proofpoint | Protect People.
Defend Data.

Adopting AI/ML to Address Human-Centric Risks

Adrian Covich
Senior Director, Systems Engineering APJ
Proofpoint

HUMAN CENTRIC CYBER SECURITY

Introducing Proofpoint

HUMAN CENTRIC CYBER SECURITY

Financial Strength

$1.87B
Proofpoint Revenue

98%
Recurring Revenue

21%
Percentage of Revenue Reinvested in R&D

4.4K
WW employees, hiring continues

Market Adoption

>510K
Customers

150+
Global ISP and Mobile Operators

87%
F100 Protected by Proofpoint

>60%
F1000 Protected by Proofpoint

#2
DLP market share

47%
F100 using Proofpoint DLP

Proofpoint's Data

People Protection

3.1T
Emails scanned per year

>1.4T
SMS/MMS scanned per year

0.8T
Attachments scanned per year

21T
URLs scanned per year

Information Protection

15.7M
Annual total archive searches

>41%
F1000 emails authenticated by Proofpoint

69P
Petabytes of archive data under management

>183M
Phishing simulations sent per year

66M
BEC attacks stopped per month

116M
Telephone Oriented Attacks stopped per year

160+ and 0
Win rate over Red Teams in Identity Threat

45M
M365/Google accounts monitored for takeover detections

proofpoint.

Let’s Talk About Two Challenges Today

HUMAN CENTRIC CYBER SECURITY

Phishing and Business Email Compromise

#1 Method of Cyber Breach in Australia H2 2023 (OIAC)

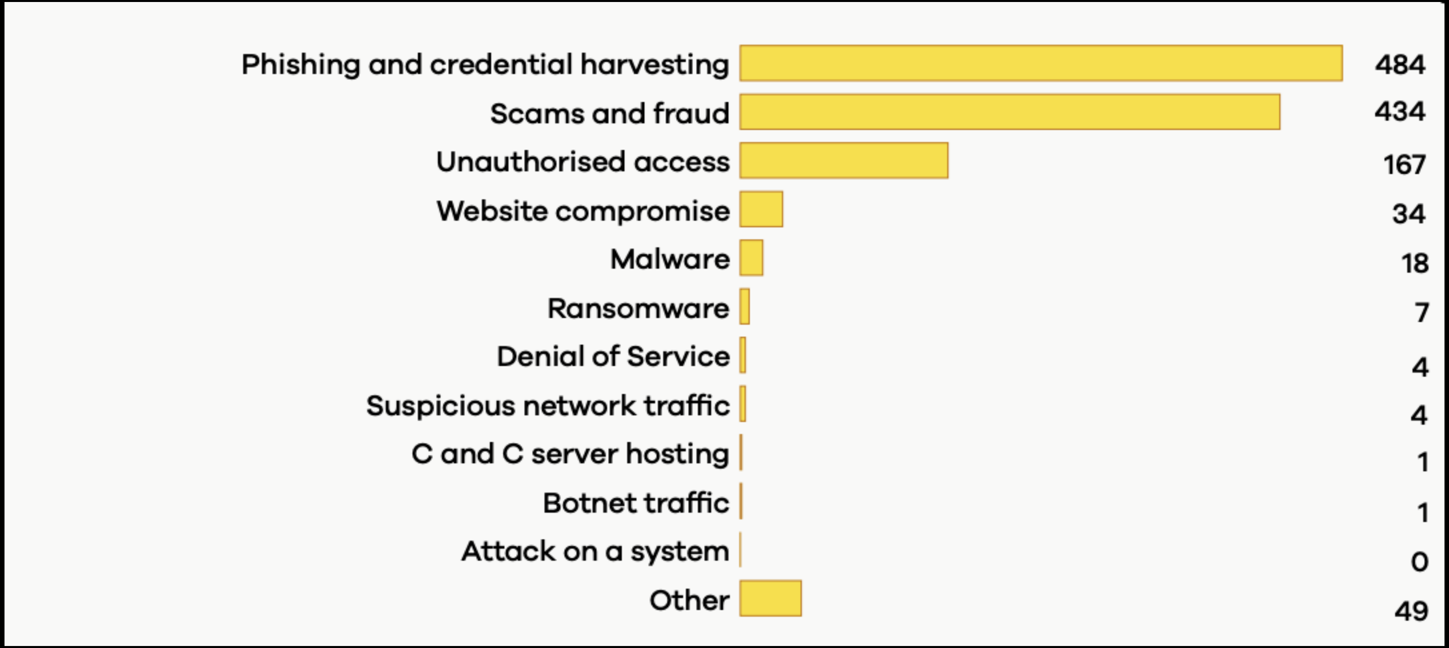
Costing Australian organisations over $220 Million Dollars annually (ACCC 2022)

Accidental Data Disclosure via Email

#1 cause of PII loss incidents via Human Error H2 2023 (OIAC)

What's Targeting New Zealanders?

