IT RCSA - Infrastructure

Entity	Apple Bank
Test Name	IT Infrastructure
Test Date	4/9/2021
Process	IT-IFR-P15 Information Transfer
Sub-process	E-Mail Security
Risk # and Description	IT-IFR-R15 - Inbound and outbound emails may not be appropriately protected, therefore exposing the bank to data loss (DL) and other threats such as business disruption and malware attacks. Furthermore, access controls to the mail infrastuctire may not be sufficient to prevent unauthorized individuals from gaining entry into the Bank's Email System
Control # and Description	**IT-IFR-C23 E-Mail Security** E-mails and e-mail systems are protected from unauthorized access, modification or denial of service, spam and phishing emails, malicious e-mails, attachments and the leaking of non-public information. E-mails with non-public information must be authorized. Its information is masked or encrypted.
Level of Risk	High
Control Frequency	As Needed
Process Owner	Debi Gupta
Procedures to ValidatePopulation	Inquiry, Observation, Inspection
SII(s) or Exception(s) Number(s)	Self Reported by Information Security

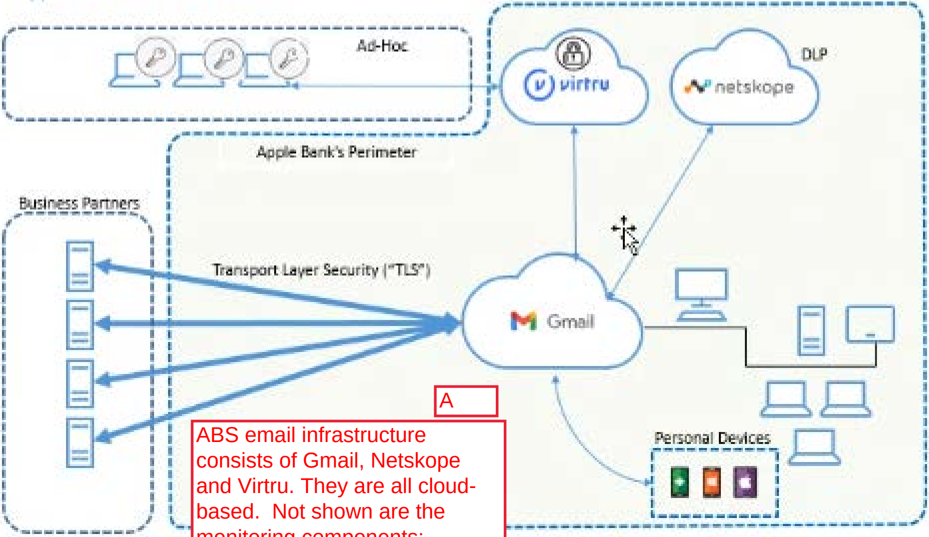
Test Sample

Control Test Procedures	
Test Step	**Test Procedure**
A	**E-mails and e-mail systems are protected from unauthorized access, modification or denial of service**
A1	Privilege access to the administration of GMAIL is restricted Pg.
A2	Privilege access to the administration of NETSKOPE is restricted Pg.
A3	Privilege access to the administration of VIRTRU is restricted Pg.
A4	The scheduled data refreshment from MISER is secured Pg.
A5	The encryption keys for e-mails and e-mail systems are protected Pg.
B	**E-mails and e-mail systems are protected from spam and phishing emails, malicious e-mails and attachments**
B1	GMAIL is configured to protect ABS e-mails from spam and phishing emails, malicious e-mails and attachments Pg.
C	E-mails and e-mail systems are protected from the leaking of non-public information
C1	Data loss prevention rules in emails and email systems are set to protect specific ABS data at-risk Pg.
C2	GMAIL is configured to protect ABS from data loss Pg.
C3	NETSKOPE is configured to protect ABS from data loss Pg.
C4	VIRTRU is configured to protect ABS from data loss Pg.
D	**E-mails and e-mail systems are appropriately and regularly monitored** Pg.

Email Encryption Diagram

ABS Email Infrastructure

Apple Bank's Modern Perimeter

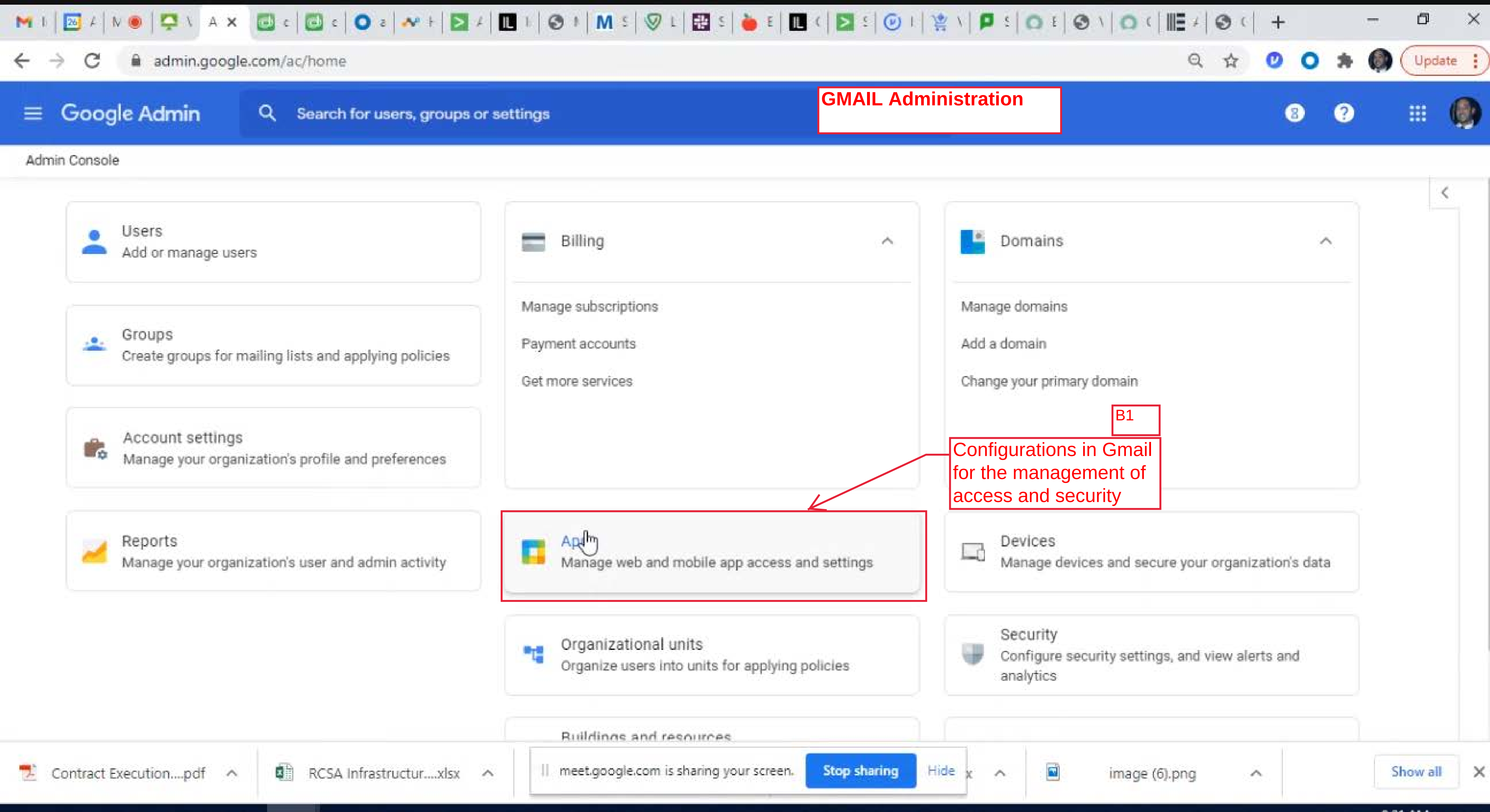


A

ABS email infrastructure consists of Gmail, Netskope and Virtru. They are all cloud-based. Not shown are the monitoring components: Marcian and Splunk

Gmail virtru netskope

Apple Bank



GMAIL Administration

admin.google.com/ac/home

Google Admin

Search for users, groups or settings

Admin Console

Users
Add or manage users

Groups
Create groups for mailing lists and applying policies

Account settings
Manage your organization's profile and preferences

Reports
Manage your organization's user and admin activity

Billing

Manage subscriptions

Payment accounts

Get more services

Apps
Manage web and mobile app access and settings

Organizational units
Organize users into units for applying policies

Buildings and resources

Domains

Manage domains

Add a domain

Change your primary domain

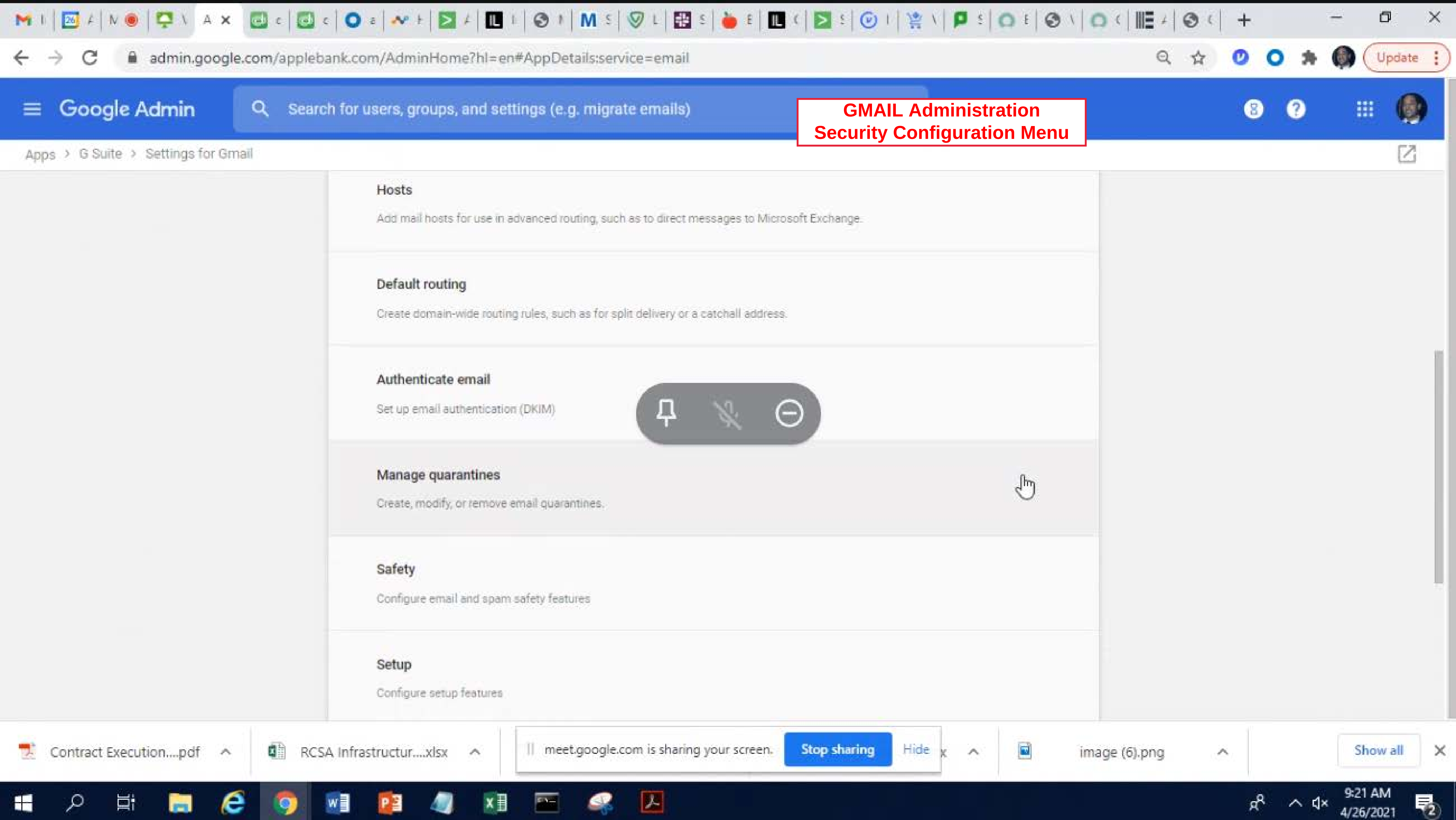
B1

Configurations in Gmail for the management of access and security

Devices
Manage devices and secure your organization's data

Security
Configure security settings, and view alerts and analytics

Contract Execution....pdf
RCSA Infrastructur....xlsx
meet.google.com is sharing your screen.
Stop sharing
Hide
image (6).png
Show all
Update



GMAIL Administration Security Configuration Menu

admin.google.com/applebank.com/AdminHome?hl=en#AppDetails:service=email
Update
Google Admin
Search for users, groups, and settings (e.g. migrate emails)
Apps › G Suite › Settings for Gmail

Hosts

Add mail hosts for use in advanced routing, such as to direct messages to Microsoft Exchange.

Default routing

Create domain-wide routing rules, such as for split delivery or a catchall address.

Authenticate email

Set up email authentication (DKIM)

Manage quarantines

Create, modify, or remove email quarantines.

