



Microsoft 365
COMMUNITY CONFERENCE

Protection in Teams as Modern Threats Evolve

Luis Orozco Martinez
Yilin Yang

04/21/2026

© Copyright Microsoft Corporation. All rights reserved.





Luis Orozco Martinez
Group Engineering Manager
Microsoft Teams
[in](#) /luisom



Yilin Yang
Senior Product Manager
Microsoft Teams
[in](#) /yilinyang93



Microsoft 365
COMMUNITY CONFERENCE

See you tomorrow at

Teams Protection Meetup

 Wednesday, April 22 | 1:30 PM – 2:15 PM
 Room Caicos 1, Sapphire Falls

The evolving cyber threat landscape



Phishing and social engineering drive 28% breach initiations



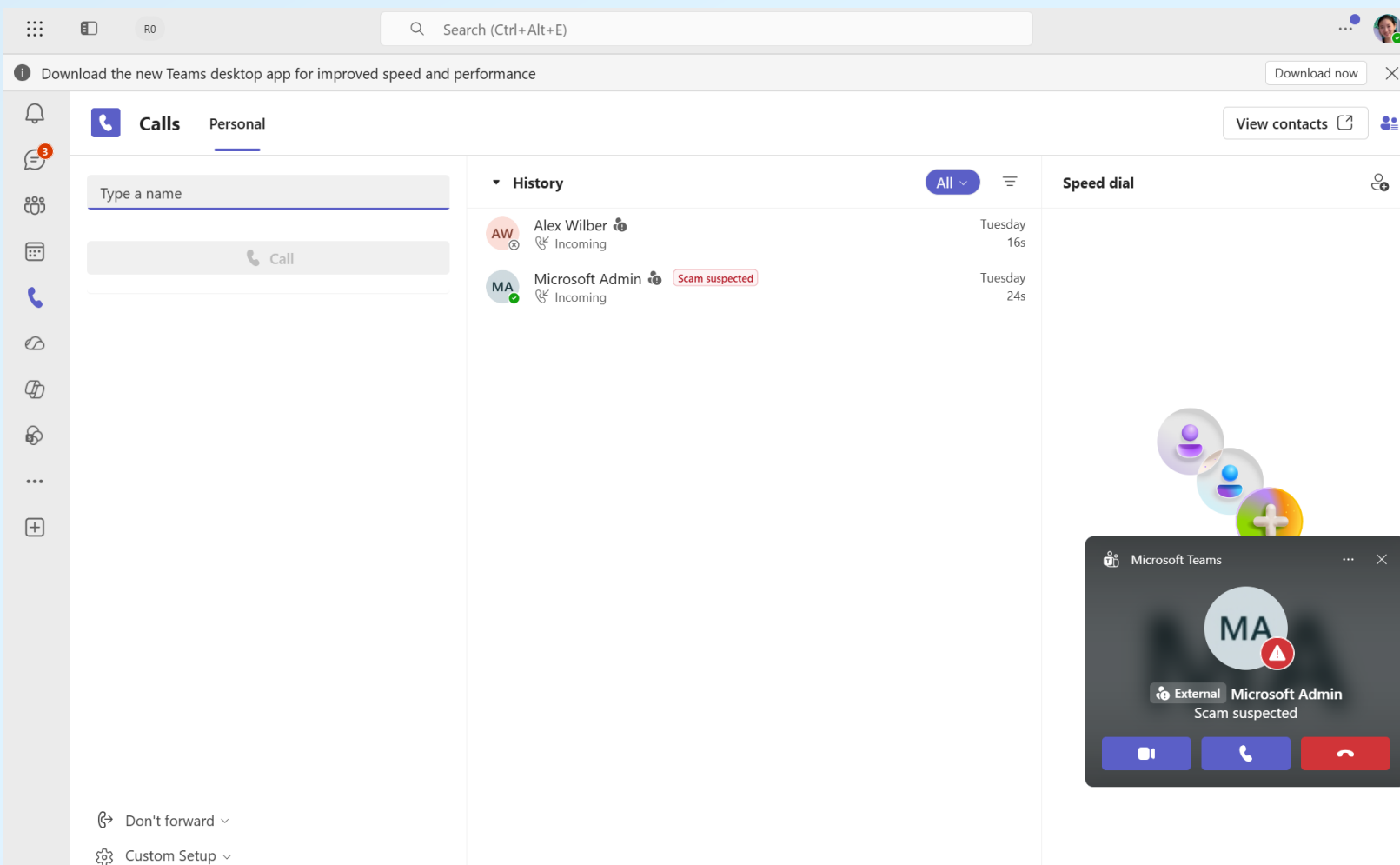
Emerging voice phishing calls & Teams-based impersonation