HUMAN CENTRIC CYBER SECURITY



https://www.cert.govt.nz/assets/Uploads/Quarterly-report/2024-q2/Cyber-Security-Insights-Q2-2024.pdf

Link to Report

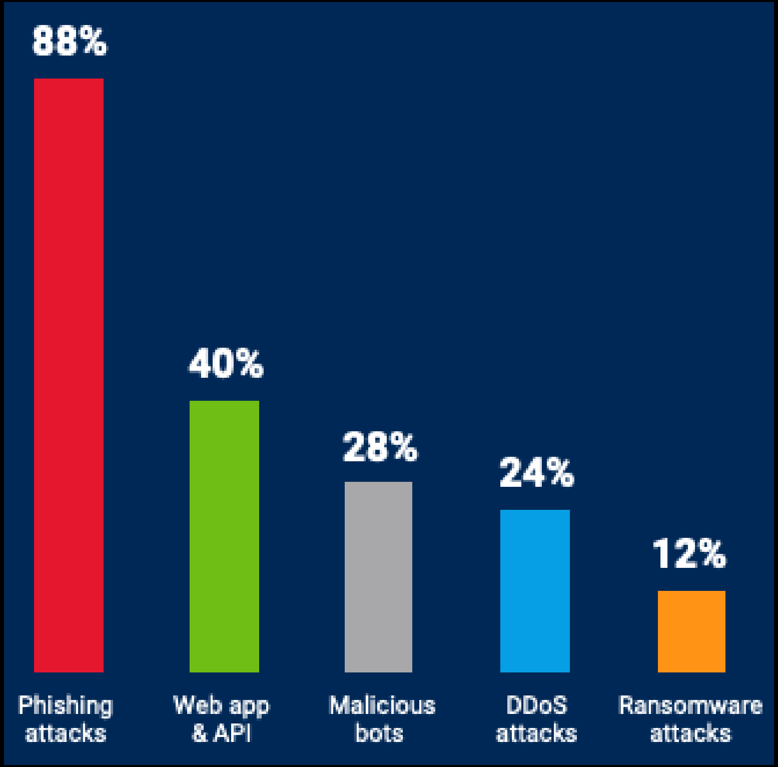
Australia

Akamai Financial Services Report

2023

Reported cyber attacks over a period of 12 months, by Australia FinServ organizations.

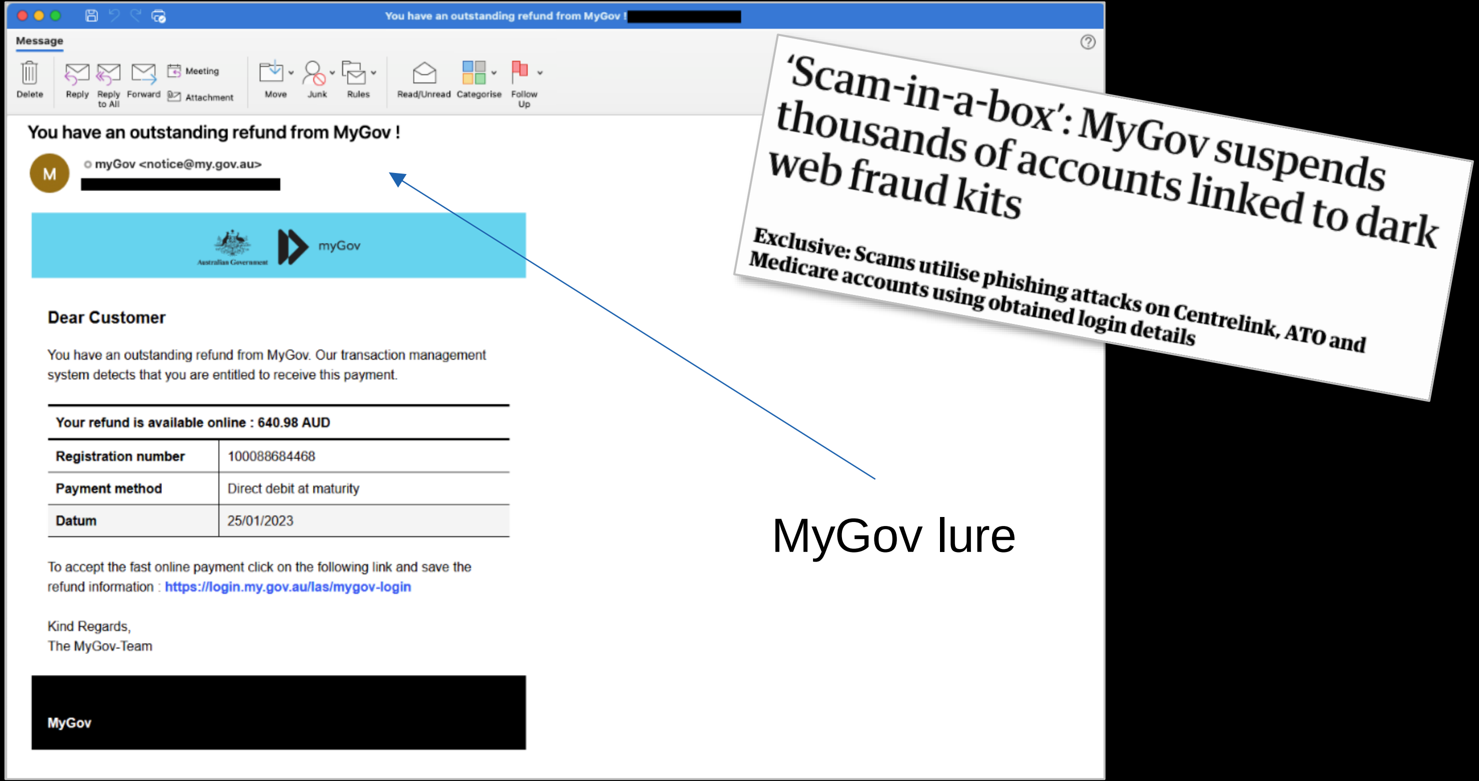
Phishing attacks at the top with 88%.[1]



