



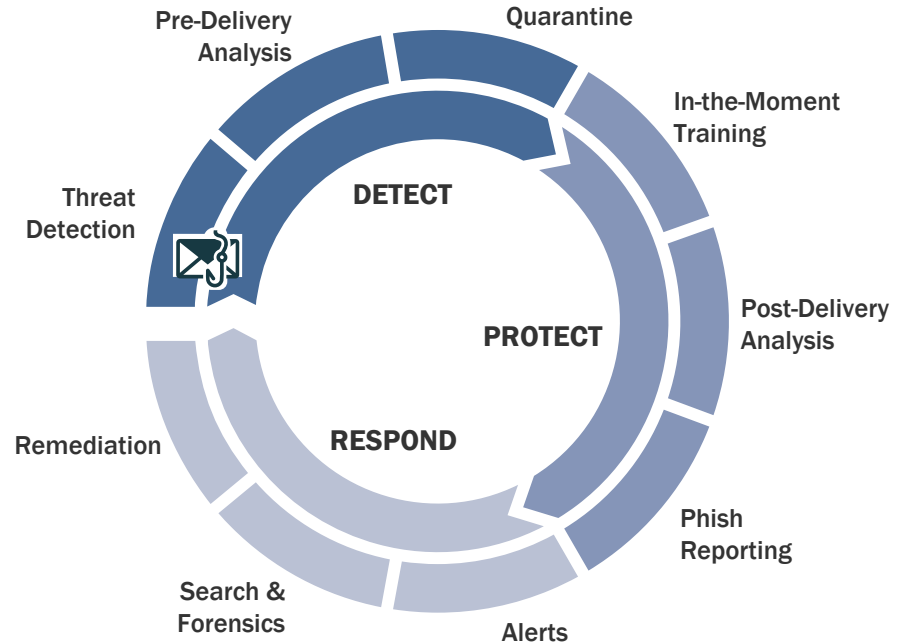
April 2020

# Threat Prevention, Detection, and Incident Response

GreatHorn

# Email Security as a Risk Management Function

- > Detect and block attacks **before** they reach users
- > Reduce attack engagement by warning users **during** an attack of potential threats
- > Limit exposure by automating incident response and remediation **after** an attack



# Detect and Block Attacks Before They Reach Users

## Policy Defaults

### Email Policies

| Status                              | Name                    |
|-------------------------------------|-------------------------|
|                                     | Domain Look-Alikes      |
|                                     | Auth Risks              |
|                                     | Name Spoofs             |
|                                     | Direct Spoofs           |
|                                     | Malicious Attachments   |
|                                     | Malicious Links         |
| <input checked="" type="checkbox"/> | Wire Transfer Content   |
| <input checked="" type="checkbox"/> | W2 Content              |
| <input checked="" type="checkbox"/> | Executive Impersonation |
| <input checked="" type="checkbox"/> | Gift Card Requests      |
| <input checked="" type="checkbox"/> | Microsoft Impersonation |
| <input checked="" type="checkbox"/> | Amazon Impersonation    |
| <input checked="" type="checkbox"/> | Banking Impersonation   |
| <input checked="" type="checkbox"/> | DocuSign Impersonation  |

## Customizable Policy Configuration

### Relationship Analysis Factors

From Address Reputation ?

No Reputation

From Domain Reputation ?

Moderate Reputation

From Recipient Relationship ?

Weak Relationship

From Organization Relationship ?

Weak Relationship

0  100

Authentication Risk Score ?

Higher than: 50 (High)

0  100

Name Spoofing Score ?

Higher than: 50 (High)

0  100

Domain Name

Display Name

## Automated Actions

### Policy Actions

Move to Trash ?

Quarantine Message ?

Send Quarantine Admin Alert To:

Please hit enter after each entry.

securityoperations@company.com

End User will receive a notification email:

- When an email is quarantined from their mailbox.
- When an email is released from quarantine back to their mailbox.

Remove Attachments ?

Add End-User Email Banners ?

Move to Folder ?

Add Label/Category ?

Archive ?

Send Admin Email Alert ?

Send End-User Email Alert ?

