as well as provide decent TLS configuration and correct certificates.

For all sites
🟥 VERY IMPORTANT
🟦 LOW EFFORT

SPF

Sender Policy Framework (SPF) enables organizations to designate servers that are allowed to send email messages on their behalf. With SPF in place, spam is easier to identify.

For important sites
🟧 IMPORTANT
🟦 LOW EFFORT

DMARC

Domain-based Message Authentication, Reporting, and Conformance (DMARC) is a mechanism that allows organizations to specify how unauthenticated email (identified using SPF and DKIM) should be handled.

For important sites
🟧 IMPORTANT
🟦 LOW EFFORT

DNS Privacy?
(Slightly off-topic)

DNS over TLS
(DoT)

DNS over HTTPS (DoH)

DNSCrypt

DNS-over-SSH
DNS-over-DTLS
DNS-over-QUIC

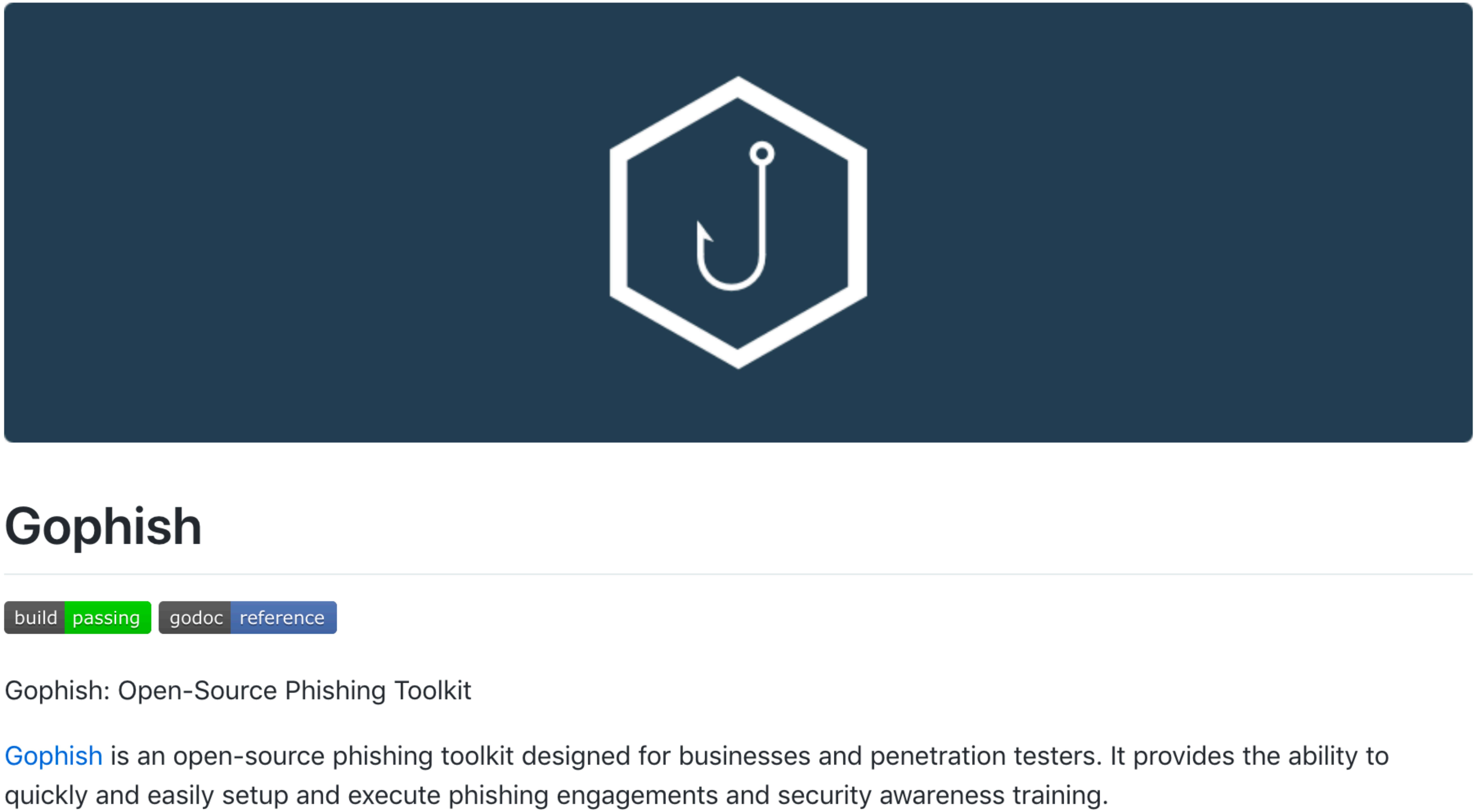
IDEA
PLAN
ACTION

Implement Regular Security Awareness training for your users

You should, really

I’m not kidding

Just do it :-)



Gophish

build passing godoc reference

Gophish: Open-Source Phishing Toolkit

Gophish is an open-source phishing toolkit designed for businesses and penetration testers. It provides the ability to quickly and easily setup and execute phishing engagements and security awareness training.

Implement (or correct) your SPF

Sign your public zones (DNSSEC)

Implement DKIM

Implement DMARC (Phased roll-out)

Publish TLSA records (DANE)

Publish CAA records

DMARC and Office365

reject and quarantine is the same

Default setup of DKIM will cause DMARC fails https://docs.microsoft.com/en-us/office365/securitycompliance/use-dkim-to-validate-outbound-email

https://bit.ly/2P7KEH6+

QUESTIONS?