TESSIAN

TESSIAN DEFENDER

# Tessian Defender Threat Catalogue

Learn how Tessian Defender detects and prevents inbound emails attacks that slip right past native email tools and legacy solutions.


Share this report

# Defender Threat Catalogue

Phishing, spear phishing, business email compromise (BEC), and other advanced impersonation attacks are top of mind for security leaders. It's easy to see why.

According to the FBI, phishing was the most common type of cybercrime in 2020—and phishing incidents nearly doubled in frequency, from 114,702 incidents in 2019, to 241,324 incidents in 2020.

Most often, the following types of data are compromised:

1. Credentials (passwords, usernames, pin numbers)
2. Personal data (name, address, email address)
3. Internal data (sales projections, product roadmaps)
4. Medical (treatment information, insurance claims)
5. Bank (account numbers, credit card information

So, what can organizations do to *prevent* successful phishing attacks? Generally, a combination of phishing awareness training, policies, and email security.

While a holistic approach is certainly best, and security leaders should leverage all of the above to protect their organization, *not all email security solutions are created equal.*

*In fact, the most sophisticated phishing attacks will slip right past Secure Email Gateways (SEGs) and native tools for O365 and G-Suite. These solutions also don't support or reinforce training.*

Tessian is different.

Tessian Defender automatically prevents both known *and* unknown email attacks that bypass Secure Email Gateways (SEGs), while *also* providing in-the-moment training to educate employees and drive them towards more secure email behavior.

See for yourself.

This catalogue includes real examples of threats detected and prevented by Tessian Defender alongside the warnings messages displayed, explaining *exactly* why the message was flagged as suspicious.

Subject [Firstname) UPDATED EMPLOYEE HANDBOOK

Michael HR Notice
<john.david@ntlworld.com>

To Michael Price <michael.price@acme.com>

Cc

Effective today Monday, September 27 we have a new Employee Handbook. The handbook is available for review below. Please review the changes and sign your acknowledgement of the handbook in section 2 immediately upon receipt of this notification.

https://ntlworld-my.sharepoint.com/hr-notice

As of this morning, approximately 20% of our employees have acknowledged the handbook and we are looking to get 100% before or by Friday! We are all required to review and sign an acknowledgement of the handbook upon receipt of this email.

Regards,

Human Resources

| RED FLAG | WHY IT SLIPS PAST OTHER DEFENSES |
|---|---|
| **Display Name**<br>The Display Name was created to look like the target's name, but the sender's domain doesn't belong to the recipient's company. | Pre-defined rule sets – which legacy solutions rely on – don't account for the almost infinite number of domain and subdomain, display name and address permutations impersonation allows for. |
| **Suspicious Link**<br>The link leads to an online Word document which – on its own – isn't malicious. But, *within* the document is another link, which leads to a fake O365 login page. | Tools that scan URLs usually won't scan URLs on the page that the initial URL leads to. |
| **Urgency**<br>Throughout the email, the attacker is employing social engineering tactics to create a sense of legitimacy and urgency. | Legacy security systems rely on detecting keywords like "wire transfer" or "account details" to identify suspicious language. |

ATTACK TYPE:
Spear Phishing

IMPERSONATED PARTY:
Internal

IMPERSONATION METHOD:
Display Name Lookalike

ATTACK OUTCOME:
Credential Harvesting

## There is something unusual about this email, please take care as it could be malicious.

Report as Unusual and Delete | Mark as Safe | I'm Not Sure

Tessian has flagged this email because it matches some common patterns seen in email impersonation attacks. Tessian found the following unusual about the email:

- The sender's email address "**ntlworld.com**" is not seen in your company's email network.
- The attack contains an unusual link "**https://ntlworld-my.sharepoint.com/hr-notice**" that matches some patterns seen in previous attacks.
- The email contains language indicating a sense of urgency (a common technique used in attacks)

