

The logo for Ticket Trick is centered on a dark grey background. The word "TICKET" is in a bold, pink, sans-serif font. The word "TRICK" is in a bold, grey, sans-serif font. Above the "T" in "TRICK" are two small circles, one teal and one orange. The entire logo is set against a background of dark grey, with blue and white geometric shapes framing it.

TICKET **TRICK**

주제 선정 이유

- 기술적 지식이 하나도 필요하지 않은 공격 기법
- 발견자가 돈 많이 벌었길래 부러워서...

주제

- 기업의 고객센터 기능을 이용한 인트라넷 침투 공격

구성원 인식

- 같은 단체에 소속된 사람을 웹상에서 인증하는 방법?

구성원 인식



asecg님, 인증메일 발송 후 해당 메일을 읽어 인증하기를 클릭해 주세요

@snu.ac.kr

인증 메일 발송

구성원 인식

- 해당 단체 사람들만 가질 수 있는 메일 주소로 인증키를 보낸다
- Nice Solution!

회사용 커뮤니케이션 채널



slack

yammer


The Enterprise Social Network

@workplace

by facebook



회사용 커뮤니케이션 채널

slack

ProductPricingSupport

⌵ Your workspaces

Sign in to COMPANY_NAME

company_name.slack.com

Enter your email address and password.

Sign in

☒ Remember me

[Forgot password?](#)

If you have an @company_name.com email address, you can [create an account](#).

고객센터

- 많은 회사들이 고객센터용 메일 계정을 사용한다.
- support@<company>.com

고객센터

- 달랑 메일만 보내라고 하기보단
- 고객센터용 어플리케이션을 운영

Contact us

What can we help you with?

-

Subject *

Description *

My tickets

Status:

Any

Subject

Id

Created

Last activity ▼

Status

.

#3422043

8 minutes ago

8 minutes ago

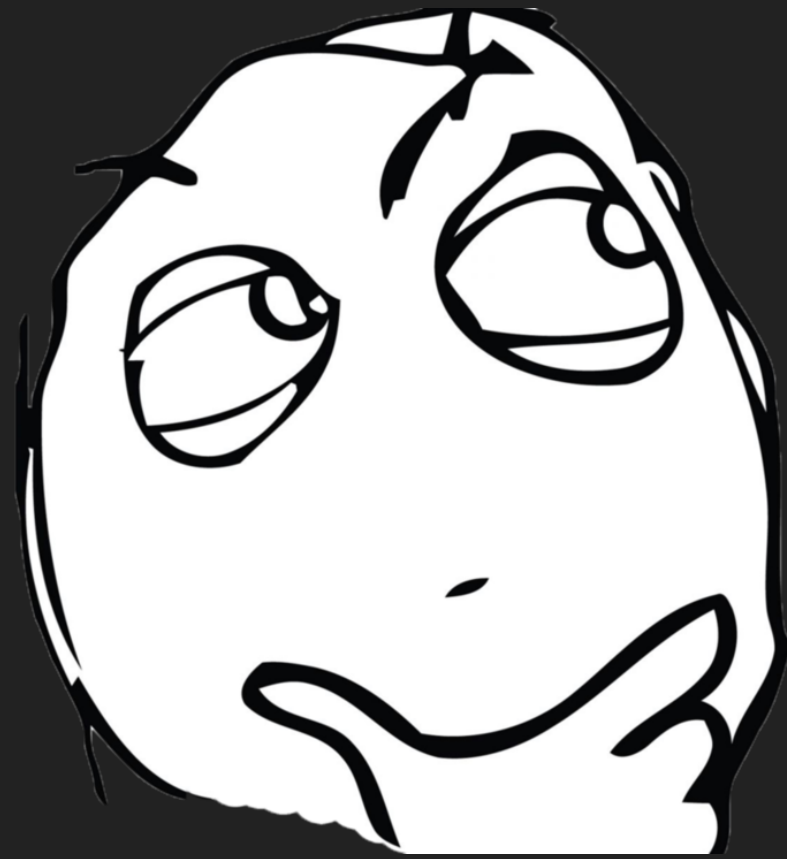
open

How it works?

