Can You Spot a Phish?

Preventing BC Public Service Employees From Getting Hooked By Scammers

BC Behavioural Insights Group, Public Service Agency

Office of the Chief Information Officer, Ministry of Citizens' Services

BRITISH COLUMBIA
BC Public Service

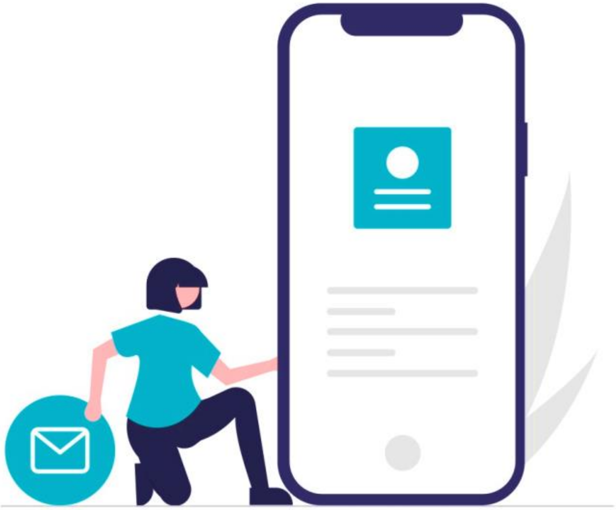
Where ideas work

The Challenge

- **Phishing attempts to capture valuable personal or financial information**

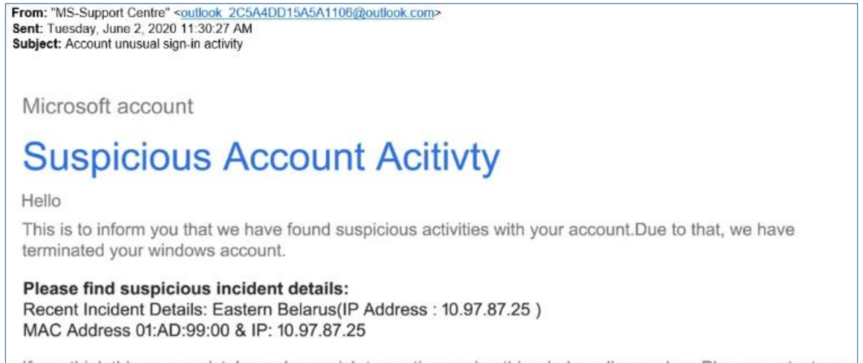
- **Billions of phishing emails are sent out daily**

- **Tactics are getting more sophisticated**



How Scammers Exploit our Human Tendencies

- Mimicry
- Authority
- Emotions
- Urgency
- Social norms



From: "MS-Support Centre" <outlook_2C5A4DD15A5A1106@outlook.com>
Sent: Tuesday, June 2, 2020 11:30:27 AM
Subject: Account unusual sign-in activity

