March 25, 2020

First Look:
Account Takeover Protection

Logistics

- You will be on mute
- Submit questions in the Q&A box (probably on the right side of your screen) in the GoToWebinar control panel
- Webinar is being recorded and will be available for replay
- Slides will be made available after the webinar

Matt Petrosky
Vice President, Customer Experience
GreatHorn

Agenda

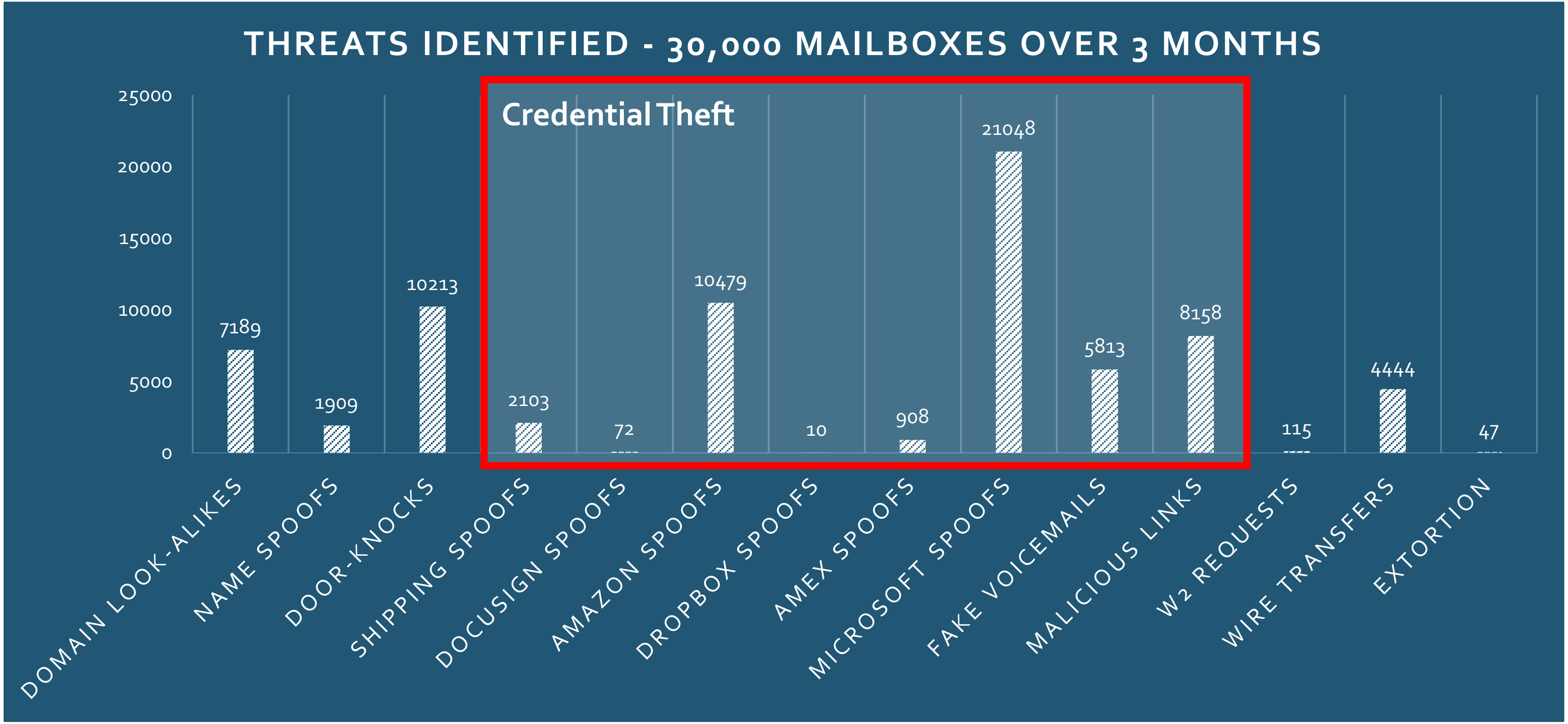
> Prevalence of credential theft attacks