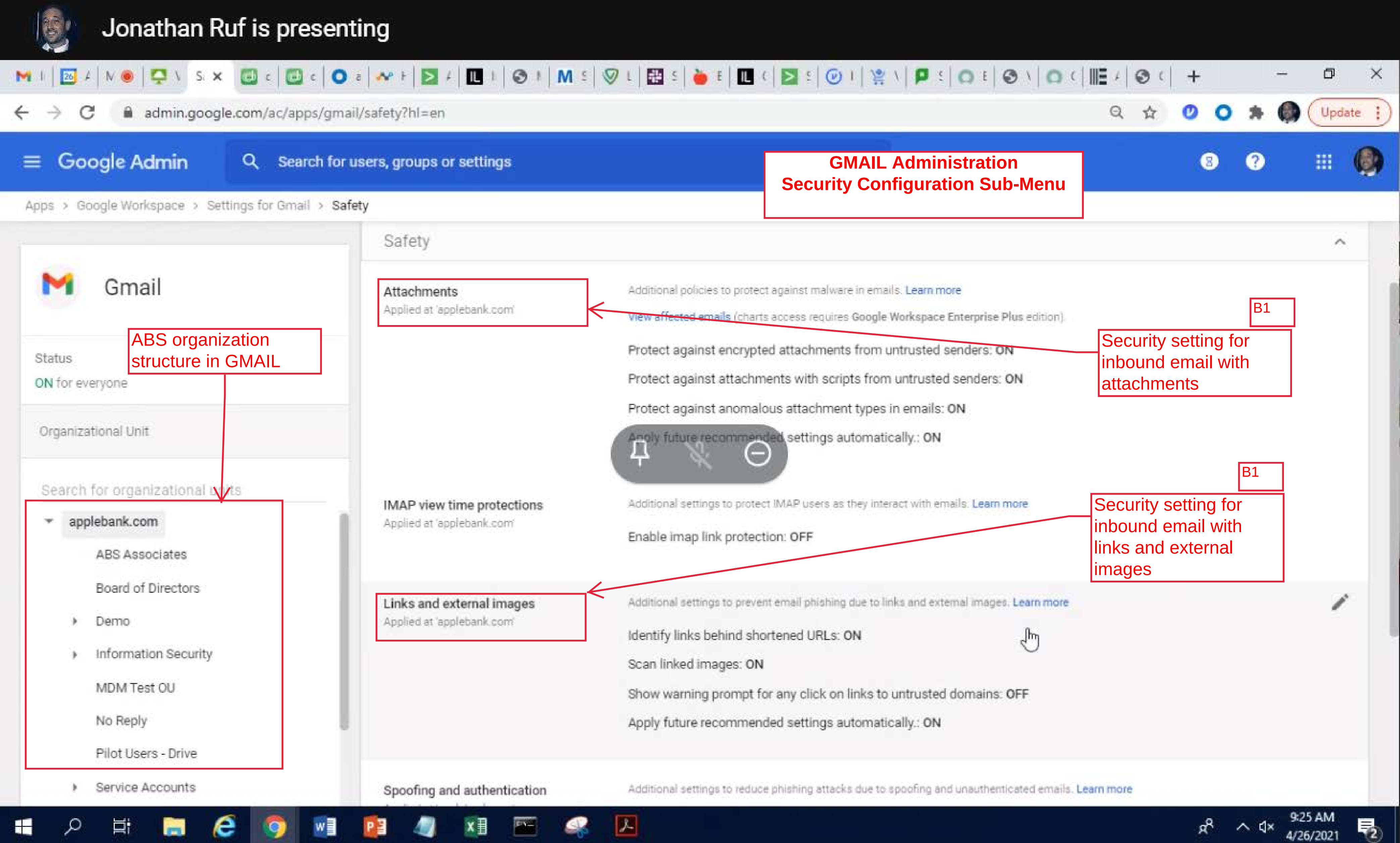
Safety

Configure email and spam safety features

Setup

Configure setup features

Contract Execution....pdf
RCSA Infrastructur....xlsx
meet.google.com is sharing your screen.
Stop sharing
Hide
image (6).png
Show all
9:21 AM
4/26/2021



Jonathan Ruf is presenting

admin.google.com/ac/apps/gmail/safety?hl=en

Google Admin

Search for users, groups or settings

GMAIL Administration Security Configuration Sub-Menu

Apps > Google Workspace > Settings for Gmail > Safety

Gmail

Status
ON for everyone

Organizational Unit

Search for organizational units

- applebank.com
  - ABS Associates
  - Board of Directors
  - Demo
  - Information Security
  - MDM Test OU
  - No Reply
  - Pilot Users - Drive
  - Service Accounts

ABS organization structure in GMAIL

Safety

Attachments
Applied at 'applebank.com'

Additional policies to protect against malware in emails. Learn more

View affected emails (charts access requires Google Workspace Enterprise Plus edition).

Protect against encrypted attachments from untrusted senders: ON

Protect against attachments with scripts from untrusted senders: ON

Protect against anomalous attachment types in emails: ON

Apply future recommended settings automatically.: ON

B1

Security setting for inbound email with attachments

IMAP view time protections
Applied at 'applebank.com'

Additional settings to protect IMAP users as they interact with emails. Learn more

Enable imap link protection: OFF

B1

Security setting for inbound email with links and external images

Links and external images
Applied at 'applebank.com'

Additional settings to prevent email phishing due to links and external images. Learn more

Identify links behind shortened URLs: ON

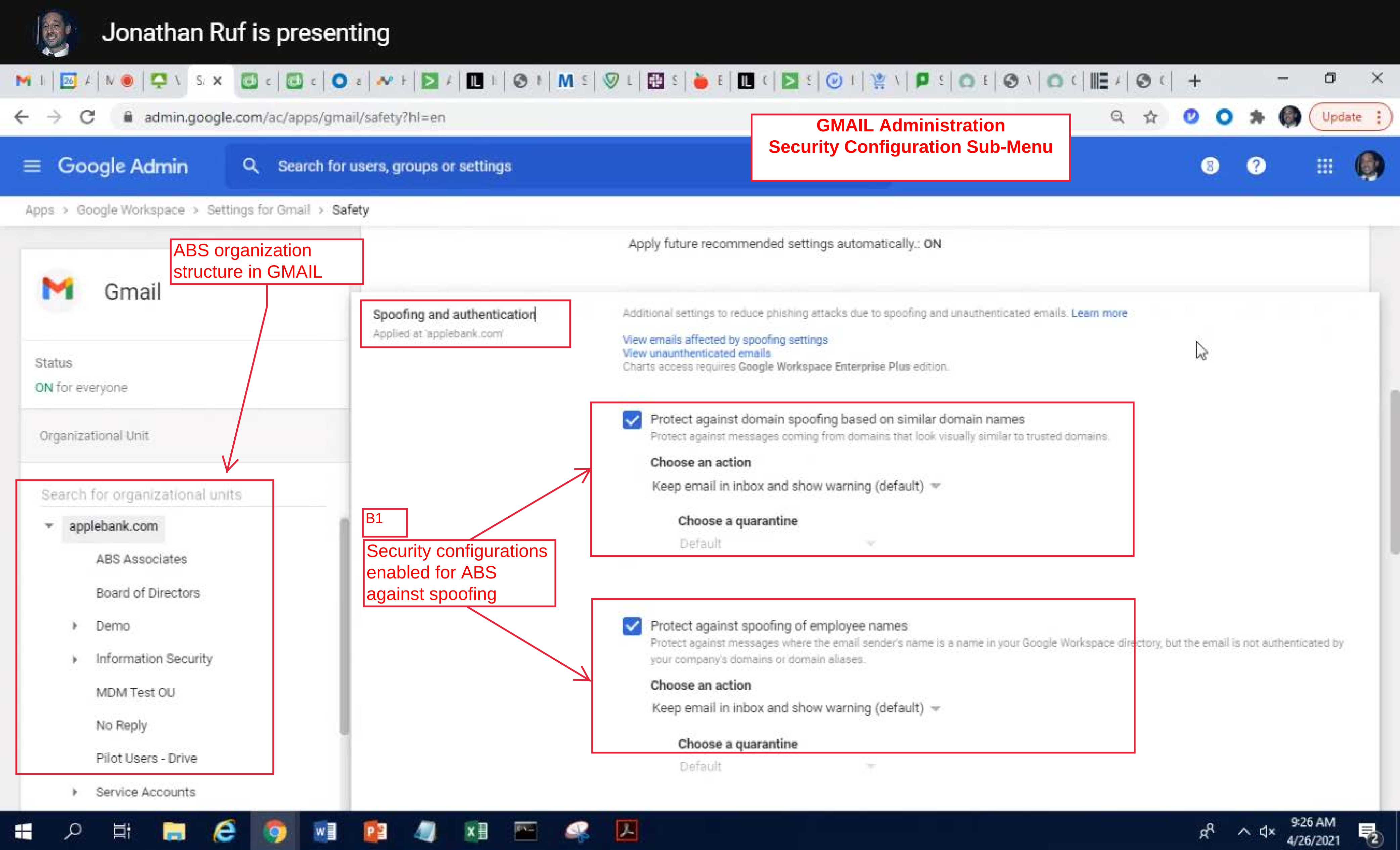
Scan linked images: ON

Show warning prompt for any click on links to untrusted domains: OFF

Apply future recommended settings automatically.: ON

Spoofing and authentication

Additional settings to reduce phishing attacks due to spoofing and unauthenticated emails. Learn more



Jonathan Ruf is presenting

admin.google.com/ac/apps/gmail/safety?hl=en

GMAIL Administration
Security Configuration Sub-Menu

Google Admin

Search for users, groups or settings

Apps > Google Workspace > Settings for Gmail > Safety

ABS organization structure in GMAIL

Gmail

Status
ON for everyone

Organizational Unit

Search for organizational units

- applebank.com
  - ABS Associates
  - Board of Directors
  - Demo
  - Information Security
  - MDM Test OU
  - No Reply
  - Pilot Users - Drive
  - Service Accounts

Apply future recommended settings automatically.: ON

Spoofing and authentication
Applied at 'applebank.com'

Additional settings to reduce phishing attacks due to spoofing and unauthenticated emails. Learn more

View emails affected by spoofing settings
View unauthenticated emails
Charts access requires Google Workspace Enterprise Plus edition.

B1

Security configurations enabled for ABS against spoofing

☑ Protect against domain spoofing based on similar domain names
Protect against messages coming from domains that look visually similar to trusted domains.

Choose an action
Keep email in inbox and show warning (default)

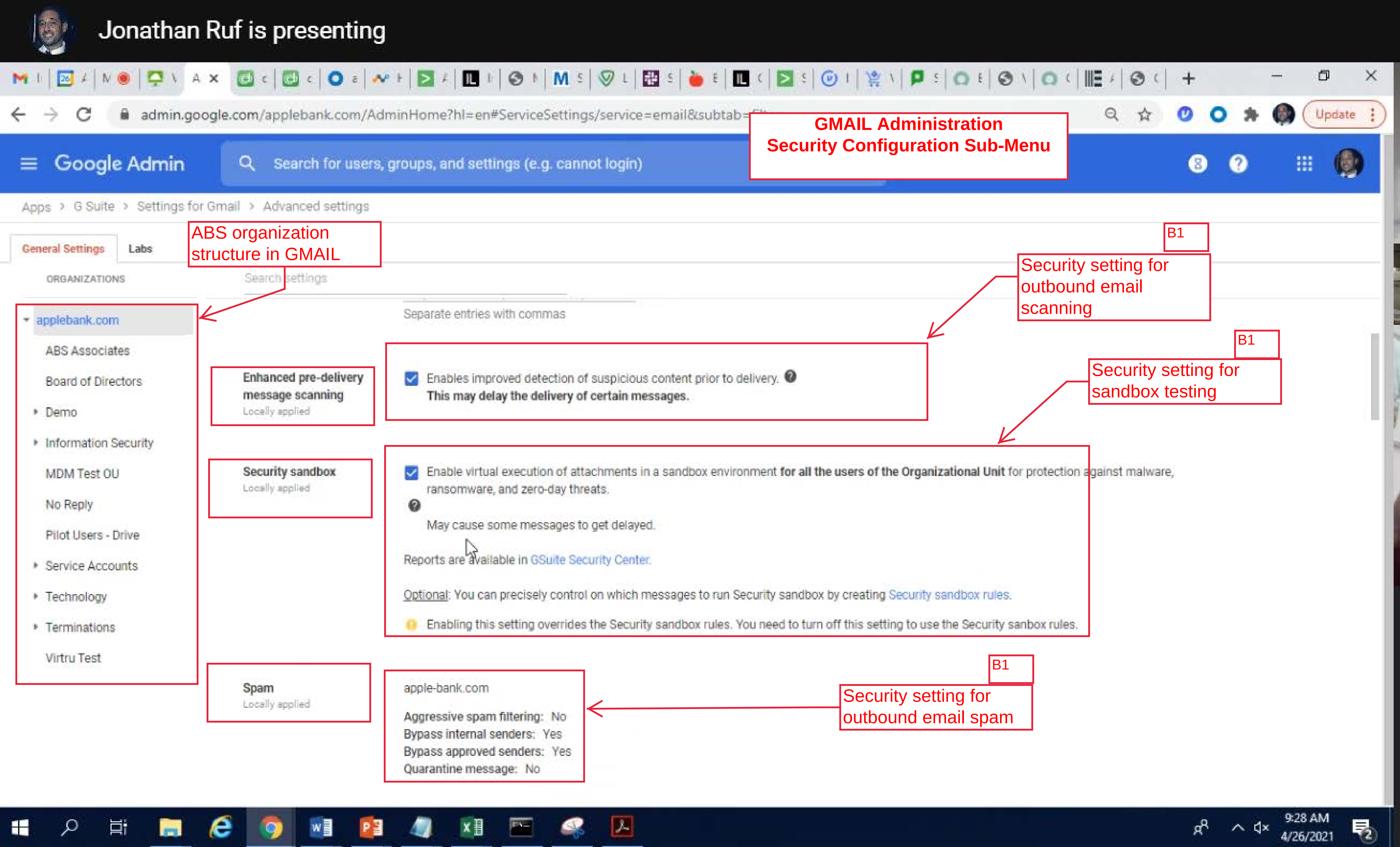
Choose a quarantine
Default

☑ Protect against spoofing of employee names
Protect against messages where the email sender's name is a name in your Google Workspace directory, but the email is not authenticated by your company's domains or domain aliases.

Choose an action
Keep email in inbox and show warning (default)

Choose a quarantine
Default

9:26 AM
4/26/2021


Jonathan Ruf is presenting
admin.google.com/applebank.com/AdminHome?hl=en#ServiceSettings/service=email&subtab=
Update
Google Admin
Search for users, groups, and settings (e.g. cannot login)
Apps › G Suite › Settings for Gmail › Advanced settings
General Settings
Labs
ORGANIZATIONS
Search settings
9:28 AM
4/26/2021

GMAIL Administration Security Configuration Sub-Menu

ABS organization structure in GMAIL

- applebank.com
  - ABS Associates
  - Board of Directors
  - Demo
  - Information Security
  - MDM Test OU
  - No Reply
  - Pilot Users - Drive
  - Service Accounts
  - Technology
  - Terminations
  - Virtru Test

Separate entries with commas

B1

Security setting for outbound email scanning

Enhanced pre-delivery message scanning
Locally applied

☑ Enables improved detection of suspicious content prior to delivery.
This may delay the delivery of certain messages.

B1

Security setting for sandbox testing

Security sandbox
Locally applied

☑ Enable virtual execution of attachments in a sandbox environment **for all the users of the Organizational Unit** for protection against malware, ransomware, and zero-day threats.

May cause some messages to get delayed.

Reports are available in GSuite Security Center.

Optional: You can precisely control on which messages to run Security sandbox by creating Security sandbox rules.

Enabling this setting overrides the Security sandbox rules. You need to turn off this setting to use the Security sanbox rules.

