

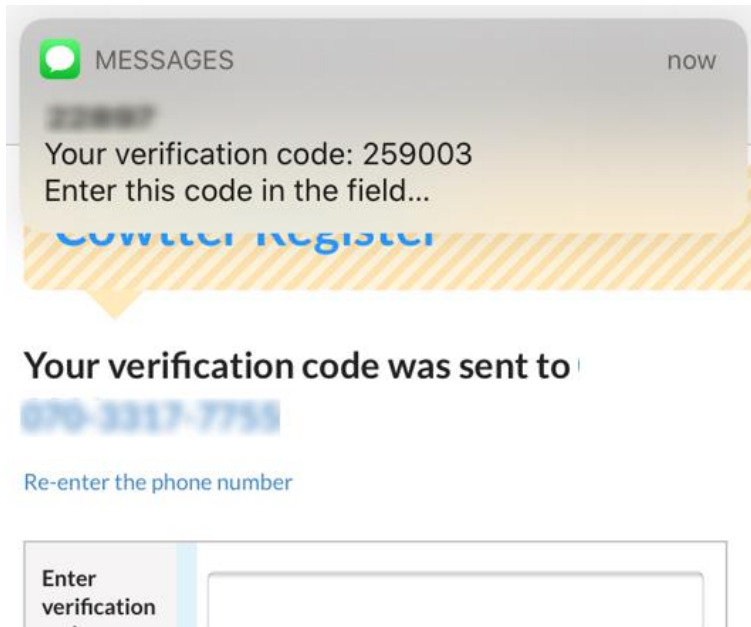
Vulnerability Exploiting SMS Push Notifications

Rina Shibayama and Hiroaki Kikuchi

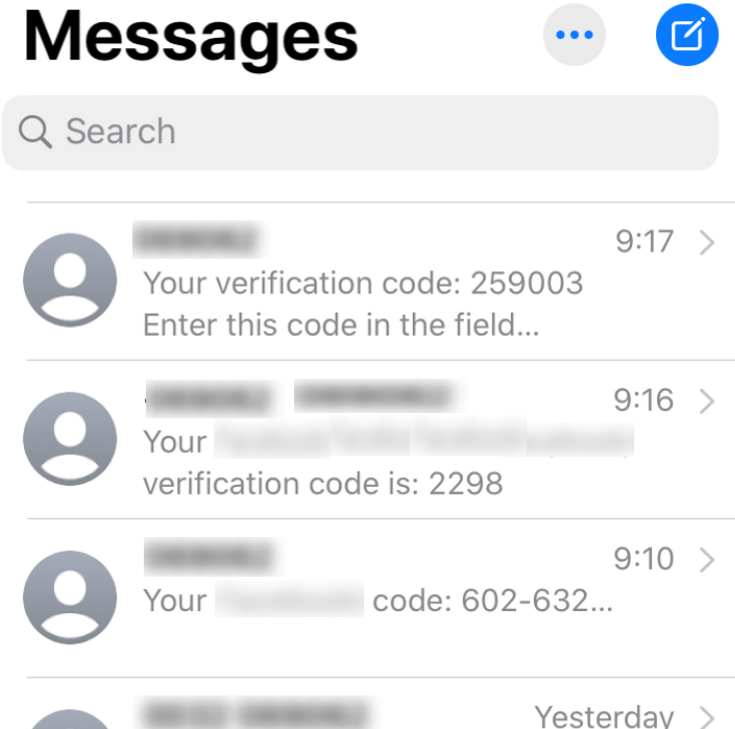
Graduate School of Advanced Mathematical Sciences, Meiji University,
Tokyo, Japan

What are new SMS features?