Attackers remain active for 58 days on average

Calling and Meeting Protection

Brand impersonation detection in calling



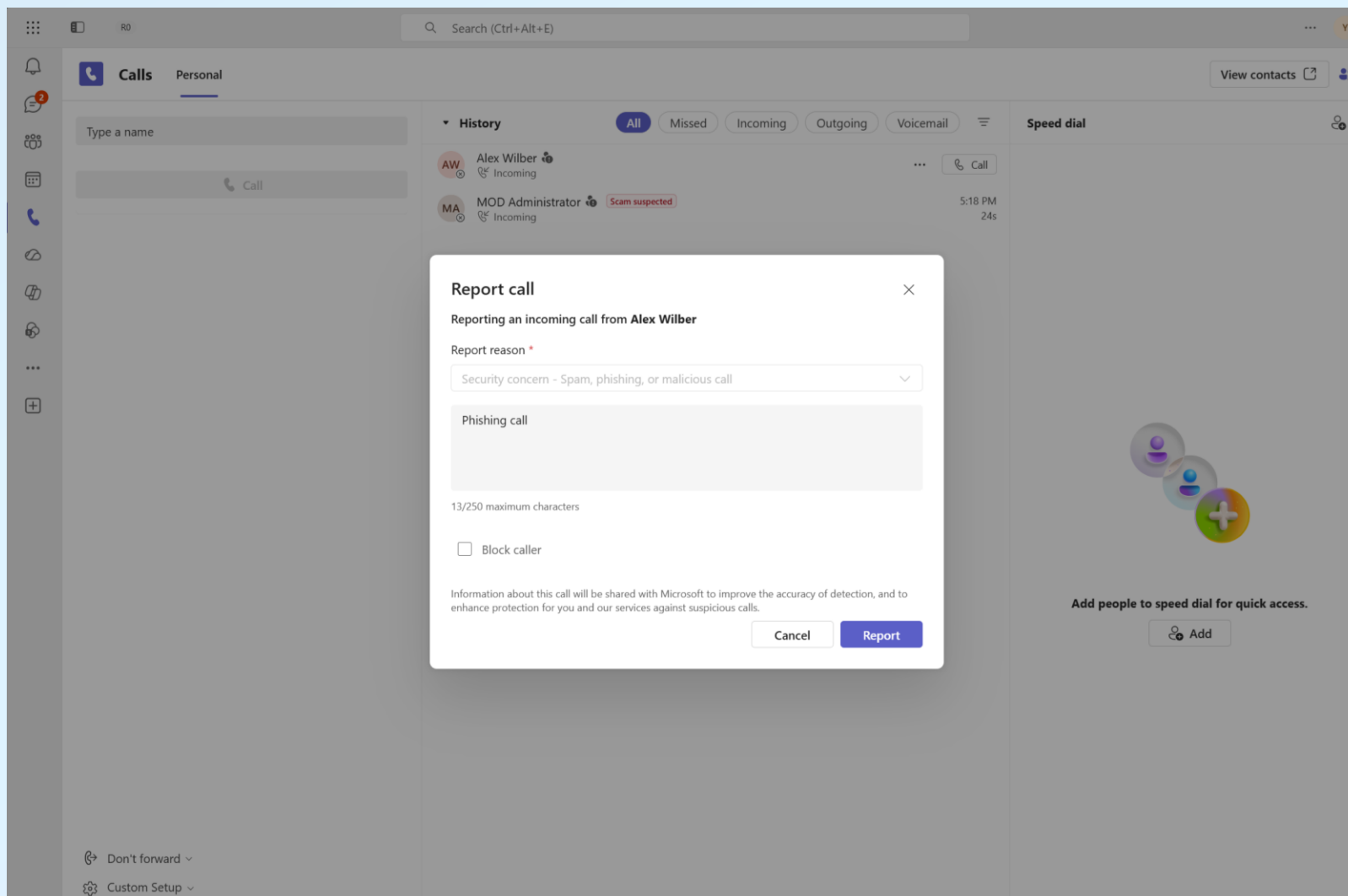
The screenshot displays the Microsoft Teams 'Calls' interface. The 'History' section shows two incoming calls:

Contact	Status	Time
Alex Wilber (AW)	Incoming	Tuesday 16s
Microsoft Admin (MA)	Incoming (Scam suspected)	Tuesday 24s

An inset window shows a call warning for 'Microsoft Admin' (MA) with a red warning icon and the text 'Scam suspected'. The interface also includes a search bar, a 'Download the new Teams desktop app' notification, and a 'View contacts' button.

- ▶ **Real-time scam detection:** Alerts users to suspected impersonation during VoIP calls by analyzing caller identity using brand impersonation algorithms—helping prevent fraudulent interactions before the call is answered
- ▶ **In-call warning:** If the user answers a flagged call, a message appears during the call indicating it may be a potential scam attempt

Report a call for security concern



- ▶ If end-users have found a call suspicious, they can **report a call** from the call history. This works for both VOIP and PSTN calls
- ▶ Users will have the ability to **pick a reason** for their reporting and add details as appropriate
- ▶ Users can also **block the caller** as part of the reporting flow to stop receiving any communication from that caller



