Microsoft Teams

Cyber Risks & Best Practices

Microsoft Teams, a collaboration platform used for video meetings, interoffice messaging, and file storage, is being increasingly used by organizations who have transitioned to a remote environment due to COVID-19. Cyber actors are quick to capitalize on tumultuous situations, which includes taking advantage of users unfamiliar with Microsoft Teams. Below are the associated risks and threats, protection recommendations, and how to secure video conferences.

Cyber Threats & Risks

- **Credential Stuffing:** cyber actors conduct credential stuffing and brute-force attacks, which consist of an automated process using stolen login credentials to gain access to accounts that do not have multi-factor authentication enabled
- **Fake Microsoft Teams Installer:** malicious files are designed to look like legitimate Microsoft Teams applications and instead install malware on the user's machine
- **Malicious Links and Phishing Attacks:** using the messaging function within Microsoft Teams, cyber actors leverage compromised accounts to send malware and phishing links or attachments that appear as originating from a "trusted" source
- **Nefarious Add-ins:** Microsoft Teams offers downloadable features for user customization, but cyber actors can create fake add-ins capable of reading and collecting data

Steps to Mitigate Cyber Risk

- Keep meeting links private – do not share these links on public forums or on social media, as unauthorized actors will have an easier time gaining access to the meeting
- Change passwords frequently and follow best practice to ensure strong passwords – this will combat the increase in phishing emails aimed at stealing credentials
- Be wary of emails and files received from unknown senders – think before you click, especially if special deals or discounts are offered
- Install the latest version of Microsoft Teams – failing to update may leave exposures to known vulnerabilities
- Identify lookalike domain names – these attempt to impersonate legitimate ones, so look for spelling errors and be cautious of unfamiliar email senders
- Learn the platform – get familiar with the features and settings so that anything unusual becomes obvious, and that the proper security settings are implemented

To learn more about Microsoft Teams, review their Privacy and Security Controls for video conferences.

ANTHONY J. FERRANTE
Global Head of Cybersecurity
Senior Managing Director
+1 202 312 9165
ajf@fticonsulting.com

JORDAN RAE KELLY
Head of Cybersecurity, Americas
Senior Managing Director
+1 202 312 9140
jordan.kelly@fticonsulting.com

KYUNG KIM
Head of Cybersecurity, APAC
Senior Managing Director
+82 2 2190 3727
kyung.kim@fticonsulting.com

JOSHUA BURCH
Head of Cybersecurity, EMEA
Senior Managing Director
+44 20 3727 1854
joshua.burch@fticonsulting.com

FTI CONSULTING | CYBERSECURITY