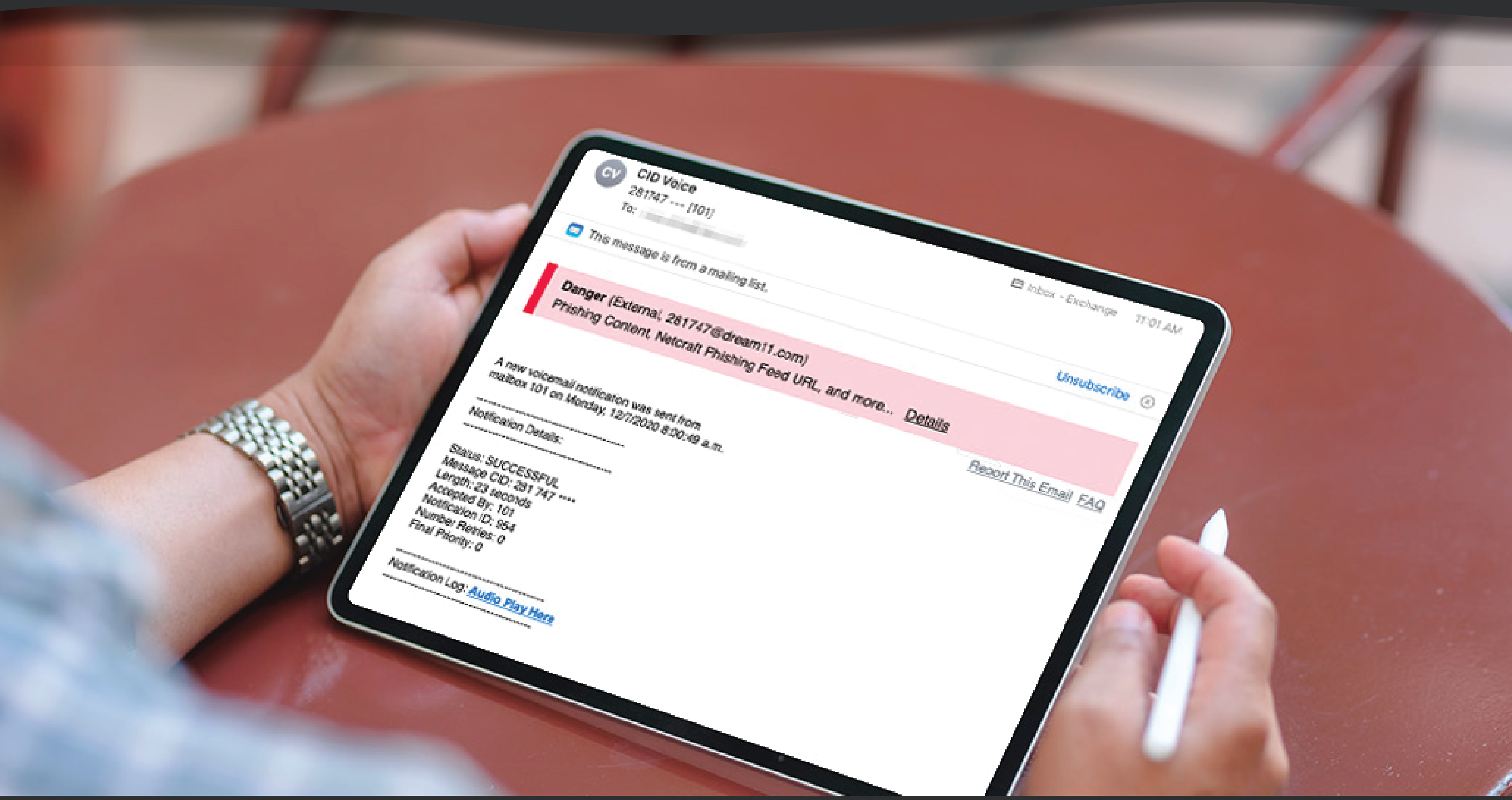
INQUEST

REPORT

Understanding Phishing: Banner Effectiveness

One of InQuest's most distinguishing features is its banner system. While most of InQuest's work detecting phish takes place "under the hood," the banners are what recipients see. These distinctive yet unobtrusive signposts tell the reader where each email sits on the safe-dangerous spectrum. The color (gray, yellow, red) gives a general impression. The brief text phrases explain why InQuest marked the email that way. The links in the banner allow the recipient to inquire further or report the mail to InQuest staff for further analysis.



CV CID Voice
281747 --- (101)
To:

This message is from a mailing list.

Inbox - Exchange 11:01 AM

Unsubscribe

Danger (External, 281747@dream11.com)
Phishing Content, Netcraft Phishing Feed URL, and more... Details

Report This Email FAQ

A new voicemail notification was sent from mailbox 101 on Monday, 12/7/2020 8:00:49 a.m.