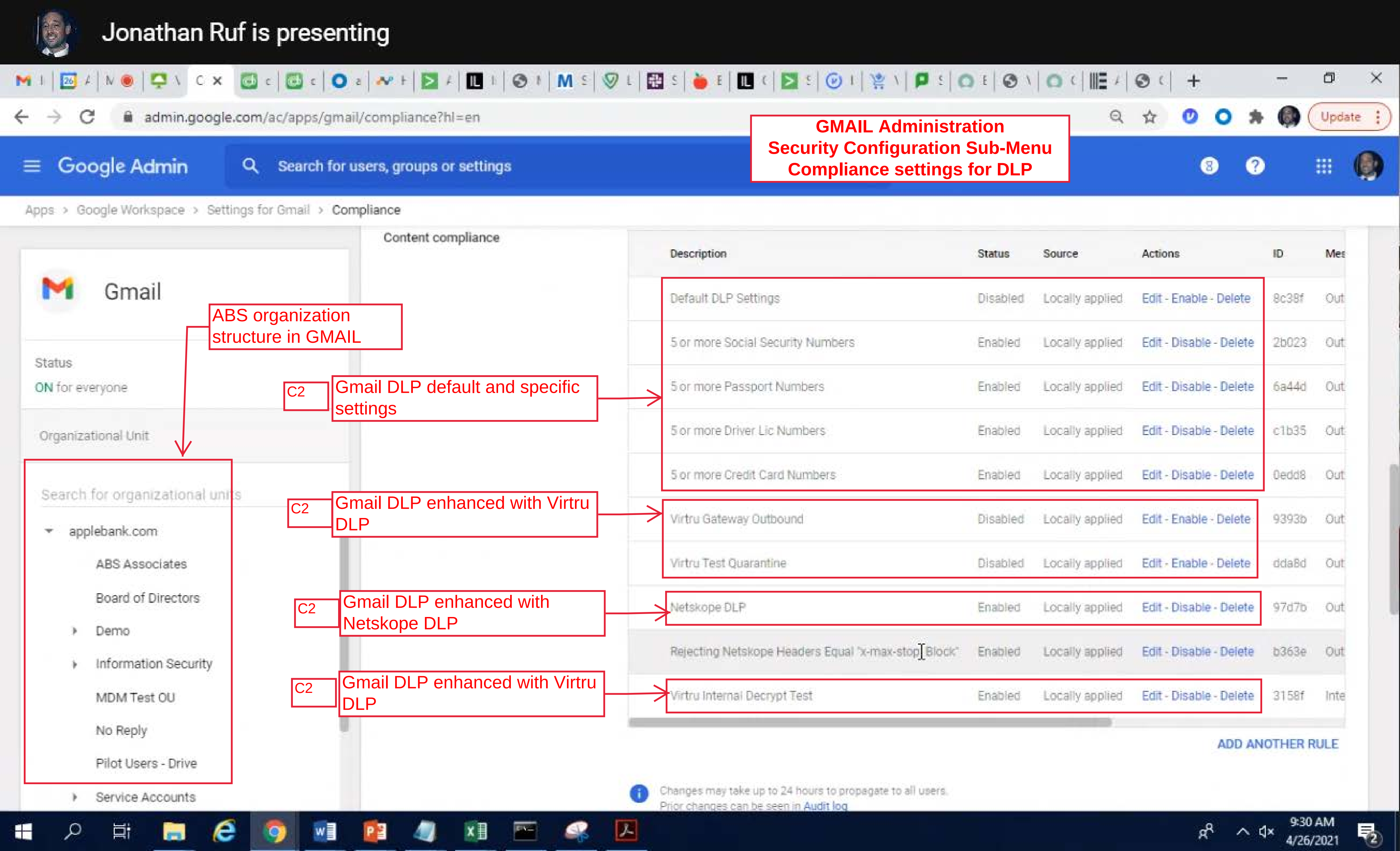
B1

Security setting for outbound email spam

Spam
Locally applied

apple-bank.com

Aggressive spam filtering: No
Bypass internal senders: Yes
Bypass approved senders: Yes
Quarantine message: No



Jonathan Ruf is presenting

admin.google.com/ac/apps/gmail/compliance?hl=en

GMAIL Administration
Security Configuration Sub-Menu
Compliance settings for DLP

Apps > Google Workspace > Settings for Gmail > Compliance

Gmail

Status
ON for everyone

Organizational Unit

Search for organizational units

- applebank.com
  - ABS Associates
  - Board of Directors
  - Demo
  - Information Security
  - MDM Test OU
  - No Reply
  - Pilot Users - Drive
  - Service Accounts

ABS organization structure in GMAIL

C2 Gmail DLP default and specific settings

C2 Gmail DLP enhanced with Virtru DLP

C2 Gmail DLP enhanced with Netskope DLP

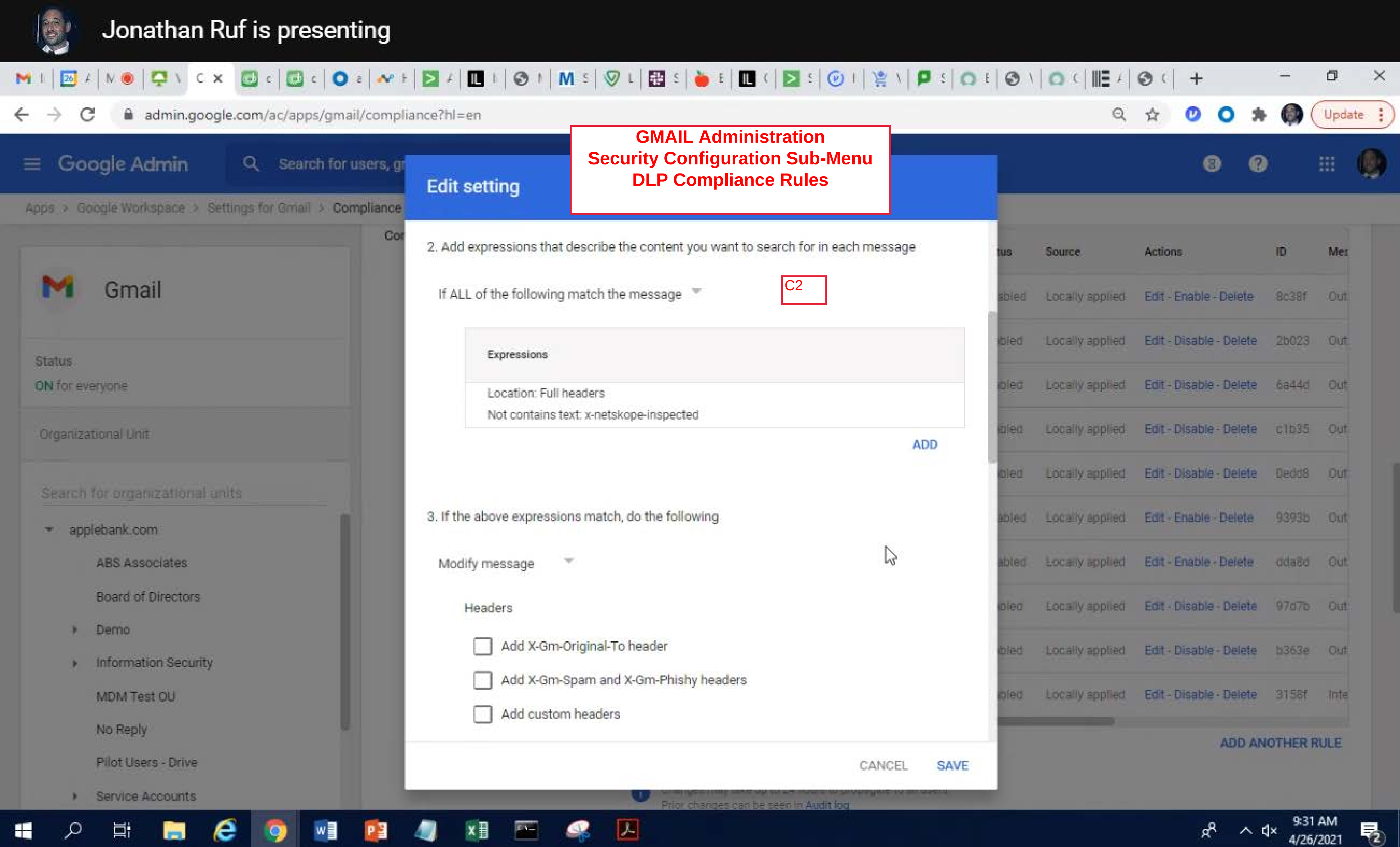
C2 Gmail DLP enhanced with Virtru DLP

Content compliance

Description	Status	Source	Actions	ID	Mes
Default DLP Settings	Disabled	Locally applied	Edit - Enable - Delete	8c38f	Out
5 or more Social Security Numbers	Enabled	Locally applied	Edit - Disable - Delete	2b023	Out
5 or more Passport Numbers	Enabled	Locally applied	Edit - Disable - Delete	6a44d	Out
5 or more Driver Lic Numbers	Enabled	Locally applied	Edit - Disable - Delete	c1b35	Out
5 or more Credit Card Numbers	Enabled	Locally applied	Edit - Disable - Delete	0edd8	Out
Virtru Gateway Outbound	Disabled	Locally applied	Edit - Enable - Delete	9393b	Out
Virtru Test Quarantine	Disabled	Locally applied	Edit - Enable - Delete	dda8d	Out
Netskope DLP	Enabled	Locally applied	Edit - Disable - Delete	97d7b	Out
Rejecting Netskope Headers Equal "x-max-stop: Block"	Enabled	Locally applied	Edit - Disable - Delete	b363e	Out
Virtru Internal Decrypt Test	Enabled	Locally applied	Edit - Disable - Delete	3158f	Inte

ADD ANOTHER RULE

Changes may take up to 24 hours to propagate to all users.
Prior changes can be seen in Audit log



**GMAIL Administration
Security Configuration Sub-Menu
DLP Compliance Rules**

C2

Edit setting

2. Add expressions that describe the content you want to search for in each message

If ALL of the following match the message

Expressions
Location: Full headers Not contains text: x-netskope-inspected

3. If the above expressions match, do the following

Modify message

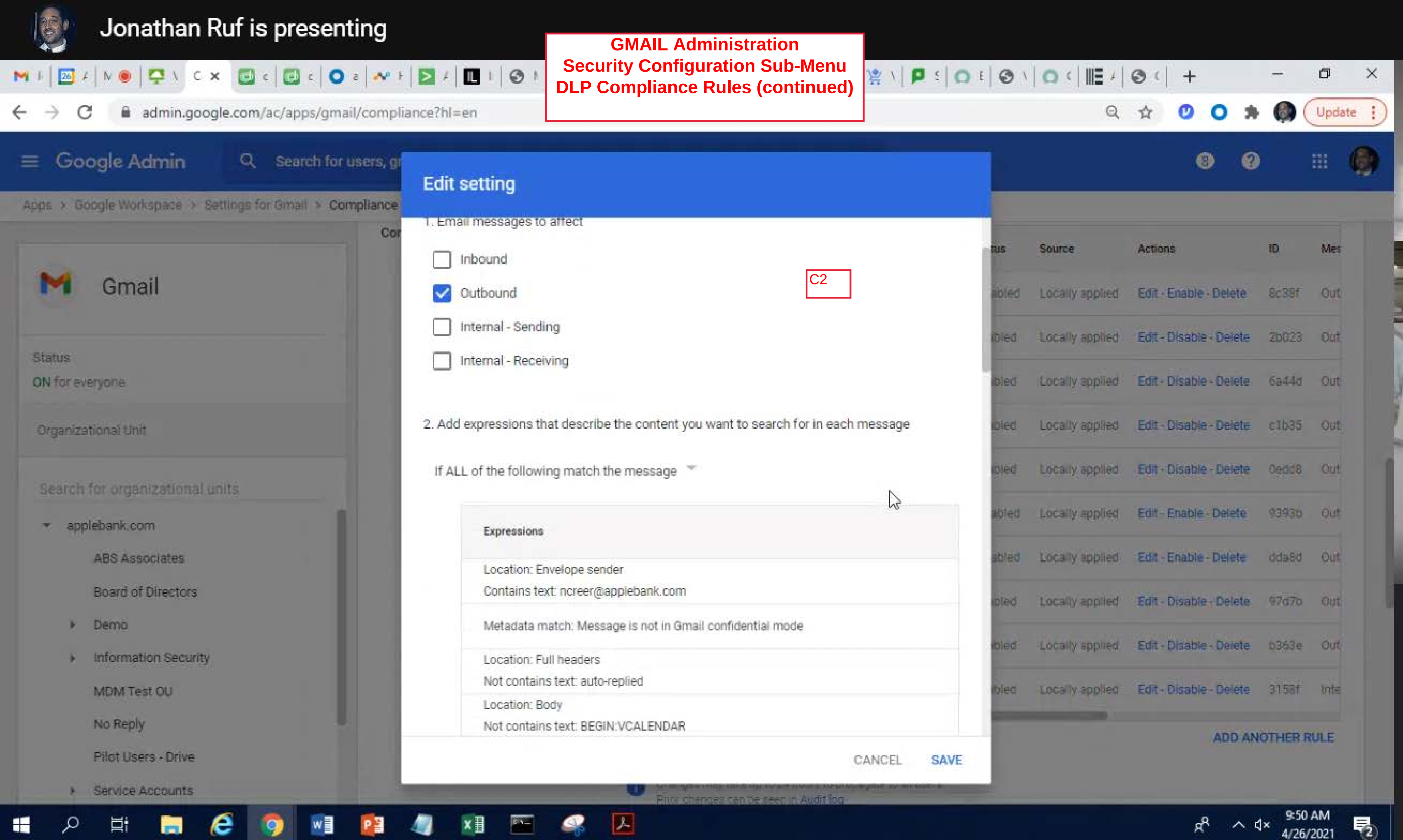
Headers

- □ Add X-Gm-Original-To header
- □ Add X-Gm-Spam and X-Gm-Phishy headers
- □ Add custom headers

Status	Source	Actions	ID	Mes
abled	Locally applied	Edit - Enable - Delete	8c38f	Out
abled	Locally applied	Edit - Disable - Delete	2b023	Out
abled	Locally applied	Edit - Disable - Delete	6a44d	Out
abled	Locally applied	Edit - Disable - Delete	c1b35	Out
abled	Locally applied	Edit - Disable - Delete	0edd8	Out
abled	Locally applied	Edit - Enable - Delete	9393b	Out
abled	Locally applied	Edit - Enable - Delete	dda8d	Out
abled	Locally applied	Edit - Disable - Delete	97d7b	Out
abled	Locally applied	Edit - Disable - Delete	b363e	Out
abled	Locally applied	Edit - Disable - Delete	3158f	Inte

Prior changes can be seen in Audit log

GMAIL Administration
Security Configuration Sub-Menu
DLP Compliance Rules (continued)



tus	Source	Actions	ID	Mes
abled	Locally applied	Edit - Enable - Delete	8c38f	Out
bled	Locally applied	Edit - Disable - Delete	2b023	Out
bled	Locally applied	Edit - Disable - Delete	6a44d	Out
bled	Locally applied	Edit - Disable - Delete	c1b35	Out
bled	Locally applied	Edit - Disable - Delete	0edd8	Out
abled	Locally applied	Edit - Enable - Delete	9393b	Out
abled	Locally applied	Edit - Enable - Delete	dda8d	Out
bled	Locally applied	Edit - Disable - Delete	97d7b	Out
bled	Locally applied	Edit - Disable - Delete	b363e	Out
bled	Locally applied	Edit - Disable - Delete	3158f	Inte