Impersonation Detection in Calling

Protect meetings against external bots

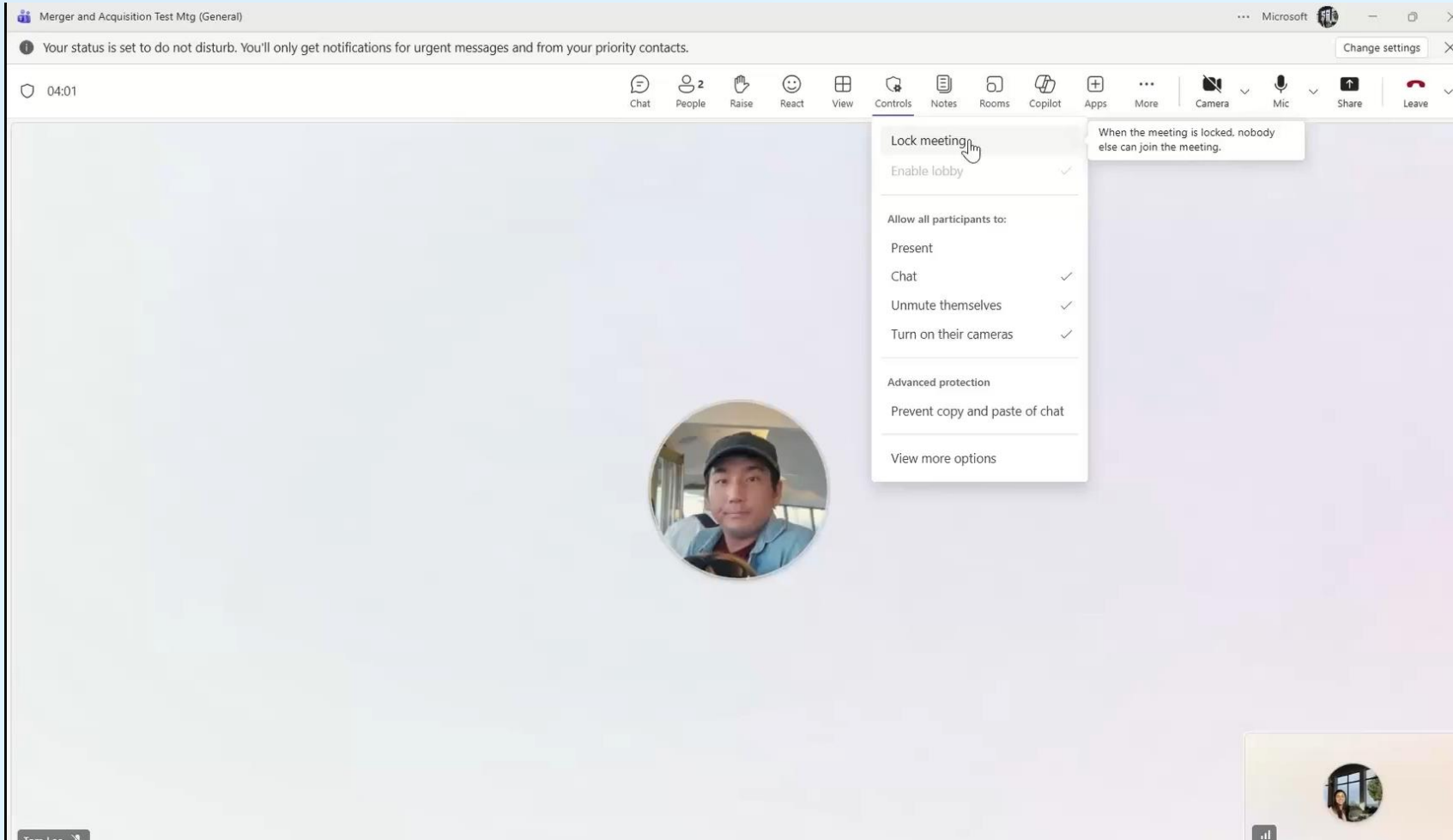
The screenshot shows a meeting lobby with a 'Participants' list on the right. The list is divided into sections: 'In the lobby (6)', 'Waiting (3)', and 'Suspected threats (3)'. The 'Suspected threats' section contains three items: 'Meeting Recording' (Unverified), 'AI Note Taker' (Unverified), and 'Microsoft Secur...' (Scam suspected). The 'In this meeting (5)' section contains one item: 'Daniela Mandera'. The interface includes a search bar, a 'Share invite' button, and buttons for 'Chat', 'Admit (3)', and 'Deny (3)'. A 'Mute all' button is also present for the meeting participants.

The dialog box is titled 'Admit this unverified bot?' and contains the following text: 'AI Note Taker Unverified', 'External bots might record or transcribe your meeting and lead to unauthorized access to sensitive information. Admit this bot only if you know and trust it.', and a checkbox labeled 'This isn't a bot'. There are 'Admit' and 'Deny' buttons at the bottom right.