Notification Details:

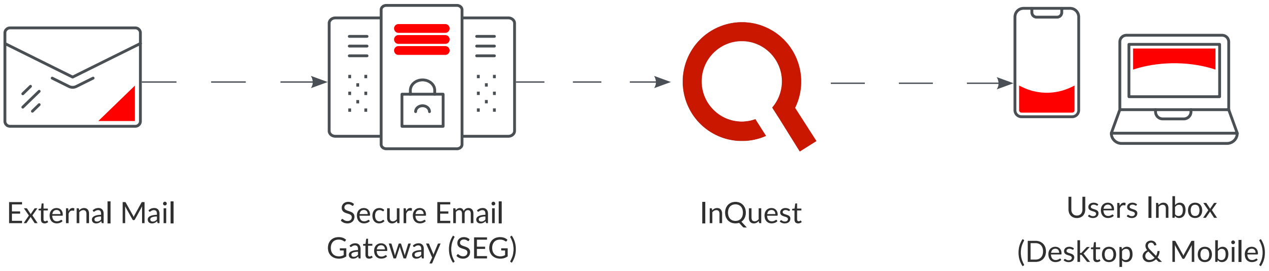
Status: SUCCESSFUL
Message CID: 281 747 ****
Length: 23 seconds
Accepted By: 101
Notification ID: 954
Number Retries: 0
Final Priority: 0

Notification Log: Audio Play Here

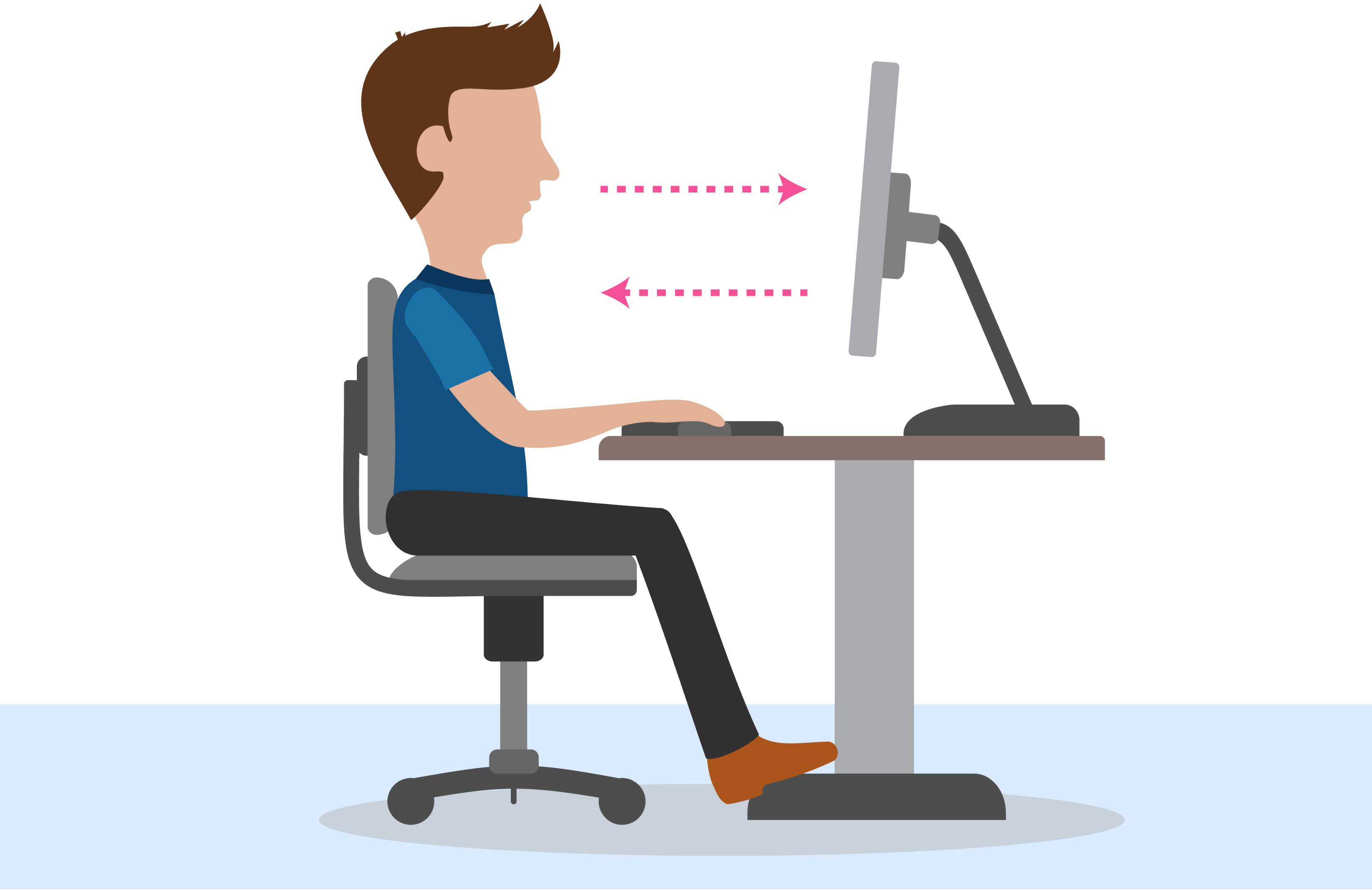
Overview

Putting banners in email to alert recipients to the potential dangers lurking in messages is a highly effective way to keep employees safe from phishing attacks. A lot of specialists in anti-phishing technology fall into a category analyst firm Gartner calls Integrated Cloud Email Security (ICES). Every one of these firms uses Microsoft's application programming interface (API) to access Office 365 (O365), which accounts for the vast majority of cloud-based email systems, but using API access means that none of these firms can insert a banner into an email before it reaches the recipient.