> GreatHorn's existing protections against account takeover

> Overview of new Account Takeover Product

> Product showcase

Prevalence of Credential Theft Attacks



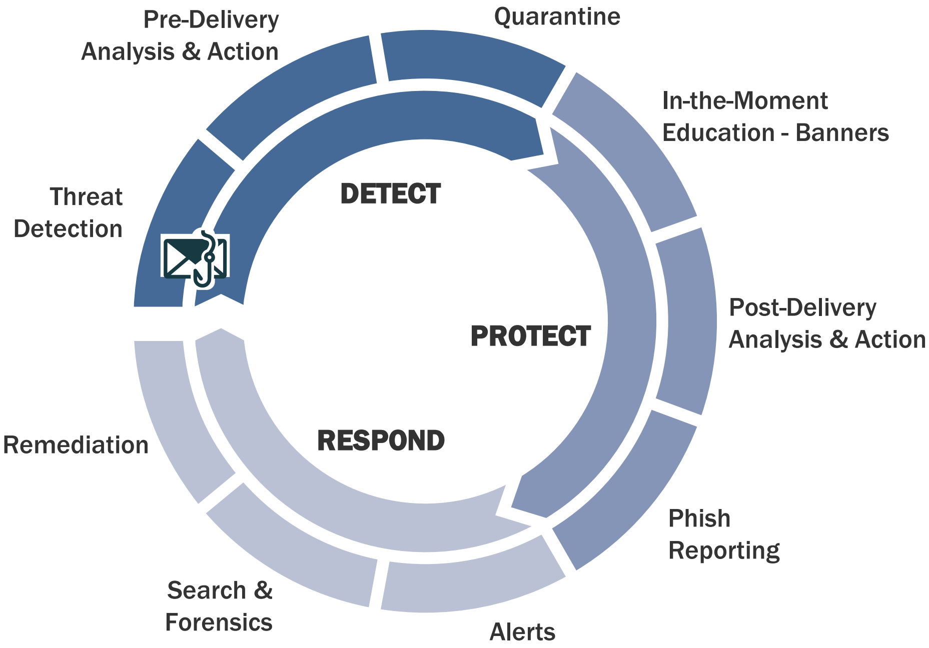
GreatHorn

GreatHorn Philosophy:
Treat Email Security as a Risk Management Function

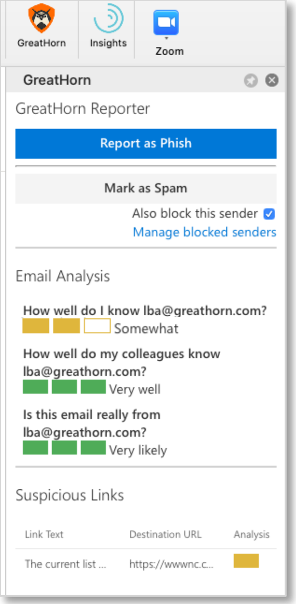
> Detect and remove attacks *before* employees see them

> Protect employees *during* an attack by alerting them to potential threats

> Respond quickly *after* an attack to limit exposure and minimize risk



Three Layers of Protection Against Account Takeover



GreatHorn

GreatHorn Reporter

Report as Phish

Mark as Spam

Also block this sender ☑

Manage blocked senders

Email Analysis

How well do I know lba@greathorn.com?
🟨🟨☐ Somewhat

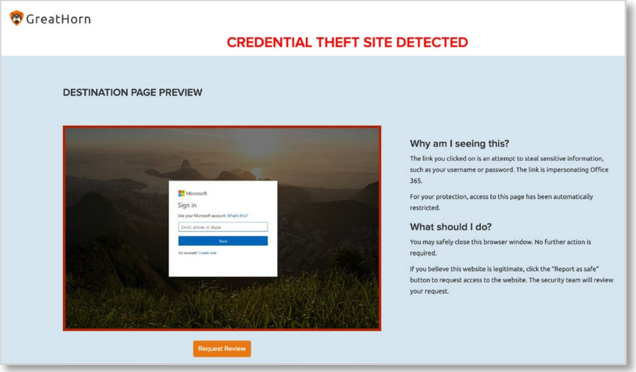
How well do my colleagues know lba@greathorn.com?
🟩🟩🟩 Very well

Is this email really from lba@greathorn.com?
🟩🟩🟩 Very likely

Suspicious Links

Link Text	Destination URL	Analysis
The current list ...	https://wwwnc.c...	🟨

Internal Email Protection



GreatHorn

CREDENTIAL THEFT SITE DETECTED

DESTINATION PAGE PREVIEW

Why am I seeing this?

The link you clicked on is an attempt to steal sensitive information, such as your username or password. The link is impersonating Office 365.

For your protection, access to this page has been automatically restricted.

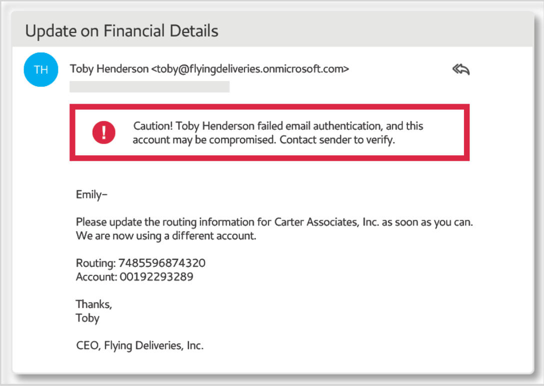
What should I do?

You may safely close this browser window. No further action is required.

If you believe this website is legitimate, click the "Report as safe" button to request access to the website. The security team will review your request.

Request Review

Credential Theft Site Identification



Update on Financial Details

TH Toby Henderson <toby@flyingdeliveries.onmicrosoft.com>

Caution! Toby Henderson failed email authentication, and this account may be compromised. Contact sender to verify.

