

Handling an Account Takeover

<https://campus.barracuda.com/doc/76283940/>

If you become aware that a malicious actor has seized control of an internal email account, you can take steps within Impersonation Protection to begin to mitigate the problem and prevent more takeovers.

Impersonation Protection can detect Account Takeovers based on many factors, including:

- Suspicious sign-ins
- Suspicious Inbox rules
- Suspicious internal emails

Notes


- You can only resolve issues with accounts that are currently being tracked by Impersonation Protection.
- You must have an Microsoft 365 global administrator account for many of the steps on this page.

Handling a New Account Takeover Alert

1. Log into Impersonation Protection.
2. From the **Spear Phishing Protection** page, in the **Account Takeover Protection** section, click **View Account Takeover Alerts**.

Alternatively, click the menu button in the top left corner and select **Account Takeover Protection**.

The **Alerts** tab displays account takeover incidents detected by Impersonation Protection's artificial intelligence system.

- New alerts are displayed as **Not Reviewed**. Continue with the steps below to review and create an incident.
- Alerts display as **Reviewed** after you click **Create Incident** for that alert. Click the clipboard icon  to review details of the alert and, optionally, to create an incident. If you create an incident, continue with [Step 5](#) below.

3. Locate the alert you want to handle and click **Review**.
4. Click **View Message** to learn more about the alert. If you are certain that the email was legitimate, click **False Positive** and confirm that the email was legitimate.
If the email was an account takeover, click **Create Incident**.
5. When prompted, change the account password. This will keep unauthorized users out of the compromised account.

You can reset the password here if your environment has only Azure Active Directory


(Azure AD), also called a *non-federated domain*. If you have a hybrid LDAP server, also called a *federated domain*, skip this step and manually reset the password on your local active directory server. For details, refer to the [Microsoft passwordProfile property documentation](#).

6. To manually block the attacker's access to your user's account, click **Sign into Microsoft 365**. Microsoft 365 opens in a new browser window. Take the steps listed on the screen. Follow the **Learn more** links to read Microsoft's documentation on how to complete these actions.

Manually block attacker's access

Sign into Office 365 and complete the following actions to prevent an attacker from accessing the compromised account:

- **Disable sign-in access for this account** (recommended)
Prevent access to the account while the additional steps are performed. [Learn more...](#)
- **Kill any existing sessions** (recommended)
Kick out any attacker currently signed into the account. [Learn more...](#)
- **Reset the account password** (critical)
Change the password to prevent the attacker from accessing the account in the future. [Learn more...](#)

SIGN INTO OFFICE 365 

[CLEAN UP MESSAGES](#)

7. Return to Impersonation Protection and click **Clean Up Messages**. The New Account Takeover Incident wizard launches.

The first step informs you of what this wizard will do. Click **Next** to continue.

- **Internal clean up:** Remove malicious emails from your users' mailboxes to prevent further takeovers.
- **External notification:** Mitigate reputation and brand risk by letting external parties know they received a malicious email from you.

New account takeover incident

1

2

3

4

5

6

Here's what we are going to do

- Internal clean up:** remove malicious emails from your users' mailboxes to prevent further takeovers.
- External notification:** mitigate reputation and brand risk by letting external parties know they received a malicious email from you.

CANCEL

NEXT

8. In Step 2, the search criteria are already entered in the form, based on the information in the alert. Review the information, then click **Next** to continue.
- Note :** When you are creating an incident based on a suspicious login alert, you might not have a sample email. In this case, the **I don't have a sample...** checkbox might be selected.

New account takeover incident

1

2

3

4

5

6

Please provide information about the incident

Compromised account *

alexey@sookasa.onmicrosoft.com ×

Subject of malicious email sent from compromised account*

☒ I don't have a sample of a malicious email sent from this account


This attack happened in the last

1 week ▼

CANCEL

BACK


NEXT

9. Impersonation Protection searches for malicious emails related to the account takeover.
- If no emails are found, the **No malicious emails found - please try again** message displays. You can change the search criteria, like extending the timeframe, to search again, repeating Step 8 above.
 - If emails are found, they are displayed in a table. Click the details icon  to view more information about an email. Continue to the next step.

New account takeover incident

1 2 3 4 5 6

Please select malicious emails

Sent	Recipients	Subject	
Apr 01, 2020 at 12:56 PM	atsitkin@barracuda.com <atsitkin@barracuda.com>	Test	


Page:

1

1 - 1 of 1

<

>


The list above includes all emails sent from alexey@sookasa.onmicrosoft.com. Please click  to remediate all malicious emails with the same subject. Otherwise, click "No malicious emails" to proceed.

CANCEL

BACK

NO MALICIOUS EMAILS


10. If you determine that none of the emails are malicious, click **No Malicious Emails** and continue with [Step 12](#) below.

If you determine that the emails are malicious, click the wrench icon  and wait a moment for the process to run. This action automatically remediates all emails with the same subject, based on your account settings, which include deleting the email or moving it to the recipient's junk email folder. See [How to Specify Attack Response Options](#).

New account takeover incident

1 2 3 4 5 6

Please confirm all emails are malicious

Sent	Recipients	Subject	
Apr 01, 2020 at 12:56 PM	atsitkin@barracuda.com <atsitkin@barracuda.com>	Test	

Page:

1

1 - 1 of 1

<

>

Clicking "Yes" will not make changes to your tenant.

