proofpoint®

Email Fraud

Spoofing and Phishing Risks

Greg Colburn, Director of Engineering

April 9, 2020

Non-proprietary content- Safe for external audience

Who am I

Background

- Role: Director of Engineering
- Studied Computer Science
- Projects:
  - SMBfs on Unix
  - Networking
  - IPv6
  - Virtualization
  - VoIP
  - Systems Engineering
  - Data Processing
  - Email

Places I've worked

digital COMPAQ hp

FONALITY

Return Path

proofpoint®

Proofpoint, Inc. (NASDAQ: PFPT)

Cybersecurity Company

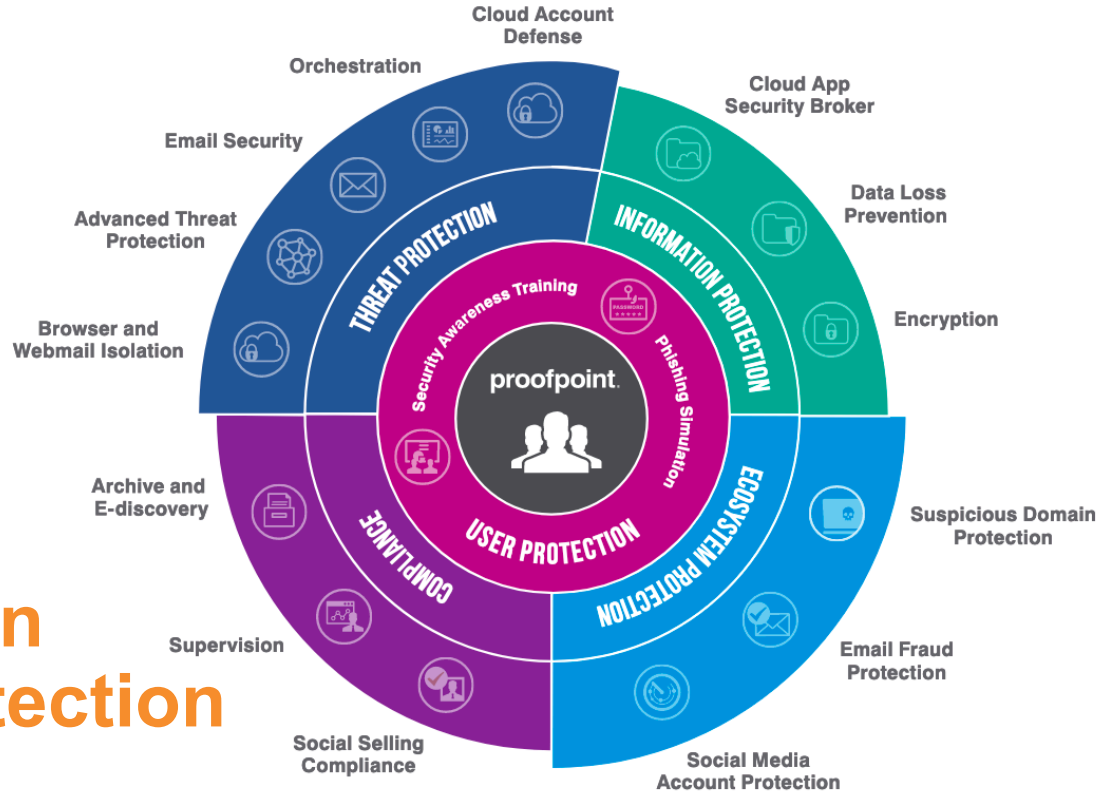
- Based in Sunnyvale, CA
- Offices worldwide
- Founded in 2002

CYBER SECURITY EXCELLENCE AWARDS ★ WINNER ★ 2019

2019 Best Cybersecurity Compa
(between 1,000 to 4,999 employees)

SC 30th ANNIVERSARY

Most Important Cybersecurity Companies of the Last 30 Years



Threat protection
Information protection
User protection
Compliance
Ecosystem protection

Email 101

SMTP

proofpoint.