# Educating Users in the Moment of Risk

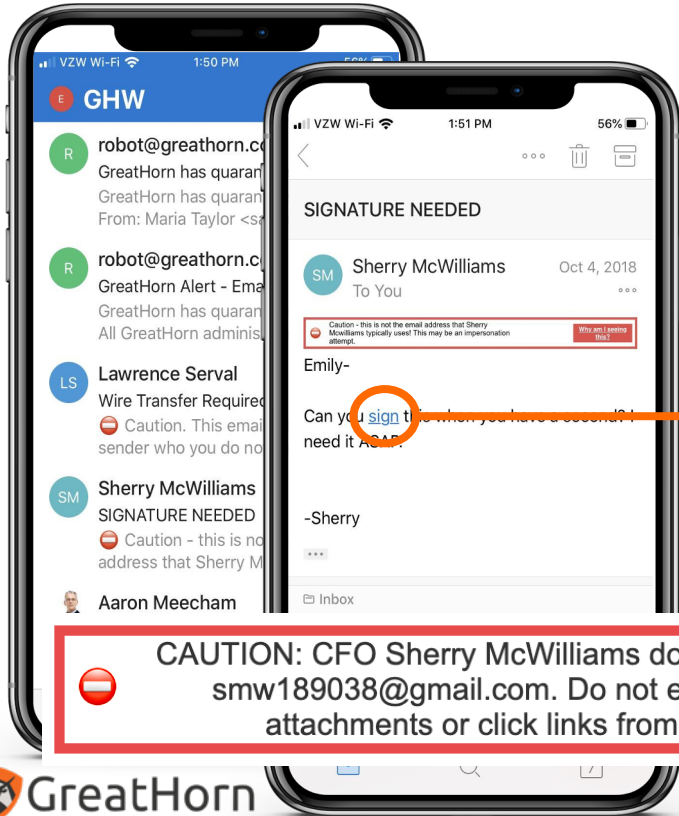
## Contextual Banning

The screenshot shows an Outlook inbox with a message from Sherry McWilliams. The message title is "Invoice - Payment Due". The sender is "Sherry McWilliams <smw189038@gmail.com>". The message body contains a PDF attachment titled "Invoice-883675-ServicesRend..." and a red banner with the text: "CAUTION: CFO Sherry McWilliams does not typically email from smw189038@gmail.com. Do not engage with, download attachments or click links from unknown senders." Below the banner, the text says "Please pay the invoice in the amount due." and there are three buttons: "Will do.", "Will do, thank you.", and "Will do, thanks!". A red box highlights the caution banner, and an arrow points from the banner in the list view to the banner in the message view.

> **Contextual  
banning  
during the  
moment of  
engagement.**

# Educating Users in the Moment of Risk

## Contextual Banning

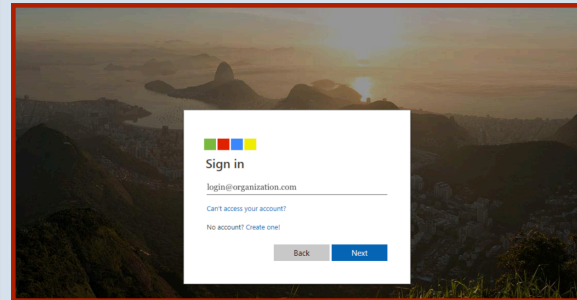


## On-Click Analysis & Link Protection

### Suspicious Link Detected

#### DESTINATION PAGE PREVIEW

Hosting Domain: <http://www.jerryflowershop.com/user-login/emilypost-flying-deliveries>



Credential Theft Check

Request Review

Take Me There


#### Why am I seeing this?

You have clicked on a link that may be an attempt to steal sensitive information, such as your username or password.

Cybercriminals often create fake "phishing" websites to steal passwords or download malware.

