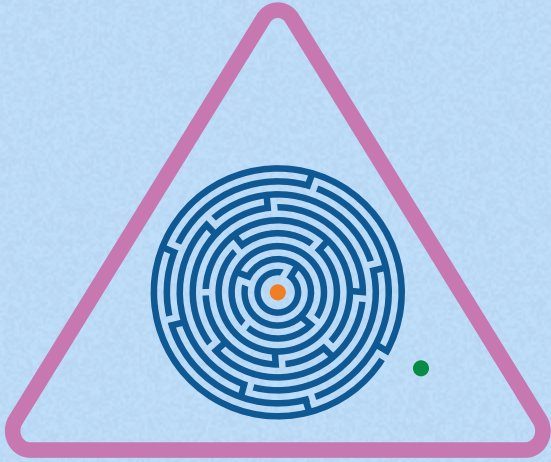


# 5 TRAPS Employees Keep Falling Into

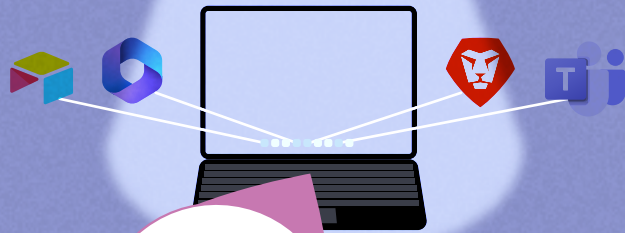


## 1 Believing believable phishing campaigns

Fake authentication pages tricked 10,000 people into sharing their user credentials.

Username  
Password  
Sign in

## 2 Connecting Shadow IT to SaaS platforms



Threat actors target Shadow IT as a side door into your enterprise SaaS apps.

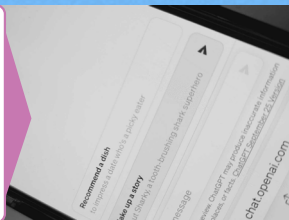
## 3 Using weak passwords that generative AI can guess



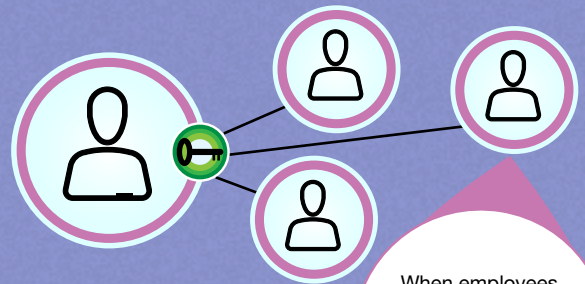
Hackers have turned to AI for password guessing. And the CAPTCHA designed to stop unauthorized logins? AI can crack that too.

## 4 Sharing sensitive data with generative AI

A ChatGPT bug exposed chat titles that users thought were private, potentially exposing confidential data.



## 5 Overpermissioning end-users



When employees grant high-level access to end-users, they create more attractive targets for hackers.