SMTP

Simple Mail Transfer Protocol

- **TCP** Port 25 (smtp)
- TCP TLS Port 465, 587 (smtps)
- RFC 821 (1982)
- RFC 5321 (2008)

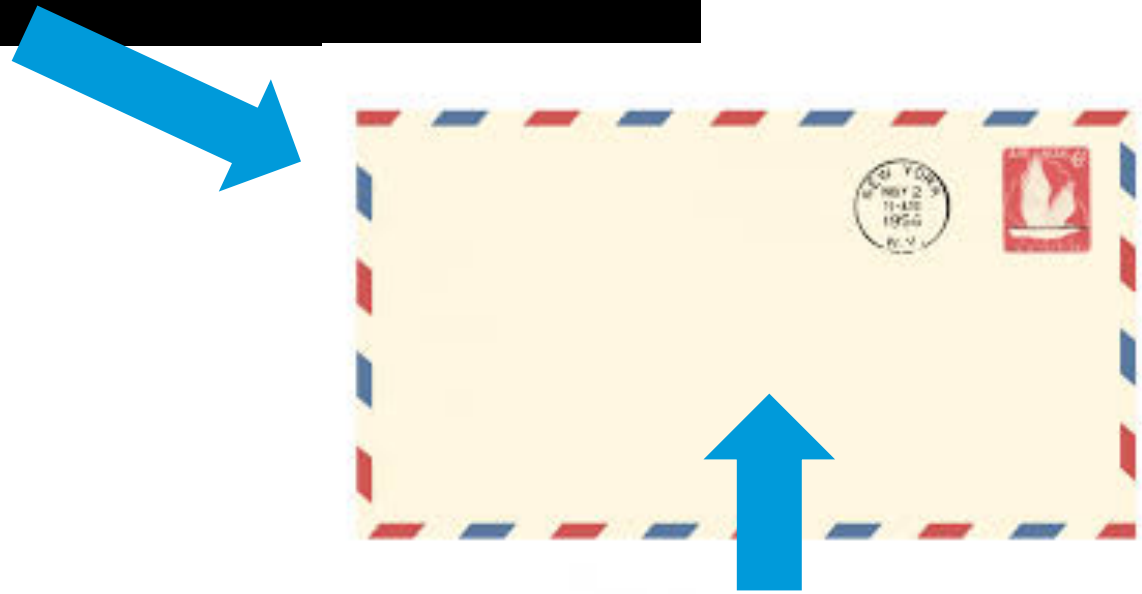
STMP - Conversation

```
telnet mxa-00148501.gslb.pphosted.com 25
Trying 10.20.0.200...
Connected to mxa-00148501.gslb.pphosted.com.
Escape character is '^]'.
220 binky.us.proofpoint.com ESMTP Sendmail 8.14.4/8.14.4; Thu, 25 Oct 2018 08:41:54 -0700
MAIL FROM: bounces@colorado.edu
250 2.1.0 bounces@Colorado.edu... Sender ok
RCPT TO: gcolburn@proofpoint.com
250 2.1.5 gcolburn@proofpoint.com... Recipient ok
DATA
354 Enter mail, end with "." on a line by itself
From: ”Darth Vader” vader@thesith.net
Subject: Training

Greetings young apprentice!  Please practice your Force skills!
.
250 2.0.0 w9PFfs9P006487 Message accepted for delivery
QUIT
221 2.0.0 binky.us.proofpoint.com closing connection
```

SMTP – Envelope

```
MAIL FROM: bounces@colorado.edu
250 2.1.0 bounces@colorado.edu... Sender ok
```



```
RCPT TO: gcolburn@proofpoint.com
250 2.1.5 gcolburn@proofpoint.com... Recipient ok
```

SMTP - Letter

```
DATA
354 Enter mail, end with "." on a line by itself
From: ”Darth Vader” vader@thesith.net
Subject: Training


Greetings young apprentice!  Please practice your
Force skills!

.
250 2.0.0 w9PFfs9P006487 Message accepted for delivery
```

Training

Greetings young apprentice! Please practice your Force skills!