InQuest — because it eschews the API approach and instead sits in line between the secure email gateway (SEG) and the recipient's inbox — can insert a simple banner into each email after performing its in-line analysis.

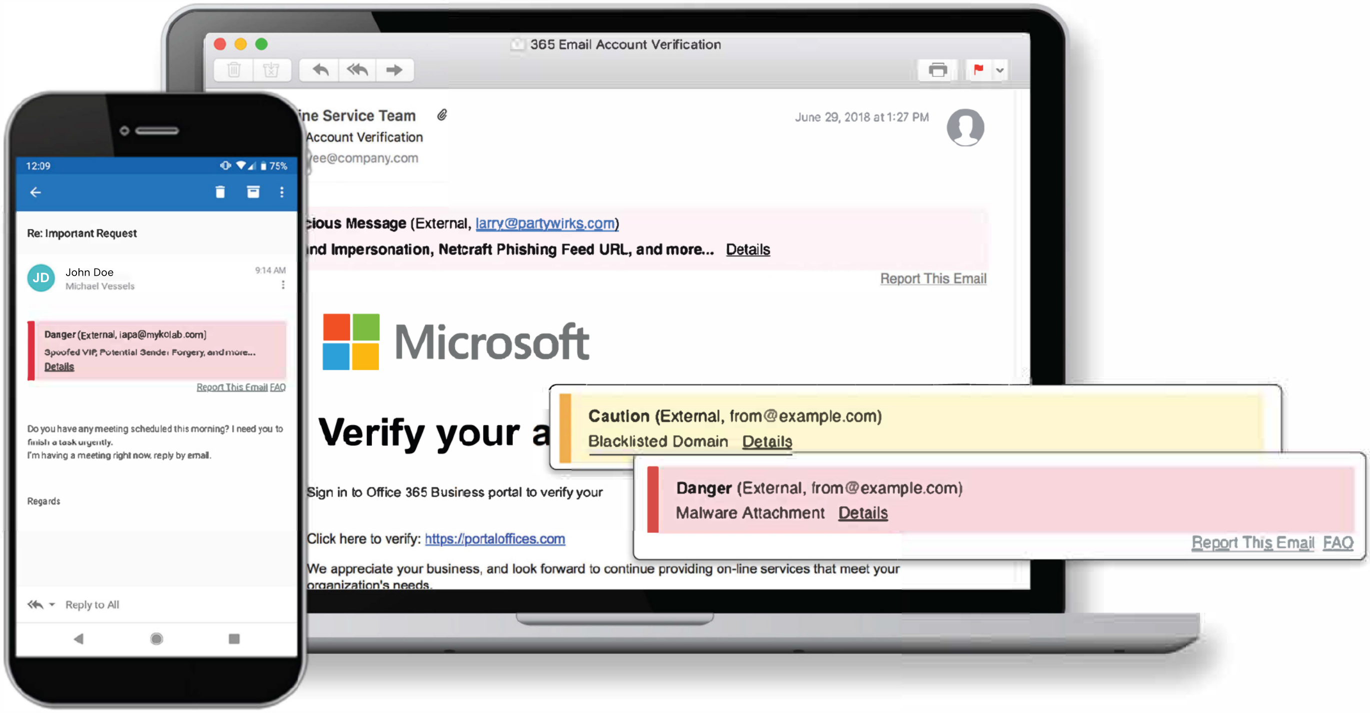


Banners serve two main purposes: they educate the user, and they let the user educate the system.



InQuest itself is a group of interacting modules, each of which has a particular job. They are all unleashed on an email at the same time. This parallelism allows them to do their analysis in less than two seconds, thus minimally interfering with mail flow. Modules do things like answer the question, “Has this sender ever sent email to this recipient before?” or “Is this email trying to look like it comes from Microsoft?” Some of the modules are quite complex.

At the end of the analysis, an aggregator module collects “scores” from the other modules to reach a total. It is this total that determines what color the InQuest banner for a particular email will be — gray for safe, yellow for caution, and red for dangerous.



Re: Important Request

John Doe
Michael Vessels
9:14 AM

Danger (External, iapa@mykolab.com)
Spoofed VIP, Potential Sender Forgery, and more...
Details

Report This Email FAQ

Do you have any meeting scheduled this morning? I need you to finish a task urgently.
I'm having a meeting right now, reply by email.