Edit setting

1. Email messages to affect

□ Inbound
☑ Outbound
□ Internal - Sending
□ Internal - Receiving

2. Add expressions that describe the content you want to search for in each message

If ALL of the following match the message

Expressions

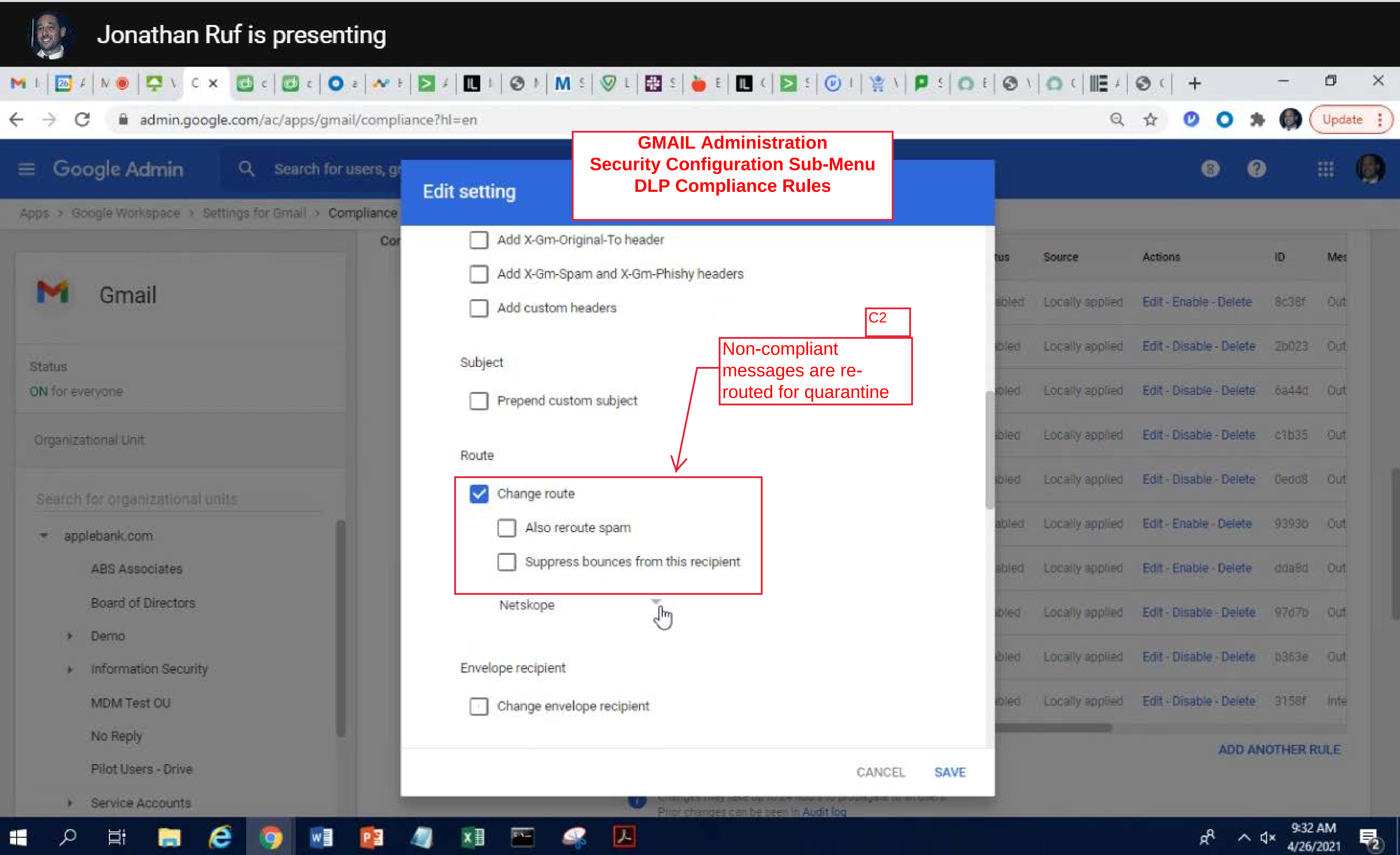
Location: Envelope sender
Contains text: ncreer@applebank.com

Metadata match: Message is not in Gmail confidential mode

Location: Full headers
Not contains text: auto-replied

Location: Body
Not contains text: BEGIN:VCALENDAR

CANCEL SAVE



Jonathan Ruf is presenting

admin.google.com/ac/apps/gmail/compliance?hl=en

GMAIL Administration
Security Configuration Sub-Menu
DLP Compliance Rules

Google Admin

Apps > Google Workspace > Settings for Gmail > Compliance

Gmail

Status
ON for everyone

Organizational Unit

Search for organizational units

- applebank.com
  - ABS Associates
  - Board of Directors
  - Demo
  - Information Security
  - MDM Test OU
  - No Reply
  - Pilot Users - Drive
  - Service Accounts

Edit setting

□ Add X-Gm-Original-To header

□ Add X-Gm-Spam and X-Gm-Phishy headers

□ Add custom headers

Subject

□ Prepend custom subject

Route

☑ Change route

□ Also reroute spam

□ Suppress bounces from this recipient

Netskope

Envelope recipient

□ Change envelope recipient

CANCEL SAVE

C2

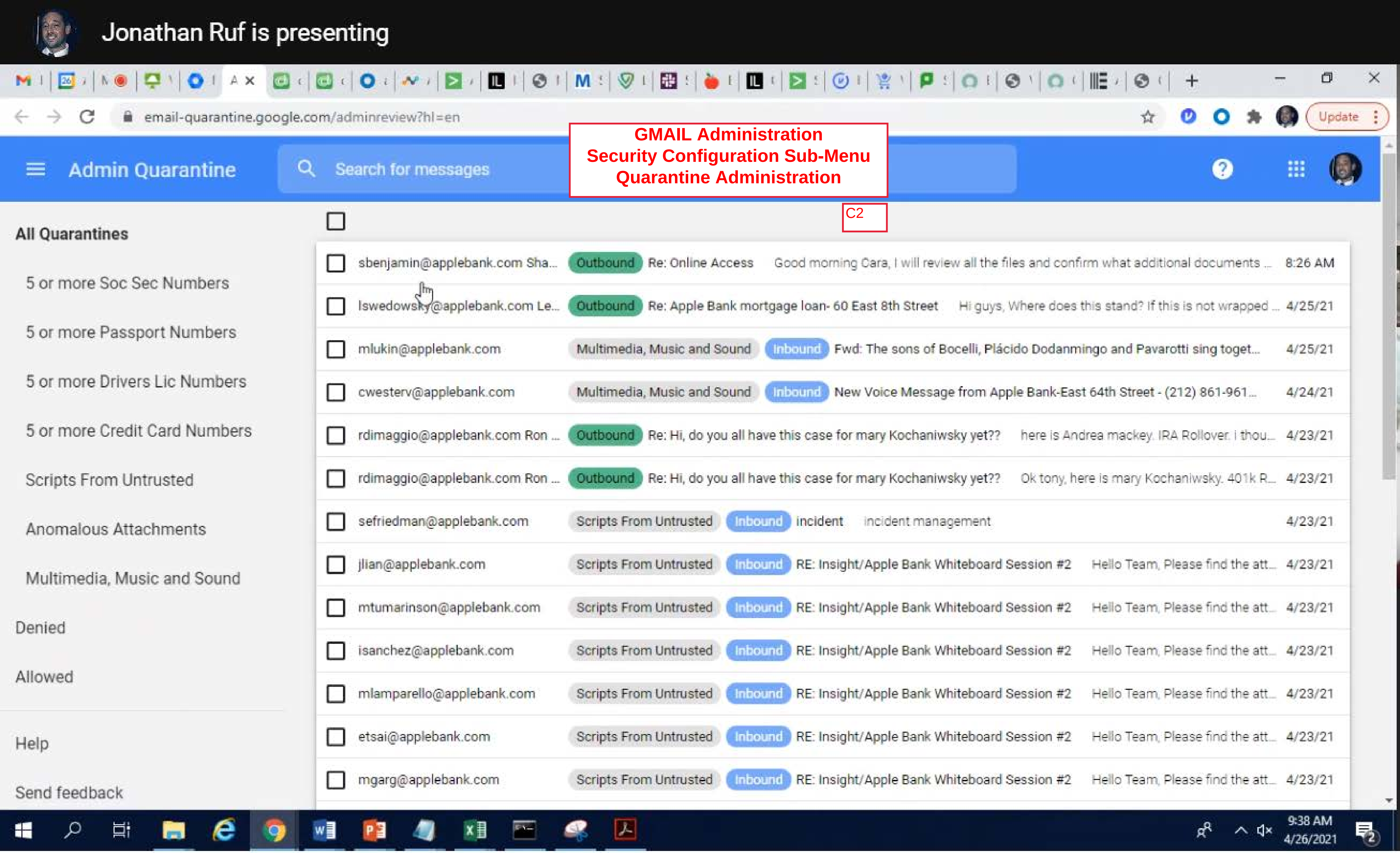
Non-compliant messages are re-routed for quarantine

...tus	Source	Actions	ID	Mes...
...abled	Locally applied	Edit - Enable - Delete	8c38f	Out...
...bled	Locally applied	Edit - Disable - Delete	2b023	Out...
...bled	Locally applied	Edit - Disable - Delete	6a44d	Out...
...bled	Locally applied	Edit - Disable - Delete	c1b35	Out...
...bled	Locally applied	Edit - Disable - Delete	0edd8	Out...
...abled	Locally applied	Edit - Enable - Delete	9393b	Out...
...abled	Locally applied	Edit - Enable - Delete	dda8d	Out...
...bled	Locally applied	Edit - Disable - Delete	97d7b	Out...
...bled	Locally applied	Edit - Disable - Delete	b363e	Out...
...bled	Locally applied	Edit - Disable - Delete	3158f	Inte...

ADD ANOTHER RULE

Prior changes can be seen in Audit log

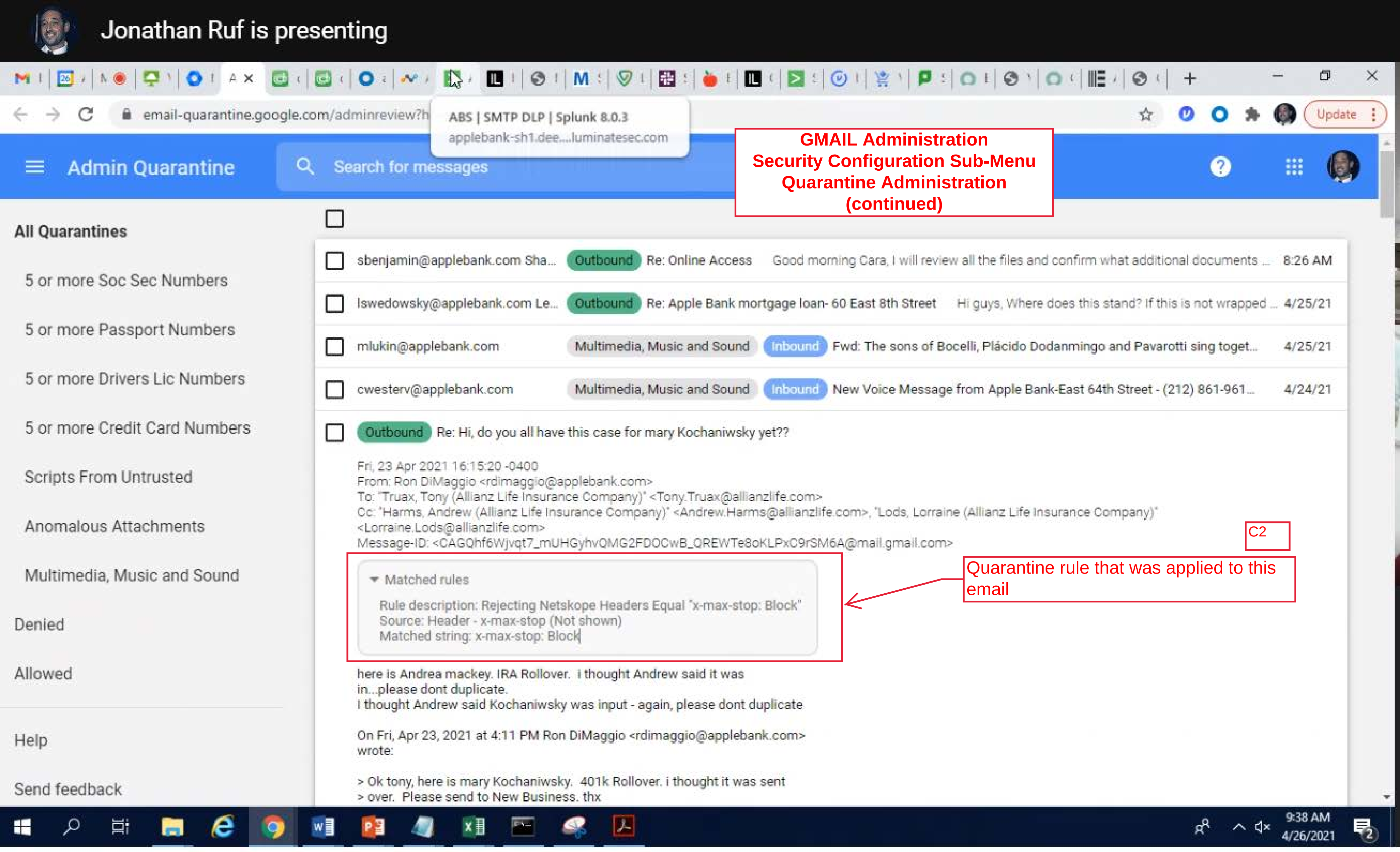
9:32 AM
4/26/2021


Jonathan Ruf is presenting
email-quarantine.google.com/adminreview?hl=en
Update
Admin Quarantine
Search for messages
All Quarantines
5 or more Soc Sec Numbers
5 or more Passport Numbers
5 or more Drivers Lic Numbers
5 or more Credit Card Numbers
Scripts From Untrusted
Anomalous Attachments
Multimedia, Music and Sound
Denied
Allowed
Help
Send feedback
9:38 AM
4/26/2021