**COVID-19 Update:** Phishing attacks are increasing to take advantage of the current situation, please take extra care.

Subject [Firstname) UPDATED EMPLOYEE HANDBOOK

Michael HR Notice
<john.david@ntlworld.com>

To Michael Price <michael.price@acme.com>

Effective today Monday, September 27 we have a new Employee Handbook. The handbook is available for review below. Please review the changes and sign

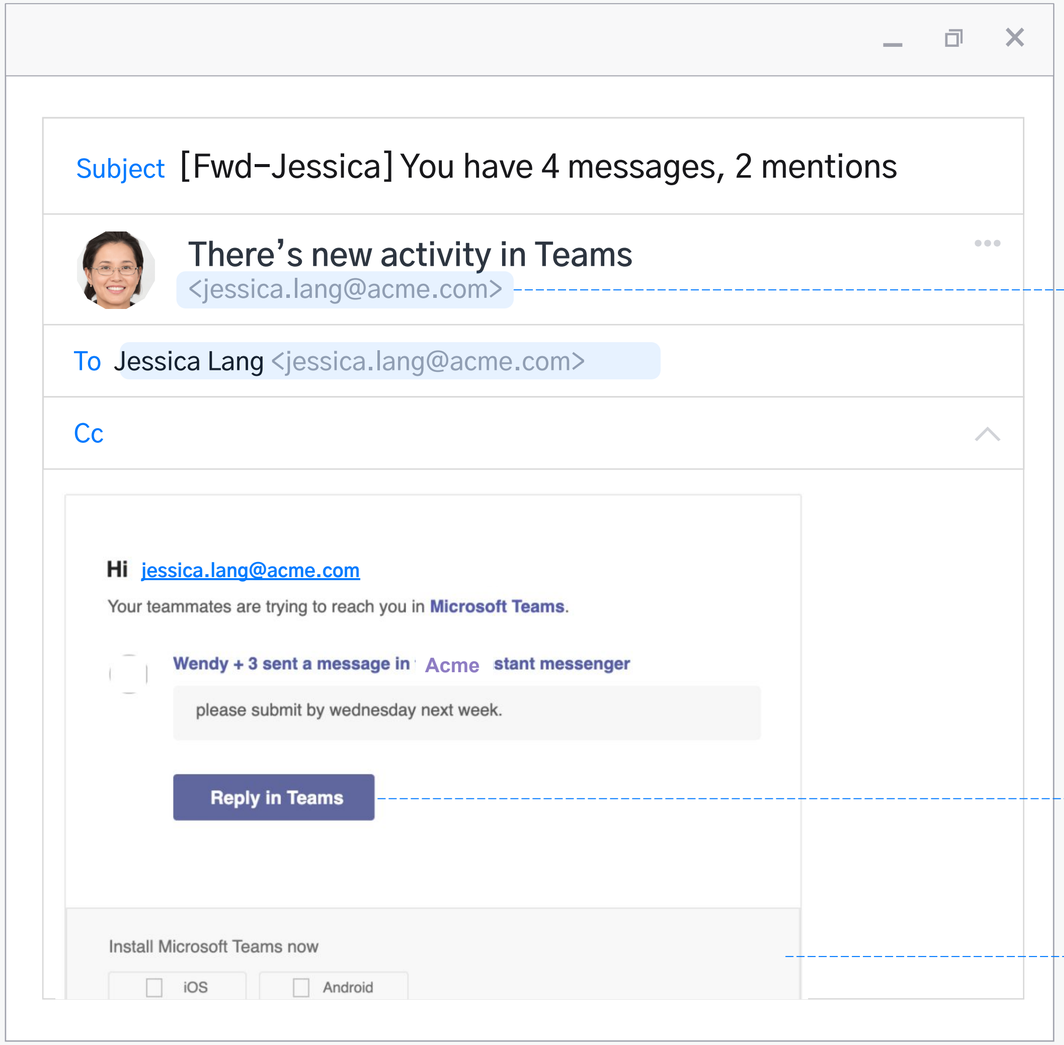
| RED FLAG | HOW TESSIAN DEFENDER CAUGHT IT |
|---|---|
| **Display Name**<br>The Display Name was created to look like the target's name, but the sender's domain doesn't belong to the recipient's company. | The Tessian platform ingests historical email data and knows what's "normal" and what isn't. No rules required. In this case, it recognized that the sender's email address is rarely seen on the network. |
| **Suspicious Link**<br>The link leads to an online Word document which – on its own – isn't malicious. But, *within* the document is another link, which leads to a fake O365 login page. | Tessian Defender knows that this URL looks suspicious for this user. Defender can learn from previous attacks across the Tessian network, allowing it to spot new threats. |
| **Urgency**<br>Throughout the email, the attacker is employing social engineering tactics to create a sense of legitimacy and urgency. | Tessian looks beyond keywords, using natural language processing (NLP) to understand what the email is about. |

