Spotting and Stopping Business Email Compromise Attacks

How spear phishing and BEC attacks require a full-lifecycle approach to email security

Speakers

Paul Roberts, Editor in Chief

the security ledger

Kevin O’Brien, CEO

GreatHorn

Agenda

- 2:00 - 2:05 Introductions, housekeeping
- 2:05 - 2:15 BEC attacks: state of the art
- 2:15 - 2:30 Full Lifecycle Approach
- 2:30 - 2:45 Developing Business Processes to Minimize BEC Risk
- 2:45 – 3:00 Question and answers

the security ledger GreatHorn

Business Email Compromise Attacks

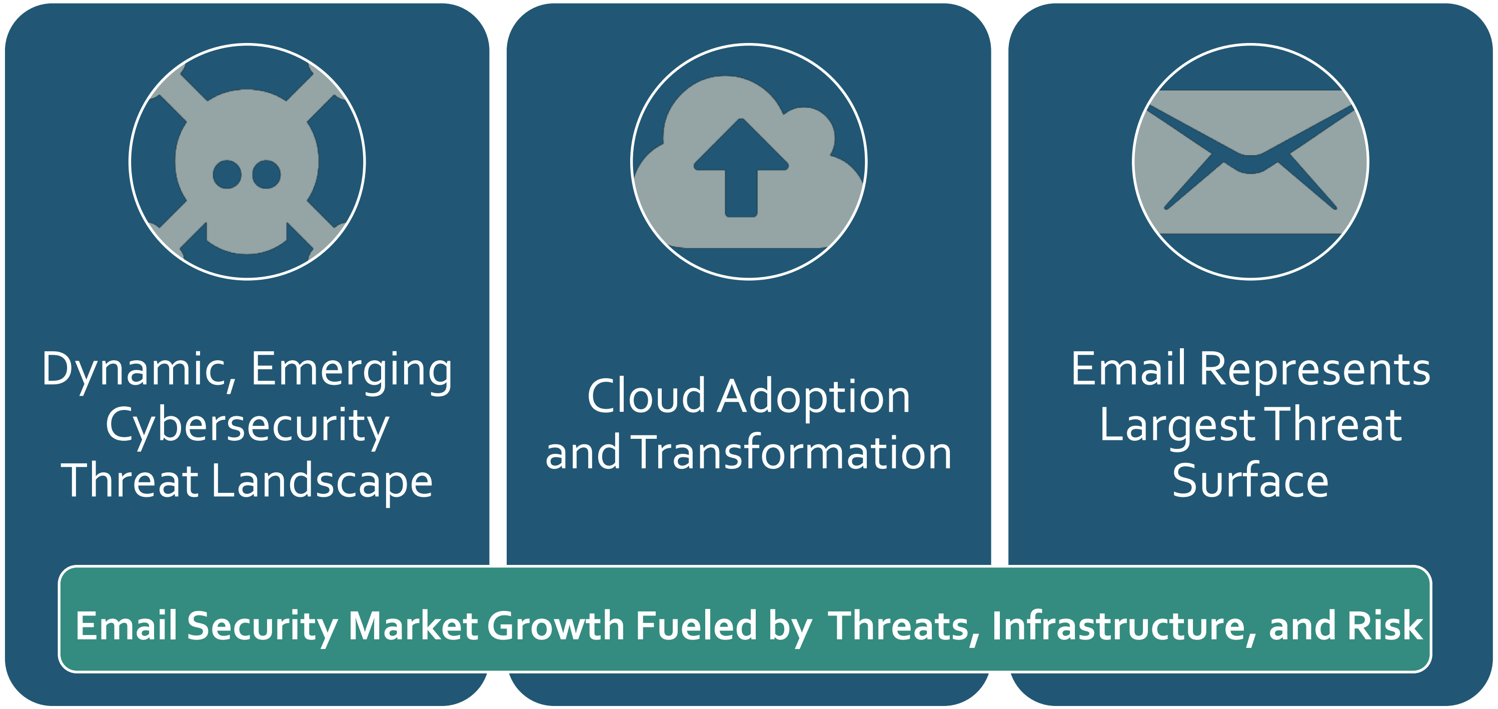
understanding BEC risks

BEC Threats

- Definition of Business Email Compromise
  - Common characteristics
  - Who is targeted
- What BEC attacks matter
  - 90% of breaches begin with targeted email attack
  - Links to other threats – malware, account hijack, data/IP theft, etc.
- Examples of recent BEC attacks

the security ledger GreatHorn

Why Are We Talking about Email Security in 2019?