Emily–

Please update the routing information for Carter Associates, Inc. as soon as you can. We are now using a different account.

Routing: 7485596874320
Account: 00192293289

Thanks,
Toby

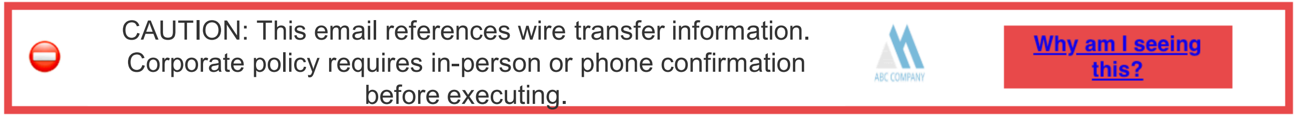
CEO, Flying Deliveries, Inc.

Account Takeover Protection

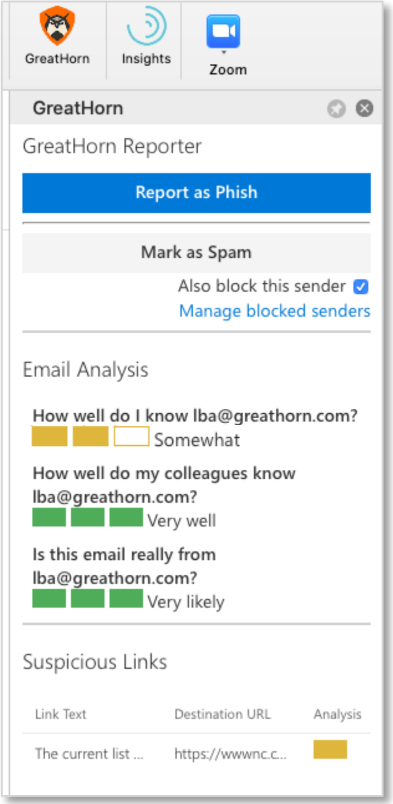
Layer 1: Internal Email Protection

- Internal email is protected in the same way as external
  - Adaptive threat detection, e.g. analyzing for relationships, communication patterns, authentication drift, etc.
  - Link analysis and rewriting

- Warning banners can be particularly effective to reinforce policies



CAUTION: This email references wire transfer information. Corporate policy requires in-person or phone confirmation before executing.



GreatHorn

GreatHorn Reporter

Also block this sender ☑

Manage blocked senders

Email Analysis

How well do I know lba@greathorn.com?
🟨🟨□ Somewhat

How well do my colleagues know lba@greathorn.com?
🟩🟩🟩 Very well

Is this email really from lba@greathorn.com?
🟩🟩🟩 Very likely

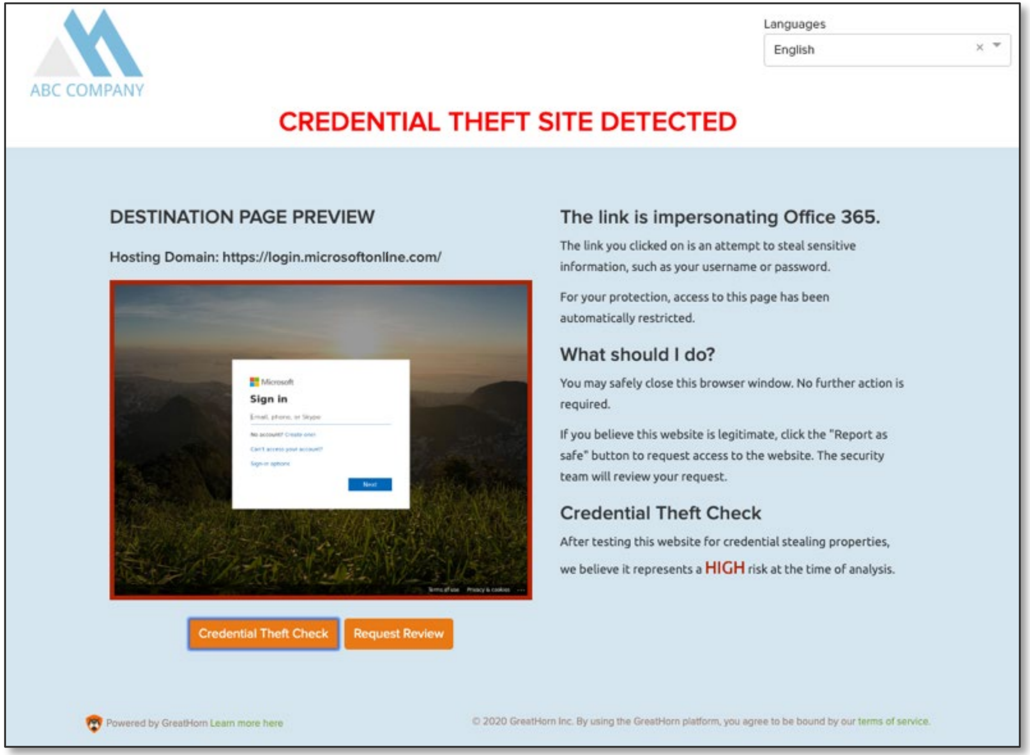
Suspicious Links

Link Text	Destination URL	Analysis
The current list ...	https://wwwnc.c...	🟨

Layer 2: Credential Theft Protection

- Scanned upon delivery and again at time-of-click

- Combines computer vision and email / link analysis to identify credential theft sites



CREDENTIAL THEFT SITE DETECTED

DESTINATION PAGE PREVIEW

Hosting Domain: https://login.microsoftonline.com/

The link is impersonating Office 365.

