Risk Based Multi-factor Authentication

Overview

Multi-factor authentication (MFA) is a security method that ensures that only you can log into your account. It does this by requiring at least 2 methods of authentication – your password and another piece of information (Microsoft Authenticator App, Text message code or a phone call). You will have probably come across MFA already if you use mobile banking or some social media platforms.

When will I get an MFA challenge?

Multi-factor authentication (MFA) works with Single Sign-On (SSO) to reduce the amount of MFA challenges and sign-ins a user will receive.

You will be challenged on each new session login that requires a new authentication token.

Example:

A user is logged into Outlook in internet browser. They can open Surrey Learn in a new tab or window.

If a new In-Private internet browser is opened or the above session is ended with a logout / sign-out they will be required to login again and will receive an MFA challenge.

Why am I getting additional challenges?

Risk based MFA

We have introduced new factors on when a user will be given an MFA challenge.

Multi-factor authentication can now be triggered based on your overall risk score; this risk score is calculated based on several risk detections broken into two groups: User risk and Sign-in risk detailed below.

These risks are calculated using Microsoft's threat intelligence sources.

User Risk

A user risk is the probability that identity or account is compromised.

Risk detection	Description
Leaked credentials	This risk detection type indicates that the user's valid credentials have been leaked. When cybercriminals compromise valid passwords of legitimate users, they often share those credentials. This sharing is typically done by posting

Risk detection	Description
	publicly on the dark web, paste sites, or by trading and selling the credentials on the black market. When the Microsoft leaked credentials service acquires user credentials from the dark web, paste sites, or other sources, they are checked against Azure AD users' current valid credentials to find valid matches.
Azure AD threat intelligence	This risk detection type indicates user activity that is unusual for the given user or is consistent with known attack patterns based on Microsoft's internal and external threat intelligence sources.

Sign-in Risk

A sign-in risk represents the probability that a given authentication request isn't authorised by the identity owner.

Risk detection	Detection type	Description
Anonymous IP address	Real-time	This risk detection type indicates sign-ins from an anonymous IP address (for example, Tor browser or anonymous VPN). These IP addresses are typically used by actors who want to hide their login telemetry (IP address, location, device, etc.) for potentially malicious intent.
Atypical travel	Offline	This risk detection type identifies two sign-ins originating from geographically distant locations, where at least one of the locations may also be atypical for the user, given past behaviour. Among several other factors, this machine learning algorithm considers the time between the two sign-ins and the time it would have taken for the user to travel from the first location to the second, indicating that a different user is using the same credentials. The algorithm ignores obvious "false positives" contributing to the impossible travel conditions, such as VPNs and locations regularly used by other users in the organization. The system has an initial learning period of the earliest of 14 days or 10 logins, during which it learns a new user's sign-in behaviour.
Malware linked IP address	Offline	This risk detection type indicates sign-ins from IP addresses infected with malware that is known to actively communicate with a bot server. This detection is determined by correlating IP addresses of the user's device against IP addresses that were in contact with a bot server while the bot server was active.
Unfamiliar sign-in properties	Real-time	This risk detection type considers past sign-in history (IP, Latitude / Longitude and ASN) to look for anomalous sign-ins. The system stores information about previous locations used by a user and considers

Risk detection	Detection type	Description
		these "familiar" locations. The risk detection is triggered when the sign-in occurs from a location that's not already in the list of familiar locations. Newly created users will be in "learning mode" for a period in which unfamiliar sign-in properties risk detections will be turned off while our algorithms learn the user's behaviour. The learning mode duration is dynamic and depends on how much time it takes the algorithm to gather enough information about the user's sign-in patterns. The minimum duration is five days. A user can go back into learning mode after a long period of inactivity. The system also ignores sign-ins from familiar devices, and locations that are geographically close to a familiar location. We also run this detection for basic authentication (or legacy protocols). Because these protocols do not have modern properties such as client ID, there is limited telemetry to reduce false positives. We recommend our customers to move to modern authentication.
Admin confirmed user compromised	Offline	This detection indicates an admin has selected 'Confirm user compromised' in the Risky user's UI or using riskyUsers API. To see which admin has confirmed this user compromised, check the user's risk history (via UI or API).
Malicious IP address	Offline	This detection indicates sign-in from a malicious IP address. An IP address is considered malicious based on high failure rates because of invalid credentials received from the IP address or other IP reputation sources.
Suspicious inbox manipulation rules	Offline	This detection is discovered by Microsoft Cloud App Security (MCAS). This detection profiles your environment and triggers alerts when suspicious rules that delete or move messages or folders are set on a user's inbox. This may indicate that the user's account is compromised, that messages are being intentionally hidden, and that the mailbox is being used to distribute spam or malware in your organization.
Impossible travel	Offline	This detection is discovered by Microsoft Cloud App Security (MCAS). This detection identifies two user activities (is a single or multiple sessions) originating from geographically distant locations within a time period shorter than the time it would have taken the user to travel from the first location to the second, indicating that a different user is using the same credentials.