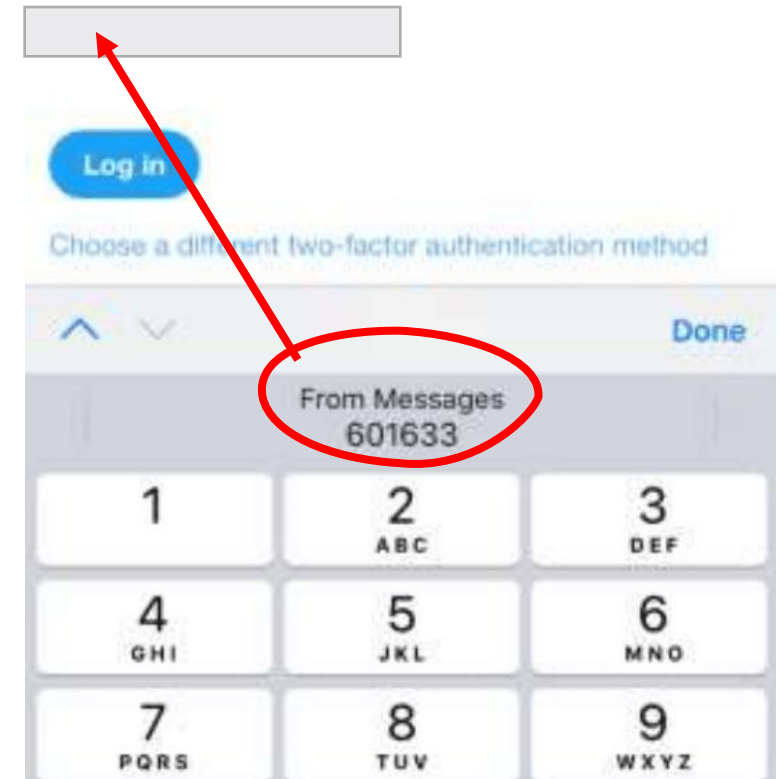
1. Push Notifications



2. Listing messages



3. Auto-input



What happen if we receive code via SMS?

Join Majebook

Your verification code was sent to your phone number

Re-enter the phone number

Enter verification code

[I Don't enter verification code](#)

