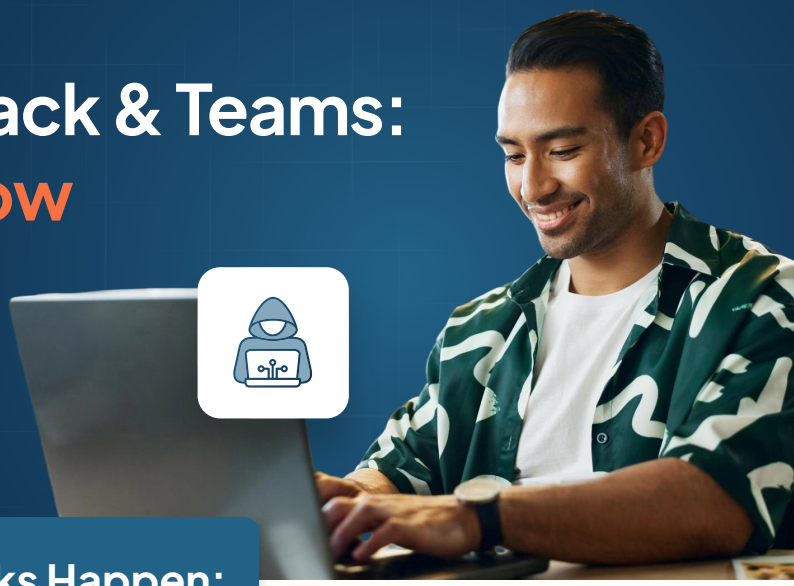
Getting Phished on Slack & Teams: What You Need to Know

Collaboration tools like Slack and Microsoft Teams make work easier, but they also make a tempting target for attackers. When messages come from supposed colleagues, employees often let their guard down, making scams easier to pull off than traditional email phishing.



How Attacks Happen:

Compromised Accounts

Hackers may hijack a colleague's account and use it to share malicious links or files. Since the messages appear to come from someone you already trust, they can blend in with normal work conversations and catch you off guard.

Tip: *Treat unexpected messages with caution, even from known colleagues.*

Fake Accounts

Attackers may create accounts pretending to be coworkers or executives. They can send fake meeting invites, urgent requests, or links to "important" documents. Even well-trained employees can be fooled if the fake account is convincing.

Tip: *Always verify requests for money, credentials, or urgent actions.*

Malicious Links and Files

Links or files shared in chat can install malware or steal login credentials. Hackers rely on the casual, fast-paced nature of chat; people are more likely to click without thinking. Even seemingly harmless files can be dangerous.

Tip: *Watch for spelling differences in usernames or email addresses tied to accounts, and think twice before clicking or opening attachments.*

Reporting Suspicious Activity

Reporting suspicious messages helps stop attacks and protect your team. The faster a malicious account is flagged, the less damage it can do.

Tip: *Report and block any suspicious users immediately.*