# GoSecure Titan® Inbox Detection & Response (IDR)

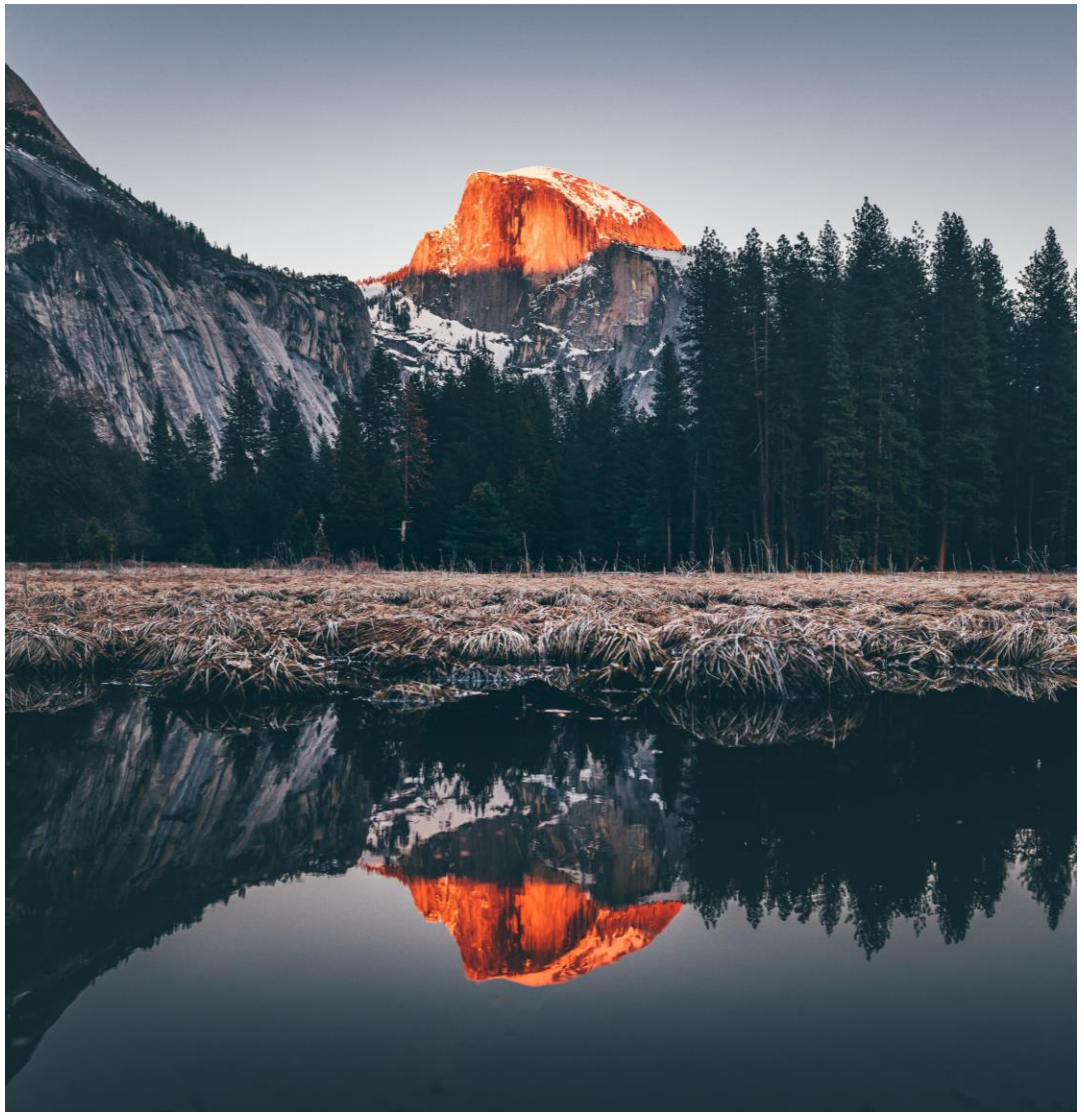
User Guide



GoSECURE

# PHISHING

Phishing has become the main IT threat targeting businesses in the digital age, making it a major topic of discussion these days.



# BETTER PROTECTION AGAINST SUSPICIOUS EMAILS

[What to do when you receive an email]

1. Determine the source of the e-mail
2. Identify the actual sender
3. Examine content

# DETERMINE THE SOURCE OF THE EMAIL

- When you receive an email, the first step is to distinguish between those from **colleagues** and those from **external senders**.
- It's essential to note that emails from **external senders potentially present a higher threat**.