#### What should I do?

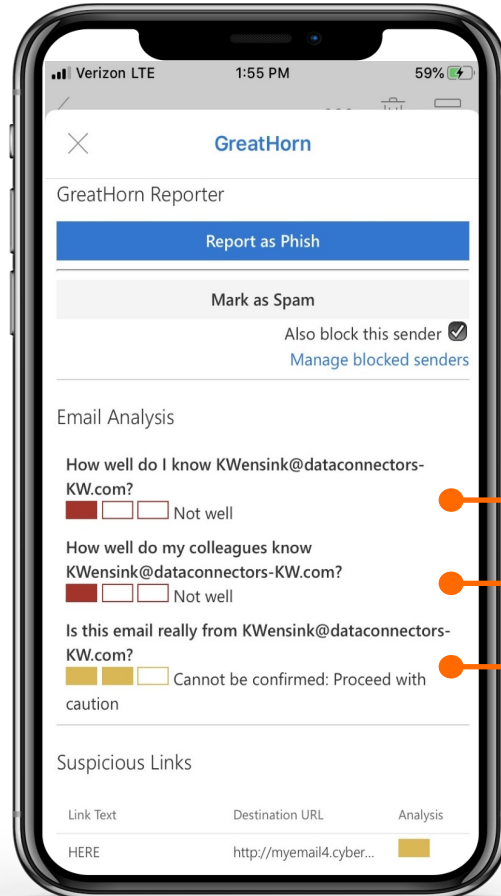
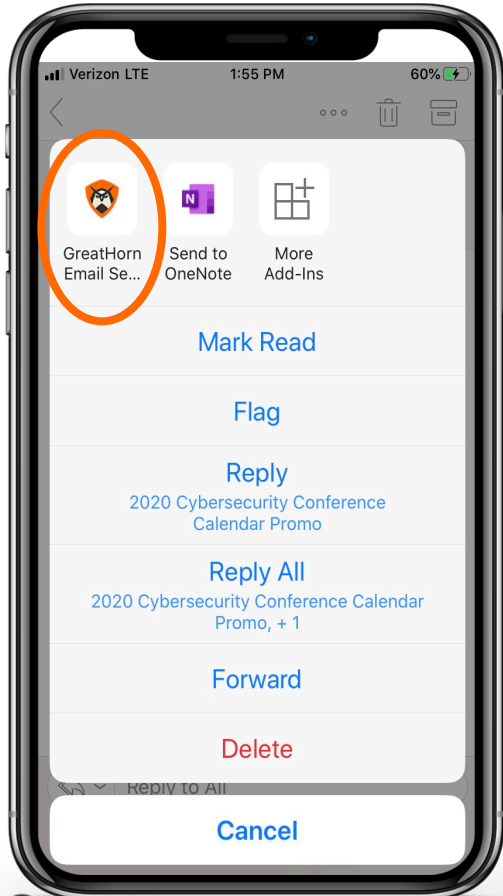
- 1 Carefully review both the website preview and the actual destination URL
- 2 Watch out for fake login screens requesting username & password details
- 3 "Take Me There" to visit the website anyway. "Request review" if you are certain that the website is trustworthy.

 **CAUTION: CFO Sherry McWilliams does not typically email from smw189038@gmail.com. Do not engage with, download attachments or click links from unknown senders**



**'Why am I seeing this?'**

# Educating Users in the Moment of Risk – Phish Reporting



> Give users the contextual information to make **better decisions**

"I've never engaged with this user"

"No one at my organization has ever engaged with this user"

"Is this really who they say it is?"

# Mitigate Threats During or After an Attack

## Advanced Search Capability on Common Criteria

### Email Search

**To** <sup>?</sup>  
Please use full addresses or the username.  
**Recipient** <sup>?</sup>  
Please hit enter after each entry.

**Exclude Recipient** <sup>?</sup>  
Please hit enter after each entry.

**Mailbox** <sup>?</sup>  
Please hit enter after each entry.

**Sent On/Between**  
Select a Date Range:  One Day  Multi Day  
February - 2020  

|    |    |    |    |    |    |    |    |
|----|----|----|----|----|----|----|----|
| Su | Mo | Tu | We | Th | Fr | Sa | Su |
| 26 | 27 | 28 | 29 | 30 | 31 | 1  | 1  |
| 2  | 3  | 4  | 5  | 6  | 7  | 8  | 8  |
| 9  | 10 | 11 | 12 | 13 | 14 | 15 | 15 |
| 16 | 17 | 18 | 19 | 20 | 21 | 22 | 22 |
| 23 | 24 | 25 | 26 | 27 | 28 | 29 | 29 |
| 1  | 2  | 3  | 4  | 5  | 6  | 7  | 5  |

**From** <sup>?</sup>  
Please use full addresses or the username.  
**Sender** <sup>?</sup>  
Please hit enter after each entry.