Dynamic, Emerging Cybersecurity Threat Landscape

Cloud Adoption and Transformation

Email Represents Largest Threat Surface

Email Security Market Growth Fueled by Threats, Infrastructure, and Risk

the security ledger GreatHorn

The Proof: BEC Threats Still Working

1 in **5**

security professionals have to take direct remediation action at least weekly

the security ledger GreatHorn

BEC Threats

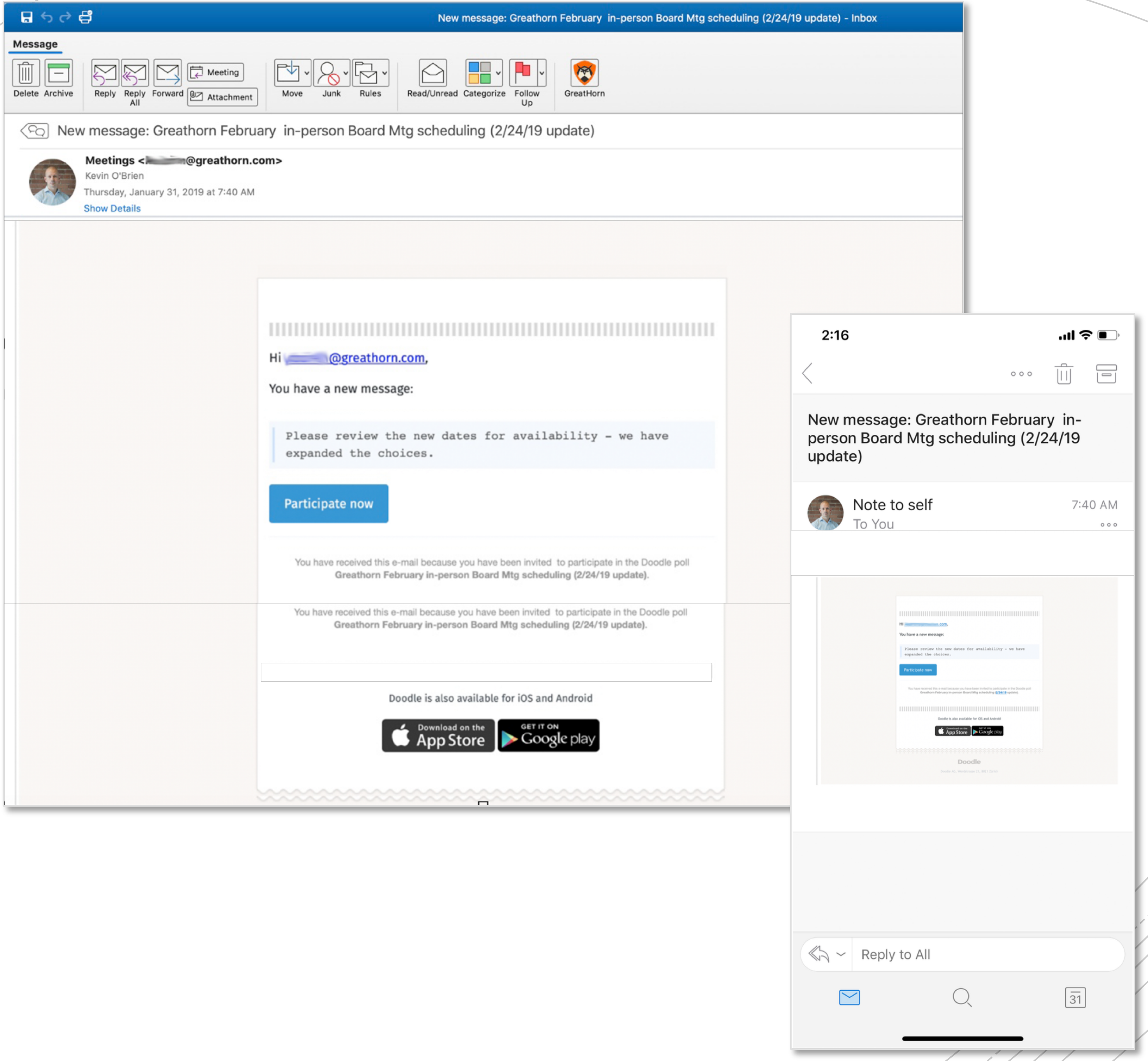
From: Google <no-reply@accounts.googlemail.com>;
Date: March 19, 2016 at 4:34:30 AM EDT
To: john.podesta@gmail.com
Subject: Someone has your password

Hi John
Someone just used your password to try to sign in to your Google Account

john.podesta@gmail.com.
Details:
Saturday, 19 March, 8:34:30 UTC
IP Address: 134.249.139.239
Location: Ukraine
Google stopped this sign-in attempt. You should change your password immediately.

CHANGE PASSWORD <https://bit.ly/1PibSU0>
Best,
The Gmail Team

Real Executive Attack



New message: Greathorn February in-person Board Mtg scheduling (2/24/19 update) - Inbox

New message: Greathorn February in-person Board Mtg scheduling (2/24/19 update)

Meetings <[redacted]@greathorn.com>
Kevin O'Brien
Thursday, January 31, 2019 at 7:40 AM
Show Details

Hi [redacted]@greathorn.com,

You have a new message:

> Please review the new dates for availability - we have expanded the choices.

