



## MICROSOFT TEAMS SCAM SAFETY

# STOP BEFORE YOU RESPOND



A little caution today  
can prevent a big  
problem tomorrow.

Attackers are using external Teams chats and calls to impersonate IT, steal information, and gain access to your computer or account.

### 6 WARNING SIGNS



#### 1 UNEXPECTED IT CONTACT

Someone contacts you about a technical problem you did not report.



#### 2 EXTERNAL SENDER

Teams identifies the person as outside your organization or asks you to accept a new conversation.



#### 3 PRESSURE OR URGENCY

You are told you must act immediately to prevent an account or computer problem.



#### 4 REMOTE ACCESS REQUESTS

Asked to approve Request Control in Teams or open Quick Assist.



#### 5 PASSWORDS OR VERIFICATION CODES

Legitimate IT support will NEVER ask for your password or multifactor authentication (MFA) code.



#### 6 UNEXPECTED LINKS OR FILES

You are asked to visit a website, download software, or open a file as part of the support request.

### 5 QUICK STEPS – WHAT TO DO



#### 1 STOP

Don't respond or follow instructions right away.



#### 2 VERIFY

Check if the sender is external. Verify the request through a separate, trusted method (such as calling your IT provider).



#### 3 DON'T CLICK

Don't click links, open attachments, or visit websites.



#### 4 DON'T APPROVE

Don't approve remote access requests or install software.



#### 5 REPORT

Report suspicious messages to your IT provider right away.

### NEED HELP?



#### Not sure if a Teams message is legitimate?

Stop before responding. PCC clients can contact us and we will help verify whether the request is real.

#### PROFESSIONAL COMPUTER CONCEPTS

☎ 415-897-0078

✉ [support@calpcc.com](mailto:support@calpcc.com)

💻 [Open the PCC Client Portal](#)



SCAN TO OPEN  
CLIENT PORTAL



### IF YOU ALREADY RESPONDED

#### Contact your IT provider immediately if you:

- Allowed someone to remotely access your computer
- Entered your Microsoft 365 password
- Shared a verification or MFA code
- Opened a file or installed software
- Clicked a suspicious link



The sooner we know,  
the sooner we can help  
keep your data and  
accounts secure.



**STAY SAFE. STAY SMART.**  
When in doubt, reach out. We're here to help.



Learn more about cybersecurity and best practices at  
[www.calpcc.com/learning-center](http://www.calpcc.com/learning-center)