Microsoft account

Suspicious Account Acitivty

Hello

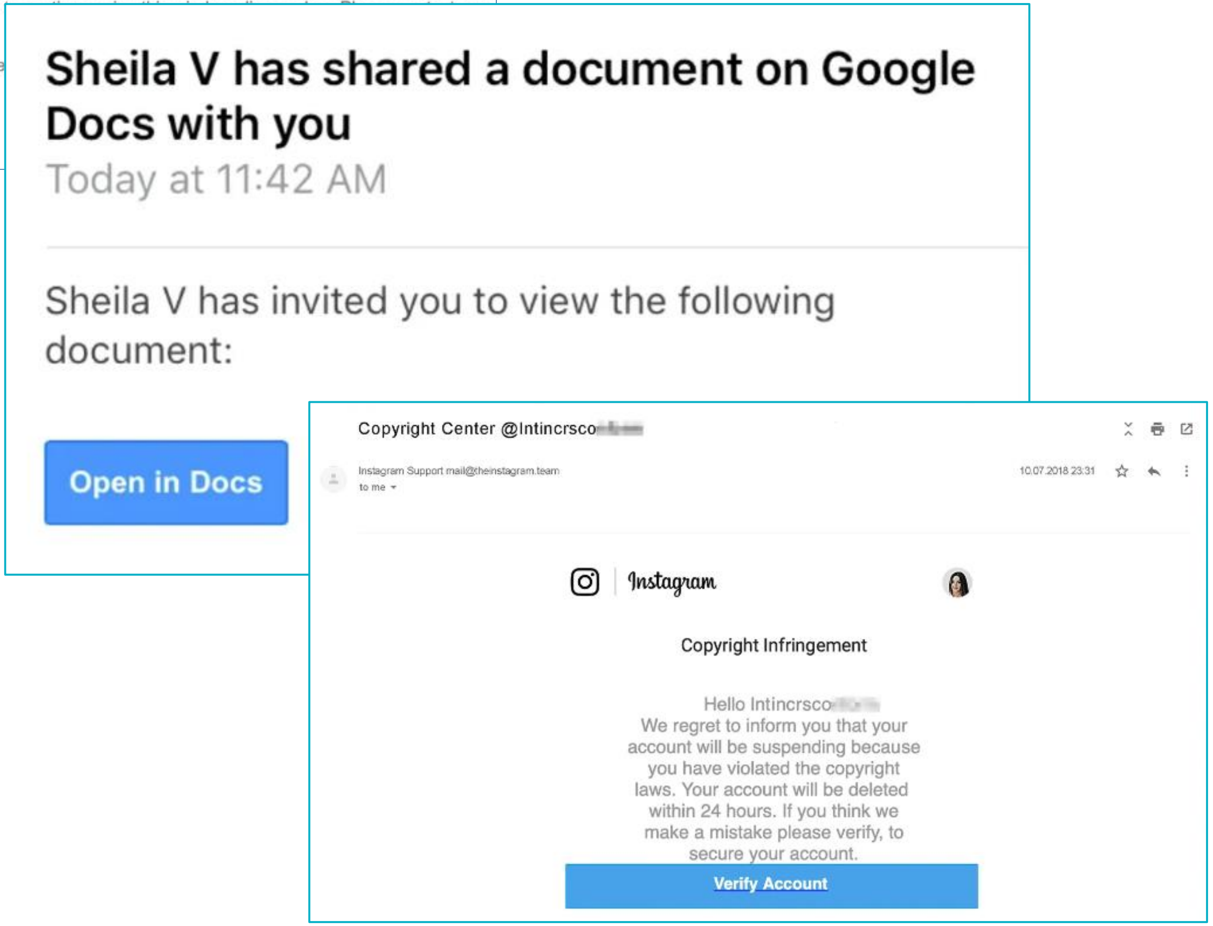
This is to inform you that we have found suspicious activities with your account.Due to that, we have terminated your windows account.

Please find suspicious incident details:
Recent Incident Details: Eastern Belarus(IP Address : 10.97.87.25)
MAC Address 01:AD:99:00 & IP: 10.97.87.25

If you think this was a mistake and you wish
technical support at 1-800-341-8835.

PS NOTE: Please be at your computer while

Windows Help
1-800-341-8835.



Sheila V has shared a document on Google Docs with you

Today at 11:42 AM

Sheila V has invited you to view the following document:

Copyright Center @Intincrsco[redacted]

Instagram Support mail@theinstagram.team
to me

10.07.2018 23:31

Copyright Infringement

Hello Intincrsco[redacted]
We regret to inform you that your account will be suspending because you have violated the copyright laws. Your account will be deleted within 24 hours. If you think we make a mistake please verify, to secure your account.

The Context

- Digital security is a priority for organizations as cybercrime becomes more common
- Phishing attacks can result in losses to data, funds, and trust and can also impact individuals
- There are layers of defence, however employees remain the strongest defence to protect information and assets
- Training grounded in behavioural science may enable employees to better recognize phishing
- Objectives were to raise awareness, increase accurate identification, and decrease the rate of interaction with phishing emails

Purpose and Research Questions

Does behaviourally informed training reduce the likelihood that an employee interacts with a simulated phishing email?