[1] ”Cybersecurity in Financial Services Australia." *Akamai* link

Credential Phishing Targeting Users

HUMAN CENTRIC CYBER SECURITY



You have an outstanding refund from MyGov ! [redacted]

You have an outstanding refund from MyGov !

myGov <notice@my.gov.au>
[redacted]

Dear Customer

You have an outstanding refund from MyGov. Our transaction management system detects that you are entitled to receive this payment.

Your refund is available online : 640.98 AUD	
Registration number	100088684468
Payment method	Direct debit at maturity
Datum	25/01/2023

To accept the fast online payment click on the following link and save the refund information : https://login.my.gov.au/las/mygov-login

Kind Regards,
The MyGov-Team

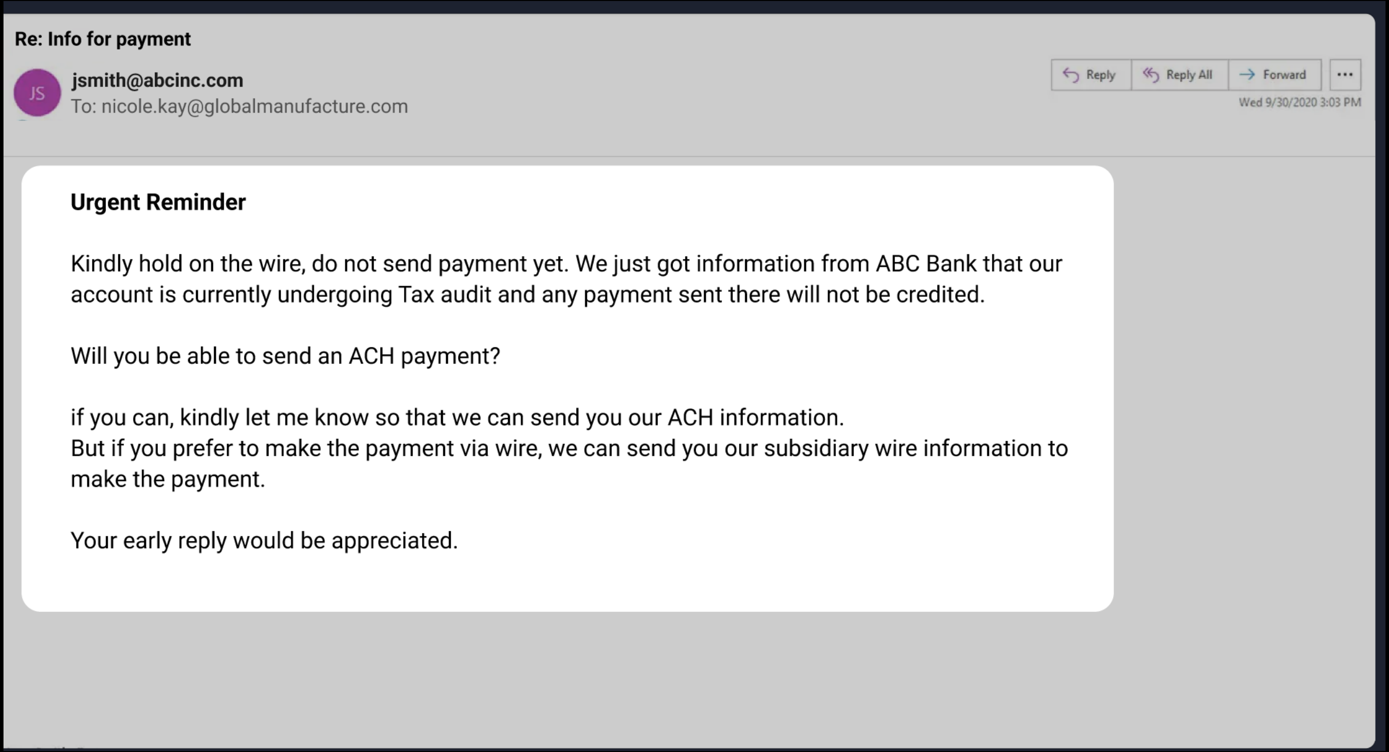
MyGov

'Scam-in-a-box': MyGov suspends thousands of accounts linked to dark web fraud kits

Exclusive: Scams utilise phishing attacks on Centrelink, ATO and Medicare accounts using obtained login details

MyGov lure

How can AI and LLM Help?



Re: Info for payment

jsmith@abcinc.com
To: nicole.kay@globalmanufacture.com

Wed 9/30/2020 3:03 PM

Urgent Reminder

Kindly hold on the wire, do not send payment yet. We just got information from ABC Bank that our account is currently undergoing Tax audit and any payment sent there will not be credited.

