SECURITY INSIGHTS:

Microsoft Teams Is the New Phishing Playground

Genady Vishnevetsky, Chief Info Security Officer, Stewart Title Guaranty Company

Have you ever received a message in Microsoft Teams from someone you didn't recognize? Most of us have. But here's what's changing: a new Teams feature now lets anyone send you a direct message—even people outside your organization.

Attackers are already exploiting this.

Microsoft Teams recently introduced a "Chat with Anyone" feature that allows external users to send direct messages to any email address, even if the recipient doesn't have a Teams account. While convenient for collaboration, it opens a door that hackers are walking right through.

Here's how the attack works. First, an attacker sends a Teams message posing as IT support. The next day, they follow up with a Teams call—creating urgency and building trust. During the call, they convince the victim to open **Quick Assist**, a legitimate remote support tool built into Windows. To do this, they send a link that requires the victim to enter their Microsoft credentials. Once logged in, the attacker takes control of the computer and installs malware that steals passwords, browsing history, and other sensitive information.

What makes this attack particularly dangerous is the use of legitimate tools. Quick Assist isn't malware—it's a Microsoft application designed to help IT professionals assist users remotely. But in the wrong hands, it becomes a weapon. Since the victim willingly grants access, security software doesn't flag it as suspicious.

This attack also bypasses traditional email security. Most phishing defenses focus on email, but Teams messages often get less scrutiny. We trust messages in our corporate tools more than emails from strangers.

The timing matters too. Microsoft plans a full global rollout of this feature by **January 2026**. Expect these attacks to increase as more organizations enable external messaging without realizing the risk.

SO HOW DO YOU PROTECT YOURSELF?

- **Verify before you trust.** If someone claiming to be IT support contacts you through Teams, especially from outside your organization, don't engage. Call your IT helpdesk using a known number to confirm the request is legitimate.
- **Never share credentials through links.** Your IT department will never ask you to log in through a link sent via chat to download remote support tools. If they need remote access, they'll use established, verified procedures.
- **Be skeptical of urgency.** Attackers put pressure on you to act without thinking. "I need to fix this right now" is a red flag, not a reason to bypass your instincts.
- **Know what Quick Assist is.** If someone asks you to open Quick Assist or any remote access tool, stop. Legitimate IT support doesn't cold-call employees and request remote access the same day.
- **Report suspicious messages.** If you receive unexpected Teams messages from external contacts claiming to be IT support, report them immediately. Your security team needs to be aware of these attempts.

Contact your IT or Managed Services provider and discuss whether you want to keep this "new feature" enabled. Microsoft is known for enabling features it believes its customers want, even though most clients don't.