- ▶ Bots are detected by the system
- ▶ Speedbumps and markers in the lobby help **organizers make an intentional decision to admit** them into meetings

The screenshot shows a meeting grid with nine participants. The participants are: Babak Shammis, Aadi Kapoor, Charlotte De Crum, Aaron Buxton, Daniela Mandera, Danielle Booker, Jessica Kline, Kai Larsson, and Allan Munger. The interface includes a top bar with various controls like 'Chat', 'People', 'Rate', 'React', 'View', 'Notes', 'Rooms', 'Copilot', 'Whiteboard', 'Apps', 'More', 'Camera', 'Mic', 'Share', and 'Leave'. The system tray at the bottom shows the time as 2:30 PM on 6/20/2024.

Meeting organizer controls



- ▶ Designed to empower organizers with enhanced security and management capabilities
- ▶ Access control and permissions
- ▶ Participant moderations
- ▶ Advanced protection capabilities with Teams Premium

Meeting label inheritance to artifacts (Premium)

The screenshot displays the Microsoft Teams interface during a meeting. On the left, a video player shows a recording of Yilin Yang. A red box highlights a 'Highly Confidential' label overlay on the video, which includes the text: 'Highly Confidential/Any User (No Protection)'. Below the video, the 'Speakers' section shows Yilin Yang's name. On the right, the 'Notes' pane is open, showing a 'Highly Confidential' label at the top. A red box highlights a tooltip that appears over the label, containing the text: 'Highly Confidential/Any User (No Protection) Access must be limited purely to business-required participants with no large or open distribution. Data is classified as Highly Confidential but is not protected. Where applicable abilities such as recording, preventing copy and paste or watermark features may be available with restrictions.' The notes pane also shows an 'Agenda' section with a bullet point for Yilin Yang and a 'Meeting' section with a list of updates.

- ▶ **Meeting recordings, transcripts and Loop notes** are now inheriting the **sensitivity label** of meeting
- ▶ Protect important artifacts for your sensitive meetings with **access control** and **copy/download restriction**
- ▶ **AI** respects sensitivity label of the meeting artifacts when accessing them and generating response

Messaging Protection and Admin Reporting

Recap: Security detections in messaging

Malicious URL detection

Bob Garcia 5/12, 9:15 AM


BG

 This message contains a link that might be harmful. [Learn about file and link protection](#)

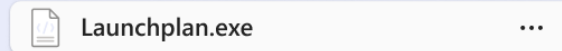
<https://www.figmaaaa.com/design/mfrB75tdUWC6VnxLRBRJpf/Dynamic-Delivery---Rough-explores?node-id=20-13696&t=q9MbV18L80LcQWtW-1>

Weaponizable file type detection

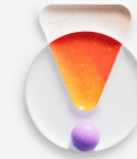
5/12, 9:15 AM

 This message was blocked because it contains a file type that's not permitted. [Learn about file and link safety](#)

So, here's what we need you to do next. Download the file attached and double click on it to install it to your computer.



Brand and domain impersonation detection



This looks like a spam or phishing attempt

Microsoft Security Team (aaronbuxton@microsoft.com) wants to chat with you.



Their name or email is suspicious



You've never communicated with them



They're outside your org

[Preview their messages safely](#)

[Learn more about spam or phishing detection](#)

Security detections report

Protection reports

Select a report to get insights and information about Teams security and compliance. These reports will help you better understand usage patterns and make better decisions to help protect your organization from unauthorized or risky activity. [Learn more about protection reports](#)

View reports Downloads

Report: Security detections Date range: Last 30 days **Run report**

Security detections
Mar 23, 2026 10:31:24 PM UTC | Date range: Feb 21, 2026 - Mar 23, 2026

Detection date	Sent from	Recipient	Recipient action	Detection type
Mar 10, 2026, 7:30 AM	John Doe <john.doe@contoso.com>	test1	-	Malicious URL
Mar 11, 2026, 2:15 AM	Jane Smith <jane.smith@fabrikam.com>	test1	Accepted (Mar 11, 2026, 2:30 AM)	Impersonation
Mar 11, 2026, 9:45 AM	Bob Johnson <bob.johnson@adventureworks>	Victor Cheng	-	Weaponizable file type
Mar 12, 2026, 4:20 AM	Alice Williams <alice.williams@tailspintoys.co>	Johnny Ahmad	Blocked (Mar 12, 2026, 4:25 AM)	Impersonation
Mar 12, 2026, 6:00 AM	Charlie Brown <charlie.brown@northwind.co>	Johnny Ahmad	-	Malicious URL

- Surfaces security detections that happened in your tenant
- Current detections in scope: impersonation, malicious URL and weaponizable file type
- Extended detection metadata available on export

External domains anomaly report

Microsoft Teams admin center

Search

Protection reports

Select a report to get insights and information about Teams security and compliance. These reports will help you better understand usage patterns and make better decisions to help protect your organization from unauthorized or risky activity. [Learn more about protection reports](#)

View reports Downloads

Report: Communication anomalies Date range: Last 10 days Type: External domains anomalies Run report

External domains anomalies Preview

Feb 18, 2026 10:13:17 PM UTC | Date range: Feb 07, 2026 - Feb 17, 2026

Domain	Total anomalies	1:1 threads	Group threads	Action
m365ds922372.onmicrosoft.com	4	16	11	Block domain
contosotacdemo1.onmicrosoft.com	2	100	73	Block domain
m365x92803932.onmicrosoft.com	1	1	0	Block domain
microsoft.com	1	0	2	Block domain

- ▶ Detects unusual & potentially risky interactions with external orgs
- ▶ Includes **sudden spikes** and **abnormal engagement activity** with external domains
- ▶ **Tailored** to your tenant
- ▶ Integrated with **notification and alerts** for configuration in Teams channel

Recap: Report a security concern in message

Report a security concern

Report message as security risk ✕

Examples of security risks include spam, phishing, and malicious content.