Submit

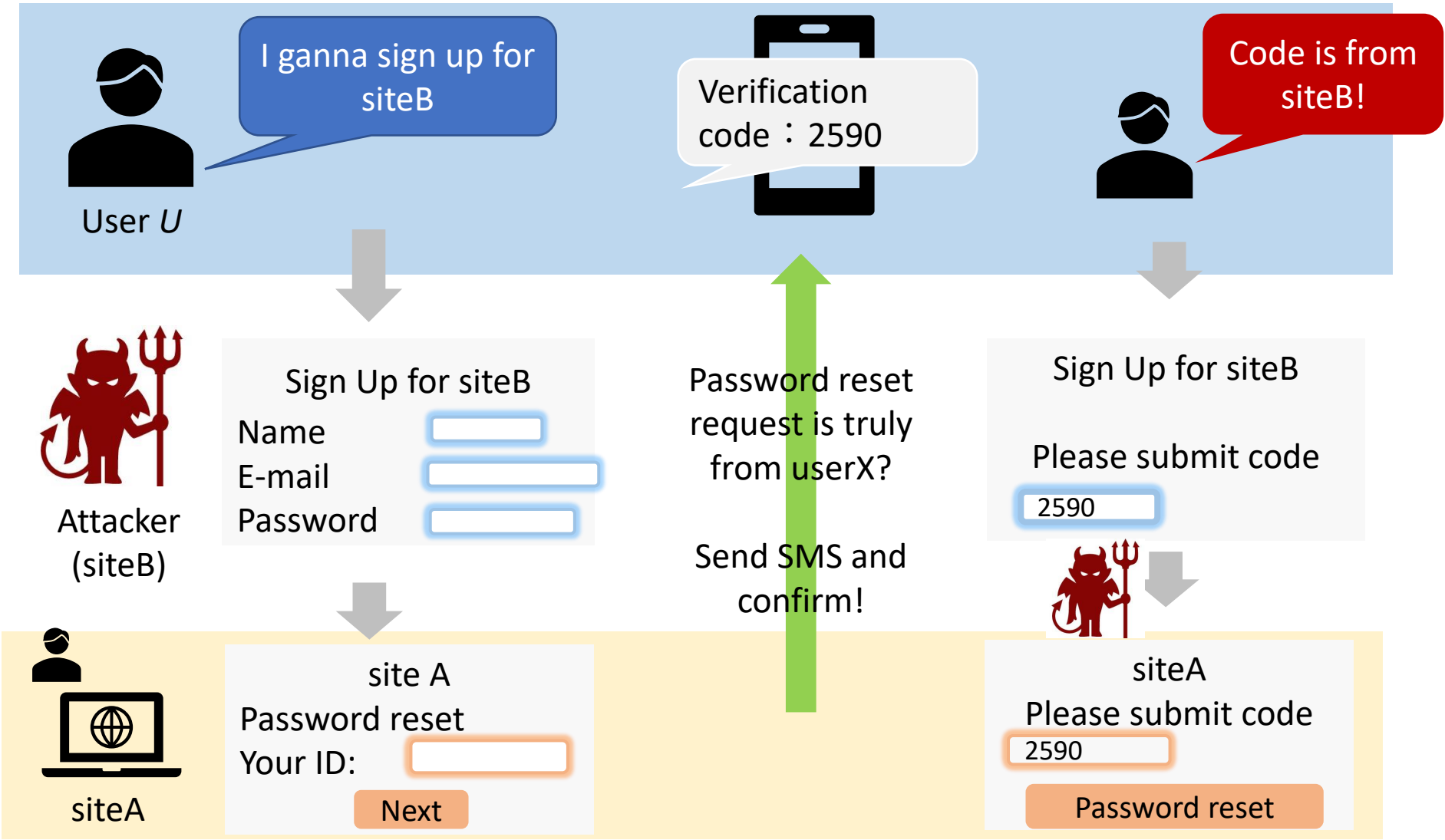


*** Vulnerability ***

Deciding to submit the code
may lead someone to reset your password!

What is Password Reset MitM attack?

[Gelernter, IEEE Symposium on Security and Privacy 2017]



Research Questions

1. Does a warning at the bottom increase attack rate?

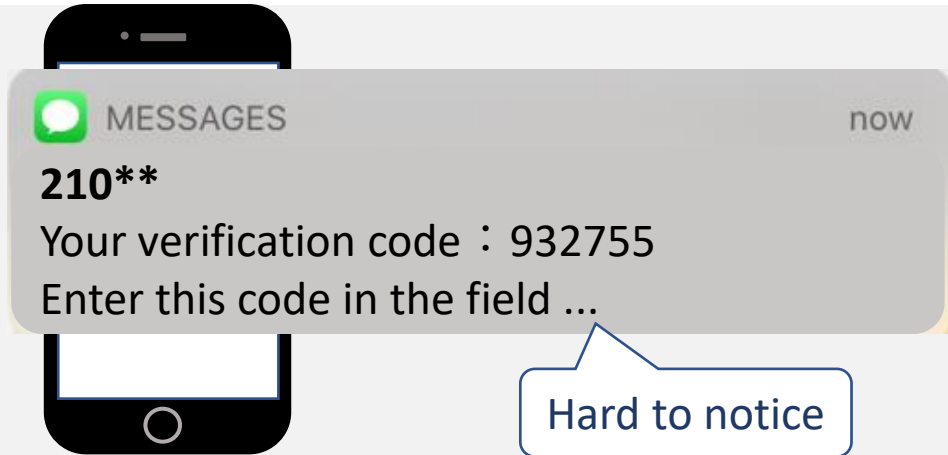
Your verification code: 259003
Enter this code in the field
Don't share this code with
others
This is **password reset code**
from **S! JAPAN**

S! JAPAN **password reset**
code : 368552
Enter this code in the field
Don't share this code with
others

2. Does a warning in English increase attack rate?
3. Do ICT skills and security knowledge help in mitigating the attack?
4. Does the auto-input feature increase attack rate?

Does a warning at the bottom increase attack rate?