The link you clicked on is an attempt to steal sensitive information, such as your username or password.

For your protection, access to this page has been automatically restricted.

What should I do?

You may safely close this browser window. No further action is required.

If you believe this website is legitimate, click the "Report as safe" button to request access to the website. The security team will review your request.

Credential Theft Check

After testing this website for credential stealing properties, we believe it represents a HIGH risk at the time of analysis.

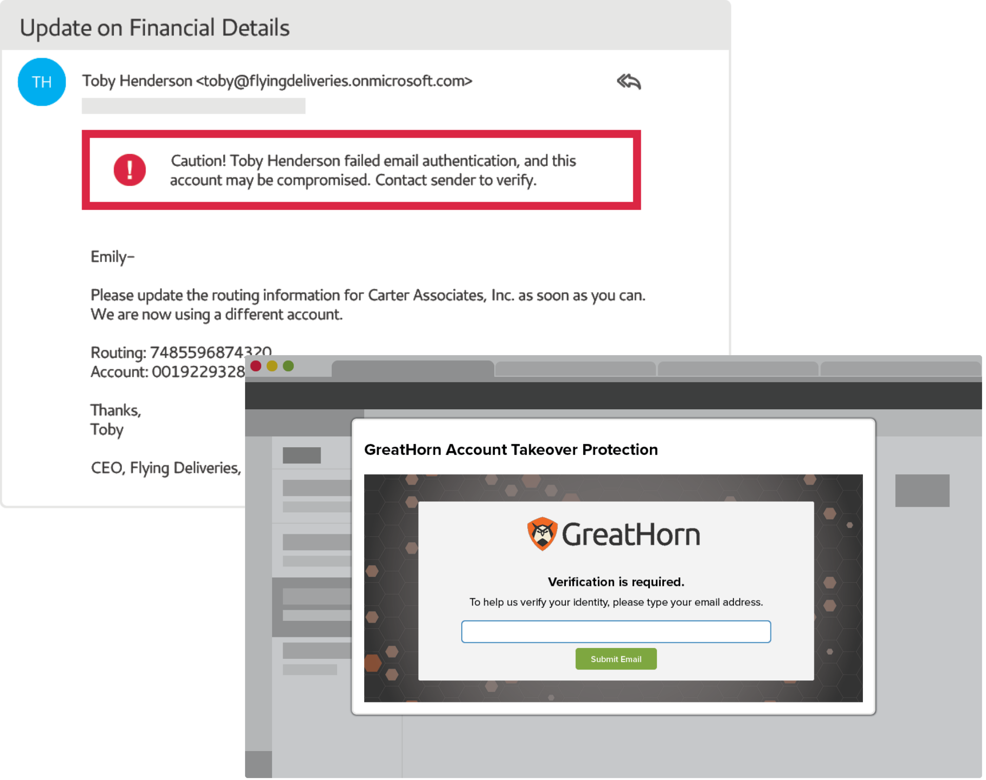
Powered by GreatHorn Learn more here

© 2020 GreatHorn Inc. By using the GreatHorn platform, you agree to be bound by our terms of service.

Layer 3: Account Takeover Protection (in Beta)

Identify compromised accounts through out-of-band authentication

- Uses biometric typing patterns as a unique identifier
- Periodic reauthorizations based on time or email volume



Update on Financial Details

TH Toby Henderson <toby@flyingdeliveries.onmicrosoft.com>

Caution! Toby Henderson failed email authentication, and this account may be compromised. Contact sender to verify.

Emily–

Please update the routing information for Carter Associates, Inc. as soon as you can. We are now using a different account.