MOD Administrator
⚠ Security alert Microsoft Security 🔒 We've detected suspicious login attempts on your account from an unknown location. Your...

This message will be shared for review (the sender will not be notified). The review process is fully determined by your organization.

Cancel Report

Report an incorrect security detection

Report this message ✕

Sankargo
http://teamsspamfortesting.contoso.com/

Not a security concern - incorrectly identified as a concern ▾

Enter an explanation (optional)

0/250 maximum characters

This message will be shared for your IT admin to review. The review process is fully determined by your organization. Reporting doesn't notify the sender or remove the warning from the message.

Cancel Report

Sankargo 3/18 1:56 PM Edited

Report an external user for security concern

The screenshot shows a Microsoft Teams chat window. On the left is a navigation pane with icons for Activity, Chat, Teams, Calendar, Calls, OneDrive, and Apps. The main chat area shows a conversation with 'Microsof Security (aaronbuxton@microsoft.com)' marked as 'External'. A large orange speech bubble with a white exclamation mark is centered on the screen. Below it, the text reads: 'Microsof Security (aaronbuxton@microsoft.com) wants to chat with you'. A grey warning box contains the text: 'You haven't communicated with this person before. Messages from unknown or unexpected people could be spam or phishing attempts. Never share your account information or authorize sign-in requests over chat. Note: This person has multiple aliases in Teams. To be safe, preview their messages.' At the bottom of the warning box are two buttons: 'Block' and 'Accept'. Below the buttons, a small note states: 'By selecting Accept, you agree to receive future communications and share your status with Aaron Buxton (External). To limit communications, you can block them at any time. Learn more'.

- Users can now **report an external user** for security concern while blocking them
- Block and Report can be done either on **Accept/Block screen** or on external user's **profile card**
- Admin can review user's reports in Teams Admin Center > Analytics & reports > Protection reports

User reported security submission report

Microsoft Teams admin center

Search

Dashboard

Add-on Licenses

Settings & policies

Teams

Users

External collabora...

Teams devices

Teams apps

Meetings

Voice

Teams client health

Locations

Frontline

Policy packages

Planning

Analytics & reports

Silent Tests

Usage reports

Protection reports

Reporting labels

Protection reports

Select a report to get insights and information about Teams security and compliance. These reports will help you better understand usage patterns and make better decisions to help protect your organization from unauthorized or risky activity. [Learn more about protection reports](#)

View reports Downloads

Report: User reported security submissio... Date range: Last 30 days Report category: Chats and channels Run report

User reported security submissions

Mar 17, 2026 4:45:53 PM UTC | Date range: Feb 15, 2026 - Mar 17, 2026

Date and time	Reporter name	Report type	Sent from	Message sent date
Mar 16, 2026, 22:02:58 UTC	Wojciech Piotrowski	Security concern	Maria Almeida <maria.a...>	Mar 7, 2026, 00:26:05 U...
Mar 16, 2026, 21:47:01 UTC	Brian Hasala	Security concern	Wojciech Piotrowski <w...>	Mar 16, 2026, 18:56:07 ...
Mar 16, 2026, 19:01:46 UTC	Wojciech Piotrowski	Security concern	Wojciech Piotrowski <w...>	Mar 16, 2026, 18:56:08 ...
Mar 16, 2026, 19:01:35 UTC	Wojciech Piotrowski	Security concern	Wojciech Piotrowski <w...>	Mar 16, 2026, 18:56:08 ...
Mar 16, 2026, 19:00:32 UTC	Wojciech Piotrowski	Security concern	Maria Almeida <maria.a...>	Mar 9, 2026, 20:37:18 U...
Mar 16, 2026, 18:11:22 UTC	Brian Hasala	Security concern	Maria Almeida <maria.a...>	Mar 12, 2026, 17:37:51 ...
Mar 16, 2026, 17:44:30 UTC	Brian Hasala	Security concern	Maria Almeida <maria.a...>	Mar 12, 2026, 17:37:52 ...