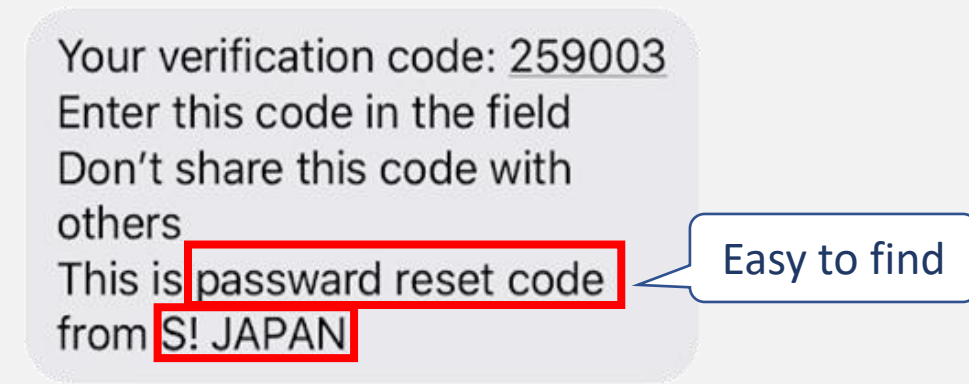
Warning at the bottom



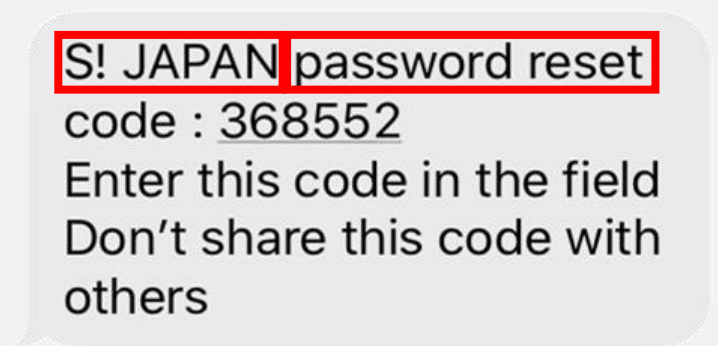
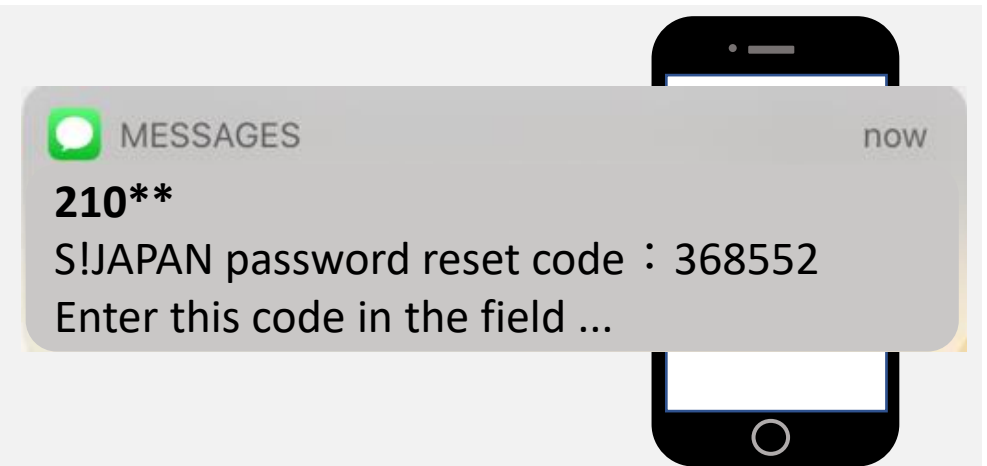
1. Notification



2. Whole text




Warning at the top



Does the auto-input feature increase attack rate?

Auto-fill feature



Your verification code: 259003
Enter this code in the field
Don't share this code with others
This is password reset code from S! JAPAN

Do not need to check

Single touch!