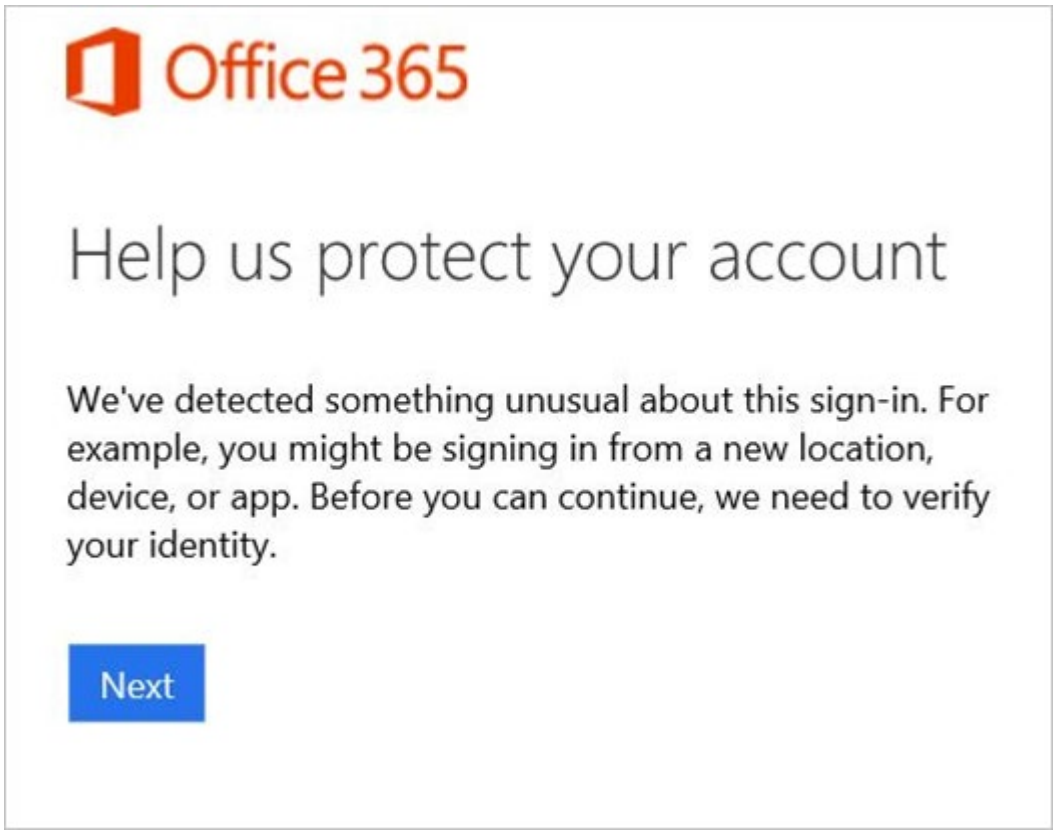
What does this mean for me?

We have activated two policies that allow auto remediation of user and sign-in risk.

If your sign-ins are flagged with medium or high risk, you will be required to pass an MFA challenge.

Risky sign-in remediation

1. The user is informed that something unusual was detected about their sign-in, such as signing in from a new location, device, or app.



2. The user is required to prove their identity by completing Microsoft MFA with one of their previously registered methods.

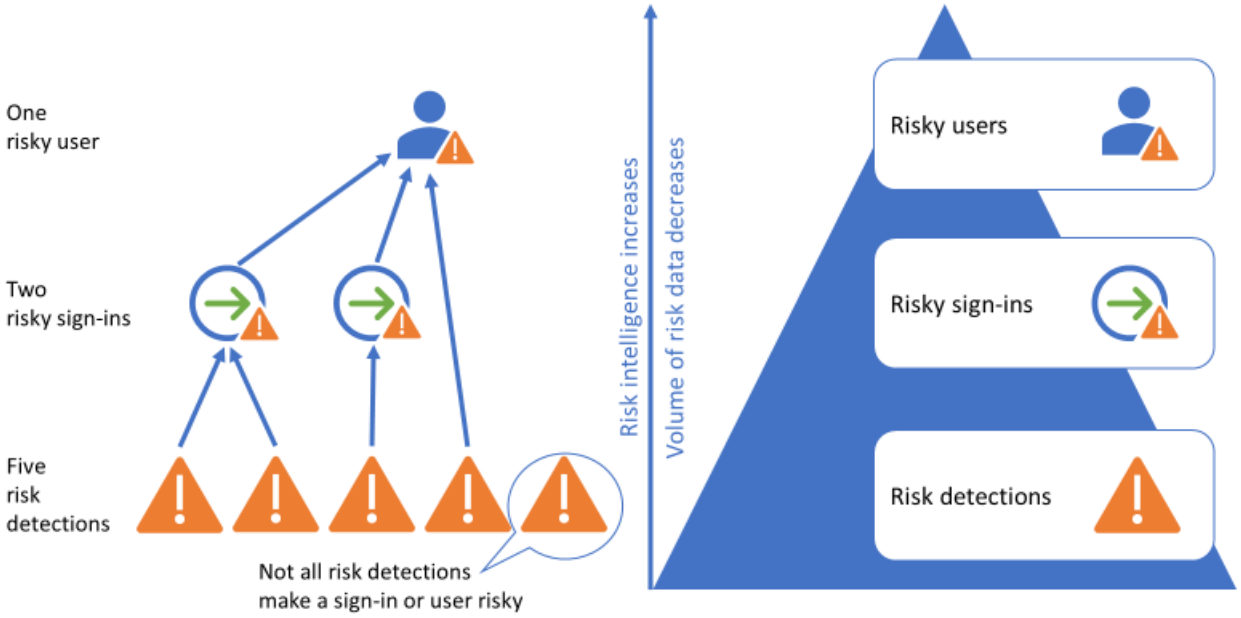
If your identity is flagged with a high user risk, you will be required to reset your password via the self-service portal.

Risky user self-remediation

1. The user is informed that their account security is at risk because of suspicious activity or leaked credentials.

2. The user is required to prove their identity by completing Microsoft MFA with one of their previously registered methods.
3. Finally, the user is forced to change their password using self-service password reset since someone else may have had access to their account.

Please note that risk detections associated with sign-ins can aggregate and raise your user risk level.


One
risky user
Two
risky sign-ins
Five
risk
detections
Not all risk detections
make a sign-in or user risky
Risk intelligence increases
Volume of risk data decreases
Risky users
Risky sign-ins
Risk detections