Darth Vader

Reply-to: vader@thesith.net

Email Authentication

SPF, DKIM

proofpoint

Sender Policy Framework (SPF)

”Path Verification” - Who is authorized to sender for Envelope From

Who = IP Address of Sender

Envelope From = bounces@Colorado.edu

hostname	TXT
colorado.edu	"v=spf1 ip4:128.138.1.0/24 ip4:128.138.48.0/20 ip4:128.138.64.0/18 ip4:128.138.128.0/17 ip4:204.228.68.242 ip4:132.194.255.30 include:_spf1.colorado.edu ~all"
spf1.colorado.edu	"v=spf1 ip4:216.69.106.22 ip4:216.177.90.7 ip4:13.111.53.159 ip4:198.37.147.217 include:_spf.google.com include:spf.protection.outlook.com ~all"

Domain Keys Identified Mail (DKIM)

Sign parts of header and body to ensure message does not change in transit

```
DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed;
        d=colorado.edu; s=google;
        h=mime-version:references:in-reply-to:reply-to:from:date:message-
id:subject:to;
        bh=HiR8NYGGGywdx5d9XCaoNbeJJf5mpP0RWD16R2Q3SkY=;
        b=cVCA+uqkH92Enx6mcgVtbohDjntC0UtnM/X6LHqYhYzERtwpo4FsWprYY/DTKHrLJR
         f+QlD1ITDzQZtRjdpYU6ApSa+oomXEsj6z1ZU9zlecEYYEQBOVF79GEENBuY0+Wh+xrb
         QPgdVXavIIXc81tV76HSMSfcsR1MWczzPFYsRRFFACTCcuZM5zAhYZD3krnjesulxQwT
         f2ErAoV9gLmRfLl9m0f1KLwP6gYnWO4bddf94bLKnuD8D7avuVhMqbhOokoOkt7R5v+j
         PGgG+sP8tZgNOXAcWoaDxx2nVZB2ILRnL4iy9ScL2XqRePirNf30EA3lHrrcqo0Rp1Lw
         Ff+w==
```

Domain Keys Identified Mail (DKIM)

hostname	TXT
google._domainkey.colorado.edu	"v=DKIM1; k=rsa; p=MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAiB9xMzToz+El7oDglrlHbZk7Tmz0cfxNPR5nzZSAeKBWlH7DMt/FiVG" "E8C2Qhgrqad3OMAddixm9s4UyztMWj5rXqIy0IK+ALH5JdVCPuNAXHHLXF1B4QizNj6PKVVcAJ6hnvuslV7hKDv4+9zUVJa2FSrgrEUEockpSmN6cJB2q" "WIef6xYKN1IEDCg/4Q8OmDiiu5RaB+lzFDrAE9vTrKKa58Ms8QcX4TRF1f9kzVvrpEMGdOk6d6v0Zmva/bLV0Hr/79keJZuDOa1KQp/KQVDssHVuPAuwVG6PSO6AwT7DWPcMoUPJm5moIMbIo2/ldg9BsTUW4DWBGZfG85q55QIDAQAB”

Email Spoofing

DMARC

proofpoint

Problem: No relationship between letter and envelope

DMARC

Domain-based Message Authentication, Reporting & Conformance

hostname	TXT
_dmarc.thesith.net	empty
_dmarc.colorado.edu	"v=DMARC1; p=none; pct=100; rua=mailto:dmarc_agg@vali.email; sp=none; aspf=r;"
_dmarc.proofpoint.com	"v=DMARC1; p=reject; sp=reject; fo=1; rua=mailto:dmarc_rua@emaildefense.proofpoint.com; ruf=mailto:dmarc_ruf@emaildefense.proofpoint.com"

DMARC

Policy applied to traffic

- If SPF pass and SPF align
  - Or --
- If DKIM Pass and DKIM Align
  - Then apply policy to email specified by p= flag in DMARC record.

