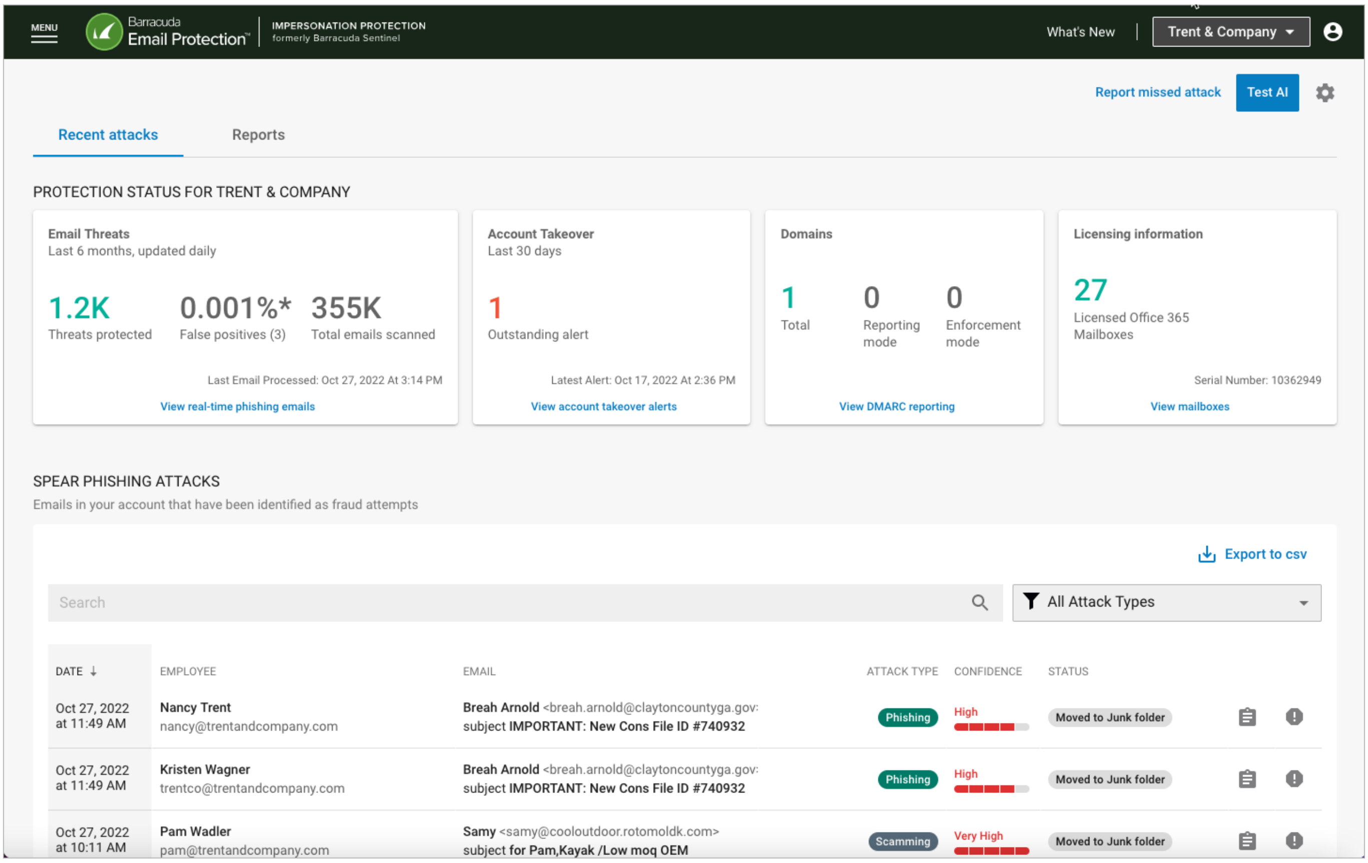
Spear Phishing Protection

https://campus.barracuda.com/doc/91984521/

When you first log into Impersonation Protection, the **Spear Phishing Protection** page appears. You can also reach the **Spear Phishing Protection** page at any time from the menu in the upper left corner of any Impersonation Protection page.