ATTACK TYPE:
Spear Phishing

IMPERSONATED PARTY:
Internal

IMPERSONATION METHOD:
Display Name Lookalike

ATTACK OUTCOME:
Credential Harvesting




| RED FLAG | WHY IT SLIPS PAST OTHER DEFENSES |
|---|---|
| **Sender's Email Address**<br>The sender's email address is spoofing the target's own email address. This is particularly clever; it's not implausible that Microsoft Teams would actually send emails "from" the user's own email address. | The domain itself isn't suspicious and the email didn't fail any authentication checks. |
| **Suspicious Link**<br>The "Reply in Teams" button leads to a fake login page | The malicious page had never been seen in previous attacks, so wasn't denylisted. |
| **Formatting**<br>The notification is well-formatted and looks like a genuine email from Microsoft Teams. There aren't any obvious spelling or grammar errors. | After slipping past technological controls, employees are left as the last line of defense. Most won't question the legitimacy of the email because it looks like the real thing. |

ATTACK TYPE:
Spear Phishing

IMPERSONATED PARTY:
Microsoft Teams

IMPERSONATION METHOD:
Direct Spoof

ATTACK OUTCOME:
Credential Harvesting

## There is something unusual about this email, please take care as it could be malicious.

Report as Unusual and Delete | Mark as Safe | I'm Not Sure

Tessian has flagged this email because the sender could be pretending to be from "**acme.com**". **Anyone can forge an email to look like it's been sent from another domain, an attack known as Direct Spoof Impersonation.**

- The domain "**acme.com**" **does not normally send emails from this server**

**COVID-19 Update:** Phishing attacks are increasing to take advantage of the current situation, please take extra care.

Subject [Fwd-Jessica] You have 4 messages, 2 mentions

There's new activity in Teams
<jessica.lang@acme.com>

To Jessica Lang <jessica.lang@acme.com>

**Hi** jessica.lang@acme.com

Your teammates are trying to reach you in **Microsoft Teams**.