CANCEL

BACK

YES, ALL ARE MALICIOUS

After the process runs, you are asked to confirm that all of the emails are malicious. Click **Yes, All Are Malicious** and proceed to the next step.

Clicking **Yes** removes the malicious emails from the users' mailboxes.

11. If the email was not sent to other internal recipients, an informational message displays. Click

Next to continue.

New account takeover incident

1

2

3

4

5

6

No malicious emails were sent to internal recipients

Good news! The attack was not sent to internal recipients so there's no risk of additional infections in your organization. Please click continue to proceed.

CANCEL

NEXT

If the email was sent to other internal recipients, select how you want to remediate it – either permanently deleting the attack from users' Inboxes or moving it to recipients' Junk email folders. Then click **Clean Up**.

If you choose to skip this step, continue with the following step.

New account takeover incident

1

2

3

4

5

6

Should we clean up the attack from 1 internal recipient accounts?

Name	Email
Azeem	azeem@barracudaonmicrosoft.com

Clicking "Clean up" will

☒ Permanently delete the attack from recipients' Inbox

☐ Move the attack to recipients' Junk Email folders

CANCEL

SKIP

CLEAN UP

- If this email was sent to external users, Impersonation Protection notifies them. Select the account from which you want to send the notifications.

New account takeover incident

1

2

3

4

5

6

Notify 1 external recipient about the attack

EXPORT TO CSV

Name	Email
	atsitkin@barracuda.com

Page:

1

1 - 1 of 1

<

>

Please select an account from which to send notifications

Notifications will be sent from *

itay@sookasa.onmicrosoft.com

×

Edit email notification

Notifications will be sent over the next 10 minutes.

CLOSE

SKIP

SEND NOTIFICATIONS

The following options are available, if you choose:

- Click **Export to CSV** to save a record of the external names and emails of those affected by this incident.
- Click **Edit Email Notification** to customize the notification email with your own wording. Click **Apply** to return to the wizard.

New account takeover incident

1 2 3 4 5 6

The following notification will be sent to all affected recipients

From: ESS <ess@cuadmarctest.net>

Subject: Warning: you have recently received a malicious email from alexey@sookasa.onmicrosoft.com

Hi there,

I would like to inform you that you have recently received an email that we believe is malicious from one of our corporate accounts. We apologize for the inconvenience and recommend that you avoid clicking links inside this email and/or opening its attachments.

Details:

The email came from: Alexey Tsitkin <alexey@sookasa.onmicrosoft.com>

The email's subject contained: "<<subject>>"

The email was sent: <<date>>

CANCEL


APPLY

Click **Send Notifications** to warn external recipients about the incident. Emails will be sent within ten minutes. Continue to the next step.

Alternatively, click **Skip** to notify recipients using a different method. Continue to the next step.

The process of locating *external* issues is not completely accurate. Some external recipients might have received the malicious message but cannot be tracked by Impersonation Protection.

If the email was not distributed externally, an informative message displays. Click **Next** to continue.

- Review the Inbox Rules for the account that was taken over. Review rules listed on this page – especially rules that move, delete, or forward emails automatically. If there is a problem with a specific rule, click the delete icon  to remove it. Click **Next** to continue.

New account takeover incident

1

2

3

4

5

6

Please review inbox rules on alexey@sookasa.onmicrosoft.com

Inbox rules are often used by attackers to cover their tracks or take advantage of the accounts they take over. Please review rules that may move, delete or forward emails automatically.

Sequence	Name	Actions	Conditions	Exceptions	Enabled	
1	Delete messages from Microsoft Azure	Delete message Stop processing rules	Subject contains: Your Azure AD Identity Protection Weekly Digest From addresses: azure-noreply@microsoft.com Sent to addresses: alexey@sookasa.onmicrosoft.com	No	Yes	
2	Move messages from Microsoft Online Services Team	Delete message Mark as read Stop processing rules	Subject contains: View your Office 365 Business Essentials (Month to Month) billing statement From addresses: msonlineserviceteam@emsa.mail.microsoftonline.com	No	Yes	

Page:

1 ▾

1 - 2 of 2

<

>

CLOSE

NEXT

14. A message displays to let you know that you and Impersonation Protection have taken care of this issue.

Barracuda Networks strongly recommends implementing multi-factor authentication (MFA) to prevent future account takeover incidents.

The incident is listed on the **Incidents** tab after you complete step 4 of the wizard (step 12 above).

If you review an alert and create an incident, even if you do not complete creating the incident, the alert is listed on the **Alerts** tab as **Reviewed**.

Figures

1. clipboard.png
2. manuallyBlockAttack1.png
3. Step1.png
4. ATOsearch.png
5. viewDetailsIcon.png
6. 2NoMalicious.png
7. wrench.png
8. 2yesMalicious.png
9. 4NoemailsSent.png
10. internal.png
11. 4notify.png
12. editEmail.png
13. deleteTrash.png
14. inboxRules1.png

© Barracuda Networks Inc., 2024 The information contained within this document is confidential and proprietary to Barracuda Networks Inc. No portion of this document may be copied, distributed, publicized or used for other than internal documentary purposes without the written consent of an official representative of Barracuda Networks Inc. All specifications are subject to change without notice. Barracuda Networks Inc. assumes no responsibility for any inaccuracies in this document. Barracuda Networks Inc. reserves the right to change, modify, transfer, or otherwise revise this publication without notice.