PROTECTION STATUS FOR TRENT & COMPANY

Email Threats
Last 6 months, updated daily

1.2K Threats protected
0.001%* False positives (3)
355K Total emails scanned

Last Email Processed: Oct 27, 2022 At 3:14 PM

View real-time phishing emails

Account Takeover
Last 30 days

1 Outstanding alert

Latest Alert: Oct 17, 2022 At 2:36 PM

View account takeover alerts

Domains

1 Total
0 Reporting mode
0 Enforcement mode

View DMARC reporting

Licensing information

27 Licensed Office 365 Mailboxes

Serial Number: 10362949

View mailboxes

SPEAR PHISHING ATTACKS

Emails in your account that have been identified as fraud attempts

Export to csv

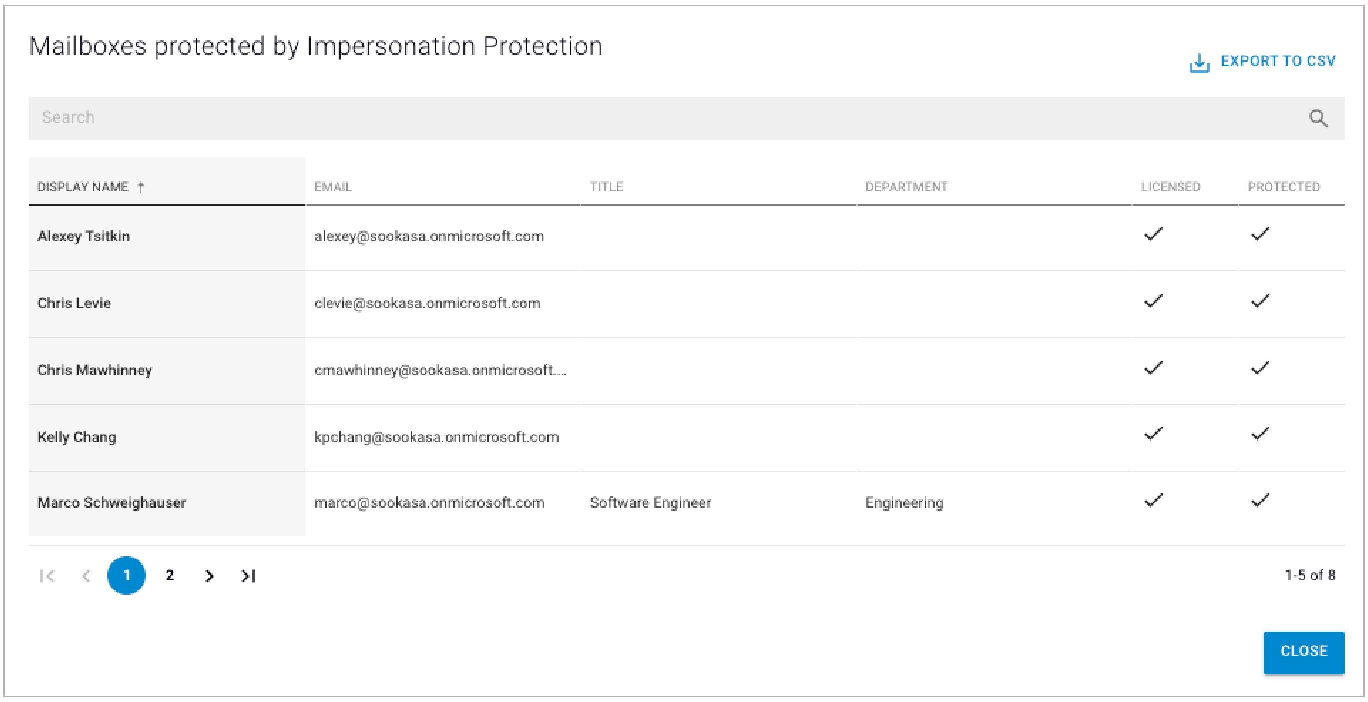
Search

All Attack Types

DATE ↓	EMPLOYEE	EMAIL	ATTACK TYPE	CONFIDENCE	STATUS
Oct 27, 2022 at 11:49 AM	**Nancy Trent** nancy@trentandcompany.com	**Breah Arnold** <breah.arnold@claytoncountyga.gov: subject **IMPORTANT: New Cons File ID #740932**	Phishing	High	Moved to Junk folder
Oct 27, 2022 at 11:49 AM	**Kristen Wagner** trentco@trentandcompany.com	**Breah Arnold** <breah.arnold@claytoncountyga.gov: subject **IMPORTANT: New Cons File ID #740932**	Phishing	High	Moved to Junk folder
Oct 27, 2022 at 10:11 AM	**Pam Wadler** pam@trentandcompany.com	**Samy** <samy@cooloutdoor.rotomoldk.com> subject **for Pam,Kayak /Low moq OEM**	Scamming	Very High	Moved to Junk folder

Viewing Licensed and Protected Mailboxes

In the **Licensing Information** box, click **View Mailboxes**. On the **Impersonation Protection for your mailboxes** page, each mailbox – for users and shared – is displayed, along with Display Names.



Mailboxes protected by Impersonation Protection

DISPLAY NAME ↑	EMAIL	TITLE	DEPARTMENT	LICENSED	PROTECTED
Alexey Tsitkin	alexey@sookasa.onmicrosoft.com			✓	✓
Chris Levie	clevie@sookasa.onmicrosoft.com			✓	✓
Chris Mawhinney	cmawhinney@sookasa.onmicrosoft....			✓	✓
Kelly Chang	kpchang@sookasa.onmicrosoft.com			✓	✓
Marco Schweighauser	marco@sookasa.onmicrosoft.com	Software Engineer	Engineering	✓	✓

Each mailbox can have either one or both status values:

- **Licensed** – Whether that mailbox has a Microsoft Exchange license.
- **Protected** – Whether the mailbox is currently monitored and protected by Barracuda.

> - A Microsoft Exchange license is not required to be protected by Barracuda.