Will you be able to send an ACH payment?

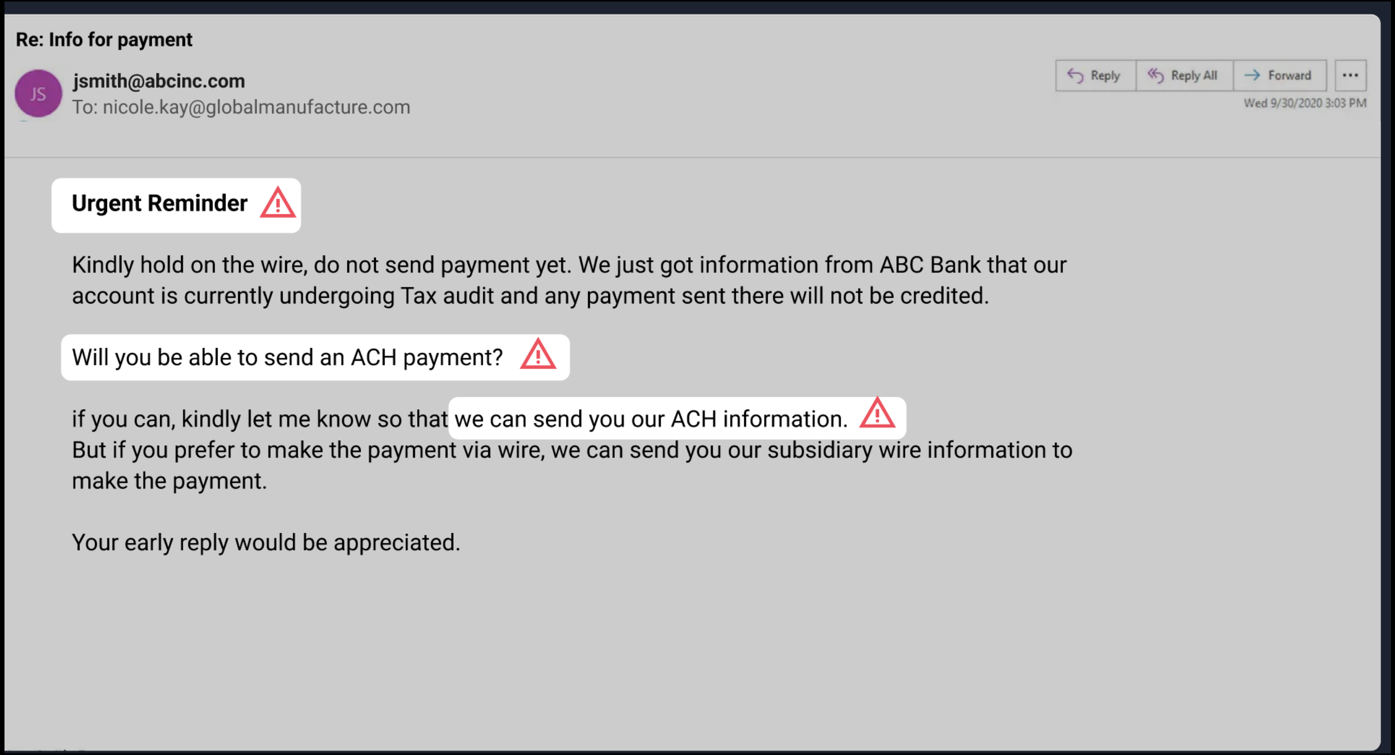
if you can, kindly let me know so that we can send you our ACH information.
But if you prefer to make the payment via wire, we can send you our subsidiary wire information to make the payment.

Your early reply would be appreciated.

This is a difficult type of email to spot

It has no malware, talks about financial transactions in an official way - similar to a normal email.

How can AI and LLM Help?



Re: Info for payment

JS **jsmith@abcinc.com**
To: nicole.kay@globalmanufacture.com

Wed 9/30/2020 3:03 PM

Urgent Reminder ⚠

Kindly hold on the wire, do not send payment yet. We just got information from ABC Bank that our account is currently undergoing Tax audit and any payment sent there will not be credited.