Routing: 7485596874320
Account: 0019229328

Thanks,
Toby

CEO, Flying Deliveries,

GreatHorn Account Takeover Protection

GreatHorn

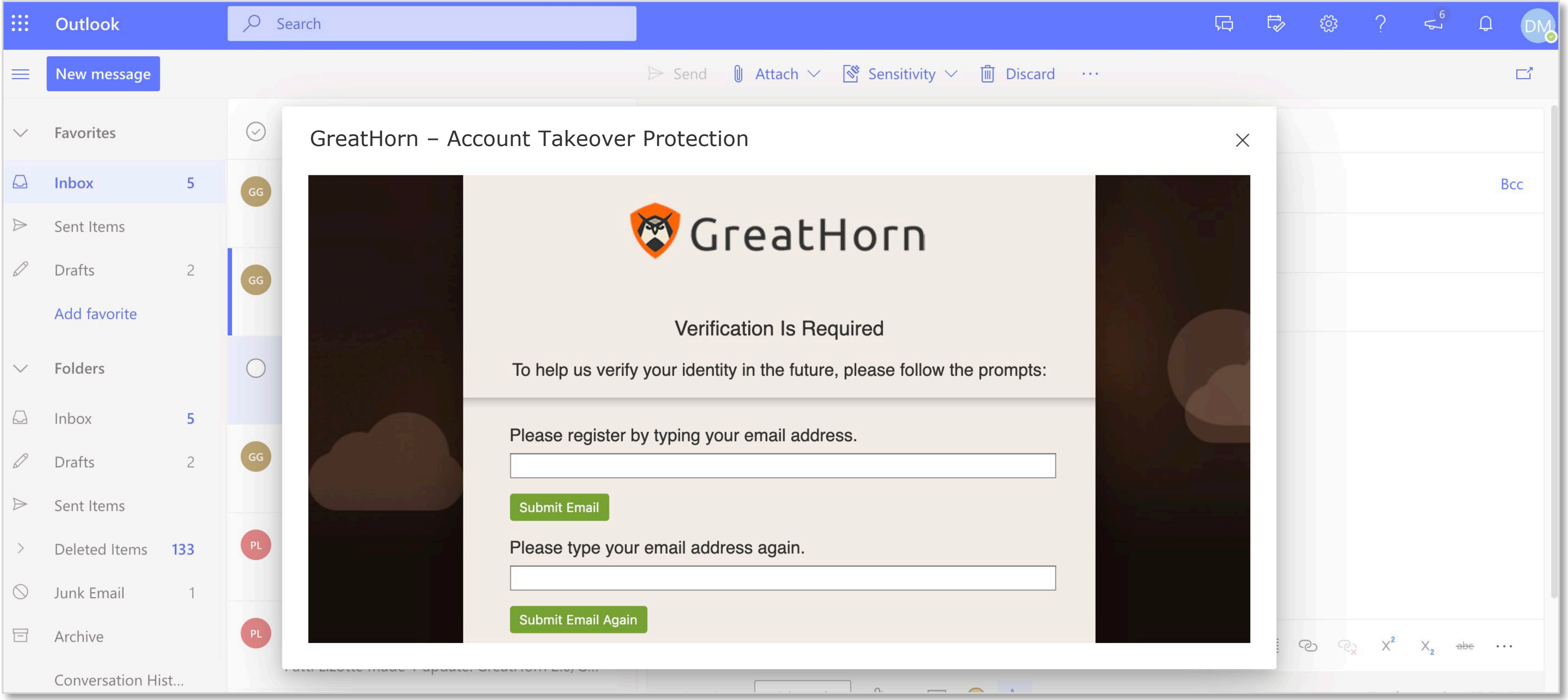
Verification is required.

To help us verify your identity, please type your email address.

GreatHorn

Demonstration

ATO Protection: Initial Set-Up



GreatHorn – Account Takeover Protection

Verification Is Required

To help us verify your identity in the future, please follow the prompts:

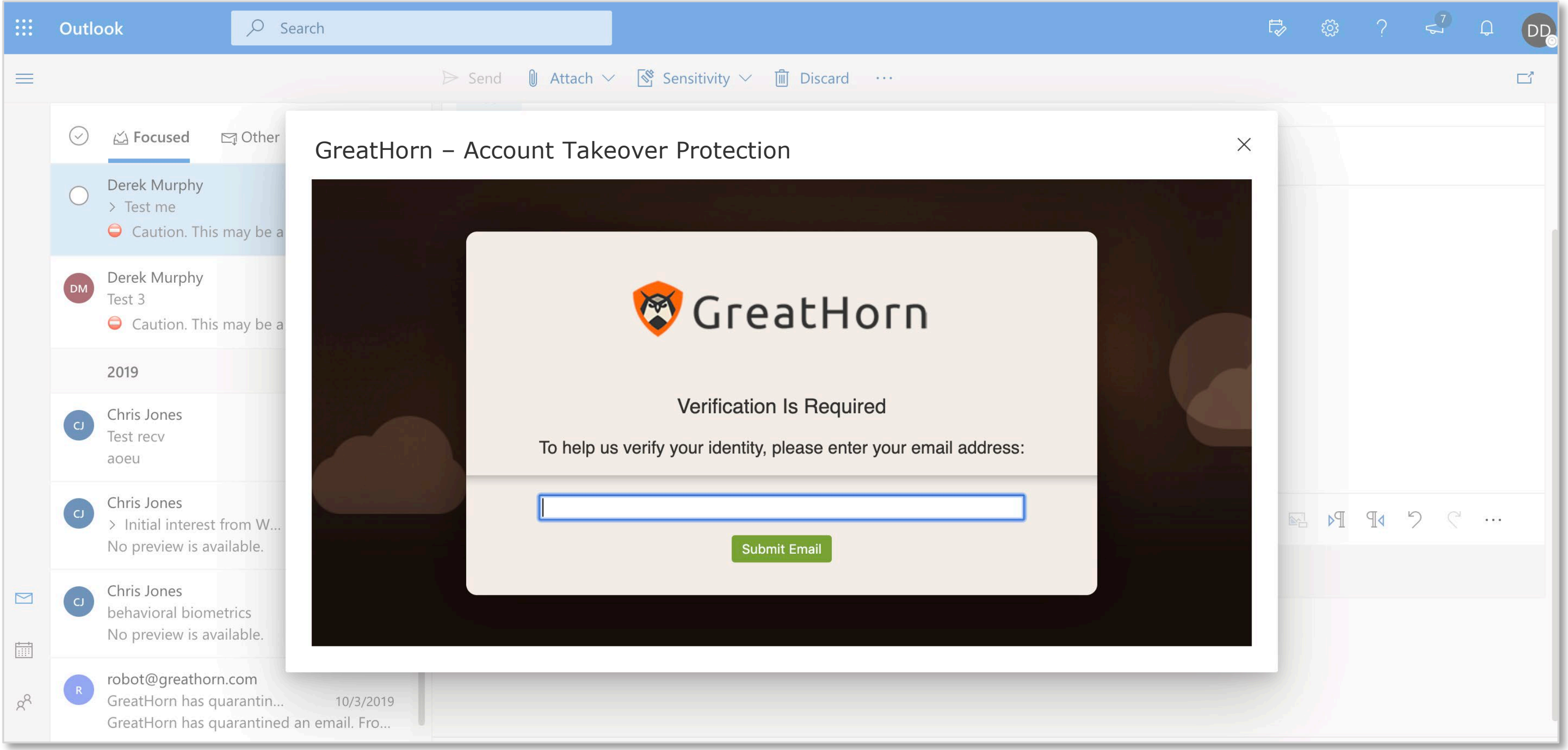
Please register by typing your email address.

Submit Email

Please type your email address again.

Submit Email Again

ATO Protection: Re-Verification



Derek Murphy
Test me
Caution. This may be a

Derek Murphy
Test 3
Caution. This may be a

2019

Chris Jones
Test recv
aoeu

Chris Jones
Initial interest from W...
No preview is available.

Chris Jones
behavioral biometrics
No preview is available.

robot@greathorn.com
GreatHorn has quarantin... 10/3/2019
GreatHorn has quarantined an email. Fro...