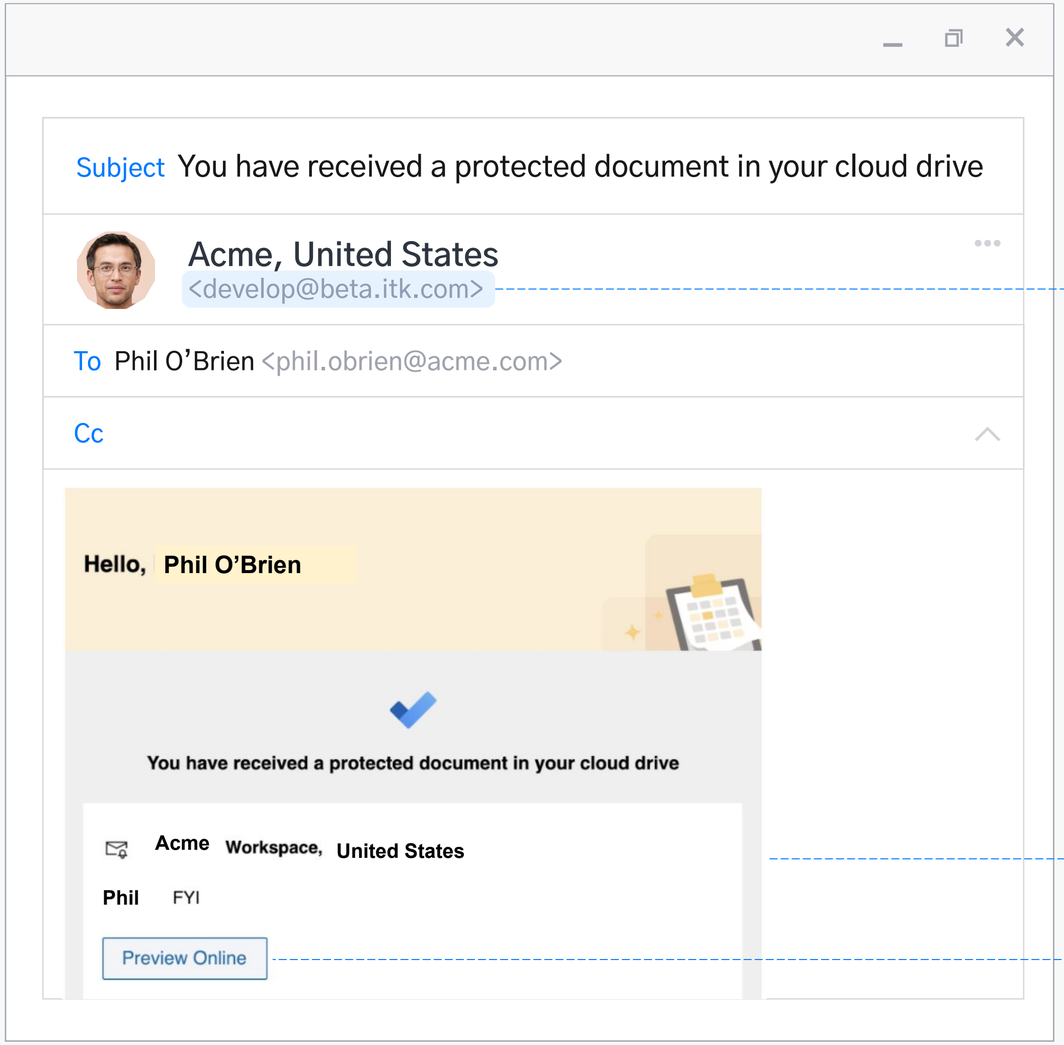
| RED FLAG | HOW TESSIAN DEFENDER CAUGHT IT |
|---|---|
| **Sender's Email Address**<br>The sender's email address is spoofing the target's own email address. This is particularly clever; it's not implausible that Microsoft Teams would actually send emails "from" the user's own email address. | Tessian Defender detects anomalies in the sender's server, IP address, and geophysical location to detect spoofed emails. |
| **Suspicious Link**<br>The "Reply in Teams" button leads to a fake login page | Tessian understands that the email is a spoof, and doesn't need to rely on detecting malicious payloads. |