Will you be able to send an ACH payment? ⚠

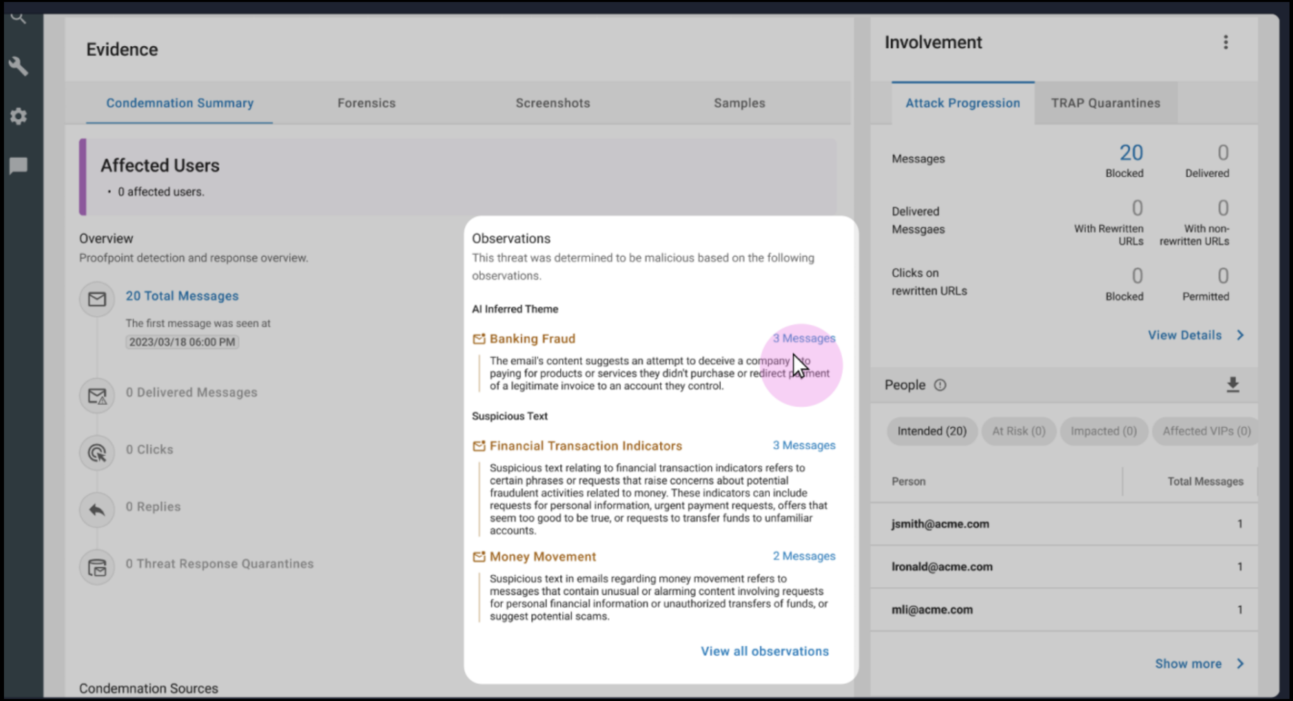
if you can, kindly let me know so that we can send you our ACH information. ⚠
But if you prefer to make the payment via wire, we can send you our subsidiary wire information to make the payment.

Your early reply would be appreciated.

LLMs help us highlight key phrases (not new) but also allow us to understand the intent of the email.

We use this in combination with other factors (previous history, characteristics) to spot the fraud

How can AI and LLM Help?



Affected Users

- 0 affected users.

Overview

Proofpoint detection and response overview.

20 Total Messages

The first message was seen at 2023/03/18 06:00 PM

0 Delivered Messages

0 Clicks

0 Replies

0 Threat Response Quarantines

Condemnation Sources

Observations

This threat was determined to be malicious based on the following observations.

AI Inferred Theme

Banking Fraud 3 Messages

The email's content suggests an attempt to deceive a company to paying for products or services they didn't purchase or redirect payment of a legitimate invoice to an account they control.

Suspicious Text

Financial Transaction Indicators 3 Messages

Suspicious text relating to financial transaction indicators refers to certain phrases or requests that raise concerns about potential fraudulent activities related to money. These indicators can include requests for personal information, urgent payment requests, offers that seem too good to be true, or requests to transfer funds to unfamiliar accounts.

Money Movement 2 Messages

Suspicious text in emails regarding money movement refers to messages that contain unusual or alarming content involving requests for personal financial information or unauthorized transfers of funds, or suggest potential scams.

Messages	20 Blocked	0 Delivered
Delivered Messgaes	0 With Rewritten URLs	0 With non-rewritten URLs
Clicks on rewritten URLs	0 Blocked	0 Permitted