# IDENTIFY THE ACTUAL SENDER

- To identify the sender, it’s **ESSENTIAL** to rely on the email address rather than the name displayed in Outlook.
- An e-mail address in the format <expeditor@domain> offers you the possibility of discerning the email's origin by identifying the sending domain.
- However, hackers frequently trick their victims into using the name displayed, as it is easily customized to gain the recipient's trust.

# EXAMINE CONTENT

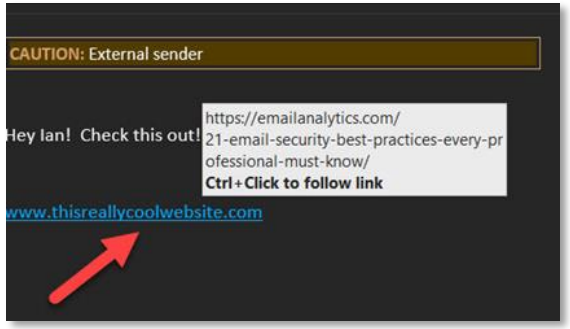
A suspicious email usually has one or more of the following elements in its content:

- An urgent or emergency situation is conveyed
- A direct threat
- A link to an unknown domain
- A potentially malicious attachment

# THE "HALT" TECHNIQUE

## HOVER

- Over hyperlinks to see where they REALLY go!




## LOOK

- Valid = www.walmart.com
- Not Valid = wa1mart.com
- Valid = help@walmart.com
- Not Valid = help@wal-mart.com