> - In rare cases, Barracuda might not be able to protect a licensed mailbox.

Exporting Mailbox Information

You can export and download this mailbox information to a CSV file, so you can use it for other administrative functions.

To export your mailbox information:

1. On the **Spear Phishing Protection** page, in the **Licensing Information** box, click **View Mailboxes**.
2. On the **Impersonation Protection for your mailboxes** page, click **Export to CSV**.
   The CSV file downloads automatically to your usual download location.

Note for larger organizations: The first 20,000 of your mailboxes are exported, based on the Display Name value. Your searching or changing the sort order does not affect the export.

Viewing Recent Spear Phishing Attacks

The **Spear Phishing Protection** page displays recent spear phishing attacks.

Each attack shows the Attack Type and Confidence Score, described below.

Exporting Spear Phishing Information

Click **Export to CSV** to export records that are displayed in the pages of the table, up to a limit of 10,000 records, sorted by date.

Locating Specific Attacks

To locate specific attacks:

- **Search** – Enter all or part of a word in the **Search** box to find matching incidents.
- **Filter Attacks** – Click to display a list where you can choose to see all attacks or one of the Attack Types described here:
  - **All Attack Types** – No filter
  - **Conversation Hijacking** – A nefarious actor uses compromised credentials to insert themselves into a legitimate email thread, using a slightly altered domain, and attempt to take over lucrative opportunities, like bank transfers. Domain Hijacking, using a slightly altered Sender domain, as just described, can be a part of a Conversation Hijacking attack.
  - **Extortion** – A nefarious actor is demanding money from your organization, threatening that if they do not receive the funds, they will publish information that will be embarrassing to your organization or to people within it.
  - **Impersonation** – A nefarious actor is sending email, pretending to a member of your organization or pretending to represent a service, like a bank or an internet service provider.
  - **Scamming** – A nefarious actor is trying to get money from you or your organization.

For any record, click the details icon 📋 to see more information about it.