From Messages
601633

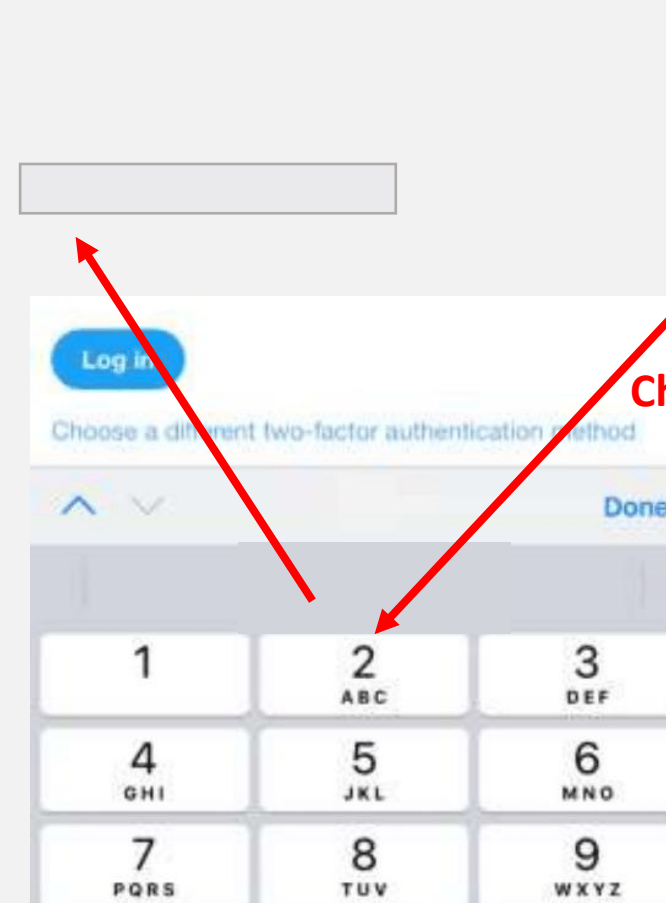
1 2 3
4 5 6
7 8 9

Log in
Choose a different two-factor authentication method
Done

PQRS TUV WXYZ

Detailed description: This screenshot shows an iPhone keyboard with an auto-fill suggestion. A red circle highlights the suggestion 'From Messages 601633'. A red arrow points from this suggestion to an empty text input field at the top of the screen. To the right, a grey text box contains a verification code '259003' and a warning 'This is password reset code from S! JAPAN'. A blue callout bubble points to the warning with the text 'Do not need to check'. The background shows a 'Log in' button and a 'Choose a different two-factor authentication method' prompt.

Without auto-fill



Your verification code: 259003
Enter this code in the field
Don't share this code with others
This is password reset code from S! JAPAN

Check and type

There is chance to notice

1 2 3
4 5 6
7 8 9

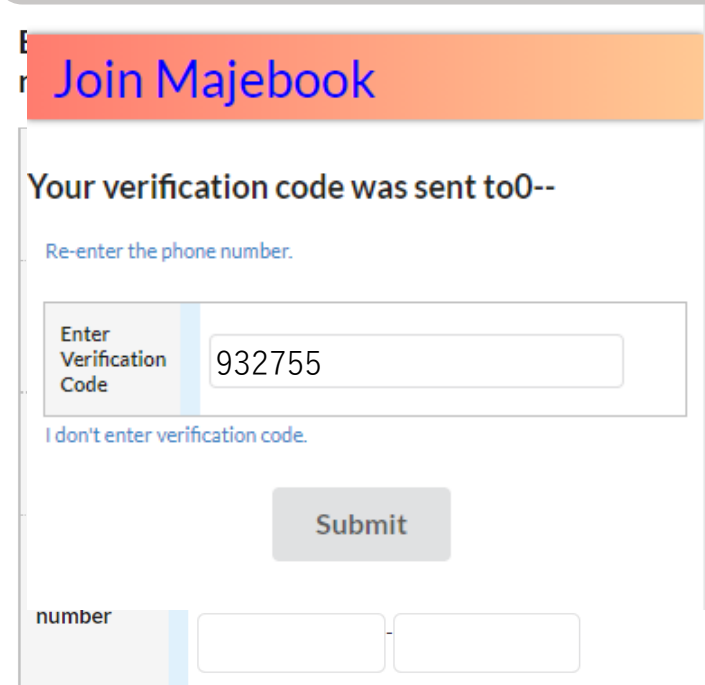
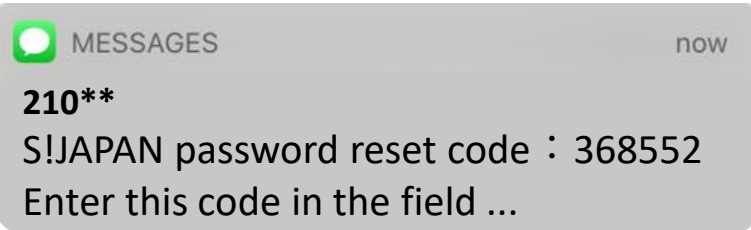
Log in
Choose a different two-factor authentication method
Done

PQRS TUV WXYZ

Detailed description: This screenshot shows the same iPhone keyboard as the left panel, but without the auto-fill suggestion. A red arrow points from the empty text input field at the top to the keyboard. A red arrow also points from the keyboard to the same input field, with the text 'Check and type' next to it. To the right, the same grey text box with the verification code and warning is present. A blue callout bubble points to the warning with the text 'There is chance to notice'. The background is identical to the left panel.