Participate now

You have received this e-mail because you have been invited to participate in the Doodle poll **Greathorn February in-person Board Mtg scheduling (2/24/19 update).**

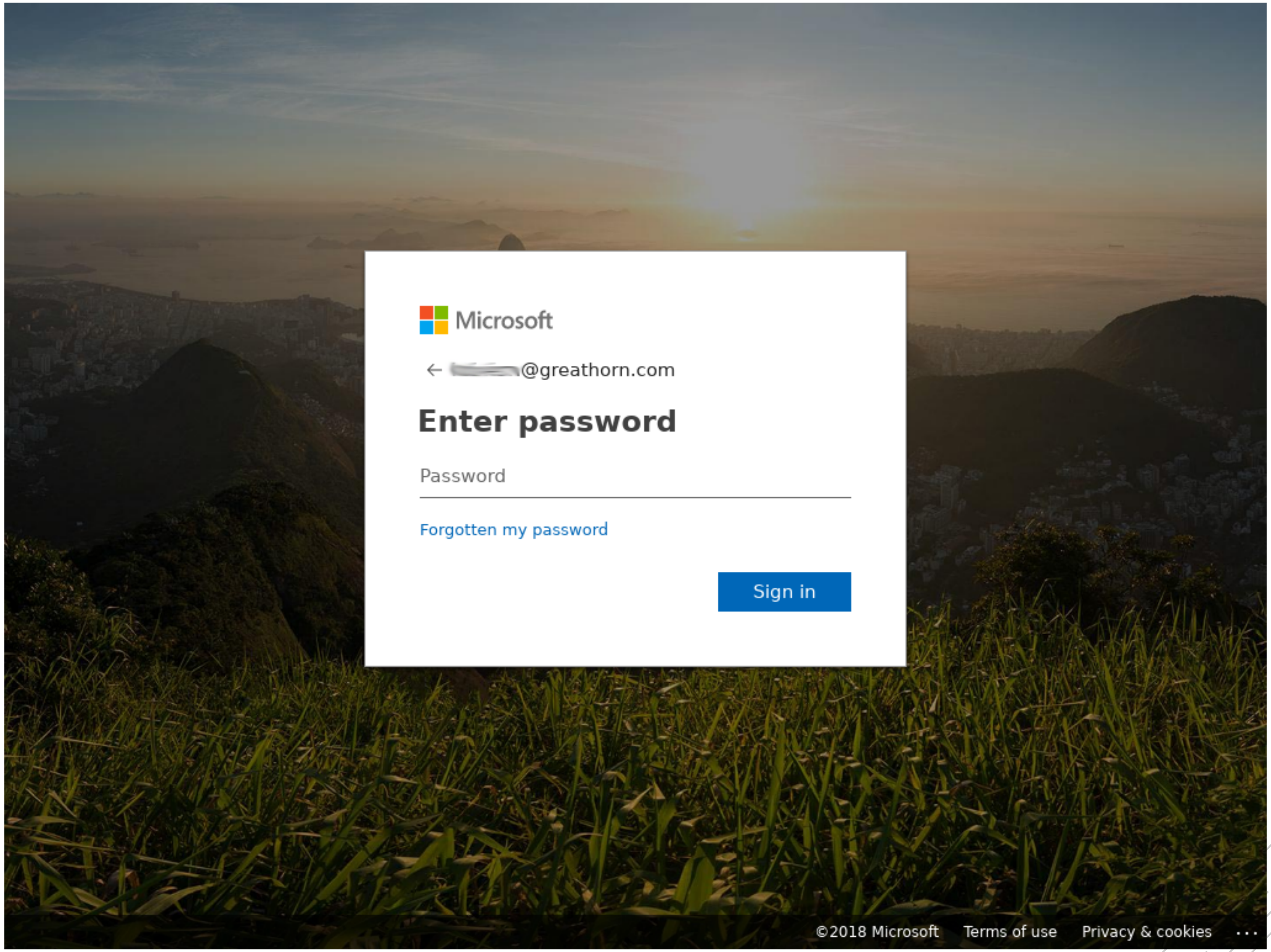
You have received this e-mail because you have been invited to participate in the Doodle poll **Greathorn February in-person Board Mtg scheduling (2/24/19 update).**

Doodle is also available for iOS and Android

New message: Greathorn February in-person Board Mtg scheduling (2/24/19 update)

Note to self 7:40 AM
To You

Real Executive Attack



Microsoft

← [redacted]@greathorn.com

Enter password

BEC Threats

- Role of threat intelligence in email security
- Where threat intelligence works
  - Links to malicious infrastructure
  - Suspicious/malicious content
  - Campaigns
- Where threat intelligence falls short
  - Social engineering attacks
  - Insider threats
  - Compromised infrastructure
  - Account Takeover (ATO)
  - ”Unknown Unknowns”