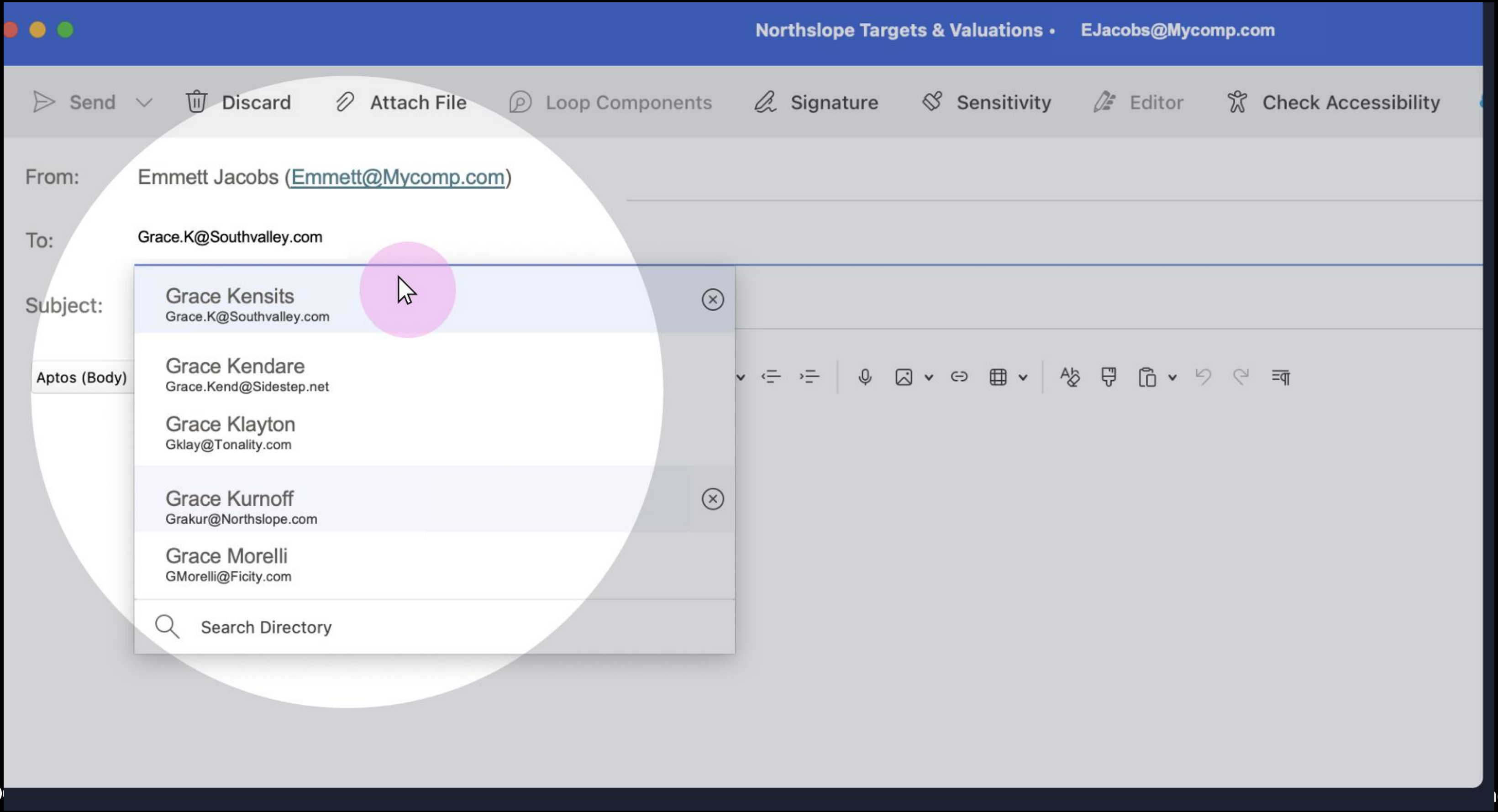
Person	Total Messages
jsmith@acme.com	1
lronald@acme.com	1
mli@acme.com	1

AI then allows us to understand the threat and gives us human instructions on why it was stopped

Further, it gives us the ability to suggest next steps and further action

Now Moving onto Accidental Email Loss

Misdirected Email – A Common Problem



Northslope Targets & Valuations • EJacobs@Mycomp.com

From: Emmett Jacobs (Emmett@Mycomp.com)

To: Grace.K@Southvalley.com

Subject:

Grace Kensits
Grace.K@Southvalley.com

Grace Kendare
Grace.Kend@Sidestep.net

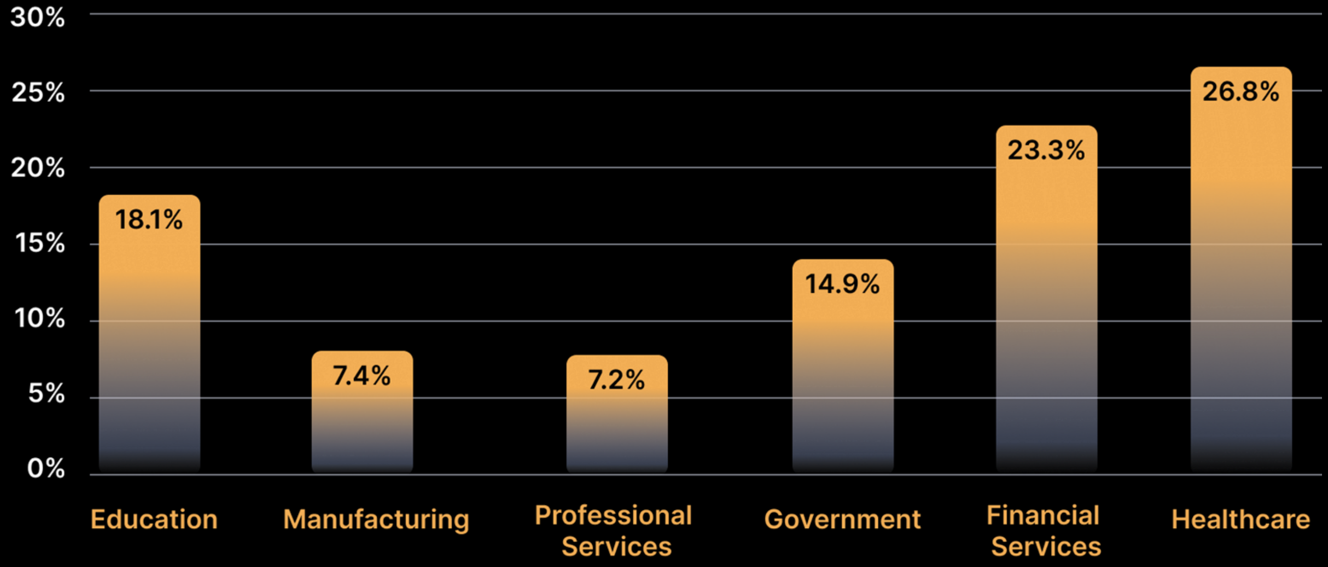
Grace Klayton
Gklay@Tonality.com

Grace Kurnoff
Grakur@Northslope.com

Grace Morelli
GMorelli@Ficity.com

Reminder: How big is the risk?