Regards

365 Email Account Verification

ine Service Team
Account Verification
ee@company.com
June 29, 2018 at 1:27 PM

cious Message (External, larry@partywirks.com)
nd Impersonation, Netcraft Phishing Feed URL, and more... Details

Report This Email

Verify your a

Sign in to Office 365 Business portal to verify your

Click here to verify: https://portaloffices.com

We appreciate your business, and look forward to continue providing on-line services that meet your organization's needs.

Caution (External, from@example.com)
Blacklisted Domain Details

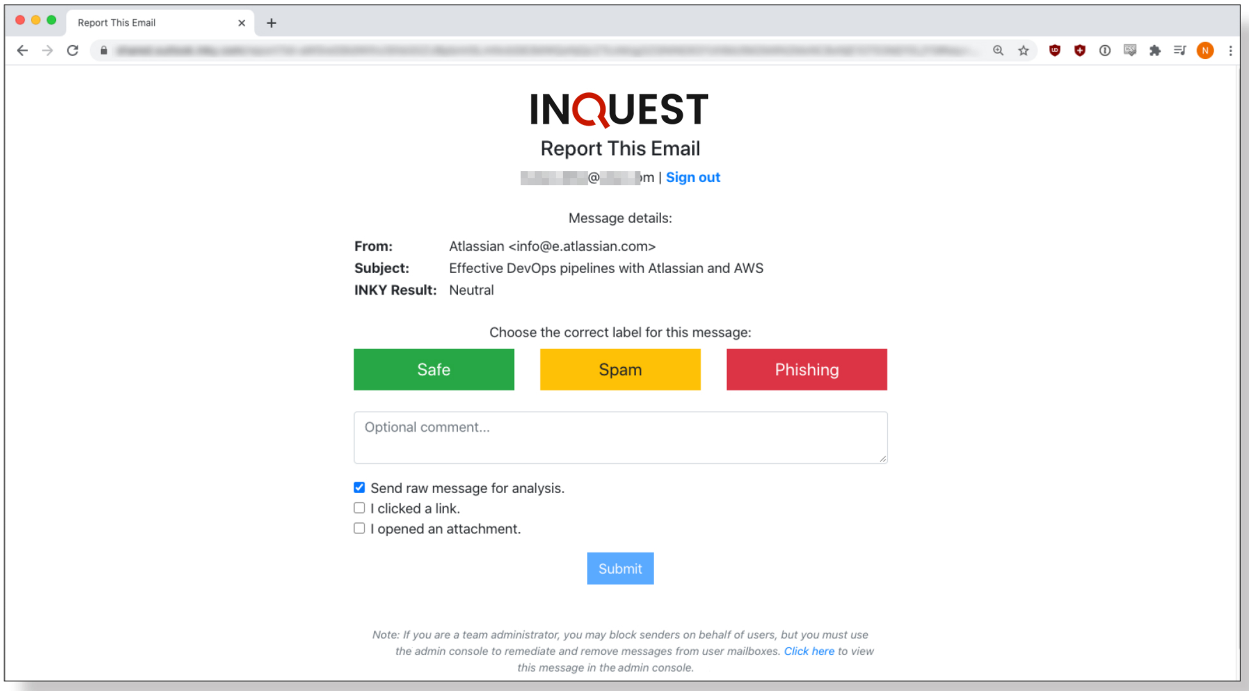
Danger (External, from@example.com)
Malware Attachment Details

Report This Email FAQ

From our customers, we have learned that banners are highly effective at reducing end-user click through on links to dangerous locations (i.e., URLs). One customer in the oil & gas sector said that clicks on malicious links by his end users were reduced by 15-20% a few months after InQuest was installed.

While InQuest does many things automatically (e.g., if a customer sets policy for it, the system can quarantine any email that would otherwise be given a red banner and delivered), we have found that human interactions are valuable.

The two-way nature of the communication is important. A recipient using the 'Report This Email' link in the banner helps train the system so that future results are more accurate.



INQUEST

Report This Email

[redacted]@[redacted]m | Sign out

Message details:

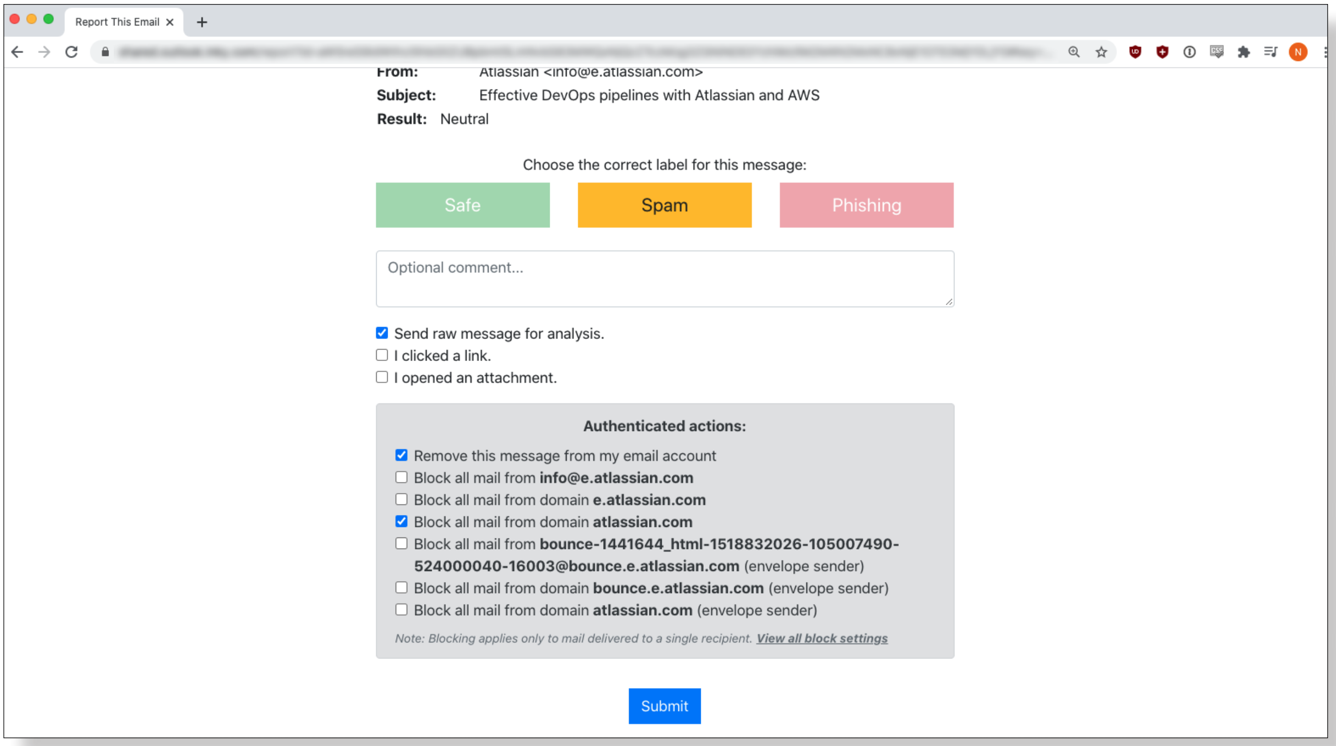
From:	Atlassian <info@e.atlassian.com>
Subject:	Effective DevOps pipelines with Atlassian and AWS
INKY Result:	Neutral

Choose the correct label for this message:

☑ Send raw message for analysis.
☐ I clicked a link.
☐ I opened an attachment.

Note: If you are a team administrator, you may block senders on behalf of users, but you must use the admin console to remediate and remove messages from user mailboxes. Click here to view this message in the admin console.

For authenticated email addresses, there's also an ability on the 'Report This Email' screen to mark something spam and block its address and even its domain (a superpower some customers just love!).



From: Atlassian <info@e.atlassian.com>
Subject: Effective DevOps pipelines with Atlassian and AWS
Result: Neutral

Choose the correct label for this message:

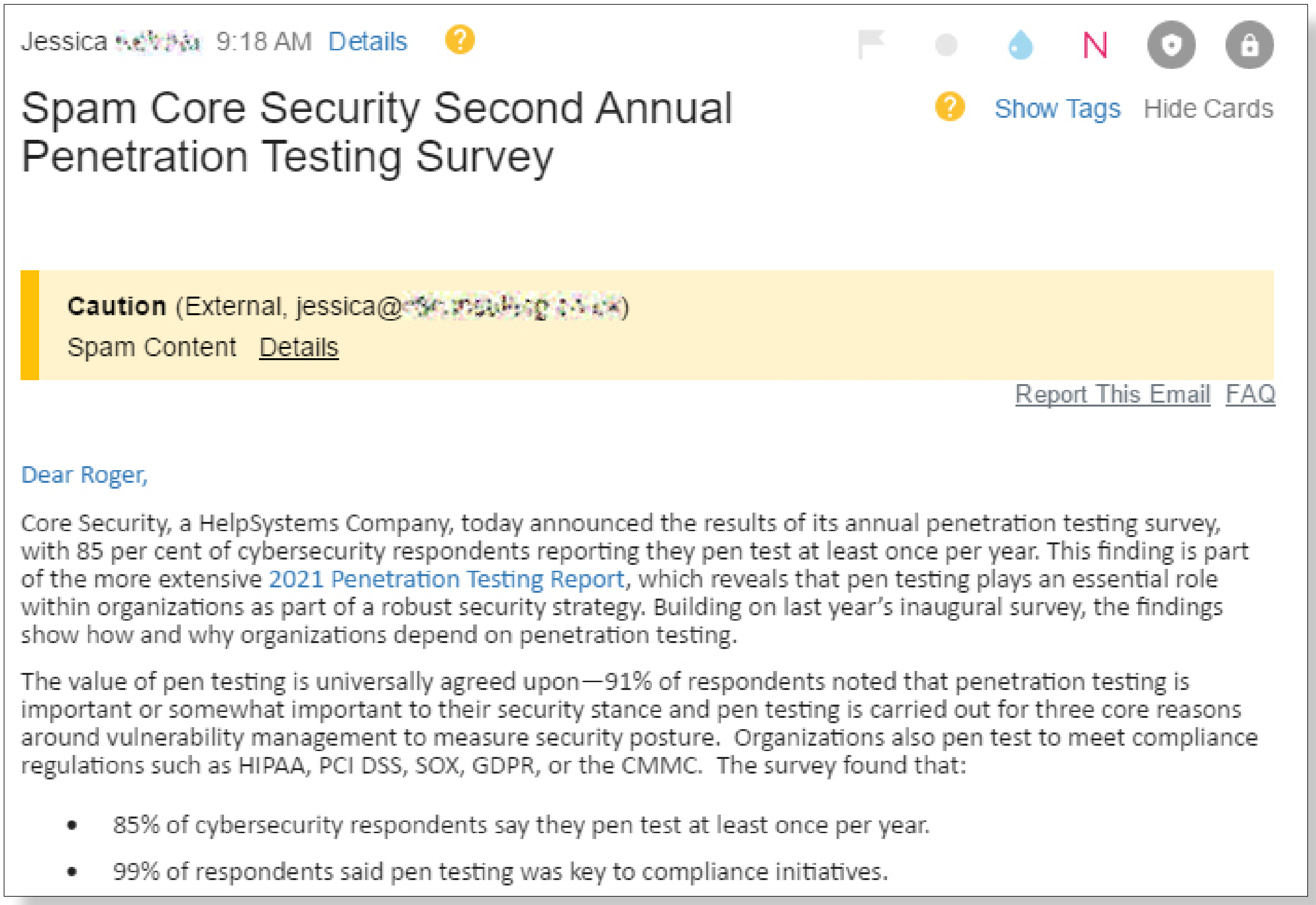
☑ Send raw message for analysis.
☐ I clicked a link.
☐ I opened an attachment.