Full Lifecycle Email Security

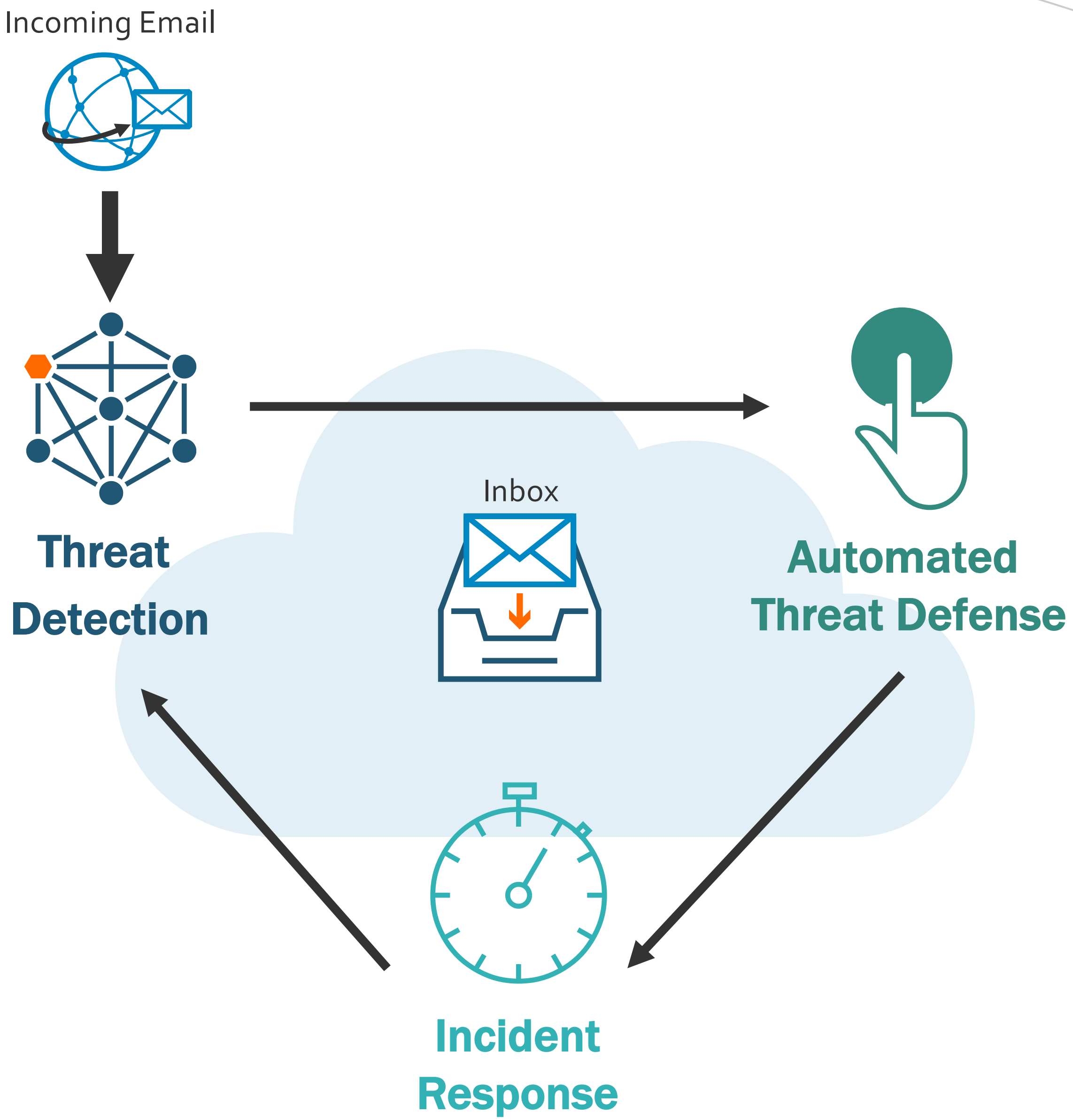
Why BEC attacks demand a new approach to email security.

Toward Full Lifecycle Email Security – Where We Came From

- Historically, email security about up front spam, malware detection
- Focus was on border checks
  - Focus on malicious applications rather than social engineering
  - Few options for threats that passed border checks
- Noisy vs. low & slow attacks
- False positives and false negative are problems