GMAIL Administration
Security Configuration Sub-Menu
Quarantine Administration

C2

□ sbenjamin@applebank.com Sha...	Outbound		Re: Online Access	Good morning Cara, I will review all the files and confirm what additional documents ...	8:26 AM
□ lswedowsky@applebank.com Le...	Outbound		Re: Apple Bank mortgage loan- 60 East 8th Street	Hi guys, Where does this stand? If this is not wrapped ...	4/25/21
□ mlukin@applebank.com	Multimedia, Music and Sound	Inbound	Fwd: The sons of Bocelli, Plácido Dodanmingo and Pavarotti sing toget...		4/25/21
□ cwesterv@applebank.com	Multimedia, Music and Sound	Inbound	New Voice Message from Apple Bank-East 64th Street - (212) 861-961...		4/24/21
□ rdimaggio@applebank.com Ron ...	Outbound		Re: Hi, do you all have this case for mary Kochaniwsky yet??	here is Andrea mackey. IRA Rollover. i thou...	4/23/21
□ rdimaggio@applebank.com Ron ...	Outbound		Re: Hi, do you all have this case for mary Kochaniwsky yet??	Ok tony, here is mary Kochaniwsky. 401k R...	4/23/21
□ sefriedman@applebank.com	Scripts From Untrusted	Inbound	incident	incident management	4/23/21
□ jlian@applebank.com	Scripts From Untrusted	Inbound	RE: Insight/Apple Bank Whiteboard Session #2	Hello Team, Please find the att...	4/23/21
□ mtumarinson@applebank.com	Scripts From Untrusted	Inbound	RE: Insight/Apple Bank Whiteboard Session #2	Hello Team, Please find the att...	4/23/21
□ isanchez@applebank.com	Scripts From Untrusted	Inbound	RE: Insight/Apple Bank Whiteboard Session #2	Hello Team, Please find the att...	4/23/21
□ mlamparello@applebank.com	Scripts From Untrusted	Inbound	RE: Insight/Apple Bank Whiteboard Session #2	Hello Team, Please find the att...	4/23/21
□ etsai@applebank.com	Scripts From Untrusted	Inbound	RE: Insight/Apple Bank Whiteboard Session #2	Hello Team, Please find the att...	4/23/21
□ mgarg@applebank.com	Scripts From Untrusted	Inbound	RE: Insight/Apple Bank Whiteboard Session #2	Hello Team, Please find the att...	4/23/21



Jonathan Ruf is presenting

email-quarantine.google.com/adminreview?h

ABS | SMTP DLP | Splunk 8.0.3
applebank-sh1.dee....luminatesec.com

GMAIL Administration
Security Configuration Sub-Menu
Quarantine Administration
(continued)

All Quarantines

5 or more Soc Sec Numbers

5 or more Passport Numbers

5 or more Drivers Lic Numbers

5 or more Credit Card Numbers

Scripts From Untrusted

Anomalous Attachments

Multimedia, Music and Sound

Denied

Allowed

Help

Send feedback

□ sbenjamin@applebank.com Sha...	Outbound	Re: Online Access	Good morning Cara, I will review all the files and confirm what additional documents ...	8:26 AM
□ lswedowsky@applebank.com Le...	Outbound	Re: Apple Bank mortgage loan- 60 East 8th Street	Hi guys, Where does this stand? If this is not wrapped ...	4/25/21
□ mlukin@applebank.com	Multimedia, Music and Sound	Inbound	Fwd: The sons of Bocelli, Plácido Dodanmingo and Pavarotti sing toget...	4/25/21
□ cwesterv@applebank.com	Multimedia, Music and Sound	Inbound	New Voice Message from Apple Bank-East 64th Street - (212) 861-961...	4/24/21

□ Outbound Re: Hi, do you all have this case for mary Kochaniwsky yet??

Fri, 23 Apr 2021 16:15:20 -0400
From: Ron DiMaggio <rdimaggio@applebank.com>
To: "Truax, Tony (Allianz Life Insurance Company)" <Tony.Truax@allianzlife.com>
Cc: "Harms, Andrew (Allianz Life Insurance Company)" <Andrew.Harms@allianzlife.com>, "Lods, Lorraine (Allianz Life Insurance Company)" <Lorraine.Lods@allianzlife.com>
Message-ID: <CAGQhf6Wjvqt7_mUHGyhvQMG2FDOCwB_QREWTe8oKLPxC9rSM6A@mail.gmail.com>

C2

▾ Matched rules

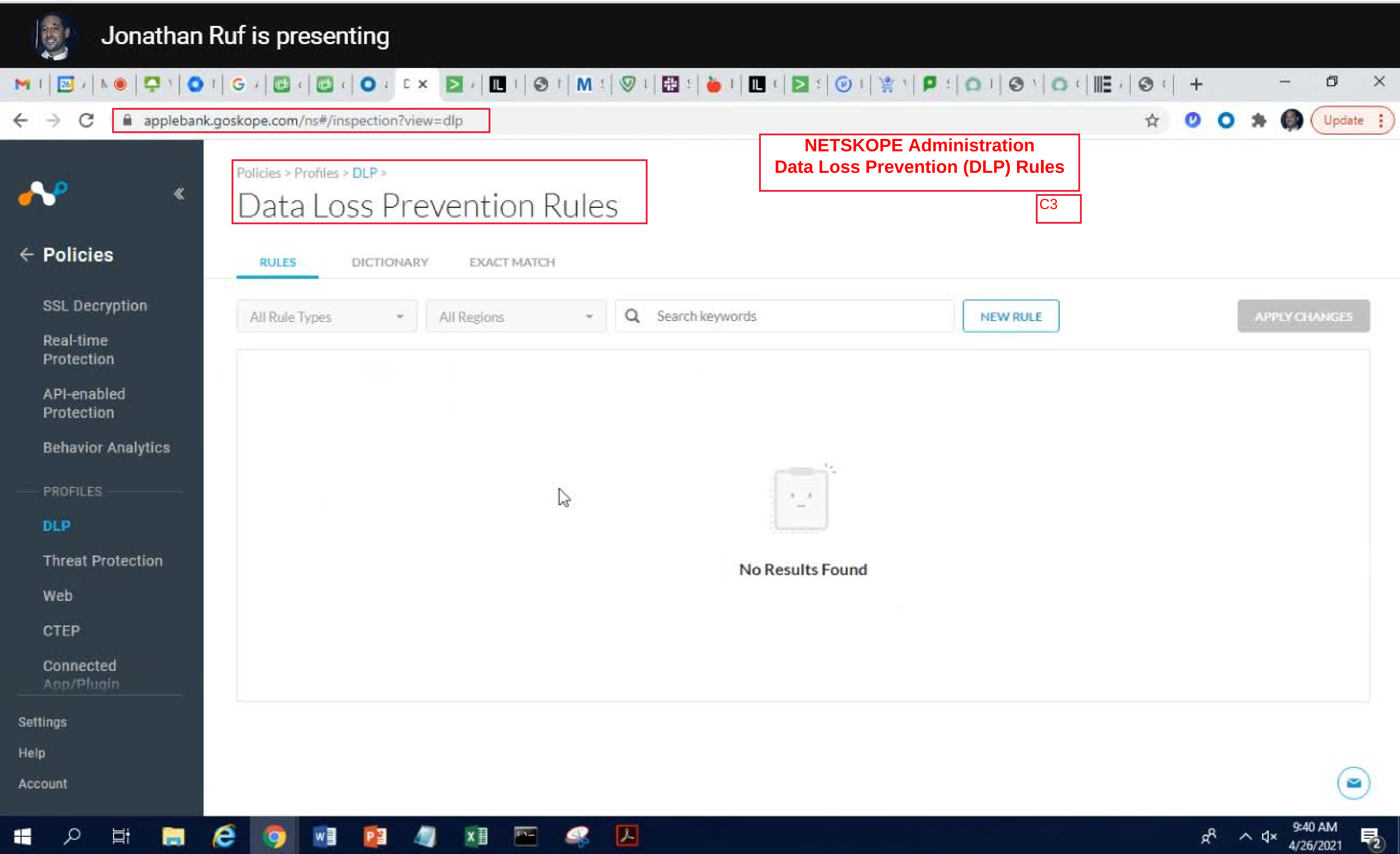
Rule description: Rejecting Netskope Headers Equal "x-max-stop: Block"
Source: Header - x-max-stop (Not shown)
Matched string: x-max-stop: Block

Quarantine rule that was applied to this email

here is Andrea mackey. IRA Rollover. i thought Andrew said it was
in...please dont duplicate.
I thought Andrew said Kochaniwsky was input - again, please dont duplicate

On Fri, Apr 23, 2021 at 4:11 PM Ron DiMaggio <rdimaggio@applebank.com>
wrote:

> Ok tony, here is mary Kochaniwsky. 401k Rollover. i thought it was sent
> over. Please send to New Business. thx



Jonathan Ruf is presenting

applebank.goskope.com/ns#/inspection?view=dlp

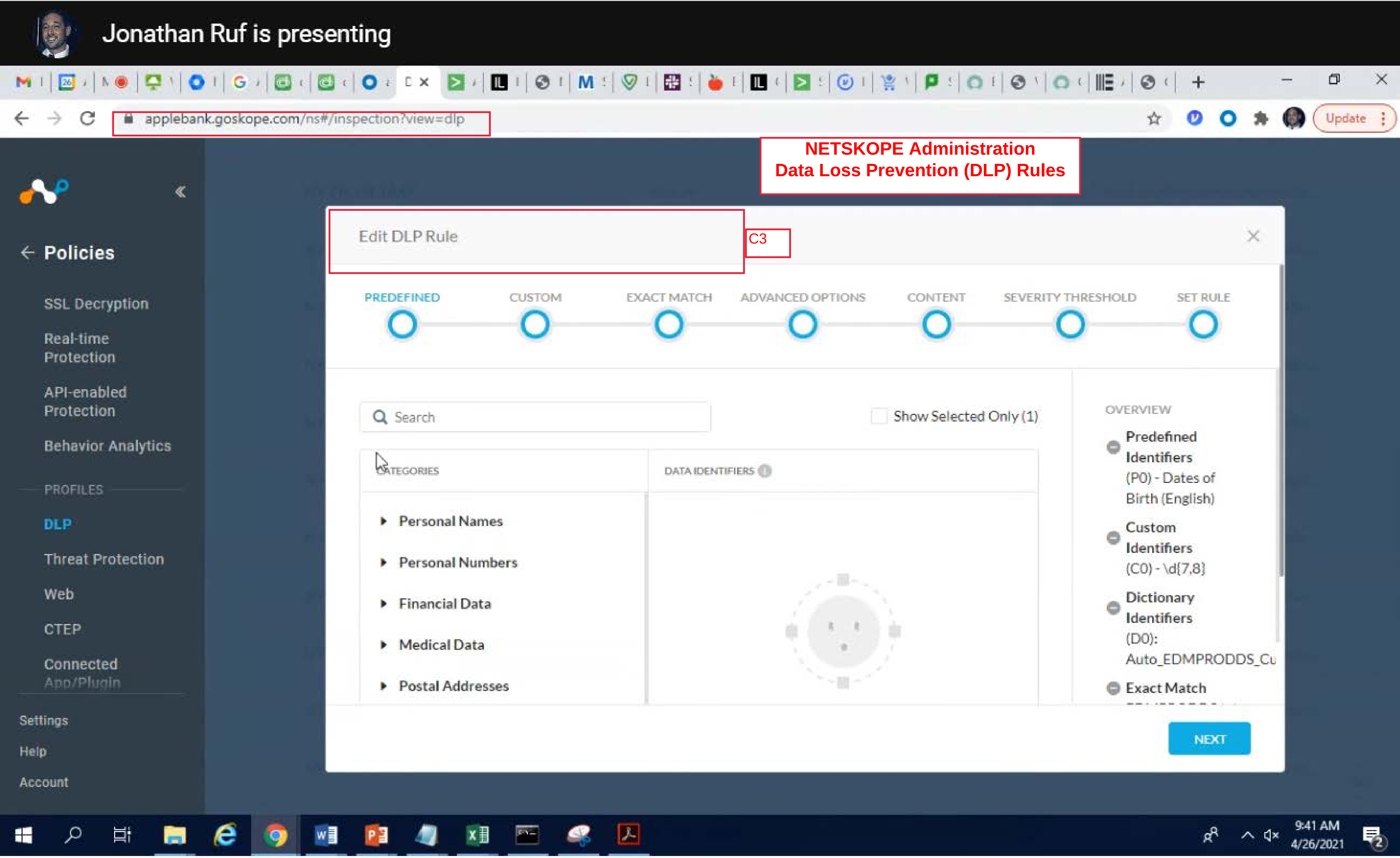
NETSKOPE Administration
Data Loss Prevention (DLP) Rules

C3

Policies > Profiles > DLP >

Data Loss Prevention Rules

No Results Found



Jonathan Ruf is presenting

applebank.goskope.com/ns#/inspection?view=dlp

NETSKOPE Administration
Data Loss Prevention (DLP) Rules

C3

Policies

- SSL Decryption
- Real-time Protection
- API-enabled Protection
- Behavior Analytics

PROFILES

- DLP
- Threat Protection
- Web
- CTEP
- Connected App/Plugin

Settings

Help

Account

Edit DLP Rule

PREDEFINED ○ — CUSTOM ○ — EXACT MATCH ○ — ADVANCED OPTIONS ○ — CONTENT ○ — SEVERITY THRESHOLD ○ — SET RULE ○

Search

□ Show Selected Only (1)

CATEGORIES

- Personal Names
- Personal Numbers
- Financial Data
- Medical Data
- Postal Addresses

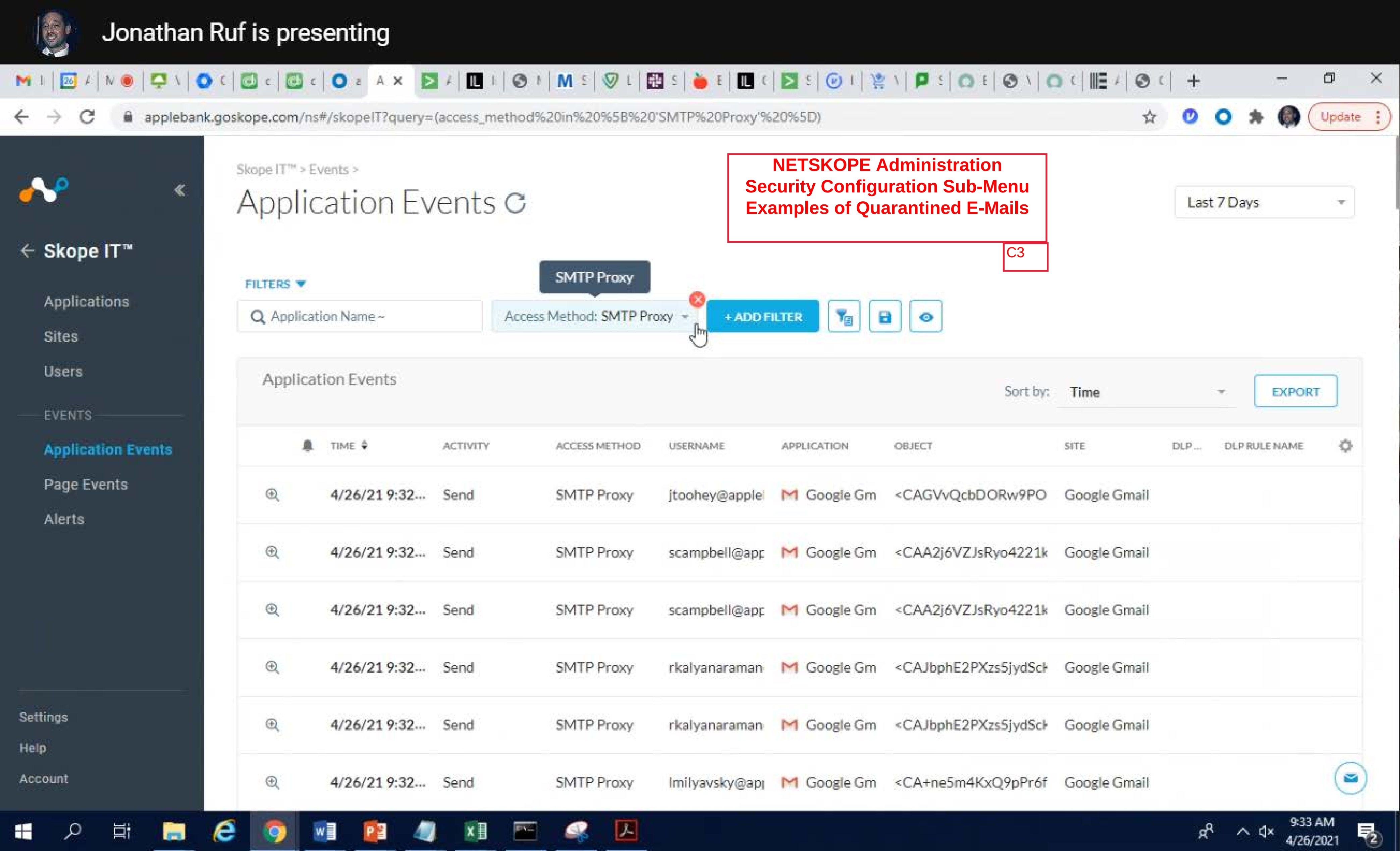
DATA IDENTIFIERS

OVERVIEW

- Predefined Identifiers (P0) - Dates of Birth (English)
- Custom Identifiers (C0) - \d{7,8}
- Dictionary Identifiers (D0): Auto_EDMPRODDS_Cu
- Exact Match