- Surfaces **end user reports** of security concerns in **1:1 calls, messages and external users**
- More detailed metadata available on export
- Take remediation such as **Block user**, as needed

Browser tabs: (2) Chat | Alex Wilber, Johanna Lorenz | Usage reports - Microsoft Teams

Address bar: https://teams.cloud.microsoft

Search: Search (Ctrl+Alt+E)

Notifications: Stay in the know. Turn on desktop notifications. [Turn on]

Chat sidebar:

- Unread
- Copilot
- Quick views
- Drafts **New**
- Favorites
- Chats
 - AV Adele Vance 3:22 PM
 - A J Alex Wilber, +2** 3:09 PM
Alex Wilber: alexw@M365x04774882....
 - MA Microsoft Admin 2:38 PM
New message
 - A M Adele Vance, +3** 4/16
New message
 - AW Alex Wilber 4/14
- Muted

Chat header: Alex Wilber, Johanna Lorenz External

Chat actions: Meet now, 3 participants, Copy, Search, Share

Warning: Some people in this chat are outside your org. It's possible they have message-related policies that will apply to the chat. [Learn more](#)

Message history:

- Alex Wilber added Yilin Yang and Johanna Lorenz to the chat.
- Alex Wilber 3:07 PM
- AW** Hi team, I prepared a demo for the customer presentation, please review
- Looks like I can't send the file in the chat
- Can you all log into the OneDrive for this account and open the demo?
- alexw@M365x04774882.onmicrosoft.com
c+nX58S7;MttH1+#
I disabled MFA already

Replying to external participants.

Type a message [emojis]



End-to-end Protection across Microsoft Teams

Evolving collaboration landscape



Teams is increasingly used for messaging, calling and meetings, expanding the attack surface

Evolving threat tactics



Phishing, impersonation and AI-powered social engineering now span across modalities and blend into normal communication

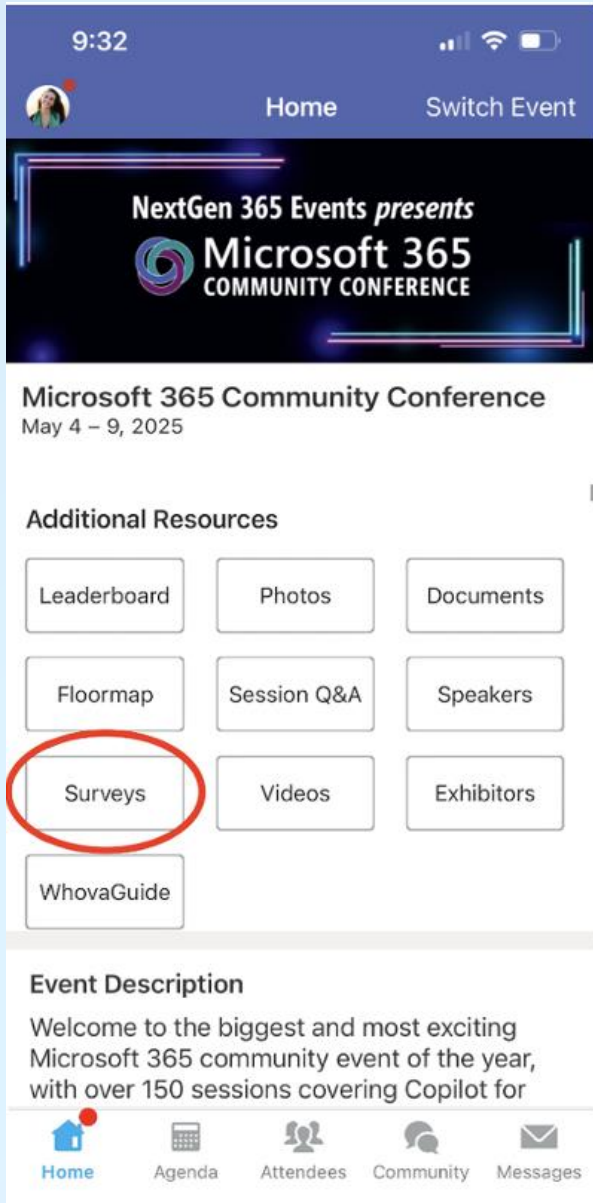
End-to-end protection and visibility



Built-in detections, user reporting and admin insights enable faster investigation and response

**We have an
exciting future ahead.**





Session feedback surveys

We want to hear from YOU!

Share your feedback to make next years conference even better!

Here's how –

- Simply go to the Whova App on your smartphone.
- Scroll down on the M365 Community Conference Homepage to 'Additional Resources' to click "Surveys".
- Click Session Feedback.
- Scroll down to find this session title.
- Complete the session feedback survey.
- Finally, click 'Submit'.

It's just that easy!



Microsoft 365
COMMUNITY CONFERENCE

See you tomorrow at

Teams Protection Meetup

 Wednesday, April 22 | 1:30 PM – 2:15 PM
 Room Caicos 1, Sapphire Falls

Uhova

The official event app for the
Microsoft 365 Community Conference

Event invitation code: Orlando2026



Join the event app to access:

- ➔ Event announcements
- ➔ Personalized agenda, session details
- ➔ Speaker & attendee profiles
- ➔ Networking, meet-ups, messages
- ➔ Event documents

Expertise and tools for your journey



Technical expertise via
our FastTrack partners

aka.ms/Microsoft/FastTrack



Tools, resources & training
on our Adoption Hub

adoption.microsoft.com



Events and real-world
knowledge in our
community

aka.ms/TechCommunity

News & community content



Microsoft Community Learning
aka.ms/Community/LearningChannel

Community led expert content on all your favorite Microsoft services.