**Exclude Sender** <sup>?</sup>  
Please hit enter after each entry.

**Return Path** <sup>?</sup>  
Please hit enter after each entry.

**Exclude Return Path** <sup>?</sup>  
Please hit enter after each entry.

**Reply-To Address** <sup>?</sup>

**Exclude Reply-To Address** <sup>?</sup>

**IP Addresses** <sup>?</sup>  
Please hit enter after each entry.

**Display Name** <sup>?</sup>

**Email Headers**

**Email Subject** <sup>?</sup>  
 Exact Text  Contains Text

**Authentication-results**

**Received**

**X-mailer**

**X-original-authentication-results**

## Purge Threats Immediately and in one Bulk Action

### Search Results

Select All | Select... | Apply to Selected | Apply to All

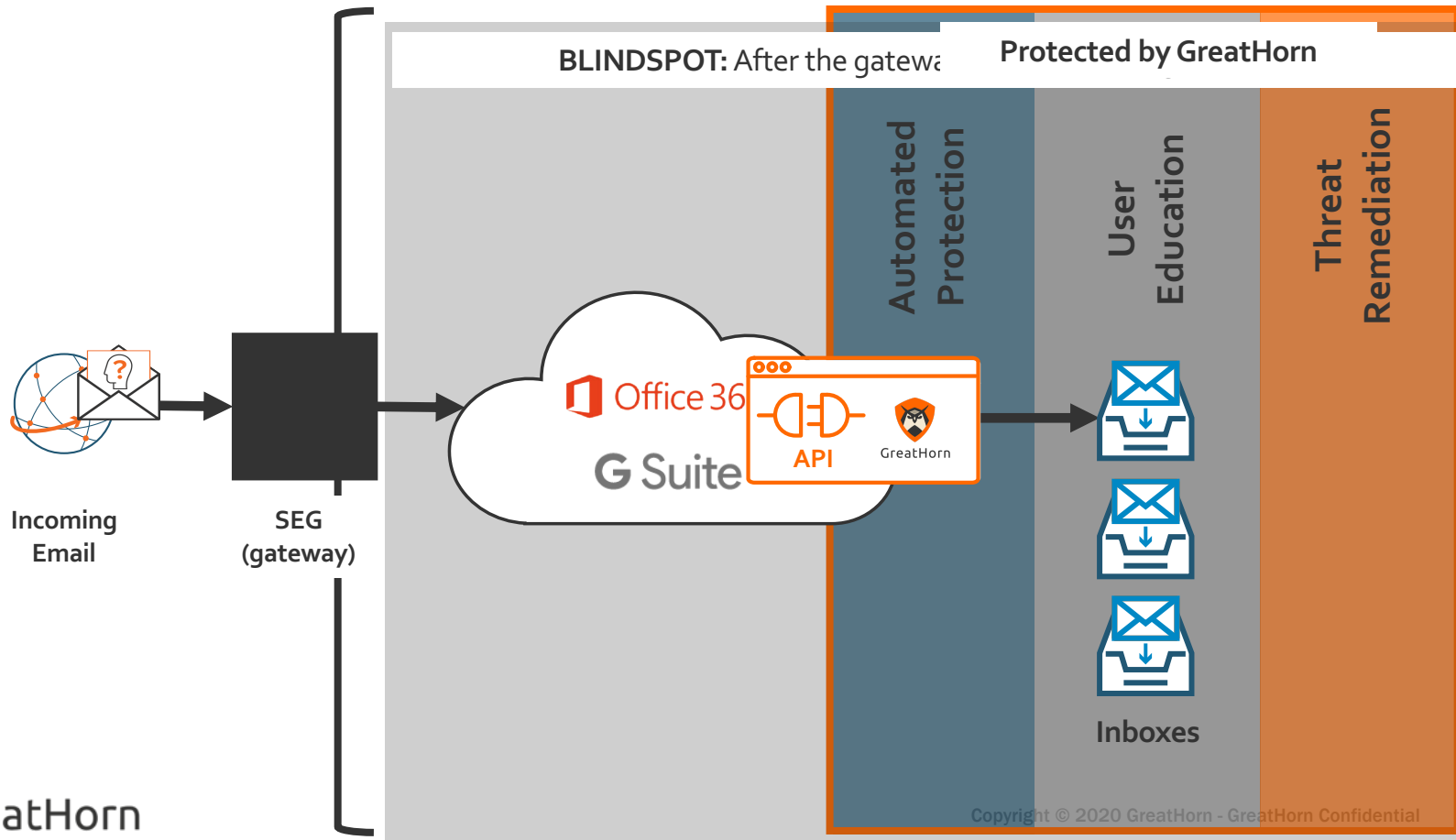
|                                     |       | Mailbox In          | Return Path                   | Subject   | Policy Violated                       |
|-------------------------------------|-------|---------------------|-------------------------------|-----------|---------------------------------------|
| <input checked="" type="checkbox"/> | 1     |                     |                               |           |                                       |
| <input checked="" type="checkbox"/> | 3     |                     | toby@flyingdeliveries.com     | gmail.com | "Invoice - Payment Due" Name Spoofs > |
| <input checked="" type="checkbox"/> |       |                     | lawrence@flyingdeliveries.com | gmail.com | "Invoice - Payment Due" Name Spoofs > |
| <input checked="" type="checkbox"/> |       |                     | emily@flyingdeliveries.com    | gmail.com | "Invoice - Payment Due" Name Spoofs > |
| <input checked="" type="checkbox"/> | 3     |                     | aaron@flyingdeliveries.com    | gmail.com | "Invoice - Payment Due" Name Spoofs > |
| <input checked="" type="checkbox"/> | 36583 | smw189038@gmail.com | morgan@flyingdeliveries.com   | gmail.com | "Invoice - Payment Due" Name Spoofs > |