NEXT

9:41 AM
4/26/2021



Jonathan Ruf is presenting

applebank.goskope.com/ns#/skopeIT?query=(access_method%20in%20%5B%20'SMTP%20Proxy'%20%5D)

NETSKOPE Administration Security Configuration Sub-Menu Examples of Quarantined E-Mails

C3

Skope IT™ > Events >

Application Events

Last 7 Days

FILTERS

Application Name ~

Access Method: SMTP Proxy

SMTP Proxy

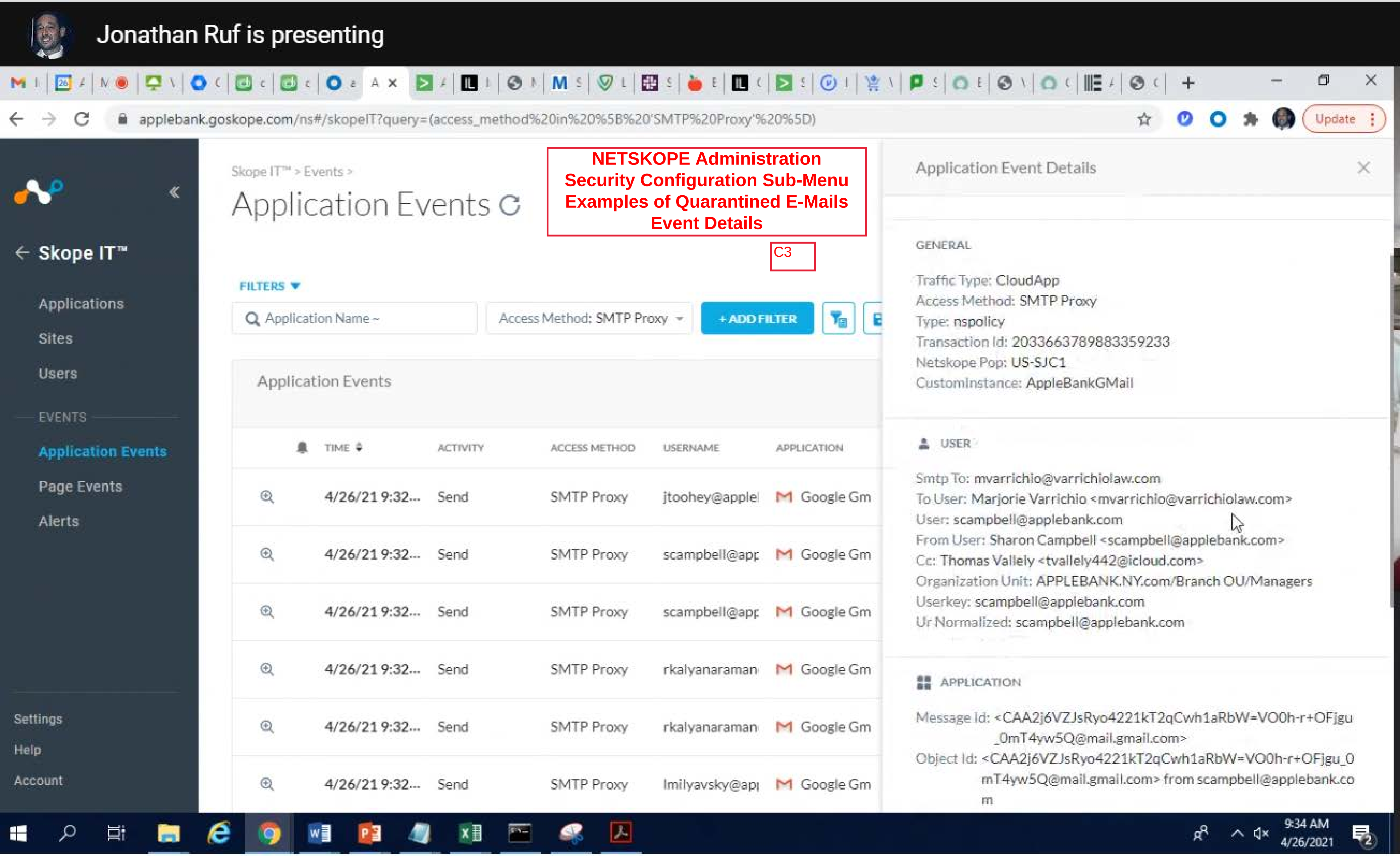
+ ADD FILTER

Application Events

Sort by: Time

EXPORT

TIME	ACTIVITY	ACCESS METHOD	USERNAME	APPLICATION	OBJECT	SITE	DLP ...	DLP RULE NAME
4/26/21 9:32...	Send	SMTP Proxy	jtoohey@applel	Google Gm	<CAGVvQcbDORw9PO	Google Gmail		
4/26/21 9:32...	Send	SMTP Proxy	scampbell@app	Google Gm	<CAA2j6VZJsRyo4221k	Google Gmail		
4/26/21 9:32...	Send	SMTP Proxy	scampbell@app	Google Gm	<CAA2j6VZJsRyo4221k	Google Gmail		
4/26/21 9:32...	Send	SMTP Proxy	rkalyanaraman	Google Gm	<CAJbphE2PXzs5jydSck	Google Gmail		
4/26/21 9:32...	Send	SMTP Proxy	rkalyanaraman	Google Gm	<CAJbphE2PXzs5jydSck	Google Gmail		
4/26/21 9:32...	Send	SMTP Proxy	lmilyavsky@ap	Google Gm	<CA+ne5m4KxQ9pPr6f	Google Gmail		



Jonathan Ruf is presenting
applebank.goskope.com/ns#/skopeIT?query=(access_method%20in%20%5B%20'SMTP%20Proxy'%20%5D)

NETSKOPE Administration
Security Configuration Sub-Menu
Examples of Quarantined E-Mails
Event Details

C3

Skope IT™
Applications
Sites
Users
EVENTS
Application Events
Page Events
Alerts
Settings
Help
Account

Skope IT™ > Events >

Application Events

FILTERS
Application Name
Access Method: SMTP Proxy
+ ADD FILTER

Application Events

TIME	ACTIVITY	ACCESS METHOD	USERNAME	APPLICATION
4/26/21 9:32...	Send	SMTP Proxy	jtoohey@applel	Google Gm
4/26/21 9:32...	Send	SMTP Proxy	scampbell@apr	Google Gm
4/26/21 9:32...	Send	SMTP Proxy	scampbell@apr	Google Gm
4/26/21 9:32...	Send	SMTP Proxy	rkalyanaraman	Google Gm
4/26/21 9:32...	Send	SMTP Proxy	rkalyanaraman	Google Gm
4/26/21 9:32...	Send	SMTP Proxy	lmilyavsky@ap	Google Gm

Application Event Details

GENERAL

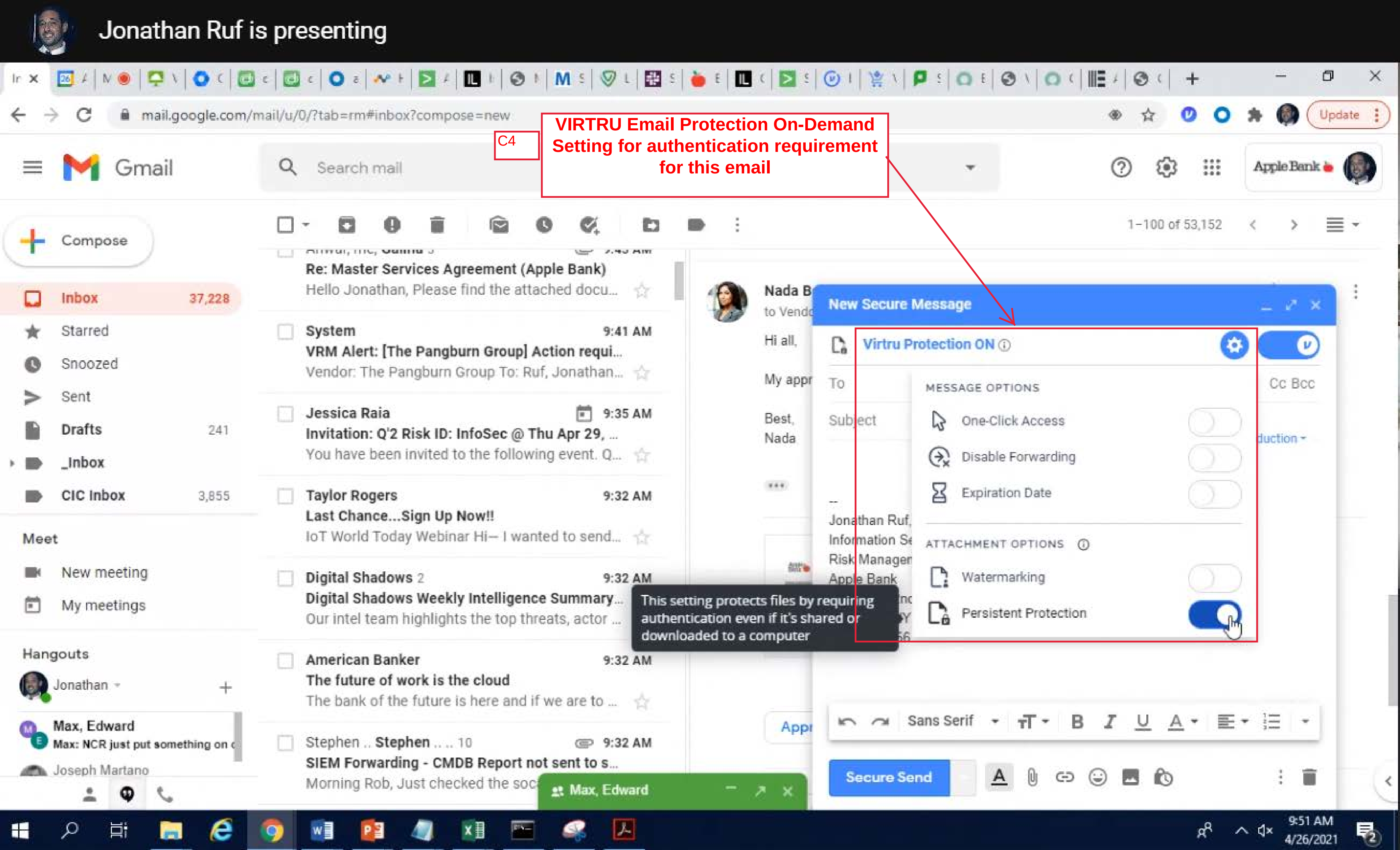
Traffic Type: CloudApp
Access Method: SMTP Proxy
Type: nspolicy
Transaction Id: 2033663789883359233
Netskope Pop: US-SJC1
CustomInstance: AppleBankGMail

USER

Smtp To: mvarrichio@varrichiolaw.com
To User: Marjorie Varrichio <mvarrichio@varrichiolaw.com>
User: scampbell@applebank.com
From User: Sharon Campbell <scampbell@applebank.com>
Cc: Thomas Vallely <tvallely442@icloud.com>
Organization Unit: APPLEBANK.NY.com/Branch OU/Managers
Userkey: scampbell@applebank.com
Ur Normalized: scampbell@applebank.com

APPLICATION

Message Id: <CAA2j6VZJsRyo4221kT2qCwh1aRbW=VO0h-r+OFjgu_0mT4yw5Q@mail.gmail.com>
Object Id: <CAA2j6VZJsRyo4221kT2qCwh1aRbW=VO0h-r+OFjgu_0mT4yw5Q@mail.gmail.com> from scampbell@applebank.com



VIRTRU Email Protection On-Demand Setting for authentication requirement for this email

Re: Master Services Agreement (Apple Bank)	Hello Jonathan, Please find the attached docu...	
System	VRM Alert: [The Pangburn Group] Action requi... Vendor: The Pangburn Group To: Ruf, Jonathan...	9:41 AM
Jessica Raia	Invitation: Q'2 Risk ID: InfoSec @ Thu Apr 29, ... You have been invited to the following event. Q...	9:35 AM
Taylor Rogers	Last Chance...Sign Up Now!! IoT World Today Webinar Hi– I wanted to send...	9:32 AM
Digital Shadows 2	Digital Shadows Weekly Intelligence Summary... Our intel team highlights the top threats, actor ...	9:32 AM
American Banker	The future of work is the cloud The bank of the future is here and if we are to ...	9:32 AM
Stephen .. Stephen 10	SIEM Forwarding - CMDB Report not sent to s... Morning Rob, Just checked the soc	9:32 AM