ATTACK TYPE:
**Spear Phishing**

IMPERSONATED PARTY:
**Microsoft Teams**

IMPERSONATION METHOD:
**Direct Spoof**

ATTACK OUTCOME:
**Credential Harvesting**



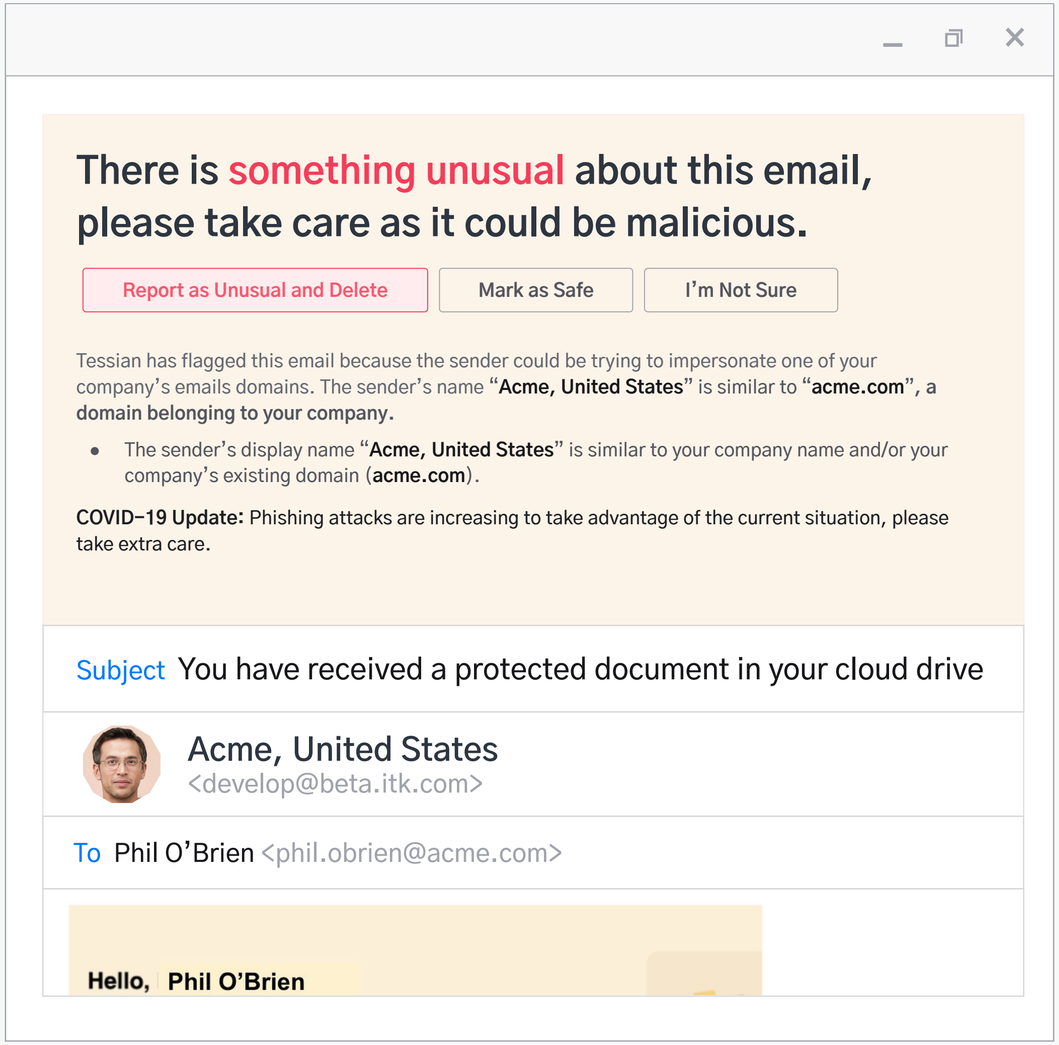

| RED FLAG | WHY IT SLIPS PAST OTHER DEFENSES |
|---|---|
| **Display Name**<br>The sender's email address and Display Name don't match; the attacker is trying to impersonate the target's company domain. | Pre-defined rule sets – which legacy solutions rely on – don't account for the almost infinite number of domain and subdomain, display name and address permutations impersonation allows for. |
| **Suspicious Link**<br>The "Preview Online" button leads to a lookalike website. | Legacy tools rely on detecting known malicious payloads to stop attacks, but this link was never used in a previous attack. |
| **Formatting**<br>The notification is well-formatted and looks like a genuine email from Microsoft File Sharing. There aren't any obvious spelling or grammar errors. | After slipping past technological controls, employees are left as the last line of defense. Most won't question the legitimacy of the email because it looks like the real thing. |