| <input checked="" type="checkbox"/> | 36571 | smw189038@gmail.com | morgan@flyingdeliveries.com   | gmail.com | "Invoice - Payment Due" Name Spoofs > |
| <input checked="" type="checkbox"/> | 36570 | smw189038@gmail.com | emily@flyingdeliveries.com    | gmail.com | "Invoice - Payment Due" Name Spoofs > |
| <input checked="" type="checkbox"/> | 36574 | smw189038@gmail.com | toby@flyingdeliveries.com     | gmail.com | "Invoice - Payment Due" Name Spoofs > |
| <input checked="" type="checkbox"/> | 36577 | smw189038@gmail.com | lawrence@flyingdeliveries.com | gmail.com | "Invoice - Payment Due" Name Spoofs > |
| <input checked="" type="checkbox"/> | 36582 | smw189038@gmail.com | aaron@flyingdeli              |           |                                       |
| <input checked="" type="checkbox"/> | 36563 | smw189038@gmail.com | emily@flyingdeli              |           |                                       |
| <input checked="" type="checkbox"/> | 36568 | smw189038@gmail.com | lawrence@flying               |           |                                       |
| <input checked="" type="checkbox"/> | 36566 | smw189038@gmail.com | aaron@flyingdeli              |           |                                       |
| <input checked="" type="checkbox"/> | 36564 | smw189038@gmail.com | toby@flyingdeli               |           |                                       |
| <input checked="" type="checkbox"/> | 36567 | smw189038@gmail.com | morgan@flyingd                |           |                                       |
| <input checked="" type="checkbox"/> | 36555 | smw189038@gmail.com | morgan@flyingd                |           |                                       |
| <input checked="" type="checkbox"/> | 36559 | smw189038@gmail.com | emily@flyingdeli              |           |                                       |
| <input checked="" type="checkbox"/> | 36553 | smw189038@gmail.com | emily@flyingdeliveries.com    | gmail.com | "Invoice - Payment Due" Name Spoofs > |