Max, Edward
Max: NCR just put something on

Joseph Martano

Nada B
to Vendo
Hi all,
My appr
Best,
Nada

New Secure Message

Virtru Protection ON

To
Subject
Cc Bcc

--
Jonathan Ruf,
Information Se
Risk Managem
Apple Bank

MESSAGE OPTIONS

- One-Click Access: off
- Disable Forwarding: off
- Expiration Date: off

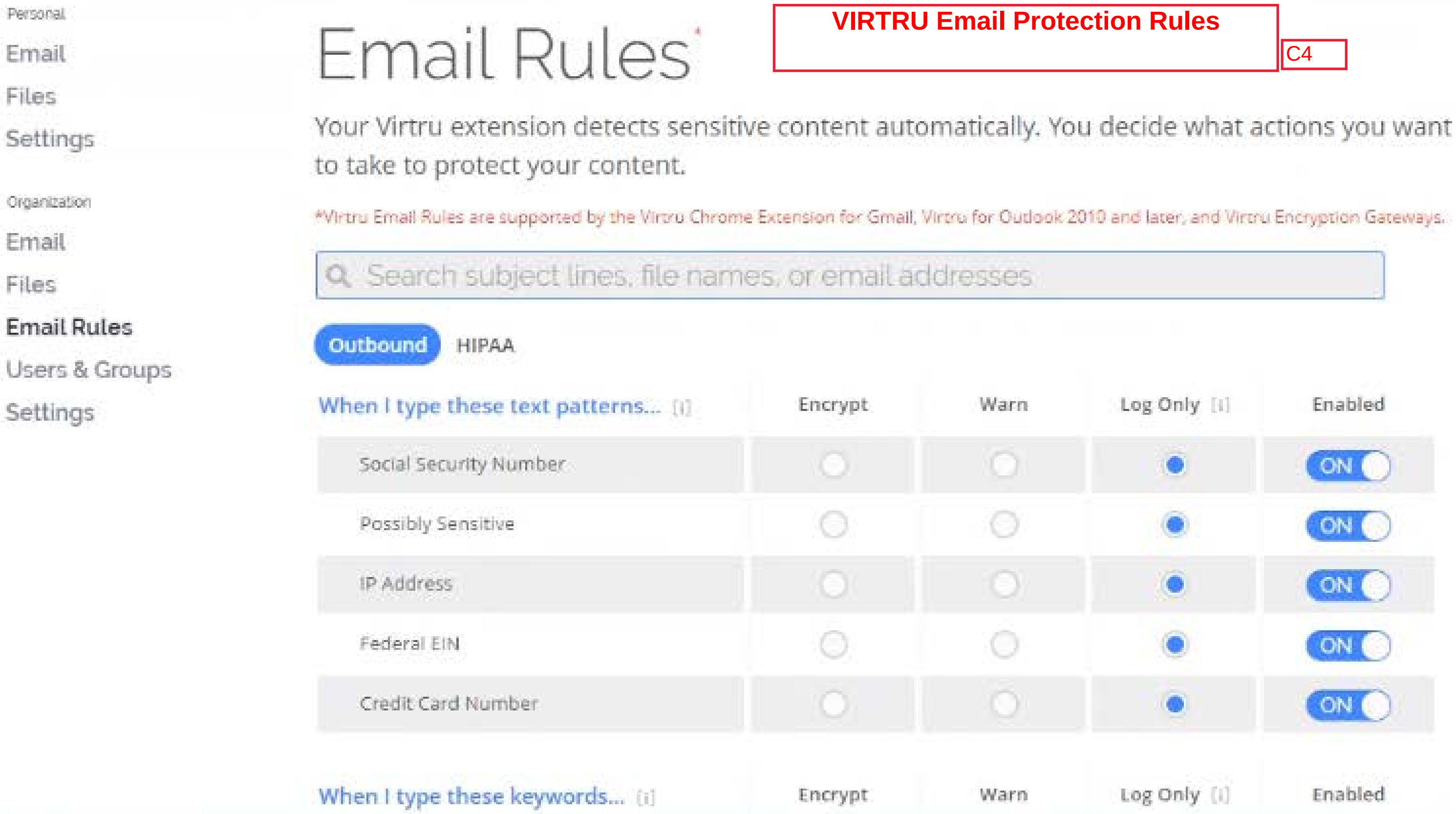
ATTACHMENT OPTIONS

- Watermarking: off
- Persistent Protection: on

This setting protects files by requiring authentication even if it's shared or downloaded to a computer

VIRTRU Email Protection Rules

C4



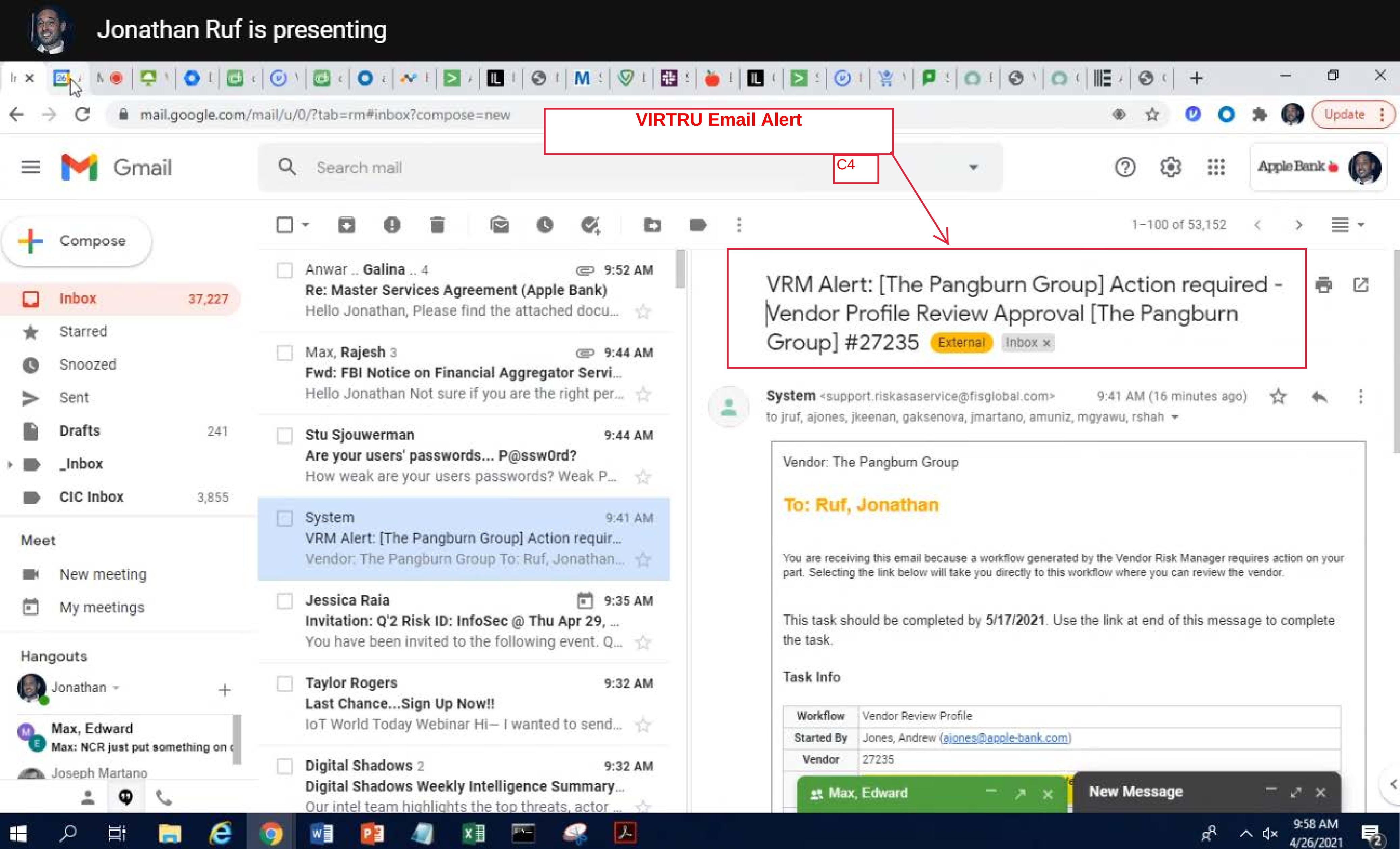
Email Rules*

Your Virtru extension detects sensitive content automatically. You decide what actions you want to take to protect your content.

*Virtru Email Rules are supported by the Virtru Chrome Extension for Gmail, Virtru for Outlook 2010 and later, and Virtru Encryption Gateways.

When I type these text patterns... [i]	Encrypt	Warn	Log Only [i]	Enabled
Social Security Number	○	○	●	ON
Possibly Sensitive	○	○	●	ON
IP Address	○	○	●	ON
Federal EIN	○	○	●	ON
Credit Card Number	○	○	●	ON

When I type these keywords... [i]	Encrypt	Warn	Log Only [i]	Enabled



VIRTRU Email Alert

C4

Anwar .. Galina .. 4	Re: Master Services Agreement (Apple Bank) Hello Jonathan, Please find the attached docu...	9:52 AM
Max, Rajesh 3	Fwd: FBI Notice on Financial Aggregator Servi... Hello Jonathan Not sure if you are the right per...	9:44 AM
Stu Sjouwerman	Are your users' passwords... P@ssw0rd? How weak are your users passwords? Weak P...	9:44 AM
System	VRM Alert: [The Pangburn Group] Action requir... Vendor: The Pangburn Group To: Ruf, Jonathan...	9:41 AM
Jessica Raia	Invitation: Q'2 Risk ID: InfoSec @ Thu Apr 29, ... You have been invited to the following event. Q...	9:35 AM
Taylor Rogers	Last Chance...Sign Up Now!! IoT World Today Webinar Hi— I wanted to send...	9:32 AM
Digital Shadows 2	Digital Shadows Weekly Intelligence Summary... Our intel team highlights the top threats, actor ...	9:32 AM

VRM Alert: [The Pangburn Group] Action required - Vendor Profile Review Approval [The Pangburn Group] #27235

System <support.riskasaservice@fisglobal.com> 9:41 AM (16 minutes ago)
to jruf, ajones, jkeenan, gaksenova, jmartano, amuniz, mgyawu, rshah

Vendor: The Pangburn Group

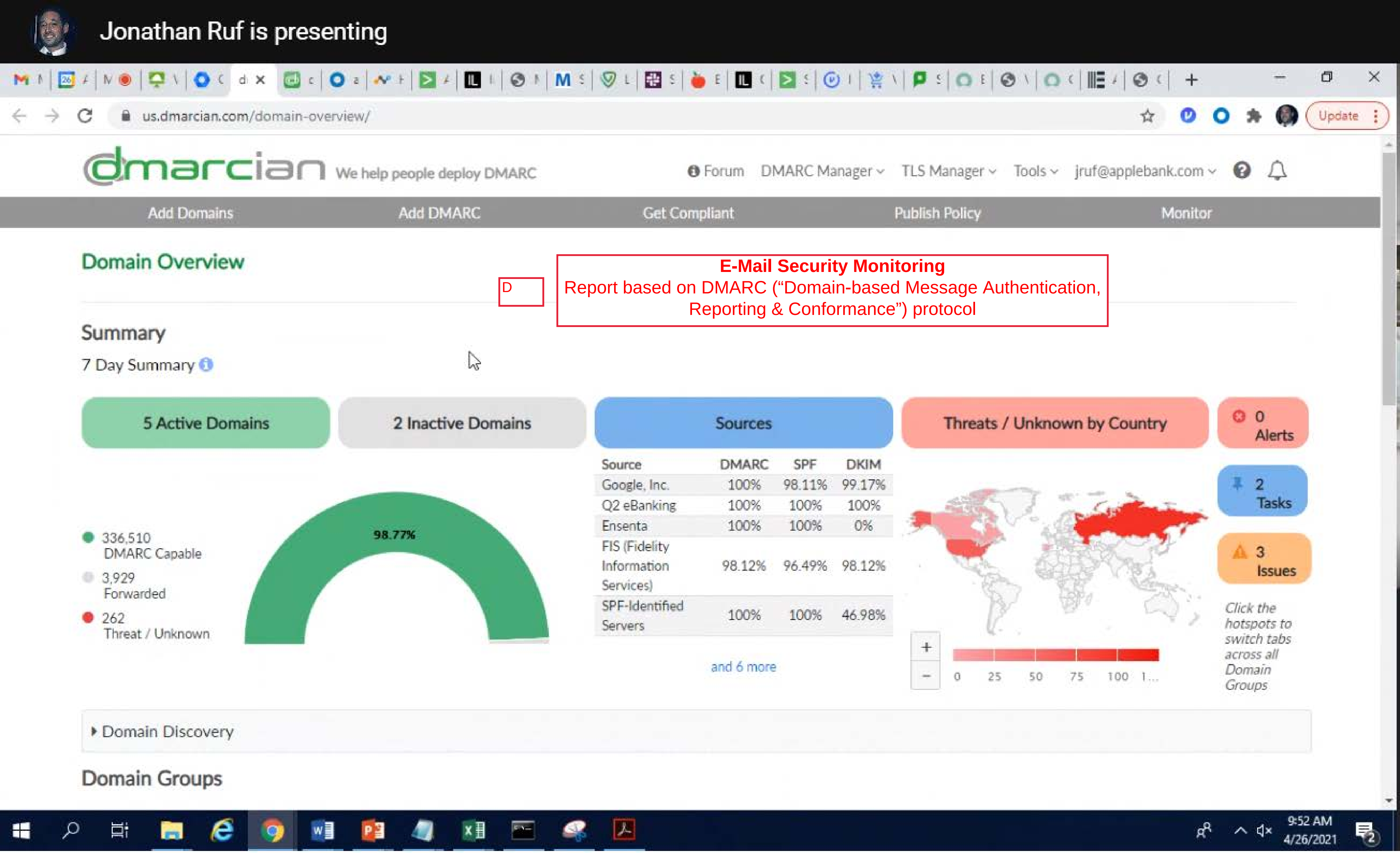
To: Ruf, Jonathan

You are receiving this email because a workflow generated by the Vendor Risk Manager requires action on your part. Selecting the link below will take you directly to this workflow where you can review the vendor.

This task should be completed by **5/17/2021**. Use the link at end of this message to complete the task.