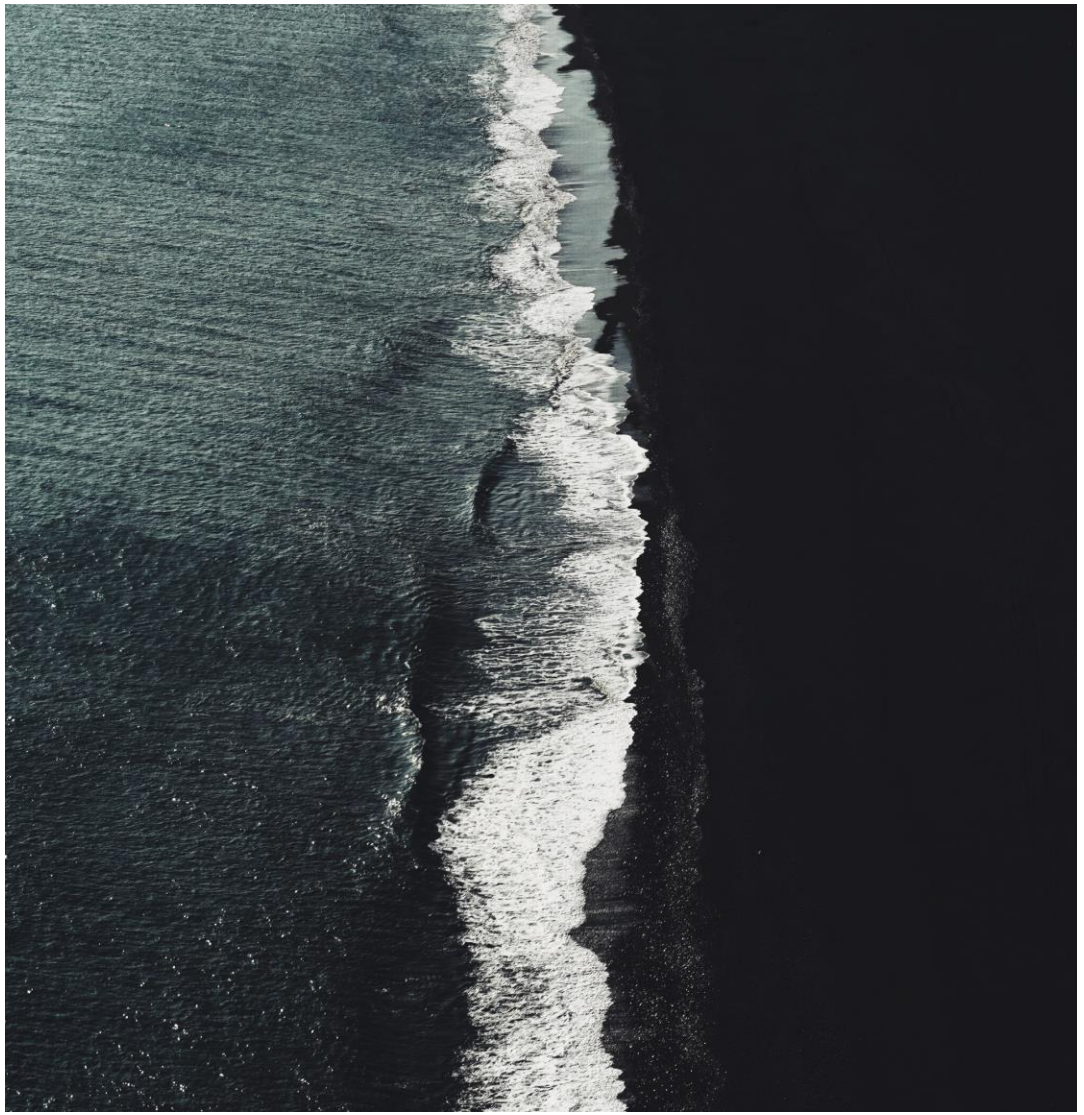
## ANALYSE

- The domain part of the email address
- Should be a valid organization
- Should be consistent

## TEST

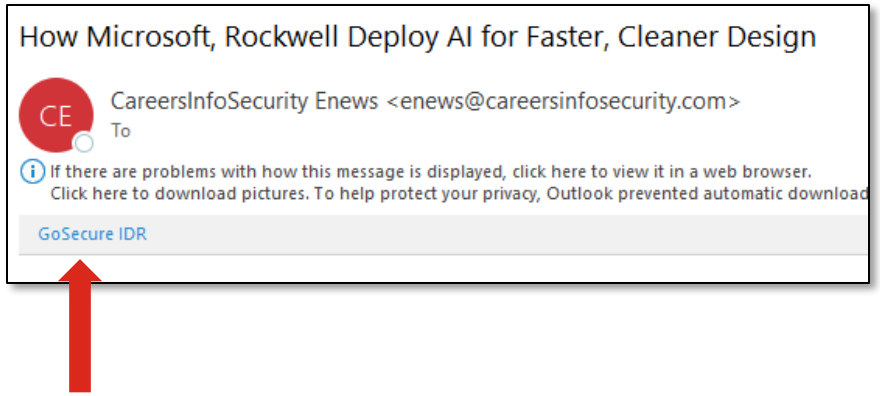
- Google it!
- Check for the real address

# WHAT TYPES OF EMAIL SHOULD I SUBMIT TO GOSECURE IDR?

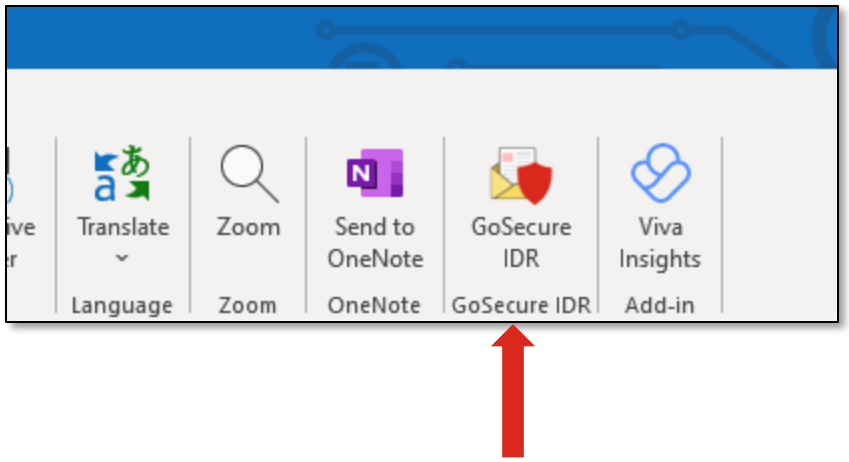


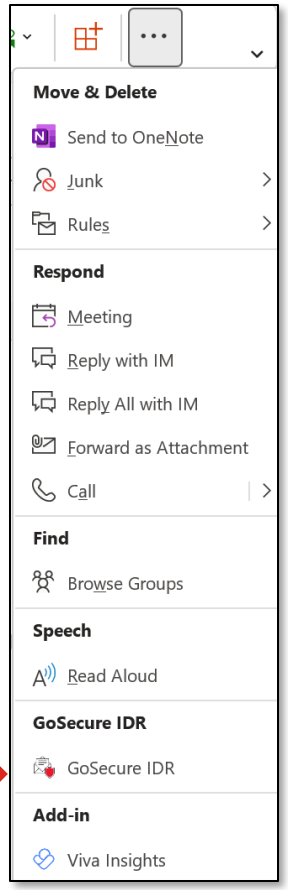
# WHEN IN DOUBT, YOU SHOULD SUBMIT

- Any email which may appear to be internal with a request to change direct deposit information or an odd request from management to do something for them, a lot of times the sender is being spoofed in those cases.
- Any email from an unknown sender with a request for anything from services to products to billing.
- Any email that seems out of character from a known sender (even known and trusted contacts can and do get compromised). The email might be an unexpected link or document or their tone in the body of the email may have changed.
- Any email that is asking you to complete a signing or to review a document. Any email that contains an attachment, especially a zip file or office document such as .doc or .xls.
- Any email that raises your suspicions