Experiment

Conducted online during Nov. ~ Dec. 2019



Register

- 81 subjects(male44, female37) were collected via the crowdsourcing services.
- Signup for enrollment of three websites.
 - Submit information (Name, Phone number, Password)
 - Verification via SMS OTP

	Sign up for	Purpose	Verification code	Expected action
1	S! JAPAN	Test sign-up	None	-
2	Cowtter	Test OTP	Cowtter verification code	Submit code
3	Majebook	PRMitM attack	S! JAPAN PW reset code	Stop submitting

- The subjects are instructed in advance to stop submitting if they have any doubts about their enrollment.

Examples of SMS text

No warning	Warning at the top	Warning at the bottom
<p>Verification code: 259003 Enter this code in the field.</p> <p>S! JAPAN</p>	<p>S! JAPAN password reset code : 368552 Enter this code in the field Don't share this code with others</p>	<p>Your verification code: 259003 Enter this code in the field Don't share this code with others This is password reset code from S! JAPAN</p>
Control	Easy to find	Hard to notice

Questionnaire

Security knowledge

To clarify RQ3

SeBIS (16questions)

- A. device securement
- B. password management
- C. proactive awareness
- D. software updating

EX for A) I set my computer screen to automatically lock if I do not use it for a prolonged period of time.

Behavior

To clarify RQ4

questionnaire(8questions) age, gender, ...

EX) How did you check the code?

1. Open the message in the application
2. Check message listing in the application (did not open the message)
3. Check OTP on the top of the screen
4. other way

Result: Attack rates by SMS types

type	SMS text		submit	cancel	Attack rate[%]
	warning	language			
①	none	JPN.	14	5	73.7
②	bottom	JPN.	15	4	78.9
③	bottom	ENG.	16	4	80.0
④	top	JPN.	0	7	0.0
⑤	top	ENG.	10	6	62.5
	total		55	26	67.9

②

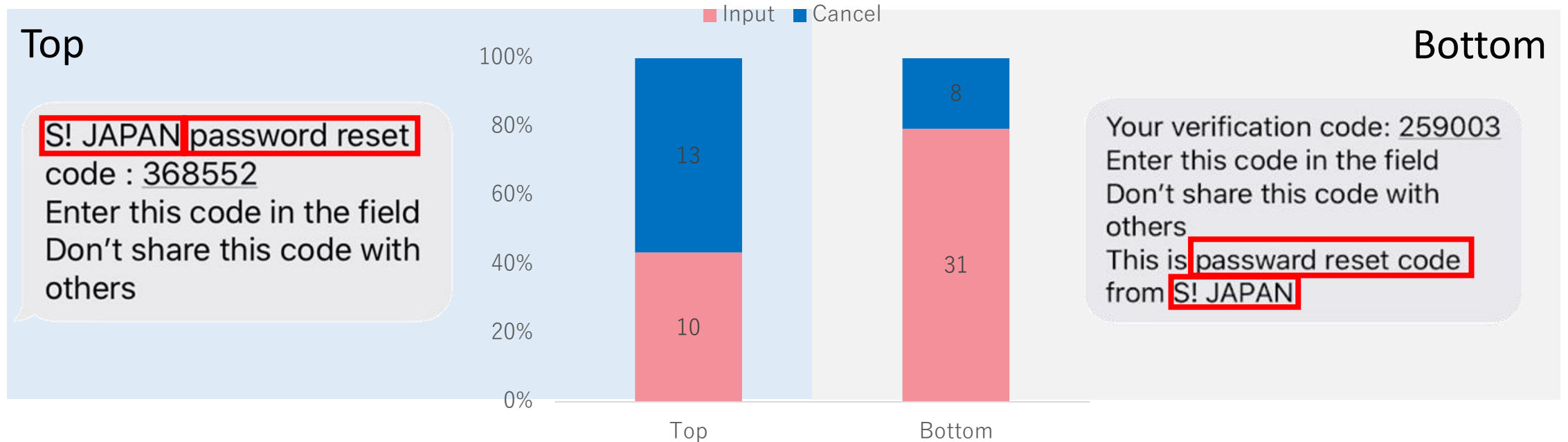
Your verification code: 259003
 Enter this code in the field
 Don't share this code with others
 This is **password reset code**
 from **S! JAPAN**