Authenticated actions:

☑ Remove this message from my email account
☐ Block all mail from **info@e.atlassian.com**
☐ Block all mail from domain **e.atlassian.com**
☑ Block all mail from domain **atlassian.com**
☐ Block all mail from **bounce-1441644_html-1518832026-105007490-524000040-16003@bounce.e.atlassian.com** (envelope sender)
☐ Block all mail from domain **bounce.e.atlassian.com** (envelope sender)
☐ Block all mail from domain **atlassian.com** (envelope sender)

Note: Blocking applies only to mail delivered to a single recipient. ***View all block settings***

On the inbound side, the banner text teaches the recipient what to look for by explaining why InQuest flagged an email. Each banner has one or more text phrases. These phrases represent the output of the various InQuest modules. If only one threshold gets tripped, only one text phrase is displayed.



Jessica [redacted] 9:18 AM

Spam Core Security Second Annual Penetration Testing Survey

Caution (External, jessica@[redacted])
Spam Content Details

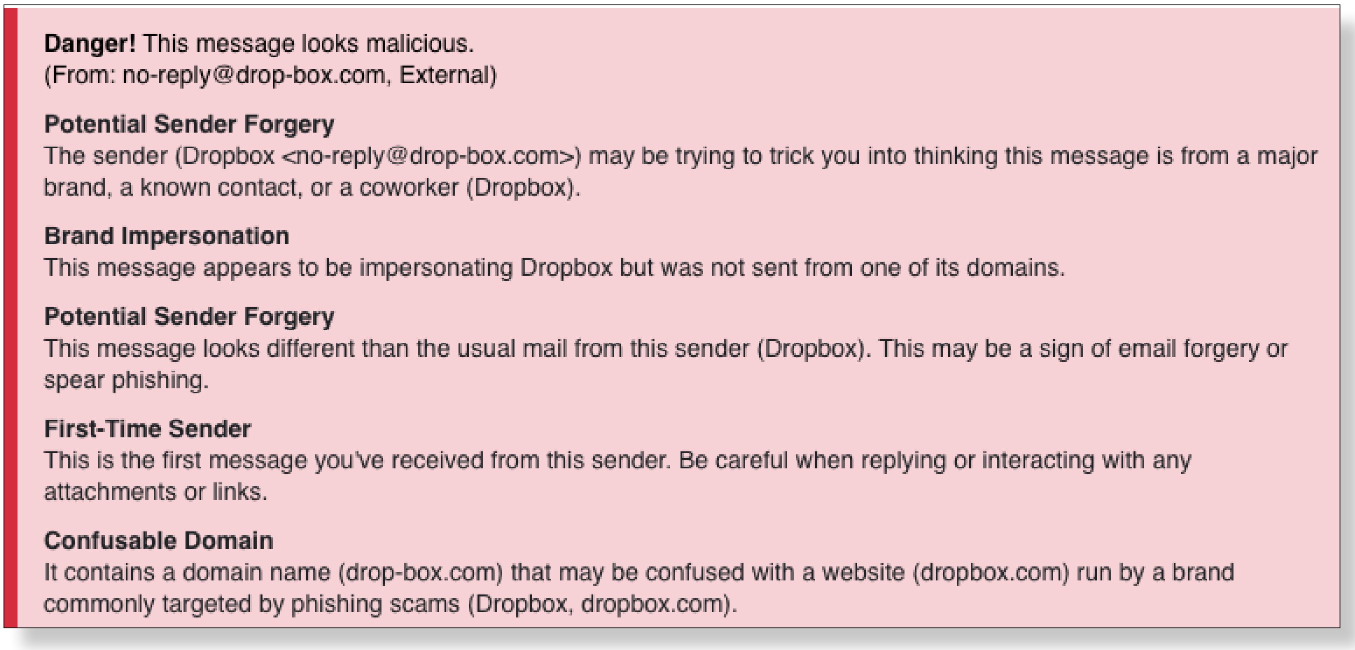
Dear Roger,

Core Security, a HelpSystems Company, today announced the results of its annual penetration testing survey, with 85 per cent of cybersecurity respondents reporting they pen test at least once per year. This finding is part of the more extensive 2021 Penetration Testing Report, which reveals that pen testing plays an essential role within organizations as part of a robust security strategy. Building on last year's inaugural survey, the findings show how and why organizations depend on penetration testing.