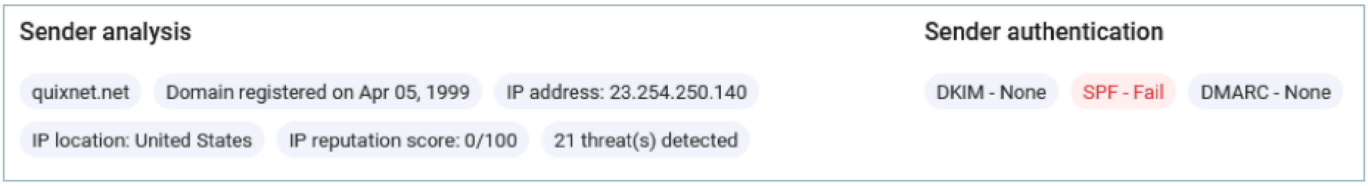
Message Details

The Message details page shows additional information for a specific attack.

Sender Information

The top of the message detail provides information pertaining to the sender as well as the results of the sender authentication checks performed by the email gateway.

Note: Impersonation protection does not do any of its own sender authentication checks and simply users the information found in the **Authentication-Results** header.



Sender analysis

quixnet.net | Domain registered on Apr 05, 1999 | IP address: 23.254.250.140

IP location: United States | IP reputation score: 0/100 | 21 threat(s) detected

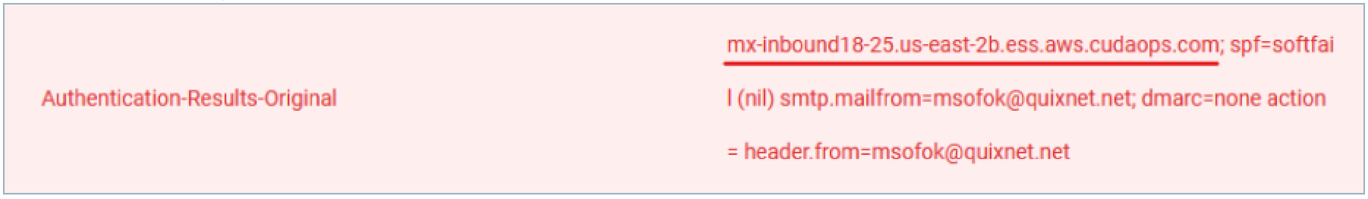
Sender authentication

DKIM - None | SPF - Fail | DMARC - None

For customers using Email Gateway Defense, the sender authentication results header injected by EGD will be used. For all other customers, the Microsoft sender authentication results will be used.

If any failures are noted in the results header, the corresponding header will be highlighted.

Here is an example of the Barracuda results header:



Authentication-Results-Original

mx-inbound18-25.us-east-2b.ess.aws.cudaops.com; spf=softfai
l (nil) smtp.mailfrom=msofok@quixnet.net; dmarc=none action
= header.from=msofok@quixnet.net

Email and Headers Tabs

Select each tab to review

- The contents of the email
- Full header information from the email
- Name, size, and type of attachments, if any