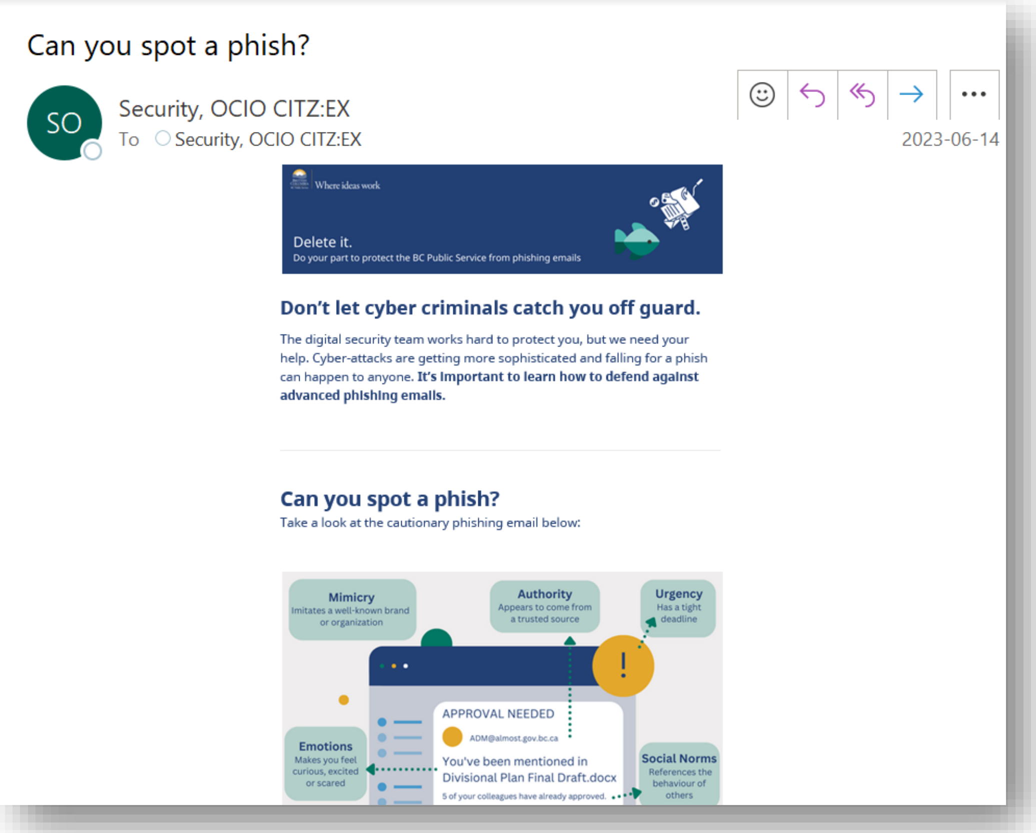
Is email-based training acceptable among employees?

Methods

The Intervention: Email-Based Training

Condition A

Behaviourally informed training email



Can you spot a phish?

SO

Security, OCIO CITZ:EX

To ○ Security, OCIO CITZ:EX

2023-06-14

Delete it.

Do your part to protect the BC Public Service from phishing emails

Don’t let cyber criminals catch you off guard.

The digital security team works hard to protect you, but we need your help. Cyber-attacks are getting more sophisticated and falling for a phish can happen to anyone. **It’s important to learn how to defend against advanced phishing emails.**

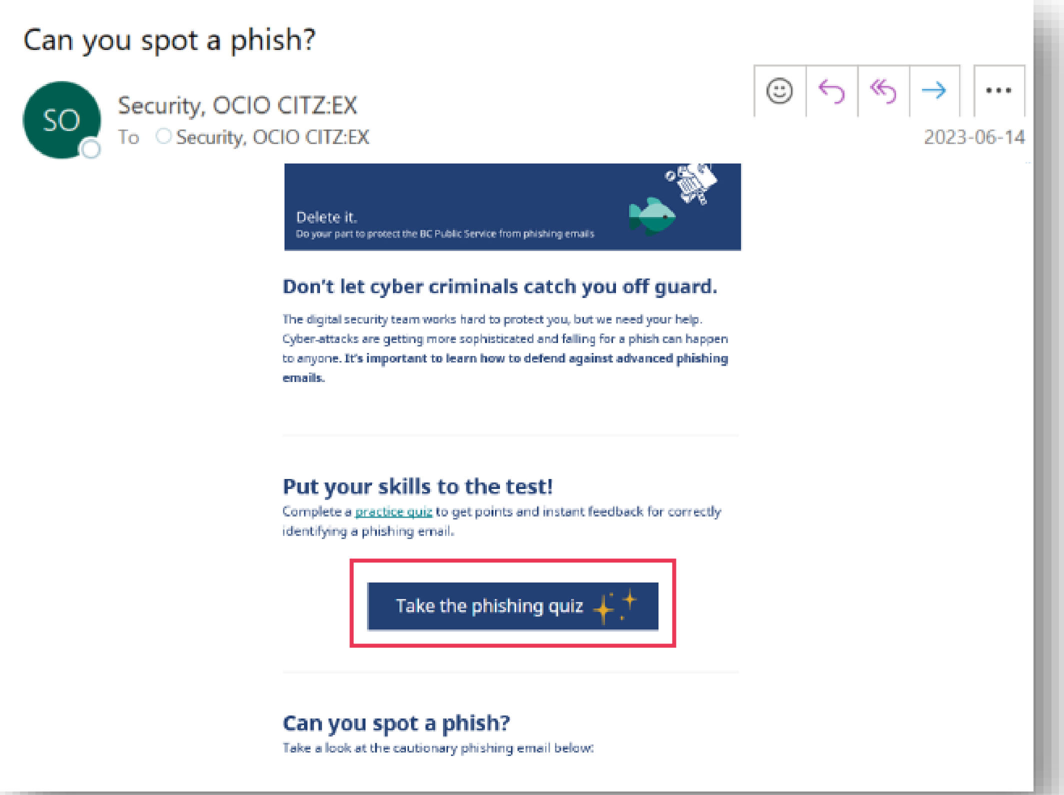
Can you spot a phish?