Start your week with live news and event updates aka.ms/MondaysatMicrosoft
Watch live or on-demand & share our blog.

Home / Microsoft 365 Copilot

Microsoft 365 Copilot

Deliver value and employee satisfaction with our tools for Microsoft 365 Copilot deployment and adoption. This powerful technology combines the power of large language models (LLMs) with your organization's data – all in the flow of work – to turn your words into one of the most powerful productivity tools on the planet.

Microsoft 365 Copilot Chat and in-app experiences provide real-time intelligent assistance, enabling users to enhance their creativity, productivity, and skills.

[Looking for Copilot resources for Small and Medium Businesses? >](#)

Copilot Success Kit

Our Success Kit empowers you to achieve rapid value with Copilot while enabling your progressive skilling journey with AI tools.

[Download here >](#)

Copilot Chat and agent starter kit

This new kit includes guidance on IT controls, setup, and resources to help prepare your tenant and enable your users to create and use agents.

[Explore the kit >](#)

Join the Copilot community

The Microsoft 365 Copilot community is your hub for the official blog, latest news, and discussions.

[Join now >](#)

Microsoft 365 Copilot

Welcome to the Microsoft 365 Copilot community. Your hub for the latest news, live events, and discussions on Microsoft 365 Copilot. For help & learning (how-to articles and training resources), please visit [Microsoft 365 Copilot Adoption hub](#).

Search this community

[Unfollow](#)

#M365Con

Microsoft 365 COMMUNITY CONFERENCE

May 6-8 Las Vegas

Your front-row seat to the future of work

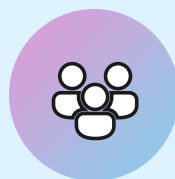
The ultimate Microsoft 365 community event

Learn directly from the experts and redefine what's possible at work—join us at the Microsoft 365 Community Conference.

[Learn more!](#)

Stay Connected!

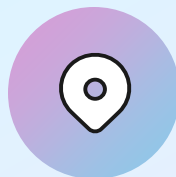
Engage with the best community in tech... There's something for everyone!



Microsoft Tech Community

The community platform for Microsoft 365 – forums, blogs, and events

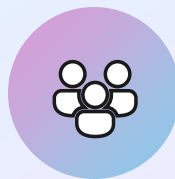
<https://aka.ms/joinMTC>



CommunityDays.org

Find or host a local event in your area or to match your interests

www.communitydays.org



Microsoft Community on LinkedIn

News, announcements and training delivered to your news feed

<https://aka.ms/microsoftcommunitylinkedin>



The one stop shop for Microsoft ecosystem community events

The screenshot displays the Microsoft Community Days website interface. At the top left is the logo "Community Days Supporting the Microsoft Community". The main heading reads "Discover Community Events happening across the world." Below this is a search bar and filter options. The "WHERE" filter is set to "Global". Under "FILTERS", "Registration Open" and "Hide Others" are checked. The main content area features a grid of event cards, each with a unique background image and event details.

Event Name	When	Where	Format	Cost
FABRIC DATA DAYS	Nov 4 - Dec 11, 2025	Your city, Your country United States	Hybrid	Free
SMARTCLOUD 365 - 2025	November 25, 2025	Germany	Virtual	Free
DYNUG AUTUMN CONFERENCE 2025	November 25 - 26, 2025	Oslo, Gardarmoen Norway	Paid	
SHIFT ENTER SUMMIT 2025	November 26, 2025	Budapest Hungary	Paid	
AI COMMUNITY CONFERENCE - TORONTO 2025	November 28, 2025	Toronto, Ontario Canada	Free	
SEASON OF AI - MCP	November 28, 2025	Gurgaon, Haryana India	Hybrid	Free
ESPC25	December 1 - 4, 2025	Dublin, Dublin 1 Ireland	Paid	
MSREBUILD 2025	December 2, 2025	Nantes, Pays de la Loire France	Free	
TECHBAYANIHAN 2025	December 3 - 4, 2025	Manila City, National Capital Region Philippines		

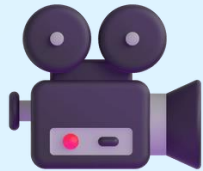
www.communitydays.org



SharePoint at 25 short film: *More than Code*

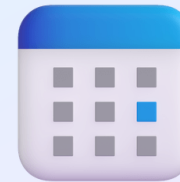
In honor of SharePoint's 25th birthday, *More Than Code* is a short film that explores the people, passion, and innovation behind one of the most transformative platforms in modern work. This film captures the stories of builders, leaders, and community champions who helped shape SharePoint into the knowledge backbone for collaboration, Copilot, and the next generation of agents.