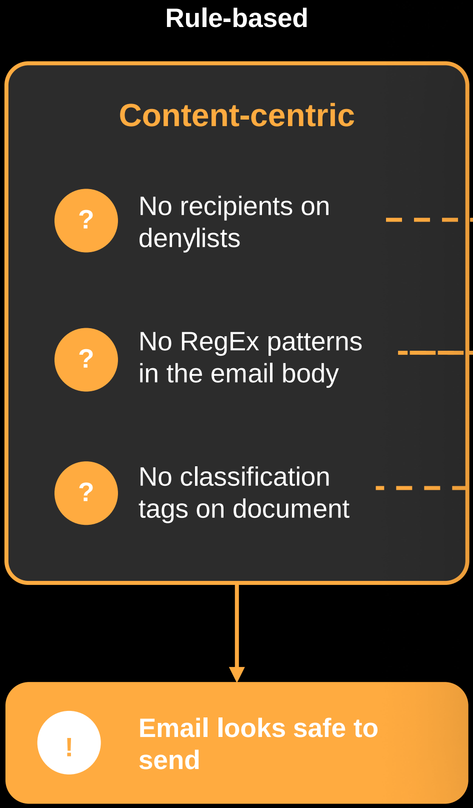
Email Misdelivery as % of Data Breaches



Source: 2022 Verizon DBIR

How can AI Help?

Rule-based Email DLP Systems Are Blind to Many Data Loss Incidents



Rule-based

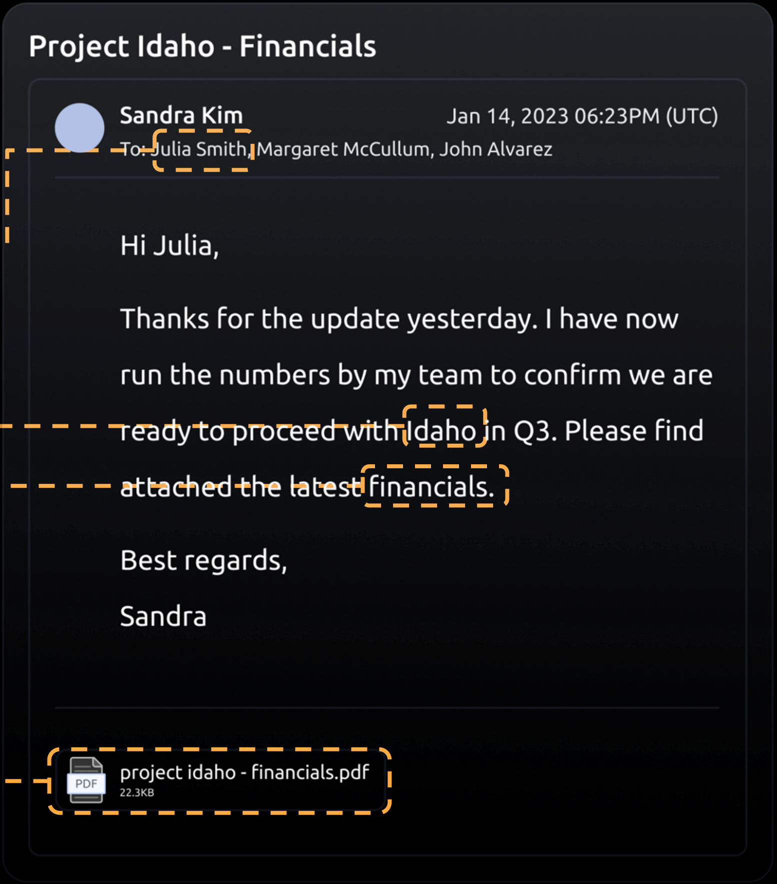
Content-centric

? No recipients on denylists

? No RegEx patterns in the email body

? No classification tags on document

! **Email looks safe to send**



Project Idaho - Financials

Sandra Kim   Jan 14, 2023 06:23PM (UTC)

To: Julia Smith, Margaret McCullum, John Alvarez

Hi Julia,

Thanks for the update yesterday. I have now run the numbers by my team to confirm we are ready to proceed with Idaho in Q3. Please find attached the latest financials.