GreatHorn – Account Takeover Protection

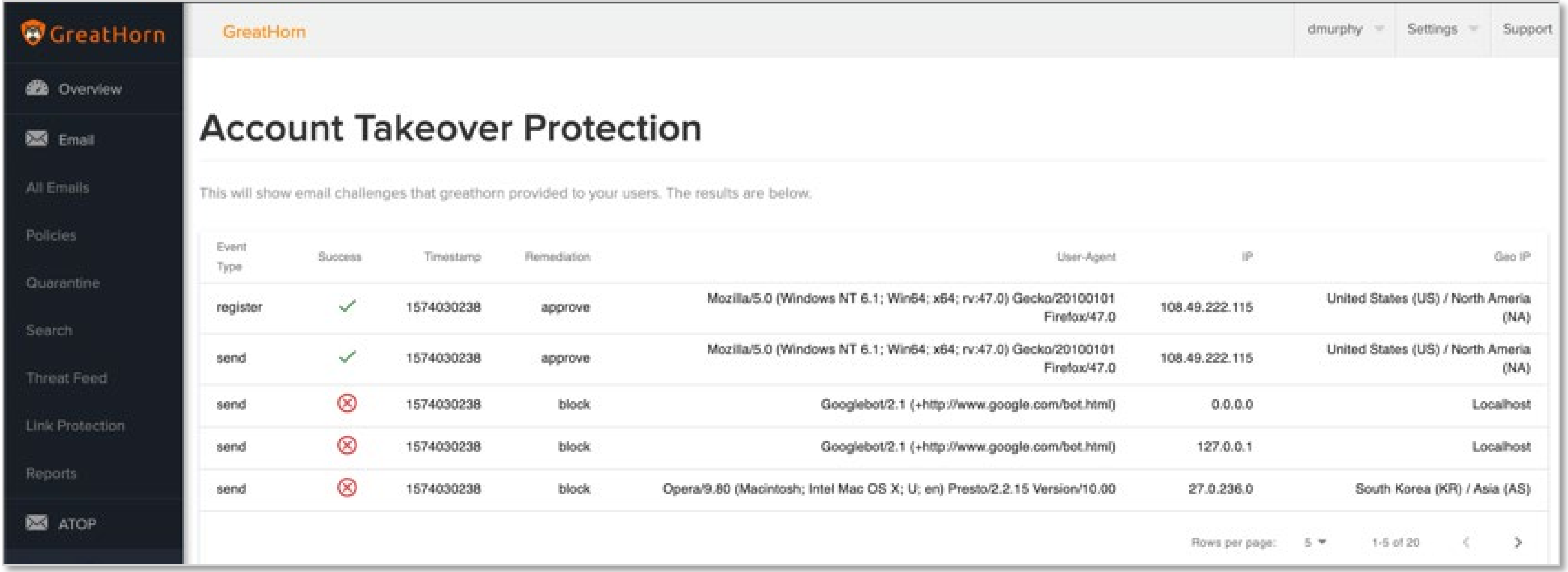
GreatHorn

Verification Is Required

To help us verify your identity, please enter your email address:

ATO Protection – Administrative Dashboard View

Admins use the GreatHorn Email Security dashboard to quickly identify accounts that failed challenges



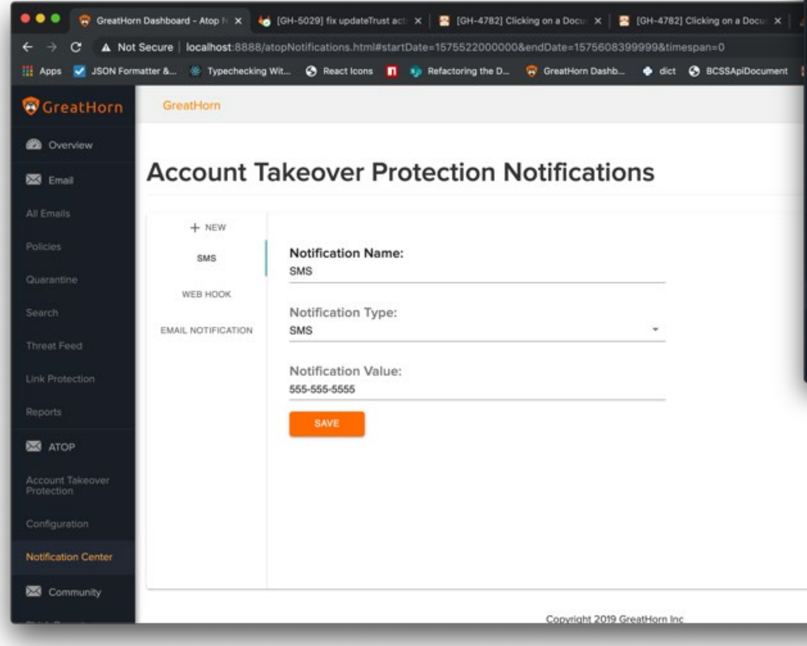
Account Takeover Protection

This will show email challenges that greathorn provided to your users. The results are below.

Event Type	Success	Timestamp	Remediation	User-Agent	IP	Geo IP
register	✓	1574030238	approve	Mozilla/5.0 (Windows NT 6.1; Win64; x64; rv:47.0) Gecko/20100101 Firefox/47.0	108.49.222.115	United States (US) / North Ameria (NA)
send	✓	1574030238	approve	Mozilla/5.0 (Windows NT 6.1; Win64; x64; rv:47.0) Gecko/20100101 Firefox/47.0	108.49.222.115	United States (US) / North Ameria (NA)
send	⊗	1574030238	block	Googlebot/2.1 (+http://www.google.com/bot.html)	0.0.0.0	Localhost
send	⊗	1574030238	block	Googlebot/2.1 (+http://www.google.com/bot.html)	127.0.0.1	Localhost
send	⊗	1574030238	block	Opera/9.80 (Macintosh; Intel Mac OS X; U; en) Presto/2.2.15 Version/10.00	27.0.236.0	South Korea (KR) / Asia (AS)

ATO Protection – Configuration & Notification

Admins can be notified through email, SMS, or webhook…



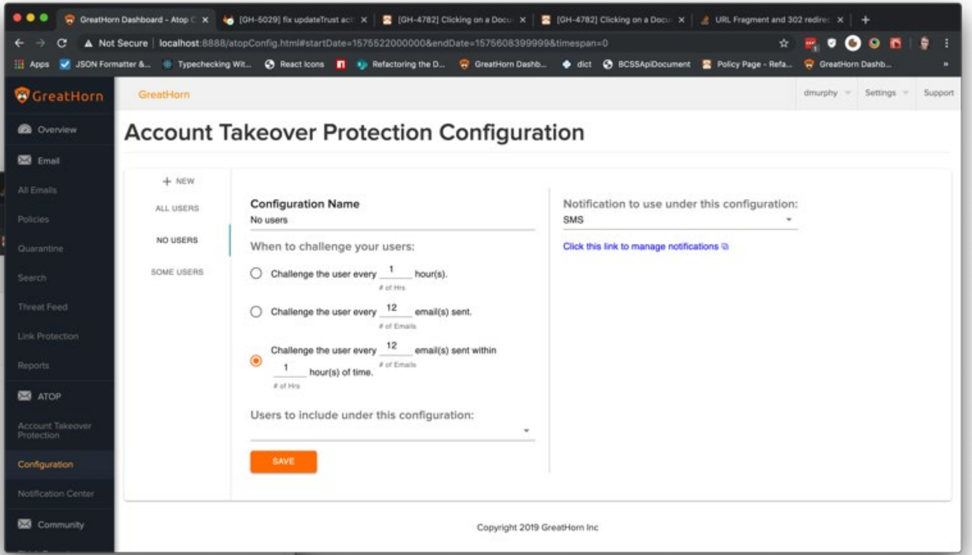
Account Takeover Protection Notifications