The value of pen testing is universally agreed upon—91% of respondents noted that penetration testing is important or somewhat important to their security stance and pen testing is carried out for three core reasons around vulnerability management to measure security posture. Organizations also pen test to meet compliance regulations such as HIPAA, PCI DSS, SOX, GDPR, or the CMMC. The survey found that:

- 85% of cybersecurity respondents say they pen test at least once per year.
- 99% of respondents said pen testing was key to compliance initiatives.

But if a lot of modules' thresholds are tripped, they all report. Thus, the recipient gets a lot of information about what InQuest saw and didn't like. A screaming red banner stuffed with an array of warnings is usually enough to cause a recipient to pause and contemplate why InQuest was so offended by that particular email. It's not without good reason.



Danger! This message looks malicious.
(From: no-reply@drop-box.com, External)

Potential Sender Forgery
The sender (Dropbox <no-reply@drop-box.com>) may be trying to trick you into thinking this message is from a major brand, a known contact, or a coworker (Dropbox).

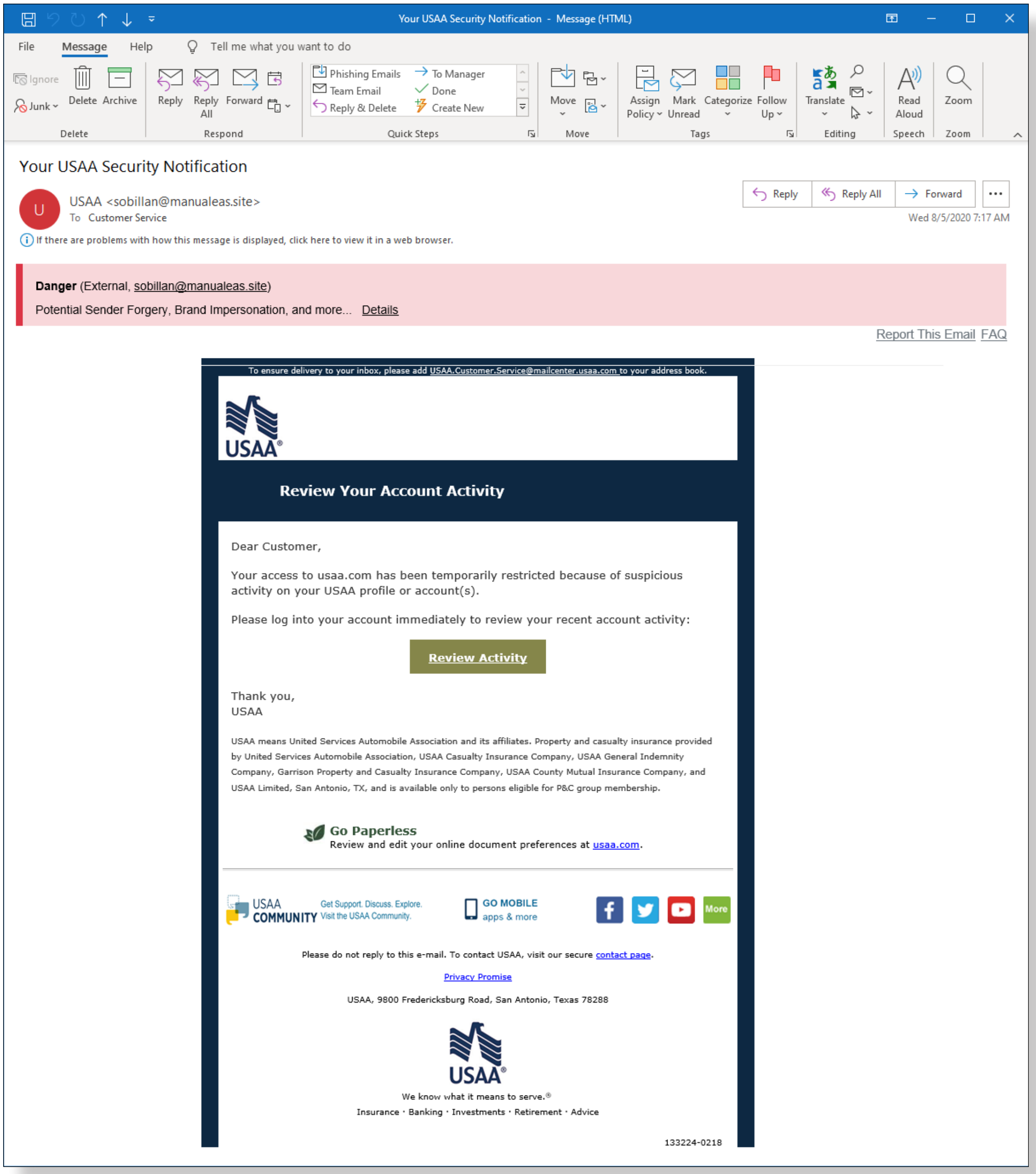
Brand Impersonation
This message appears to be impersonating Dropbox but was not sent from one of its domains.