Task Info

Workflow	Vendor Review Profile
Started By	Jones, Andrew (ajones@apple-bank.com)
Vendor	27235



Jonathan Ruf is presenting

us.dmarcian.com/domain-overview/

dmarcian We help people deploy DMARC

Forum DMARC Manager TLS Manager Tools jruf@applebank.com

Add Domains | Add DMARC | Get Compliant | Publish Policy | Monitor

Domain Overview

D

E-Mail Security Monitoring
Report based on DMARC ("Domain-based Message Authentication, Reporting & Conformance") protocol

Summary

7 Day Summary

5 Active Domains | 2 Inactive Domains | Sources | Threats / Unknown by Country | 0 Alerts

- ● 336,510 DMARC Capable
- ● 3,929 Forwarded
- ● 262 Threat / Unknown

98.77%

Source	DMARC	SPF	DKIM
Google, Inc.	100%	98.11%	99.17%
Q2 eBanking	100%	100%	100%
Ensenta	100%	100%	0%
FIS (Fidelity Information Services)	98.12%	96.49%	98.12%
SPF-Identified Servers	100%	100%	46.98%

and 6 more

2 Tasks

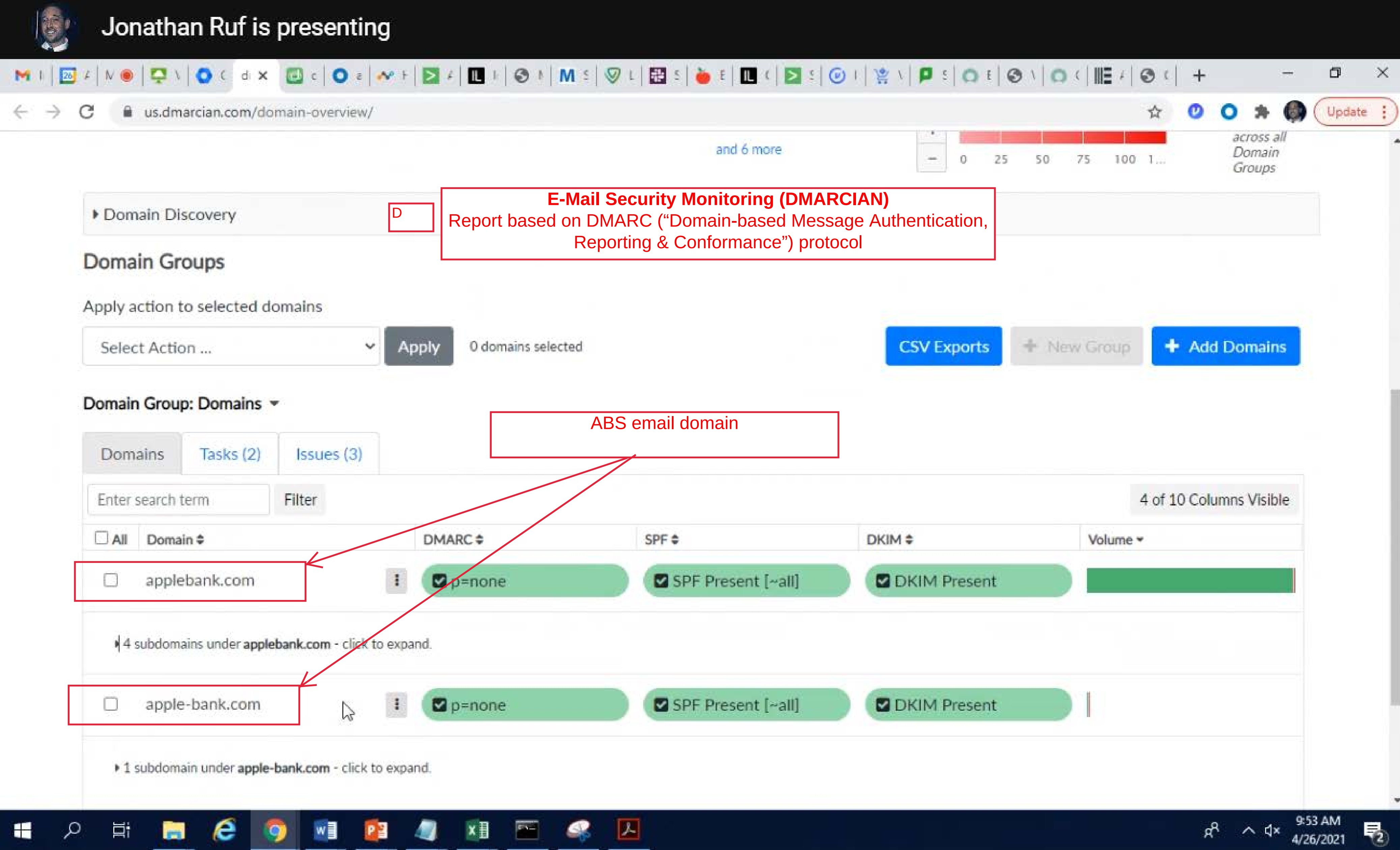
3 Issues

Click the hotspots to switch tabs across all Domain Groups

Domain Discovery

Domain Groups

9:52 AM
4/26/2021



E-Mail Security Monitoring (DMARCIAN)
Report based on DMARC (“Domain-based Message Authentication, Reporting & Conformance”) protocol

▸ Domain Discovery

Domain Groups

Apply action to selected domains

Select Action ... | Apply | 0 domains selected | CSV Exports | + New Group | + Add Domains

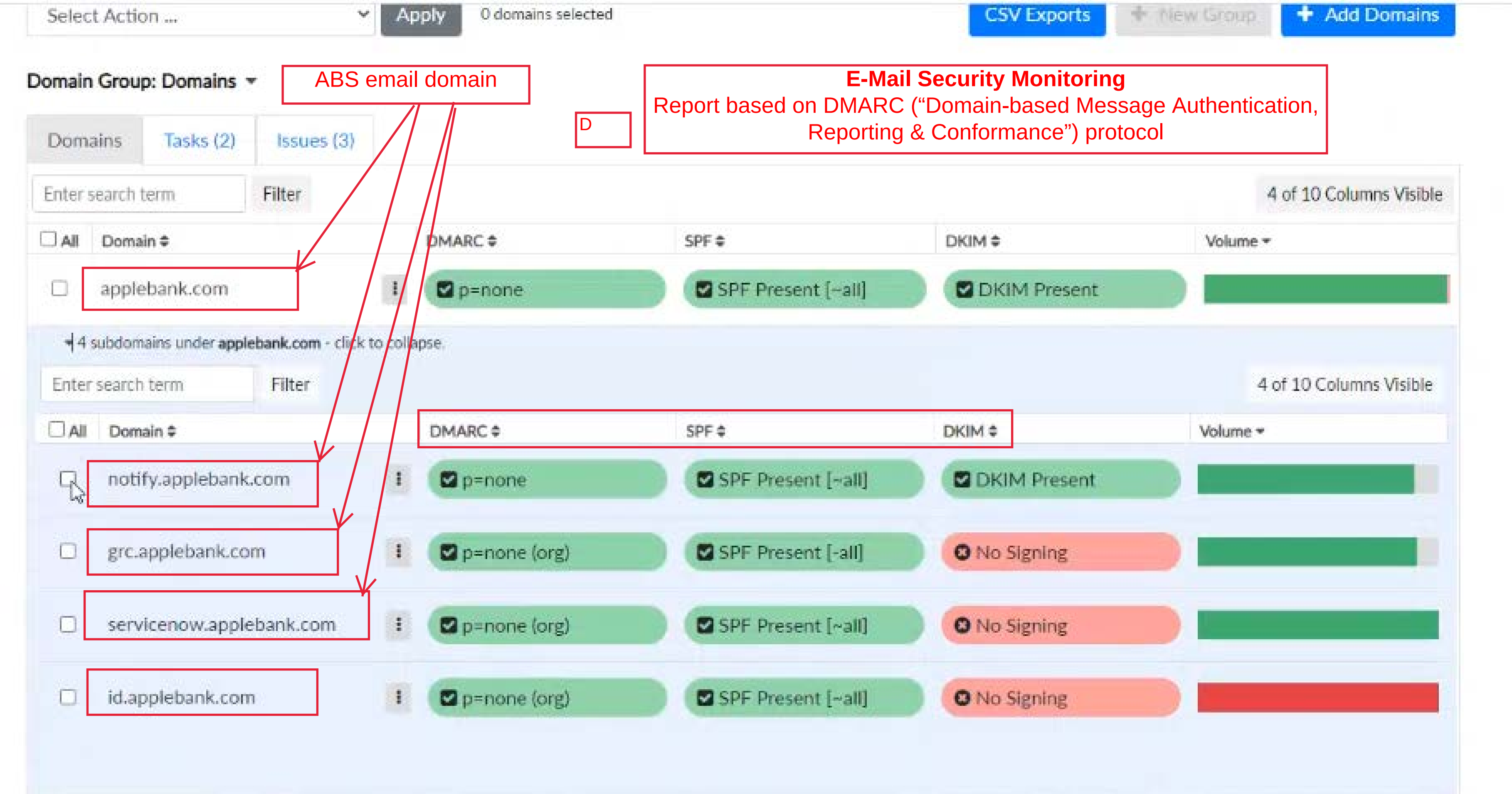
Domain Group: Domains ▾

ABS email domain

Domains | Tasks (2) | Issues (3)

Enter search term | Filter | 4 of 10 Columns Visible

□ All	Domain ⇕	DMARC ⇕	SPF ⇕	DKIM ⇕	Volume ▾
□	applebank.com	☑ p=none	☑ SPF Present [~all]	☑ DKIM Present	
	▸ 4 subdomains under **applebank.com** - click to expand.				
□	apple-bank.com	☑ p=none	☑ SPF Present [~all]	☑ DKIM Present	
	▸ 1 subdomain under **apple-bank.com** - click to expand.				



0 domains selected

E-Mail Security Monitoring

Report based on DMARC (“Domain-based Message Authentication, Reporting & Conformance”) protocol

ABS email domain

D

Domain Group: Domains

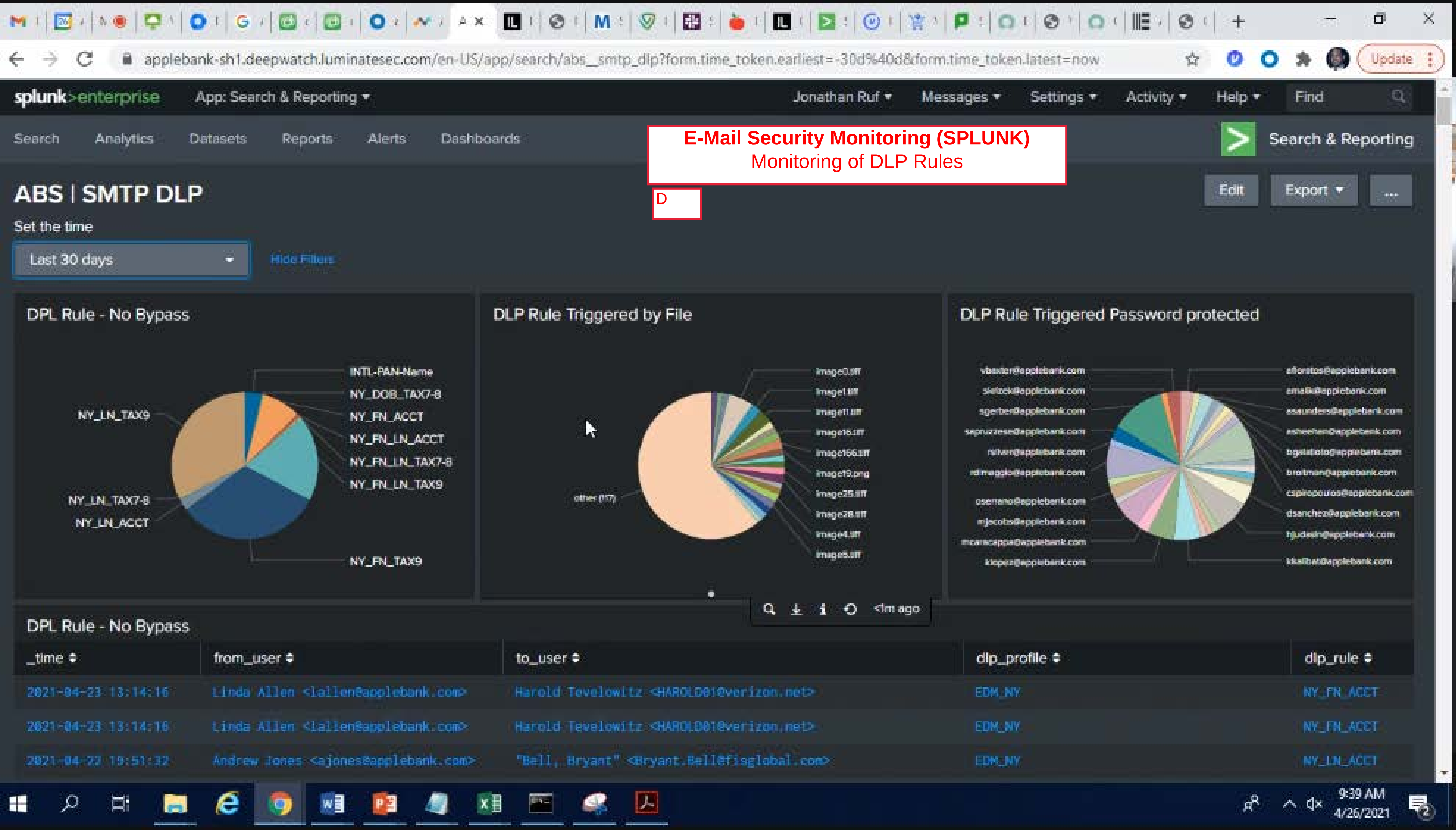
4 of 10 Columns Visible

□ All	Domain	DMARC	SPF	DKIM	Volume
□	applebank.com	☑ p=none	☑ SPF Present [~all]	☑ DKIM Present	🟩

4 subdomains under **applebank.com** - click to collapse

4 of 10 Columns Visible

□ All	Domain	DMARC	SPF	DKIM	Volume
□	notify.applebank.com	☑ p=none	☑ SPF Present [~all]	☑ DKIM Present	🟩
□	grc.applebank.com	☑ p=none (org)	☑ SPF Present [-all]	☒ No Signing	🟩
□	servicenow.applebank.com	☑ p=none (org)	☑ SPF Present [~all]	☒ No Signing	🟩
□	id.applebank.com	☑ p=none (org)	☑ SPF Present [~all]	☒ No Signing	🟥



E-Mail Security Monitoring (SPLUNK)
Monitoring of DLP Rules

D

applebank-sh1.deepwatch.luminatesec.com/en-US/app/search/abs__smtp_dlp?form.time_token.earliest=-30d%40d&form.time_token.latest=now
Update
splunk>enterprise
App: Search & Reporting ▾
Jonathan Ruf ▾
Messages ▾
Settings ▾
Activity ▾
Help ▾
Find
Search
Analytics
Datasets
Reports
Alerts
Dashboards
Search & Reporting
Edit
Export ▾
...

ABS | SMTP DLP

Set the time

Last 30 days ▾

Hide Filters

DPL Rule - No Bypass

DLP Rule Triggered by File

DLP Rule Triggered Password protected

DPL Rule - No Bypass

_time ⇕	from_user ⇕	to_user ⇕	dlp_profile ⇕	dlp_rule ⇕
2021-04-23 13:14:16	Linda Allen <lallen@applebank.com>	Harold Tevelowitz <HAROLD01@verizon.net>	EDM_NY	NY_FN_ACCT
2021-04-23 13:14:16	Linda Allen <lallen@applebank.com>	Harold Tevelowitz <HAROLD01@verizon.net>	EDM_NY	NY_FN_ACCT
2021-04-22 19:51:32	Andrew Jones <ajones@applebank.com>	"Bell, Bryant" <Bryant.Bell@fisglobal.com>	EDM_NY	NY_LN_ACCT