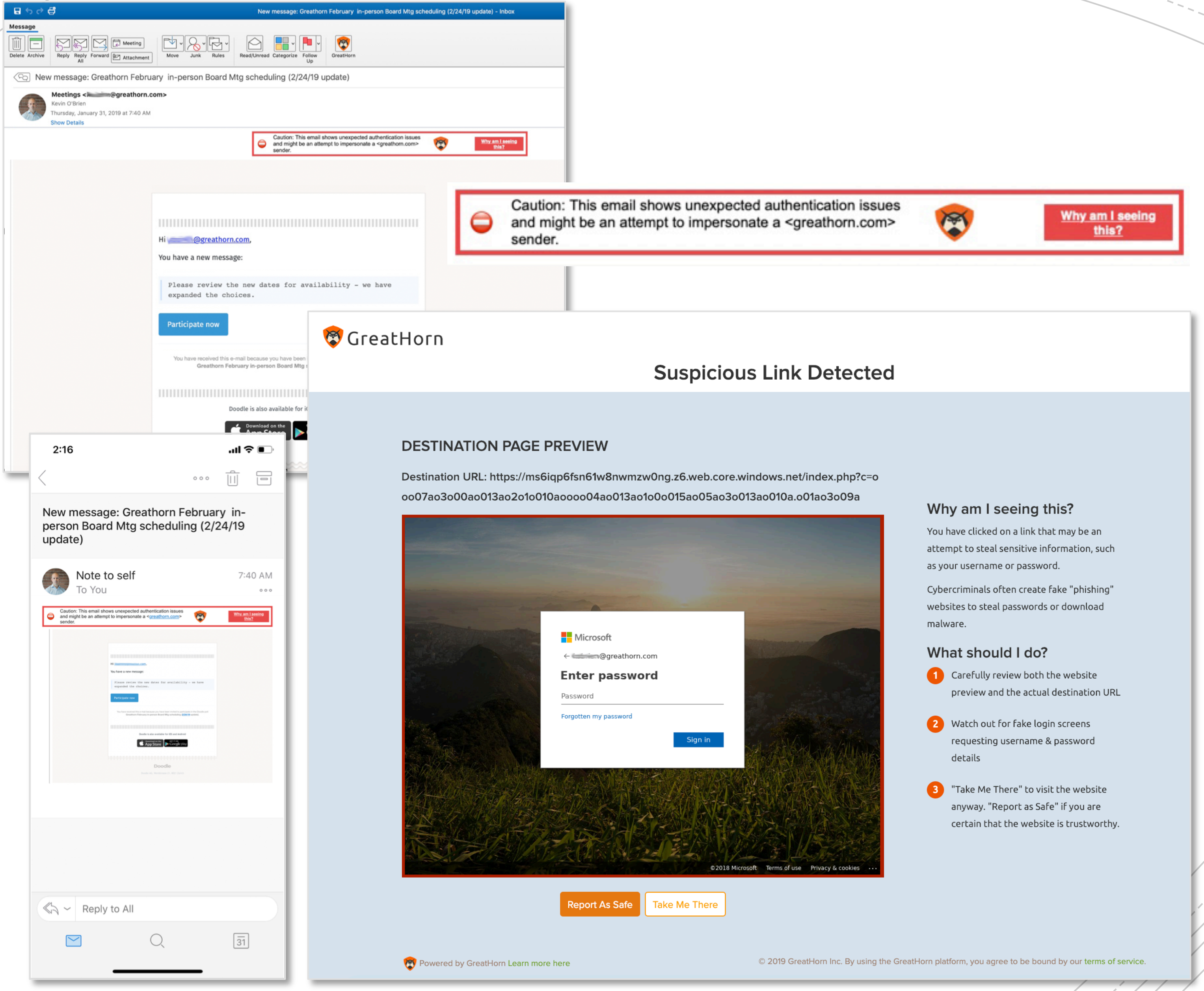
the security ledger GreatHorn

What is Full Lifecycle Email Security?



the security ledger GreatHorn

Contextualized User Protection



New message: Greathorn February in-person Board Mtg scheduling (2/24/19 update) - Inbox

New message: Greathorn February in-person Board Mtg scheduling (2/24/19 update)

Meetings <[redacted]@greathorn.com>
Kevin O'Brien
Thursday, January 31, 2019 at 7:40 AM

Caution: This email shows unexpected authentication issues and might be an attempt to impersonate a <greathorn.com> sender. Why am I seeing this?

Hi [redacted]@greathorn.com,

You have a new message:

```
Please review the new dates for availability - we have
expanded the choices.
```

You have received this e-mail because you have been
Greathorn February in-person Board Mtg

Doodle is also available for i

New message: Greathorn February in-person Board Mtg scheduling (2/24/19 update)

Note to self 7:40 AM
To You

Caution: This email shows unexpected authentication issues and might be an attempt to impersonate a <greathorn.com> sender. Why am I seeing this?

GreatHorn

Suspicious Link Detected

DESTINATION PAGE PREVIEW

Destination URL: https://ms6iqp6fsn61w8nwmzw0ng.z6.web.core.windows.net/index.php?c=ooo07ao3o00ao013ao2o1o010aoooo04ao013ao1o0o015ao05ao3o013ao010a.o01ao3o09a

Microsoft
← [redacted]@greathorn.com
Enter password
Password
Forgotten my password
Sign in
©2018 Microsoft Terms of use Privacy & cookies ...

Report As Safe 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. "Report as Safe" if you are certain that the website is trustworthy.