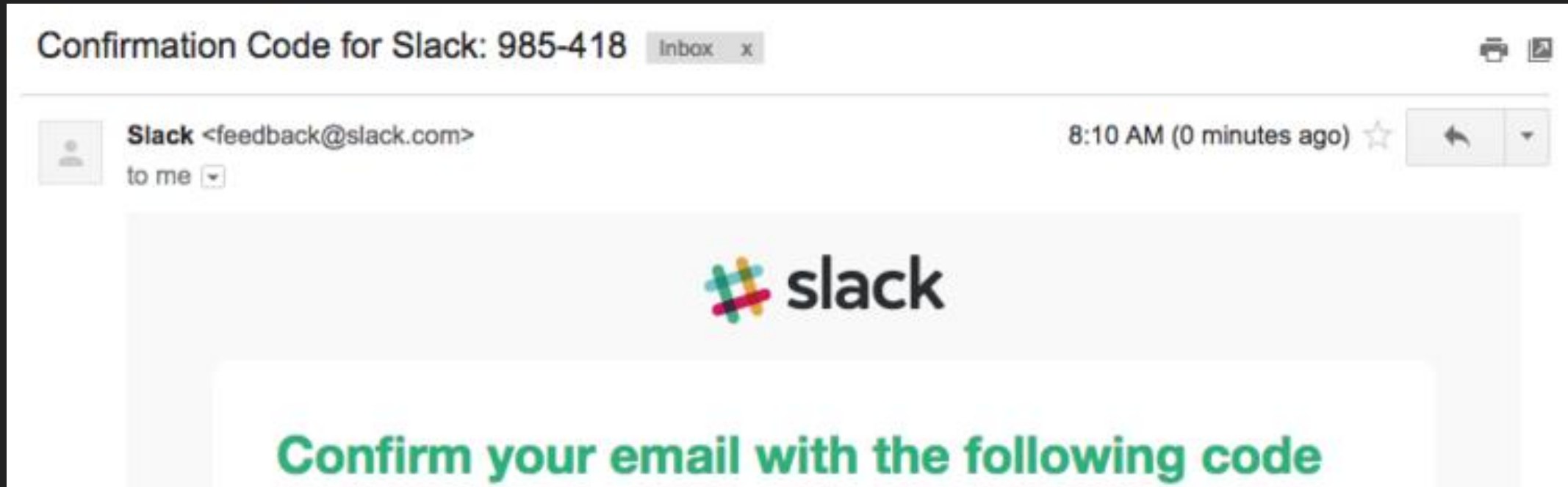
- mailto : user@email.com → support@company.com
- user@email.com 으로 가입한 유저의 고객센터란에 메일 송수신 기록이 남는다

그렇다면?

- 고객센터 어플리케이션에서 문의를 보내지 않고
- 직접 메일을 보내도 당연히 기록이 남는다



공격 시나리오



- feedback@slack.com

공격 시나리오

~~Slack~~가입 ×

이메일로 가입

공격 시나리오



Find your Slack workspace

We'll send you an email to confirm your address and find existing workspaces you've joined or can join.

support@company.com|

Confirm

Profit!

https://help[REDACTED].com/hc/en-us/requests/3264770

Search

☆

📄

⬇

🏠

Help Center

Contact us

My tickets

Upgrade

📄 Uplo

Help Center / My tickets

Confirm your email to join [REDACTED]



Feedback Slack

Today at 01:25

[https://slack.com/x-a168032647766/img/email/slack_logo.png]<https://www.slack.com>

Confirm your email to join [REDACTED].

Hello! Once you've confirmed your email address and set a password, you'll be the newest member of the Slack team [REDACTED].[sparkle emoji]

Confirm Email <https://[REDACTED].slack.com/signup/[REDACTED]>

Link not working? Try this:
[https://\[REDACTED\].slack.com/signup/\[REDACTED\]](https://[REDACTED].slack.com/signup/[REDACTED])

If you have any questions, simply reply to this email. We'd love to help.

Cheers,

The team at Slack

Made by Slack Technologies, Inc<https://slack.com> • Our Blog <http://slackhq.com>
155 5th Street, 6th Floor • San Francisco, CA • 94103

Submitted by

Feedback Slack

Created

Today at 01:25

Last activity

Today at 01:25

Id

#3264770

Status

open

Profit!



조건

1. 기업의 고객센터 기능이 존재하고 메일 내역이 유저에게 공개
2. 회원가입시 이메일 인증을 하지 않음

그게 끝이에요?

- Slack, Yammer 다 안 쓰는 회사는
- 아무 문제 없는 거 아냐?

아닙니다

- support@company.com을 다른 어플리케이션 회원 메일로 쓰고 있다면?
- ex) Twitter, Facebook, Instagram, ...