**Apply Action to All Events**

Clicking apply will remove all 2418 searched events from the respective user's mailbox.

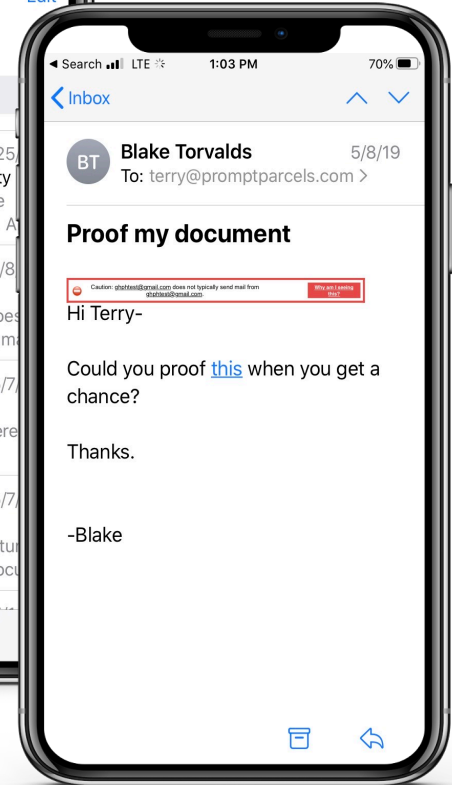
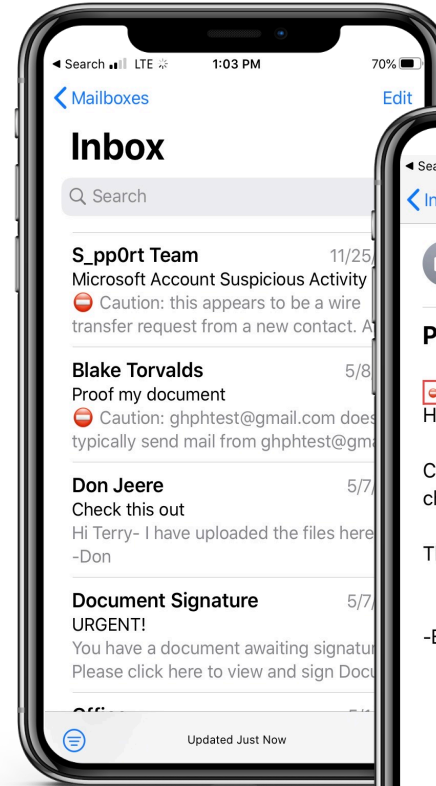
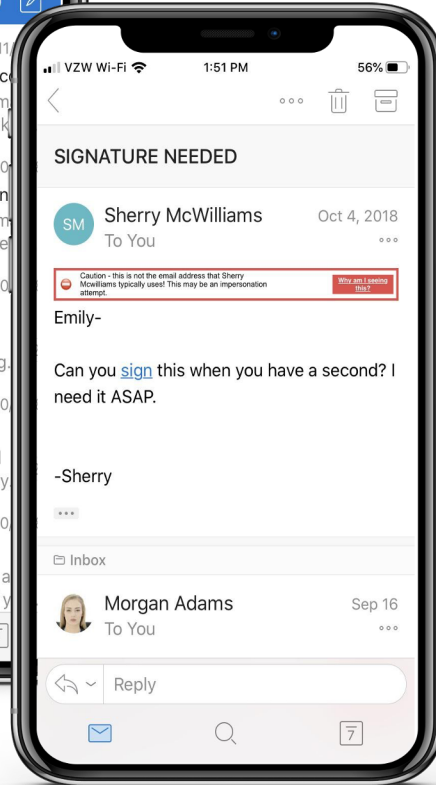
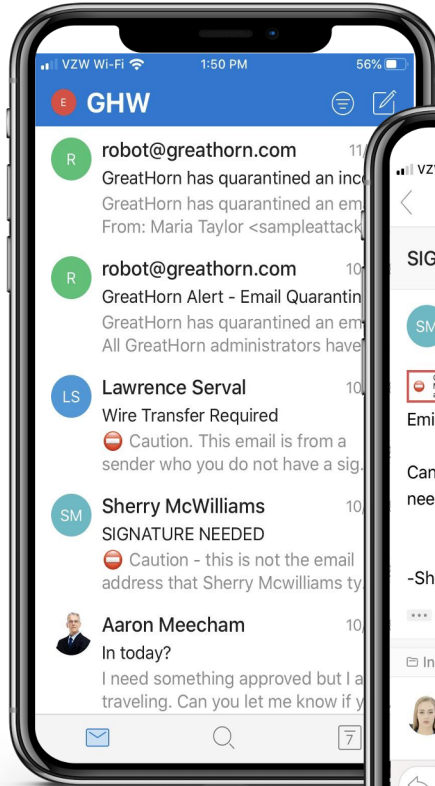
Are you sure?