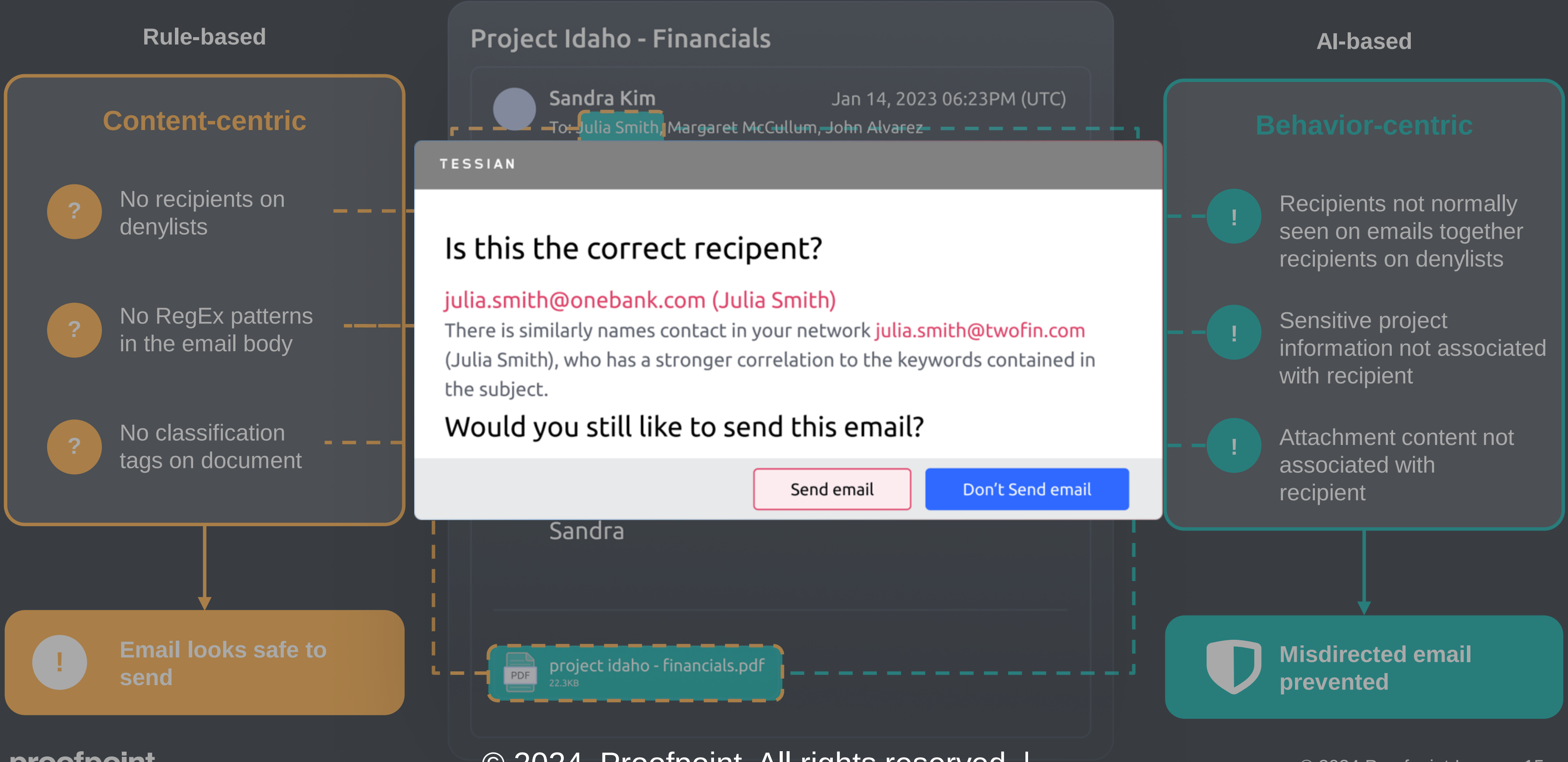
Best regards,

Sandra

project idaho - financials.pdf
22.3KB

proofpoint.

Adaptive Email DLP Automatically Detects What Rule-based DLP Misses



Rule-based

Content-centric

- ? No recipients on denylists
- ? No RegEx patterns in the email body
- ? No classification tags on document

! **Email looks safe to send**

Project Idaho - Financials

Sandra Kim

Jan 14, 2023 06:23PM (UTC)

To: Julia Smith, Margaret McCullum, John Alvarez

TESSIAN

Is this the correct recipent?

julia.smith@onebank.com (Julia Smith)

There is similarly names contact in your network julia.smith@twofin.com (Julia Smith), who has a stronger correlation to the keywords contained in the subject.

Would you still like to send this email?

Sandra

AI-based

Behavior-centric

- ! Recipients not normally seen on emails together recipients on denylists
- ! Sensitive project information not associated with recipient
- ! Attachment content not associated with recipient

Misdirected email prevented

Want more Information?

Come & see us at the **Proofpoint Booth**

We have an incentive to drop by as well….

Enter to Win!

Cloudy Bay
Deluxe Wine Hamper

1 x Bottle Cloudy Bay Sauvignon Blanc Wine
1 x Bottle Cloudy Bay Pinot Noir Wine
1 x Bottle Cloudy Bay Pelorus Sparkling Wine
1 x Bottle Cloudy Bay Chardonnay Wine

★★★★★ 5 STARS

MASTER SOMMELIER 93-94 EXCELLENT CamDouglasMS

FINE WINES OF NEW ZEALAND

nzwinerater.com NEW ZEALAND NZ Wine Rater Excellent 93+

proofpoint.

proofpoint®

Protect People.
Defend Data.