Powered by GreatHorn Learn more here

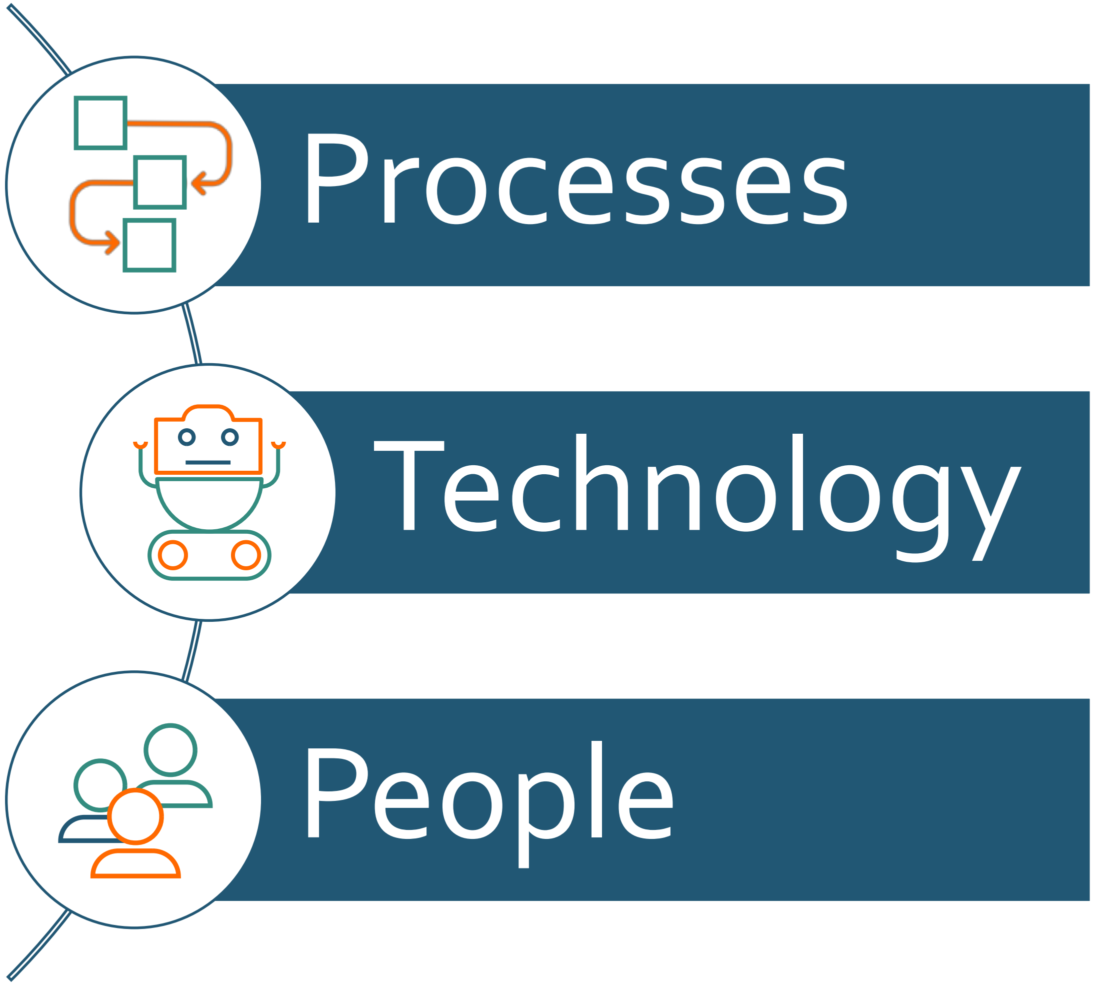
© 2019 GreatHorn Inc. By using the GreatHorn platform, you agree to be bound by our terms of service.

the security ledger GreatHorn

Operationalizing Email Security

Developing business processes that minimize email security risk

Tech is Just One Part of an Effective Strategy



Processes

Technology

People

the security ledger GreatHorn

Operationalizing Email Security

- Focus: identify and prevent email risks
- Goal: prevent successful attacks (vs. prevent/block all attacks)
- Block when possible, close detection window otherwise