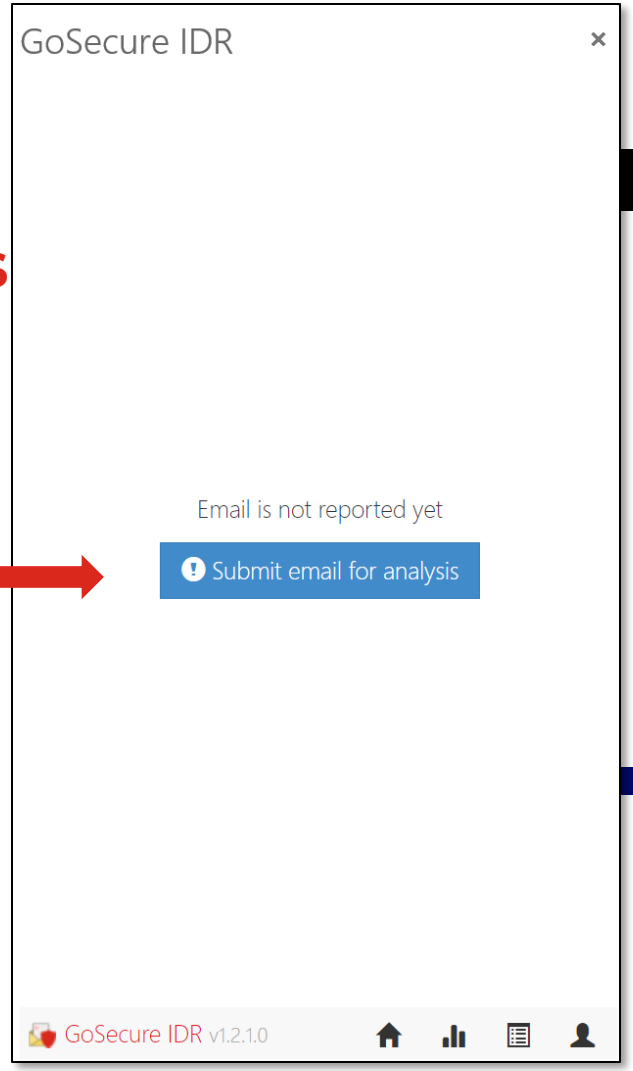



## USE THE GOSECURE IDR BUTTON

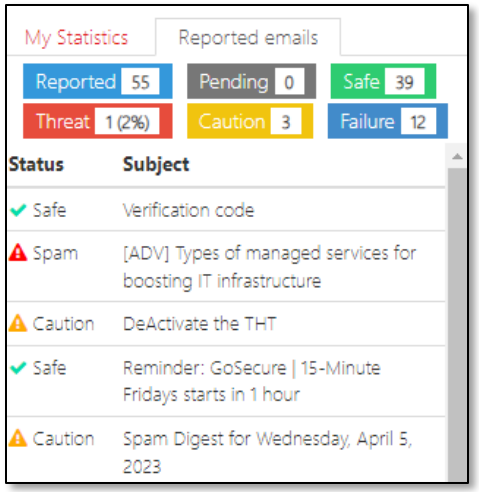


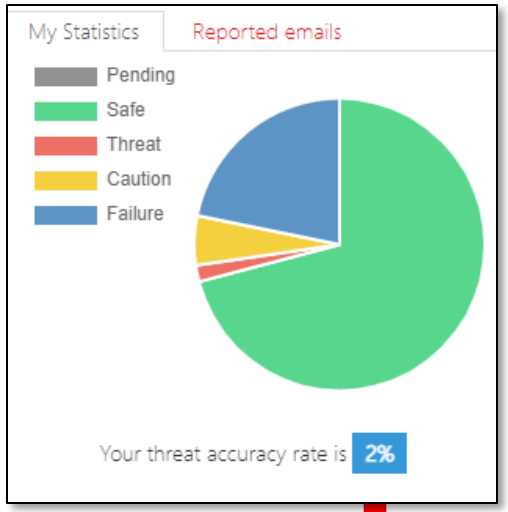




## AND SUBMIT THE EMAIL FOR ANALYSIS

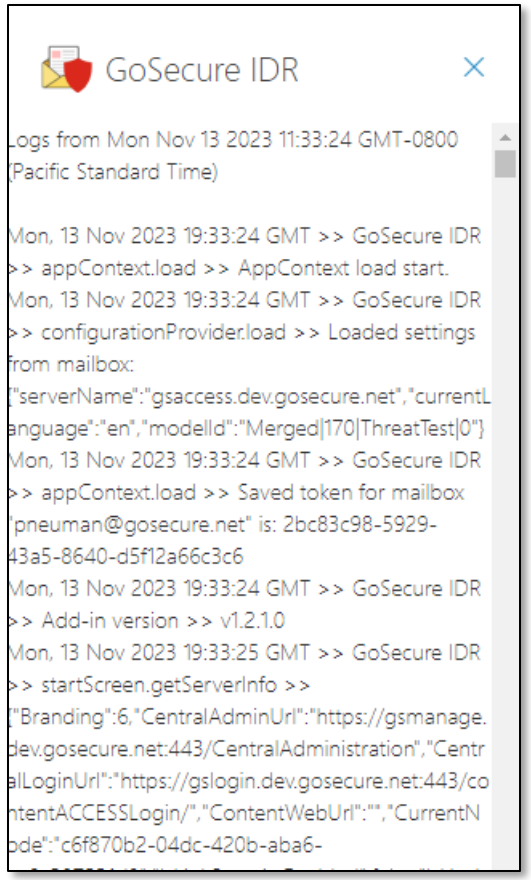


# IDR FEATURES

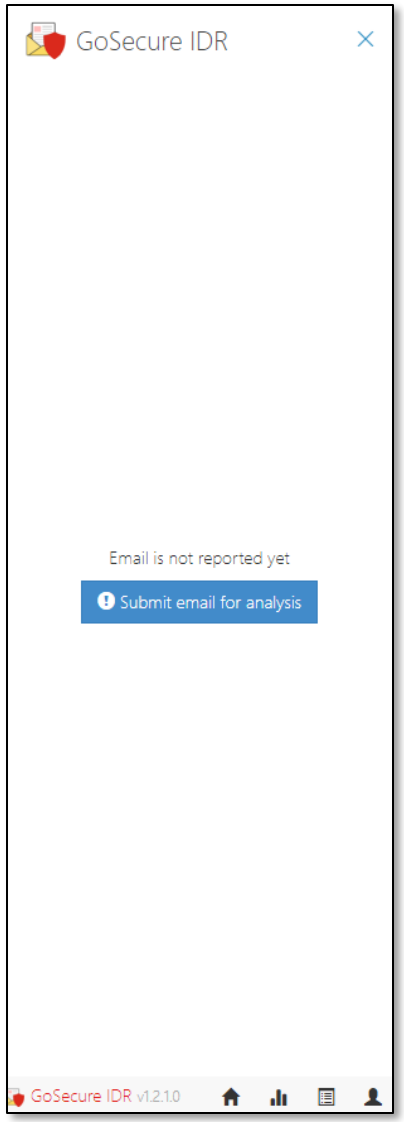



Statistics


Support Logs

# DECISION

## GREEN LIGHT

Good To Go!

This response indicates that the e-mail is not malicious, which has led GoSecure to place it in your inbox.

## YELLOW LIGHT

Be Careful

This means that the service has not clearly identified that the e-mail is malicious, but it has spotted elements that raise doubts about its legitimacy, leading to the email being quarantined or returned to your inbox depending on your organization's security settings.

If the email was returned to your inbox, we recommend that you contact the sender via phone before completing any request.

## RED LIGHT

We've found a threat!

This response indicates that the e-mail is suspicious, which has led to it being quarantined.

# FAQ

# Why do I get a yellow light when I submit an internal email to GoSecure for analysis?

- We recommend that you contact the sender via phone to confirm any request

# What should I do if I realize I've clicked on a dubious link in a fraudulent email?

- Change your password immediately
- Inform your security team
- Be sure to notify your manager

# Can I recover an email quarantined by GoSecure?

- Of course, you can ask your company's IT support team to lift the quarantine placed on an e-mail by GoSecure.

# Our team received an email, but it seems to have disappeared from all our inboxes. Can you explain why?

- This indicates that a member of your team had concerns about this email. They submitted it to GoSecure IDR for analysis and received a yellow spam or red warning. As a result, the email has been removed from all inboxes and placed in quarantine.

# I have concerns about cybersecurity. Who should I contact?

- Your IT support team will always be your first point of contact for assistance on IT and cybersecurity issues.

GoSecure.net


# Thank you!