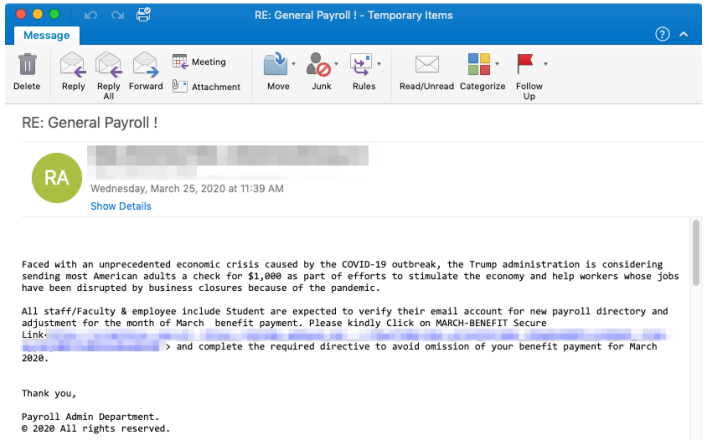
Covid-19

proofpoint.

COVID-19 Payment lures

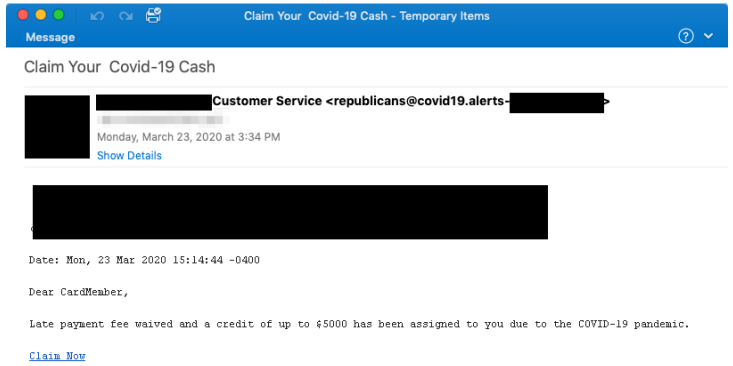
Governments

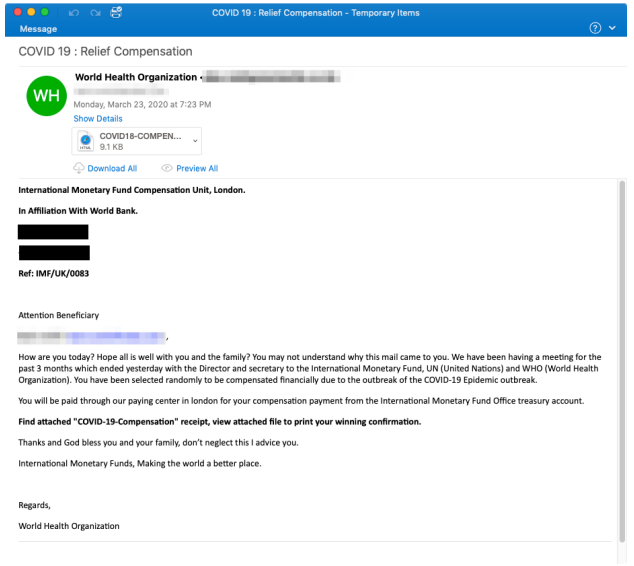
Recipients are directed to verify their information for the "new payroll directory" by clicking the malicious link in the email.



Credit Card Companies

"Claim Your Covid-19 Cash"





Nonprofits Organizations

"been randomly selected to be compensated financially due to the outbreak of the COVID-19 Epidemic outbreak"

Protect yourself

1. Be aware that you are at risk
2. Be wary of any emails, text messages, social media communications, or phone calls you receive that promise stimulus payments.
3. Don’t provide your bank account number, usernames/passwords, social security number, or other personal information in response to any online requests — and avoid clicking on email links.
4. Create unique usernames and passwords for each account.
5. Verify websites are legitimate.
6. Avoid disinformation with multiple sources.

Ref: https://www.proofpoint.com/us/security-awareness/post/six-ways-protect-yourself-covid-19-payment-fraud-attempts

proofpoint®

We're hiring

gcolburn@proofpoint.com

https://www.proofpoint.com/careers