Analysis

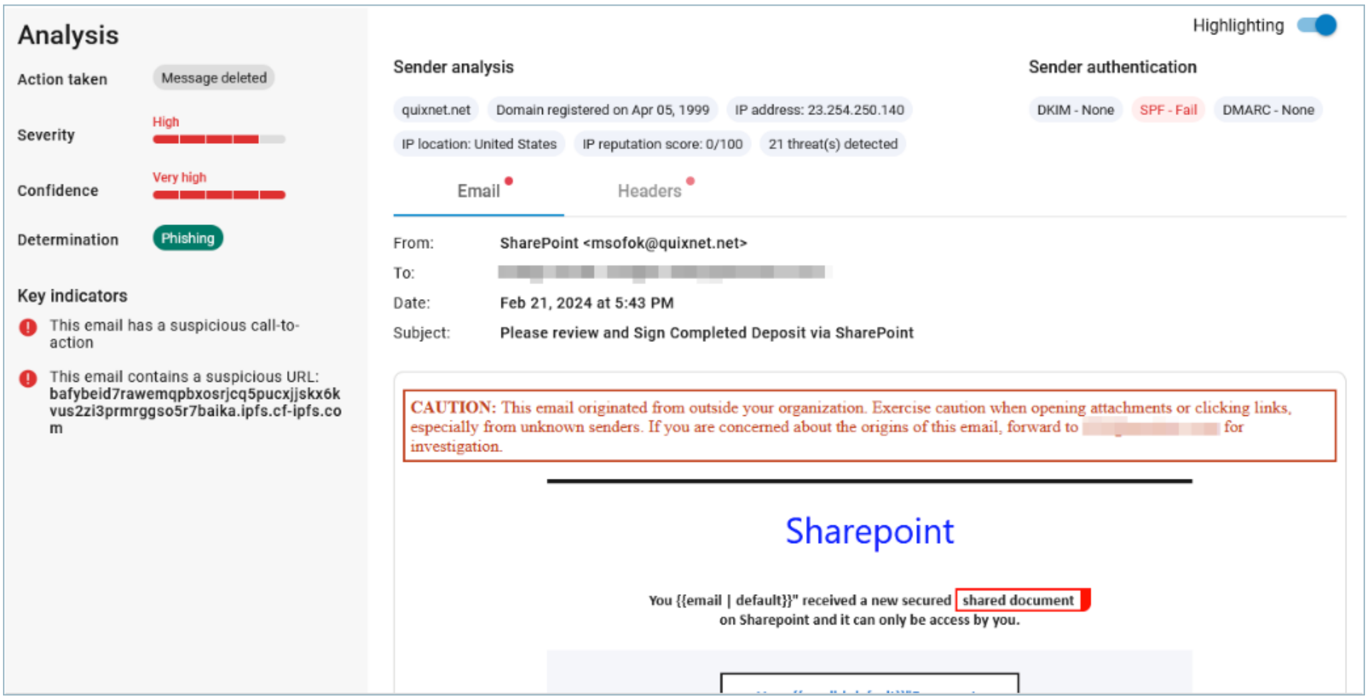
The Analysis panel provides Barracuda Networks' findings on the attack.

- **Severity** – The seriousness of this threat, based on its attack type. For example, an impersonation attack will always have a higher severity score than scamming.
- **Confidence** – A measure of the likelihood that this email is an actual threat, based on internal classifiers and calculations.
- **Determination** – The type of attack, based on Key Indicators below. Attack types are listed above in the Locating Specific Attacks section.

- **Key Indicators** – Characteristics typical of an attack type of the attack that led to its attack type determination.

Highlighting

Toggle to enable **Highlighting** at top-right to see the elements of a message that Barracuda Impersonation Protection deem as suspicious. Keywords and phrases in the message content will have red boxes around them. These keyword and phrases are those that are typically seen in fraudulent emails. Other identifiers, shown via the Sender Information chips and Header information will display in red. The **Email** and **Header** tabs will show red dots if they display suspicious information.



Analysis

Action taken: Message deleted

Severity: High

Confidence: Very high

Determination: Phishing

Key indicators

- This email has a suspicious call-to-action
- This email contains a suspicious URL: bafybeid7rawemqpbxosrjcq5pucxjjskx6kvus2zi3prmrggso5r7baika.ipfs.cf-ipfs.com

Highlighting

Sender analysis

quixnet.net | Domain registered on Apr 05, 1999 | IP address: 23.254.250.140 | IP location: United States | IP reputation score: 0/100 | 21 threat(s) detected

Sender authentication

DKIM - None | SPF - Fail | DMARC - None

From: SharePoint <msofok@quixnet.net>

To: [redacted]

Date: Feb 21, 2024 at 5:43 PM

Subject: Please review and Sign Completed Deposit via SharePoint

CAUTION: This email originated from outside your organization. Exercise caution when opening attachments or clicking links, especially from unknown senders. If you are concerned about the origins of this email, forward to [redacted] for investigation.

Sharepoint

You {{email | default}}" received a new secured shared document on Sharepoint and it can only be access by you.

Report False Positive

Click **Report False Positive** if you think this email is not an actual attack. For details, refer to False Positives.

Find Similar Messages

Finding similar messages is available only with Barracuda Email Protection Premium and Premium Plus plans.

When viewing the details of an attack, you can click **Find Similar Messages** to open the Incident Response feature, where you can locate incidents similar to the one you are currently viewing.

Figures