# Traditional LogP1 App Gateway Approach

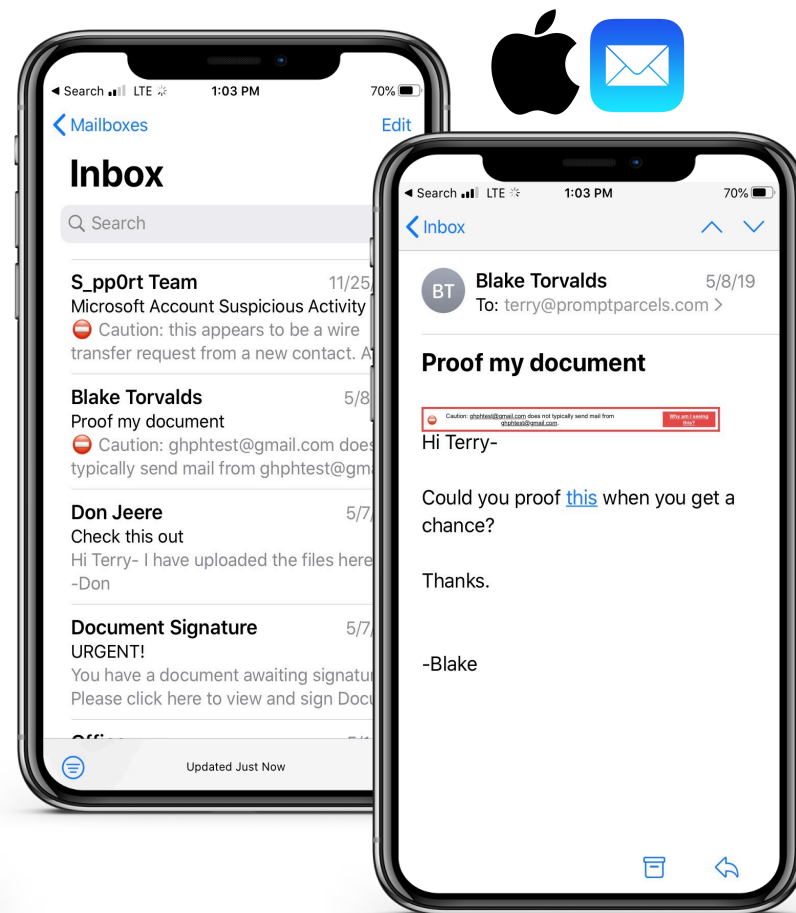
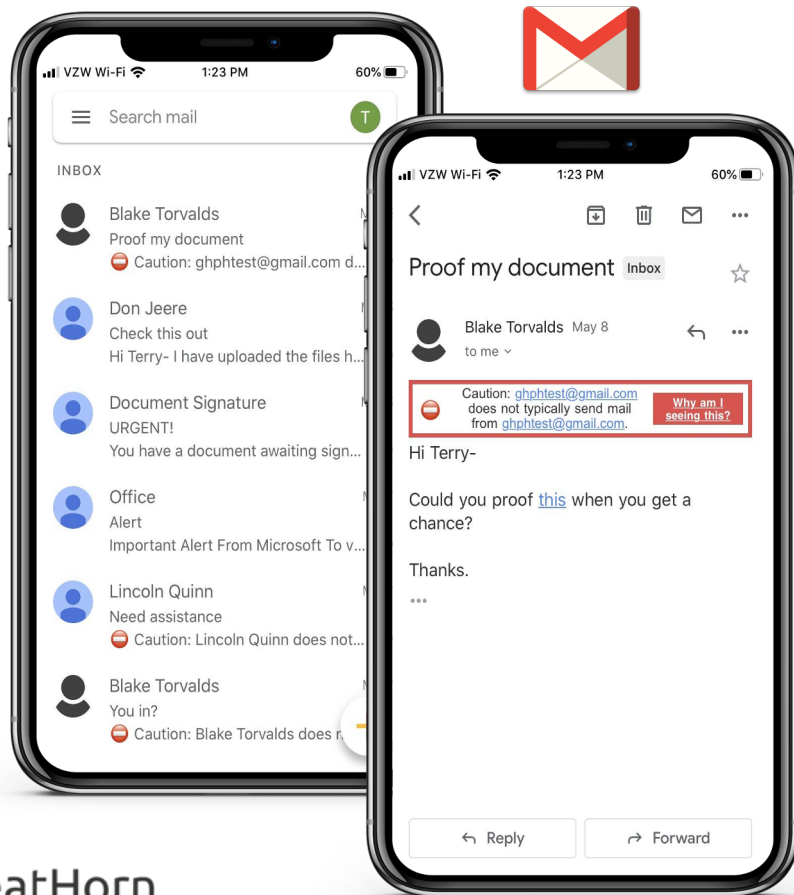




# Banners – Microsoft Office 365 Mobile View



# Banners – Google G Suite Mobile View



## Next Steps: See it in Action

- > Manage phishing risk with an integrated email security platform designed for protection, not just prevention.

**CONTACT INFO:**  
greathorn.com  
info@greathorn.com  
855-478-4676