ATTACK TYPE:
**Spear Phishing**

IMPERSONATED PARTY:
**Microsoft File Sharing**

IMPERSONATION METHOD:
**Display Name Lookalike**

ATTACK OUTCOME:
**Credential Harvesting**




| RED FLAG | HOW TESSIAN DEFENDER CAUGHT IT |
|---|---|
| **Display Name**<br>The sender's email address and Display Name don't match; the attacker is trying to impersonate the target's company domain. | The platform understands that the sender's display name imitates the target company, *Acme*, and that the sender isn't from there. |
| **Suspicious Link**<br>The "Preview Online" button leads to a lookalike website. | Tessian understands that the email is a malicious lookalike, and doesn't need to rely on detecting malicious payloads. |

ATTACK TYPE:
Spear Phishing

IMPERSONATED PARTY:
Microsoft File Sharing

IMPERSONATION METHOD:
Display Name Lookalike

ATTACK OUTCOME:
Credential Harvesting

Subject Notification: Please verify your account details.

GoDaddy Verification
<amrek500@hotmail.com>

To Tamara Smith <tamara.smith@acme.com>

Cc

Dear tamara.smith@acme.com,

We noticed some unusual activity on your GoDaddy account and we are concerned about potential unauthorized account access.

We need your help resolving an issue with your GoDaddy account.

Until you help us resolve this issue, we've temporarily limited what you can do with your account.

Please click here and prove that you are the right account holder in order to avoid account limitation.

In case you ignore this automated email, your account will be limited permanently.

GoDaddy™

| RED FLAG | WHY IT SLIPS PAST OTHER DEFENSES |
|---|---|
| **Display Name**<br>The sender's display name is Godaddy, a common website registrar, but the email was sent from hotmail | Pre-defined rule sets – which legacy solutions rely on – don't account for the almost infinite number of domain and subdomain, display name and address permutations impersonation allows for. |
| **Suspicious Link**<br>The link leads to a lookalike website. | Legacy security systems rely on detecting known malicious payloads to stop attacks, but this link was never used in a previous attack. |
| **Social engineering**<br>The attacker is employing social engineering tactics to create a sense of legitimacy and urgency. | Legacy security systems rely on detecting keywords like "wire transfer" or "account details" to identify suspicious language. |
| **Formatting**<br>The notification is well-formatted and looks like a genuine email from GoDaddy. There aren't any obvious spelling or grammar errors. | After slipping past technological controls, employees are left as the last line of defense. Most won't question the legitimacy of the email because it looks like the real thing. |

ATTACK TYPE:
Spear Phishing

IMPERSONATED PARTY:
GoDaddy

IMPERSONATION METHOD:
Freemail Impersonation

ATTACK OUTCOME:
Credential Harvesting

## There is something unusual about this email, please take care as it could be malicious.

Report as Unusual and Delete | Mark as Safe | I'm Not Sure

Tessian has flagged this email because it matches some common patterns seen in email impersonation attacks. Tessian found the following unusual about the email:

- The email's subject contains language commonly used in email attacks
- The email contains an unusual link "**lavola.intelsolut.com/vendor···**" that matches some patterns seen in previous attacks.

Please be careful when replying to or interacting with this email.

**COVID-19 Update:** Phishing attacks are increasing to take advantage of the current situation, please take extra care.

Subject Notification: Please verify your account details.

GoDaddy Verification
<amrek500@hotmail.com>

To Tamara Smith <tamara.smith@acme.com>

Dear tamara.smith@acme.com,

We noticed some unusual activity on your GoDaddy account and we are

| RED FLAG | HOW TESSIAN DEFENDER CAUGHT IT |
|---|---|
| **Display Name**<br>The sender's display name contains *Godaddy*, a common website registrar, but the email was sent from hotmail. | Defender understands that the sender's display name contains a commonly impersonated brand, but the email is sent from a hotmail account. |
| **Suspicious Link**<br>The link leads to a lookalike website. | Tessian Defender learns from previous attacks across the Tessian network to spot new threats. |
| **Social engineering**<br>The attacker is employing social engineering tactics to create a sense of legitimacy and urgency. | Tessian looks beyond keywords, using natural language processing (NLP) to understand what the email is about. |

ATTACK TYPE:
**Spear Phishing**

IMPERSONATED PARTY:
**GoDaddy**

IMPERSONATION METHOD:
**Freemail Impersonation**

ATTACK OUTCOME:
**Credential Harvesting**

Subject Joel, you've missed a phone call

Edwards
<edwards@trendfinder.com>

To Joel Kim <joel.kim@acme.com>

Cc

Good afternoon, Joel!