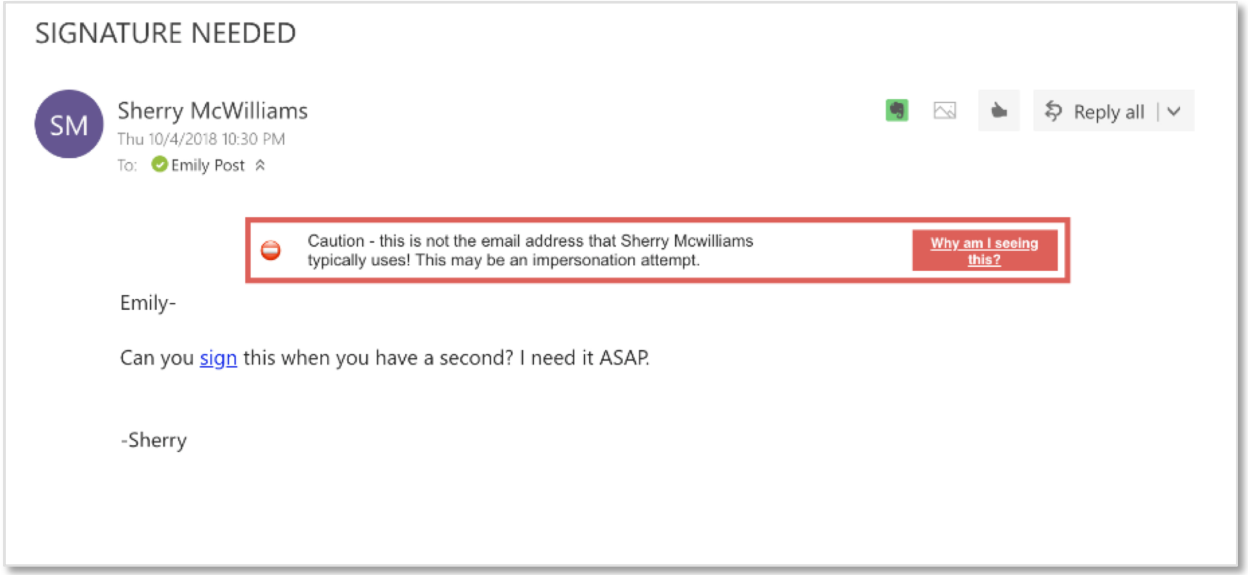
the security ledger GreatHorn

Process

- □ Work with high risk teams to minimize risk
- □ Develop internal communication processes for sharing incident information
- □ Finance – How are wire transfers authorized?
- □ HR / Execs – How do different classes of confidential information get communicated?
- □ How do executive teams communicate urgent requests?
- □ Who has access to what data? Who has access to which systems?

Operationalizing Email Security

Technology Reinforces Process



SIGNATURE NEEDED

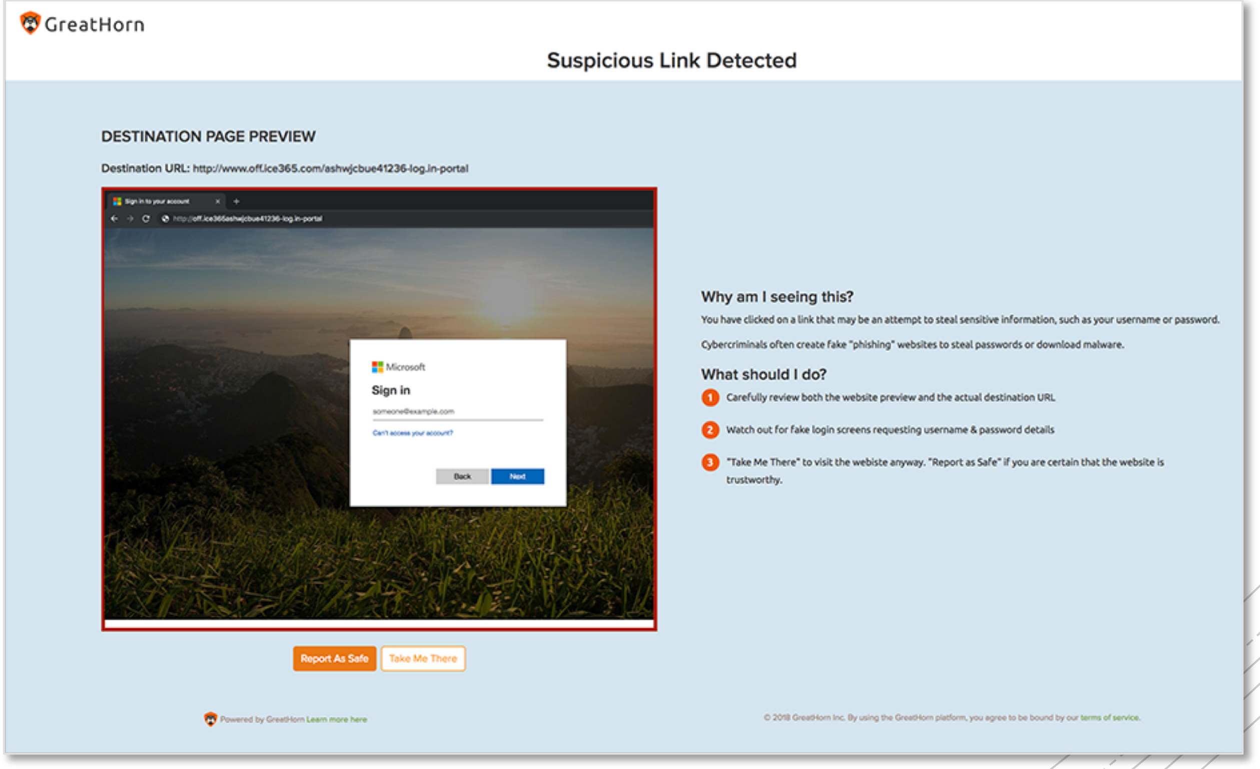
Sherry McWilliams
Thu 10/4/2018 10:30 PM
To: Emily Post

Caution - this is not the email address that Sherry Mcwilliams typically uses! This may be an impersonation attempt.

Emily-

Can you sign this when you have a second? I need it ASAP.

-Sherry



Suspicious Link Detected

DESTINATION PAGE PREVIEW

Destination URL: http://www.off.ice365.com/ashwjcbue41236-log.in-portal

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 webiste anyway. "Report as Safe" if you are certain that the website is trustworthy.