아닙니다



Password Reset

English ▼

How do you want to reset your password?

We found the following information associated with your account.

• Email a link to **su*****@** **██████** **.*****

Continue

[I don't have access to any of these](#)

아닙니다

[Knowledge Base Home](#) > [My Cases](#) > Password reset request



Password reset request

Twitter - May 08, 2017 07:15PM

Twitter

Reset your password?

If you requested a password reset for @██████████, click the link below.
If you didn't make this request, ignore this email.

Reset password

> https://twitter.com/account/confirm_email_reset?reset_type=e&user_id=██████████&token=████████████████████████████████████████████████████████████████████████████████&confirm_pending_email=0&token_version=0&password_reset_cause=user

Getting a lot of password reset emails?

You can change your account settings to require personal information to reset your password.

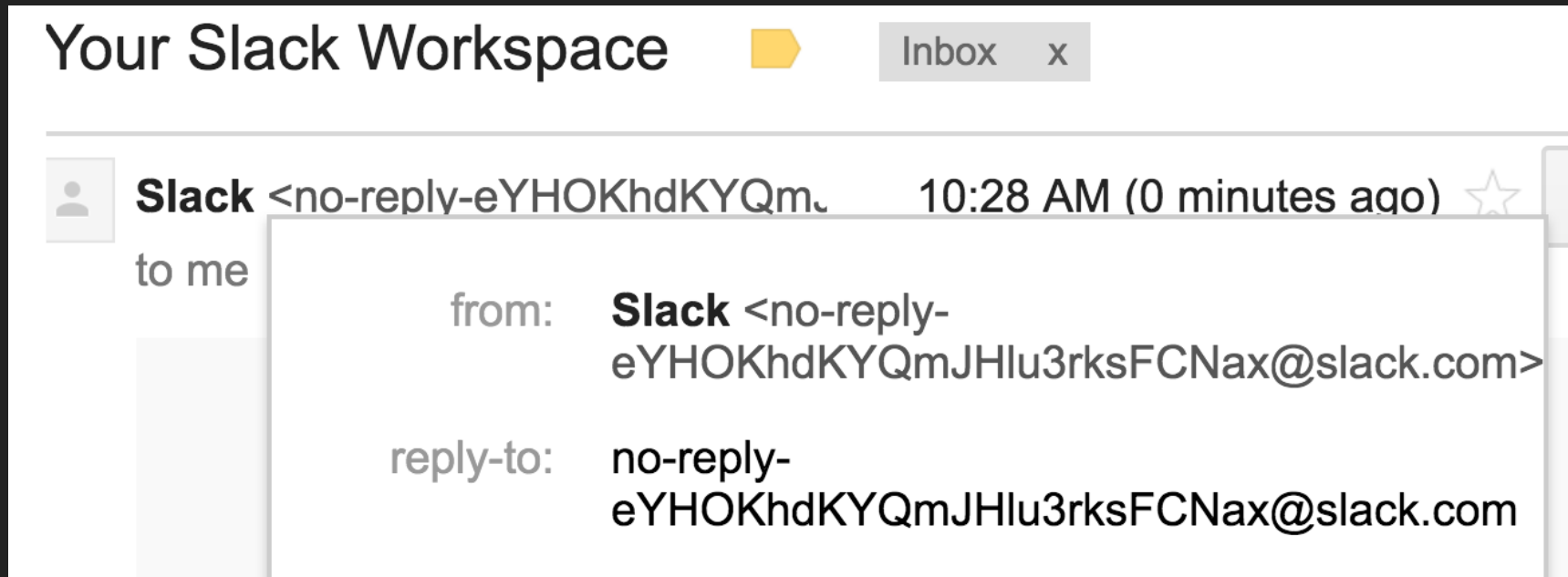
Get More Help

Have a question, and can't find the answer in the Knowledge Base?

[CUSTOMER
RESOURCES](#)

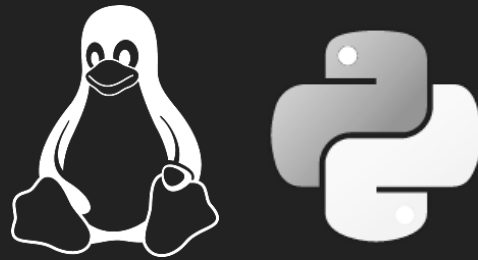


- Slack's Solution
 - email 계정 random-token 추가



결론

- 이런 거 찾아서 돈 벌고 싶다...



감사합니다

Question?