I am a newbie in Acme. I attempted to call you twice today.

I have to ask, what about our consumer complaint request #75-01/28/21?

Online preview in PDF.

I need to debit fees of of your payroll within the next 2 hours.

Edwards

Acme HR Outsource Manager

| RED FLAG | WHY IT SLIPS PAST OTHER DEFENSES |
|---|---|
| **Display Name**<br>The sender's Display Name and email address – while seemingly legitimate – haven't been seen in the company's network before | The attacker has simply invented the person that's being impersonated, so legacy tools can't "match" them against existing employees |
| **Suspicious Link**<br>The link is malicious. If the target were to download the PDF, malware would likely be deployed. | Legacy solutions only scan for *known* malicious payloads, but this link has never been seen in previous attacks. |
| **Social engineering**<br>The attacker is employing social engineering tactics to create a sense of legitimacy and urgency. | Legacy security systems rely on detecting keywords like "wire transfer" or "account details" to identify suspicious language. |

ATTACK TYPE:
Spear Phishing

IMPERSONATED PARTY:
Internal

IMPERSONATION METHOD:
Display Name Impersonation

ATTACK OUTCOME:
Malware

## There is something unusual about this email, please take care as it could be malicious.

Report as Unusual and Delete | Mark as Safe | I'm Not Sure

Tessian has flagged this email because it matches some common patterns seen in email impersonation attacks. Tessian found the following unusual about the email:

- The sender's email domain **"@trendfinder.com"** is not often seen across the networks that Tessian protects
- The email contains an unusual link **"https://bit.ly/93gsye"** that matches some patterns seen in previous attacks.
- The email contains a 'shortened' link, meaning it's more difficult to know which website you will be taken to if you click on it.

Please be careful when replying to or interacting with this email.

Subject Joel, you've missed a phone call

Edwards
<edwards@trendfinder.com>

To Joel Kim <joel.kim@acme.com>

Good afternoon, Joel!

I am a newbie in Acme. I attempted to call you twice today.

| RED FLAG | HOW TESSIAN DEFENDER CAUGHT IT |
|---|---|
| **Display Name**<br>The sender's Display Name and email address – while seemingly legitimate – haven't been seen in the company's network before | The platform ingests historical email data and knows that this sender is new. |
| **Suspicious Link**<br>The link is malicious. If the target were to download the PDF, malware would likely be deployed. | Tessian Defender knows that this URL looks suspicious for this user. Defender can learn from previous attacks across the Tessian network, allowing it to spot new threats. |
| **Social engineering**<br>The attacker is employing social engineering tactics to create a sense of legitimacy and urgency. | Tessian looks beyond keywords, using natural language processing (NLP) to understand what the email is about. |

ATTACK TYPE:
Spear Phishing

IMPERSONATED PARTY:
Internal

IMPERSONATION METHOD:
Display Name Impersonation

ATTACK OUTCOME:
Malware

Subject RFP Enclosed

William Kruger
<willian.kruger@ABCconstruction.co.uk>

To Penny Minite <penny.minite@acme.com>

Cc

Hello

Please find the Request for Proposal in this shared folder.

>>Accessible link here<<

Enclosed is a scope of work, and we request your proposal and availability by end of week.

To confirm receipt of our RFP, please reply to this email.

Please don't hesitate to contact us with any questions.