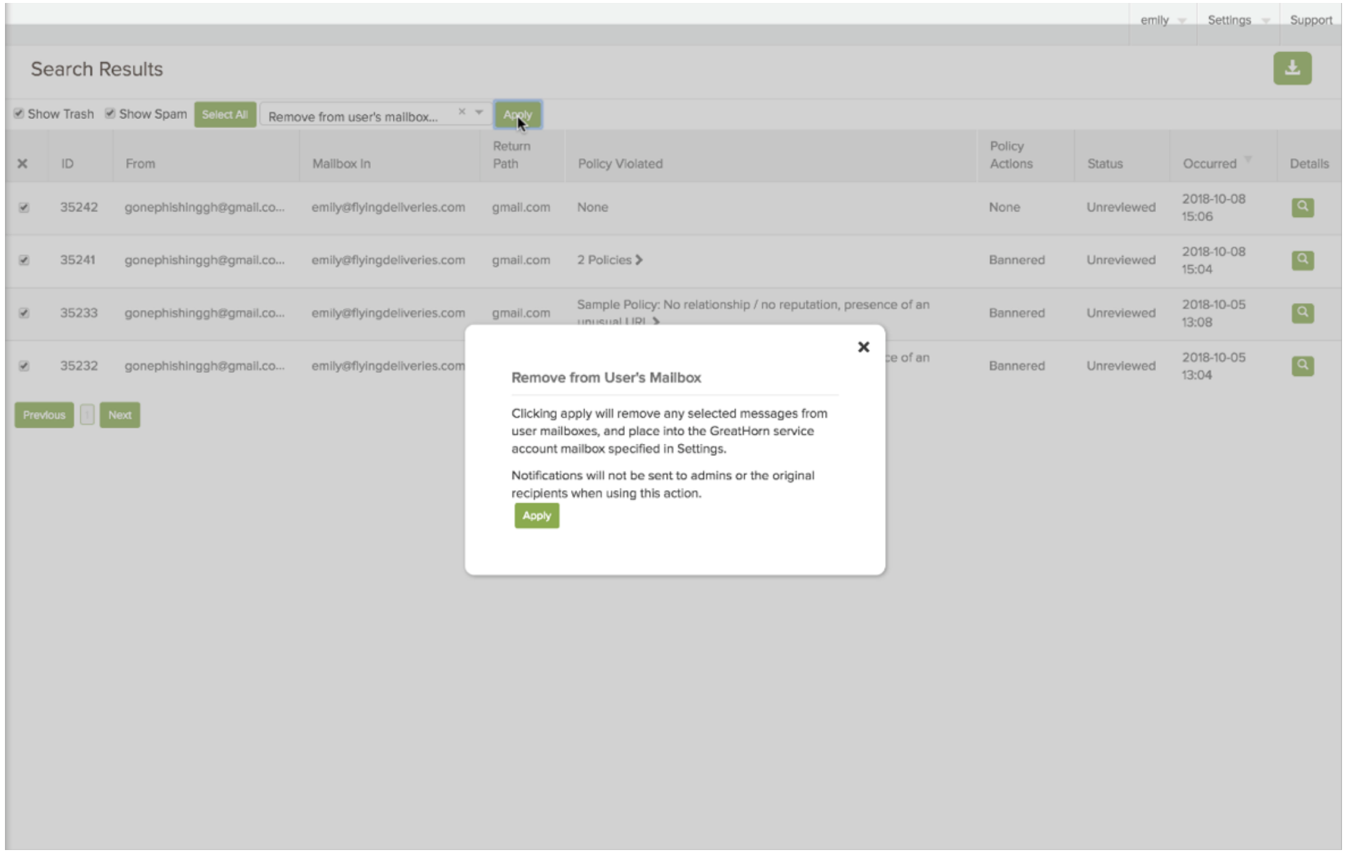
Powered by GreatHorn Learn more here

Operationalizing Email Security at the User Level

- Involve users in detection & remediation
- Provide administrators with tools to rapidly respond to incidents
- Feed lessons learned back into detection process

Operationalizing Email Security

How to reduce email security risk at your organization.



Search Results

☑ Show Trash ☑ Show Spam Select All Remove from user's mailbox... Apply

✕	ID	From	Mailbox In	Return Path	Policy Violated	Policy Actions	Status	Occurred	Details
☑	35242	gonephishinggh@gmail.co...	emily@flyingdeliveries.com	gmail.com	None	None	Unreviewed	2018-10-08 15:06	🔍
☑	35241	gonephishinggh@gmail.co...	emily@flyingdeliveries.com	gmail.com	2 Policies ❯	Bannered	Unreviewed	2018-10-08 15:04	🔍
☑	35233	gonephishinggh@gmail.co...	emily@flyingdeliveries.com	gmail.com	Sample Policy: No relationship / no reputation, presence of an unusual URL ❯	Bannered	Unreviewed	2018-10-05 13:08	🔍
☑	35232	gonephishinggh@gmail.co...	emily@flyingdeliveries.com		ce of an	Bannered	Unreviewed	2018-10-05 13:04	🔍

Remove from User's Mailbox

Clicking apply will remove any selected messages from user mailboxes, and place into the GreatHorn service account mailbox specified in Settings.

Notifications will not be sent to admins or the original recipients when using this action.

Apply

Questions…