④

S! JAPAN password reset
 code : 368552
 Enter this code in the field
 Don't share this code with others

Result: Position of the warning

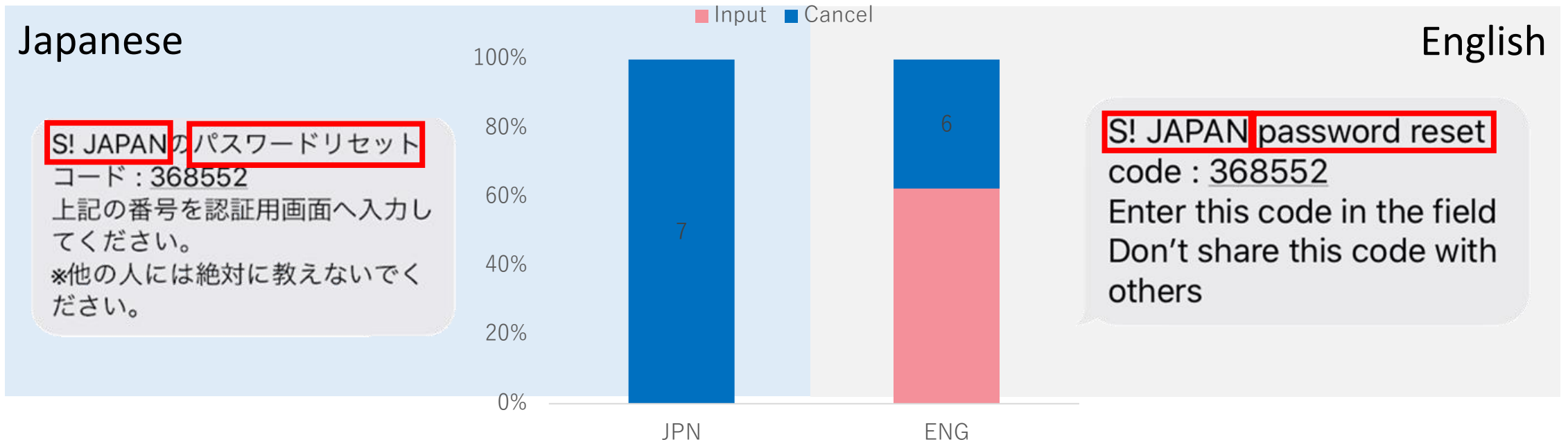
【RQ1】 Does a warning at the bottom increase attack rate? ✓ **yes**



⇒ Note that usage of the code at the top decreases the attack acceptance ratio.

Result: Language

【RQ2】 Does warning in English increase attack rate? ✓ yes



⇒ If the message is not immediately understandable (English), the user will not stop and submit it.