Will

| RED FLAG | WHY IT SLIPS PAST OTHER DEFENSES |
|---|---|
| **Email address**<br>Because the email is being sent from a compromised vendor account, neither the email address nor the display name are suspicious. | The email address is legitimate and the display name and the email address match. Because the recipient often communicates with the sender, their domain is commonly seen on the target company's email network and appears legitimate. |
| **Suspicious Link**<br>The link is malicious. If the target were to open the shared folder, malware would likely be deployed. | Legacy security systems rely on detecting known malicious payloads to stop attacks, but this link was never used in a previous attack. |

ATTACK TYPE:
Vendor Account Takeover (ATO)

IMPERSONATED PARTY:
External

IMPERSONATION METHOD:
Vendor Email Compromise

ATTACK OUTCOME:
Malware

## There is something unusual about this email, please take care as it could be malicious.

Report as Unusual and Delete | Mark as Safe | I'm Not Sure

**william.kruger@ABCconstruction.co.uk**'s mailbox may be compromised. Tessian found the following unusual about the email:

- The email looks like it was sent from the **United States of America,** a country the sender doesn't normally send emails from.
- The email contains an unusual link **"app.box.com/s/gu2gti9"** to a shared file on **Box**. The sender doesn't usually share attachments this way.
- The sender has sent an unusually high number of emails today. This is a common pattern for attacks using compromised accounts.

Please be careful when replying to or interacting with this email. Try contacting the sender from a different channel to confirm the email was sent by them.

Subject RFP Enclosed

William Kruger
<willian.kruger@ABCconstruction.co.uk>

To Penny Minite <penny.minite@acme.com>

Hello

Please find the Request for Proposal in this shared folder.

| RED FLAG | HOW TESSIAN DEFENDER CAUGHT IT |
|---|---|
| **Email address**<br>Because the email is being sent from a compromised vendor account, neither the email address nor the display name are suspicious. | Tessian Defender ingests and analyzes historical email data to catch anomalous sending patterns. Here, it detected that the sender was based in an unusual country and was sending an unusually high number of emails. |
| **Suspicious Link**<br>The link is malicious. If the target were to download the PDF, malware would likely be deployed. | Tessian Defender knows that this URL looks suspicious for this user, who doesn't usually share attachments this way. |

ATTACK TYPE:
Vendor Account Takeover (ATO)

IMPERSONATED PARTY:
External

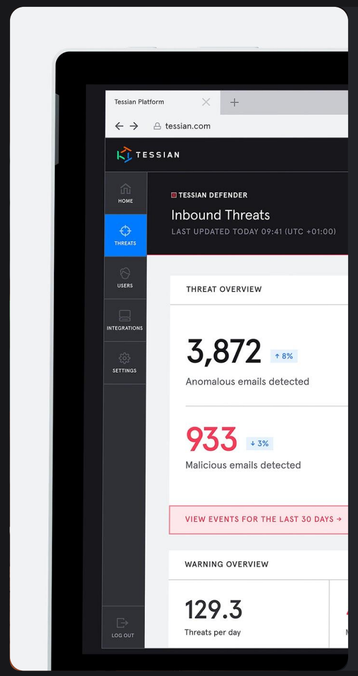
IMPERSONATION METHOD:
Vendor Email Compromise

ATTACK OUTCOME:
Malware

TESSIAN

Tessian's mission is to secure the human layer. Using machine learning technology, Tessian automatically stops data breaches and security threats caused by human error – like data exfiltration, accidental data loss, business email compromise and phishing attacks – with minimal disruption to employees' workflow. As a result, employees are empowered to do their best work, without security getting in their way. Founded in 2013, Tessian is backed by renowned investors like Sequoia, Accel and Balderton and has offices in San Francisco and London.

TESSIAN.COM




## DEFENDER

Tessian Defender is a comprehensive inbound email security solution that automatically prevents a wide range of attacks that bypass Secure Email Gateways (SEGs), while providing in-the-moment training to drive employees toward secure email behavior.

REQUEST A DEMO →

## Trusted by World-Leading Businesses

大成 DENTONS
GRAPHCORE
rightmove
Investec
arm
gubra
JTC
affirm
CHOATE
fieldfisher
REALPAGE OUTPERFORM
HILL DICKINSON
cordaan
EVERCORE
Schroders

Share this report

TESSIAN.COM/RESEARCH →