Headline computer solutions

PREVENT PHISHING WITHIN MICROSOFT TEAMS:

5 CHANGES TO MAKE TODAY

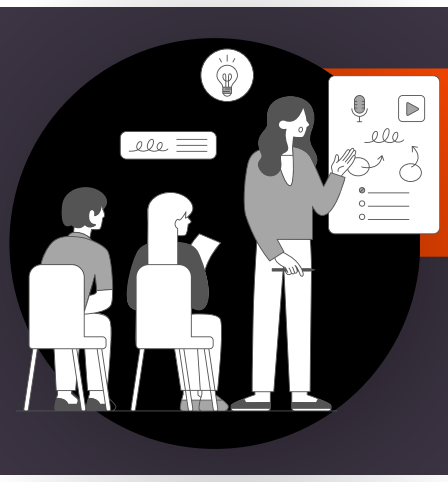
Microsoft has detailed a new phishing campaign in which corporate employees are targeted via **Microsoft Teams.** Below are 5 ways that you can instantly make your communication **more secure.**

LImit External Communication on Microsoft Teams

This entails designating **trusted Microsoft 365 organizations** to identify permitted external domains for chat and choosing optimal access configurations specific to your organization.

Limit Device Types That Can Connect In Organization

Only permit **recognized devices** that comply with Microsoft's suggested security guidelines. For users accessing from unmanaged devices, make sure to apply **conditional access** within Microsoft Defender.

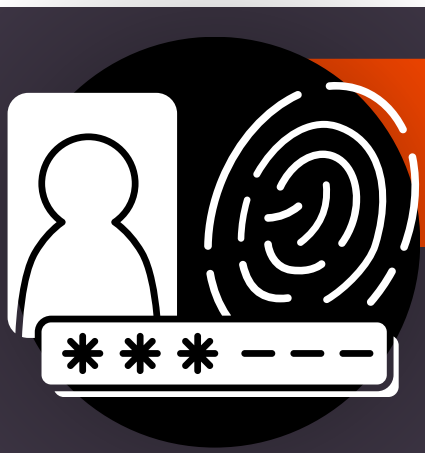


Building Awareness Among Current Users

Provide employees with **up-to-date training** on social engineering and credential phishing techniques through Teams. Teach users to check for **"External"** tags in messages.

Secure Link Scanning to Minimize Vulnerability

Set up Microsoft Defender for Office 365 to **verify links on click.** This measure complements the standard anti-spam and malware safeguards present for **incoming messages.**



Acess Management for Users Within Your Organization

Practice the principle of **least privilege**, and avoid the use of **domain-wide, administrator-level service accounts.** Start deploying phishing-resistant **authentication** for users.

NEED HELP IMPLEMENTING? **REACH OUT TODAY!**

(210) 533 - 2600 info@headlinepc.com headlinepc.com