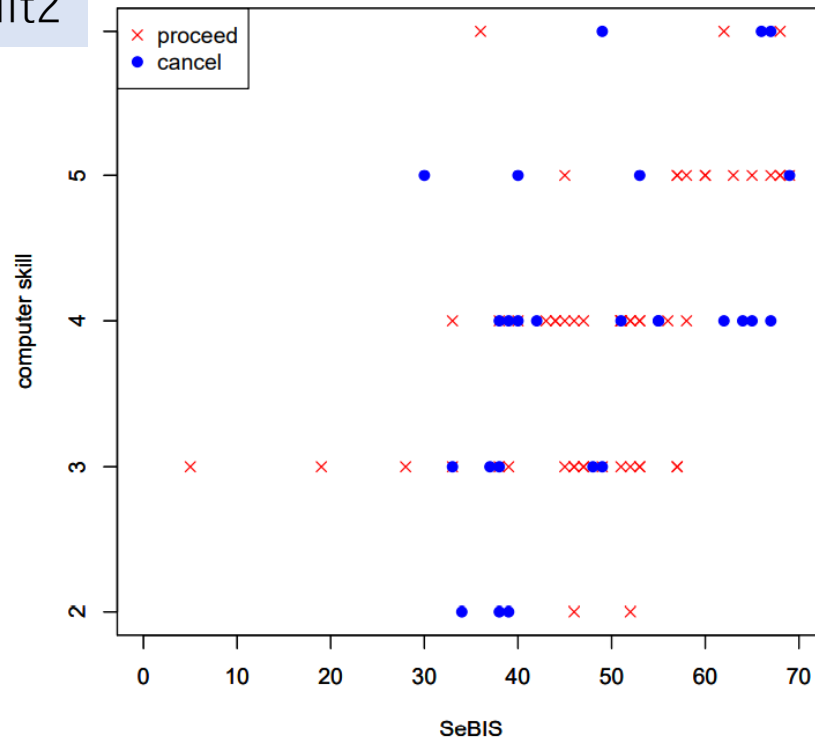
Result: SeBIS

【RQ3】 Does security knowledge help in mitigating the attack? → **No**

Result1

	Mean		SD	<i>t</i>	<i>p</i>
	accept	cancel			
SeBIS	49.6	48.8	12.0	0.132	0.896

Result2



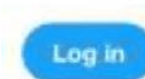
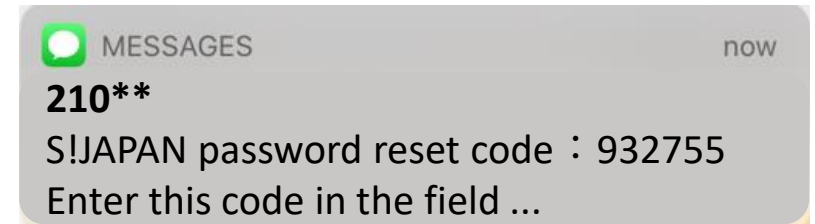
- Analysis showed no difference between security knowledge and susceptibility.

Result: Way for Checking and inputting the code

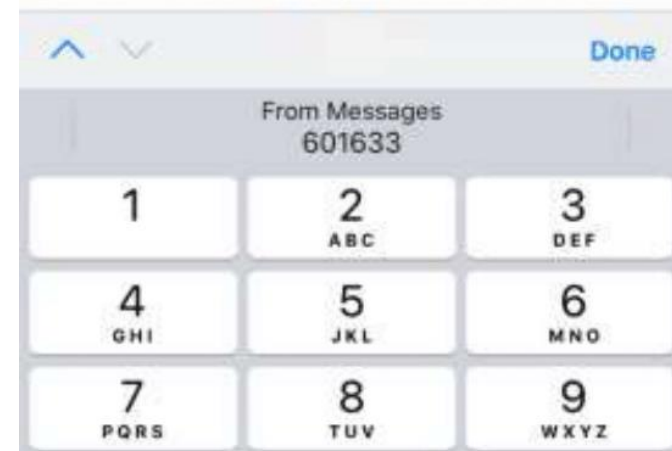
【RQ4】 Does an auto-input feature increase attack rate? → **No**

	Input	Cancel	Attack rate[%]
Manual	44	64	78.8
Copy&paste	7	10	70.0
Auto-input	4	6	66.7

Attack acceptant rate when using auto-input was rather low compared to other methods(66.7%).



Choose a different two-factor authentication method



Countermeasures

1. Specify the servicer and the purpose explicitly in SMS.
2. Disable auto-fill function at different domains.

Observe URL in the SMS message and enables auto-input only when the URL in the message matches the one the user is trying to enter the code into.

Sender and purpose are unknown
in the notification

1
S!JAPAN password reset code :
932755
Enter this code in the field.
*Don't share this code with others.
@sjapan-example.com

Your verification code: 259003
Enter this code in the field.
*Don't share this code with others
as this is password reset code for
S! JAPAN

2
✓ Good

NG

Conclusions

We have conducted subject experiment to clarify whether new smartphone features are Vulnerable to PRMitM attack.

In SMS message notifying password reset OTP,

Warning at the **bottom** increases the risk.

Warning in **Japanese** reduces the risk.

Security knowledge does not mitigate the PRMitM attack.