Notification Name:
SMS

Notification Type:
SMS

Notification Value:
555-555-5555

Copyright 2019 GreatHorn Inc



Account Takeover Protection Configuration

Configuration Name
No users

When to challenge your users:

○ Challenge the user every 1 (# of Hrs) hour(s).

○ Challenge the user every 12 (# of Emails) email(s) sent.

● Challenge the user every 12 (# of Emails) email(s) sent within 1 (# of Hrs) hour(s) of time.

Users to include under this configuration:

Notification to use under this configuration:
SMS

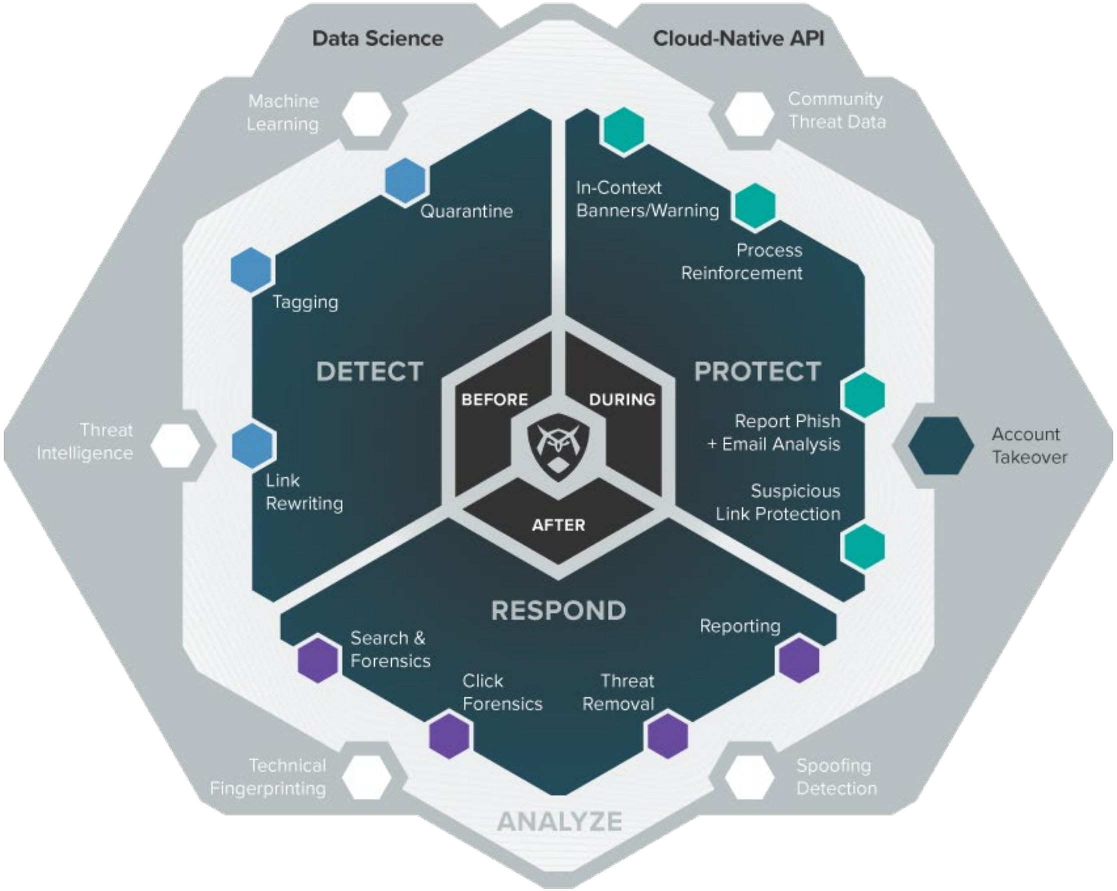
Click this link to manage notifications

Copyright 2019 GreatHorn Inc

…and determine how to handle failed authentications, e.g. silently blocking or bannering the email

Questions?

- **Cloud-native –** for greater visibility, control, and analysis
- **Multi-layered –** to protect before, during, and after an attack
- **Fast Response –** to quickly detect and/or remove emerging threats
- **Robust –** for enterprise configuration and management
- **Accurate –** using data science, technical fingerprints, and organization context



GreatHorn

GreatHorn

Thank you.