Potential Sender Forgery
This message looks different than the usual mail from this sender (Dropbox). This may be a sign of email forgery or spear phishing.

First-Time Sender
This is the first message you've received from this sender. Be careful when replying or interacting with any attachments or links.

Confusable Domain
It contains a domain name (drop-box.com) that may be confused with a website (dropbox.com) run by a brand commonly targeted by phishing scams (Dropbox, dropbox.com).

And the experience can be quite ominous when a perfectly crafted phishing email that looks completely innocuous is topped with an armada of bright red alarms.



Your USAA Security Notification

USAA <sobillan@manualeas.site>
To Customer Service

Wed 8/5/2020 7:17 AM

If there are problems with how this message is displayed, click here to view it in a web browser.

Danger (External, sobillan@manualeas.site)
Potential Sender Forgery, Brand Impersonation, and more... Details

Report This Email FAQ

To ensure delivery to your inbox, please add USAA.Customer.Service@mailcenter.usaa.com to your address book.

USAA®

Review Your Account Activity

Dear Customer,

Your access to usaa.com has been temporarily restricted because of suspicious activity on your USAA profile or account(s).

Please log into your account immediately to review your recent account activity:

Review Activity

Thank you,
USAA

USAA means United Services Automobile Association and its affiliates. Property and casualty insurance provided by United Services Automobile Association, USAA Casualty Insurance Company, USAA General Indemnity Company, Garrison Property and Casualty Insurance Company, USAA County Mutual Insurance Company, and USAA Limited, San Antonio, TX, and is available only to persons eligible for P&C group membership.

Go Paperless
Review and edit your online document preferences at usaa.com.

USAA COMMUNITY Get Support. Discuss. Explore. Visit the USAA Community.

GO MOBILE apps & more

More

Please do not reply to this e-mail. To contact USAA, visit our secure contact page.

Privacy Promise

USAA, 9800 Fredericksburg Road, San Antonio, Texas 78288

USAA®

We know what it means to serve.®
Insurance · Banking · Investments · Retirement · Advice

133224-0218

Such a display should give the recipient pause, preventing them from falling for the ruse. But it also lets them know that just because an email looks good doesn't mean that it is. It's not the Nigerian Price scams that most people fall for. Those tend to sink to the level of spam, unwanted mail. It's the ones that really do look like your boss (or the HR department, your Internet service provider, your colleague from another company, your bank, American Express, DocuSign, or the U.S. Treasury) sent them that can let phishers into your organization and trigger a whole chain of events that leads to a ransomware shutdown, theft of intellectual property, pilfered identities, stolen money, disrupted operations, or a damaged reputation.

Why InQuest?

InQuest provides the most comprehensive malware and email phishing protection available.

InQuest uses a proprietary blend of Machine Learning and Artificial Intelligence that blocks even the most sophisticated phishing attacks that get past other systems.

InQuest uses proprietary technology and algorithms to "see" each email as the recipient would. Unlike a person, however, it can detect an email forgery and/or malicious or suspicious content. Once detected, it can redirect the email to a quarantine area or deliver it with disabled links and warnings.

Alerts shown within the email itself, which allows it to be viewed on desktop or mobile. This is a significant difference from other systems, which display warnings in headers and may not render properly in mobile applications.

InQuest sits downstream of any email system, including Microsoft Office 365 and Gmail.

InQuest scans every sent and delivered email automatically and flags malicious emails.

A comprehensive dashboard allows admins to both see the bigger picture and drill down to specific attacks, individuals, and individual messages. A robust search allows for detailed reporting at the granular level.

It can be set up and ready to go in just a few minutes.

We're passionate about email.

Ready to talk about an issue you're facing with email security at your organization?

www.inquest.net