SharePoint is more than code—it's 25 years of connection, innovation and impact.



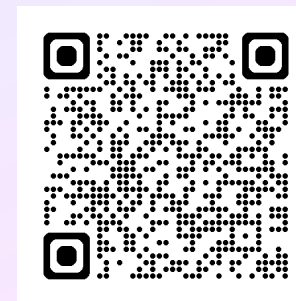
Watch the digital premiere

Stream the documentary online globally in late April and celebrate SharePoint's 25-year journey from anywhere.



Watch the SharePoint at 25 digital event

Prepare for the film with a special digital event featuring insights, stories, and what's next for SharePoint in the era of AI.



Join MGCI – Learn, Share, Grow.

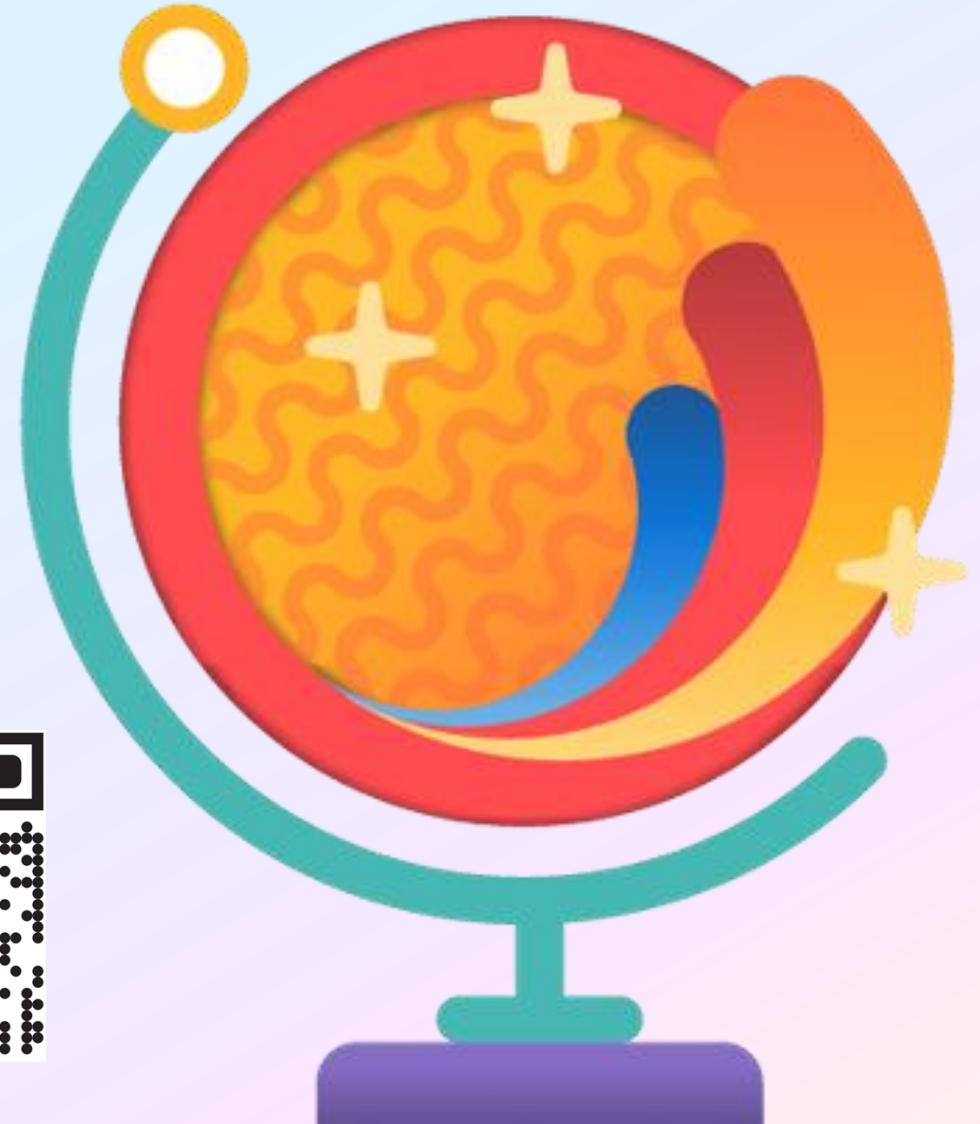
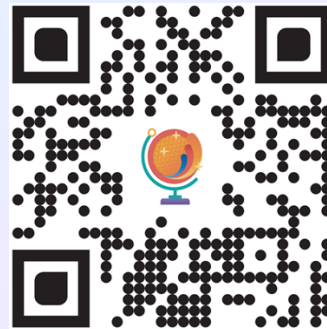
The Microsoft Global Community Initiative (MGCI) - Empowering global Microsoft communities with the tools, training, and resources to create impactful events and amplify diverse voices.

Learn, Share, Grow.

Event producers unite!

Join MGCI today!

<https://aka.ms/MGCI>



Thank you to our
Microsoft
Most Valuable
Professionals (MVP)
and Regional Directors!