Take a look at the cautionary phishing email below:

Mimicry
Imitates a well-known brand or organization
Authority
Appears to come from a trusted source
Urgency
Has a tight deadline
APPROVAL NEEDED
ADM@almost.gov.bc.ca
You've been mentioned in Divisional Plan Final Draft.docx
5 of your colleagues have already approved.
Emotions
Makes you feel curious, excited or scared
Social Norms
References the behaviour of others

Condition B

Behaviourally informed training email with gamified quiz



Can you spot a phish?

SO

Security, OCIO CITZ:EX

To ○ Security, OCIO CITZ:EX

2023-06-14

Delete it.

Do your part to protect the BC Public Service from phishing emails

Don’t let cyber criminals catch you off guard.

The digital security team works hard to protect you, but we need your help. Cyber-attacks are getting more sophisticated and falling for a phish can happen to anyone. **It’s important to learn how to defend against advanced phishing emails.**

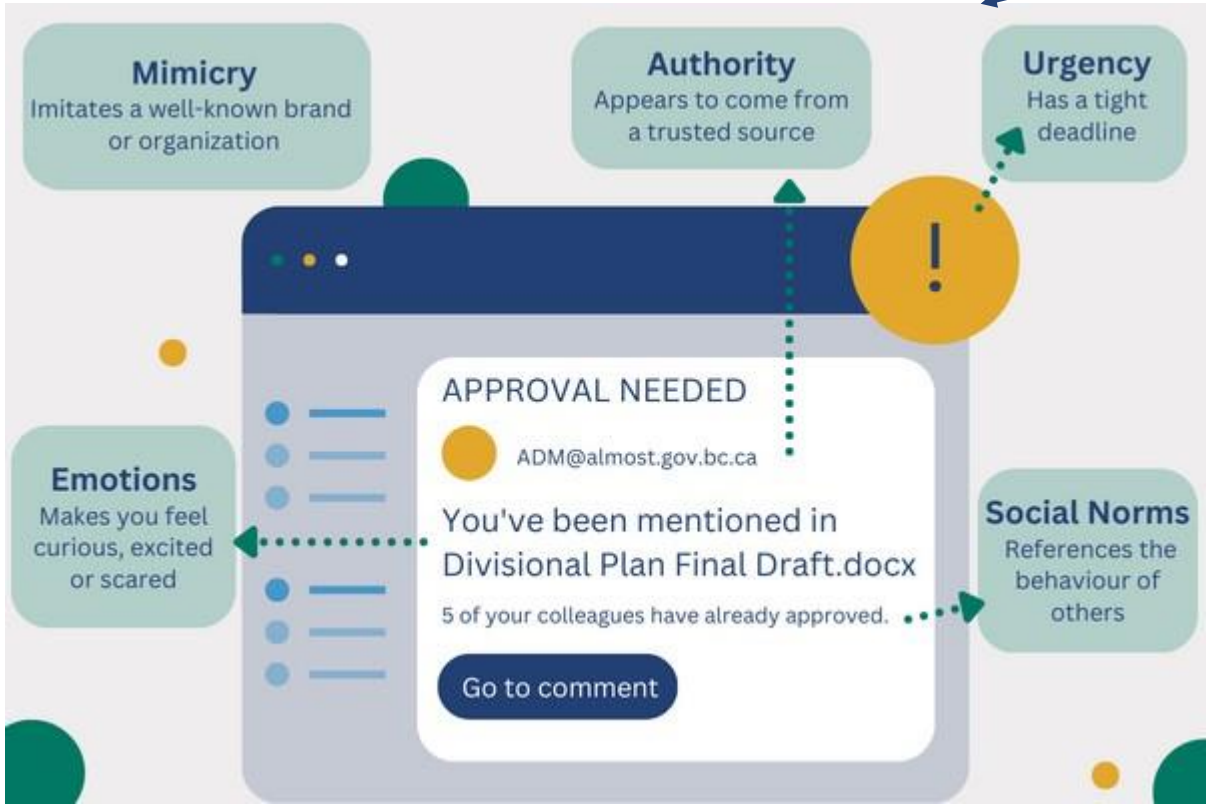
Put your skills to the test!

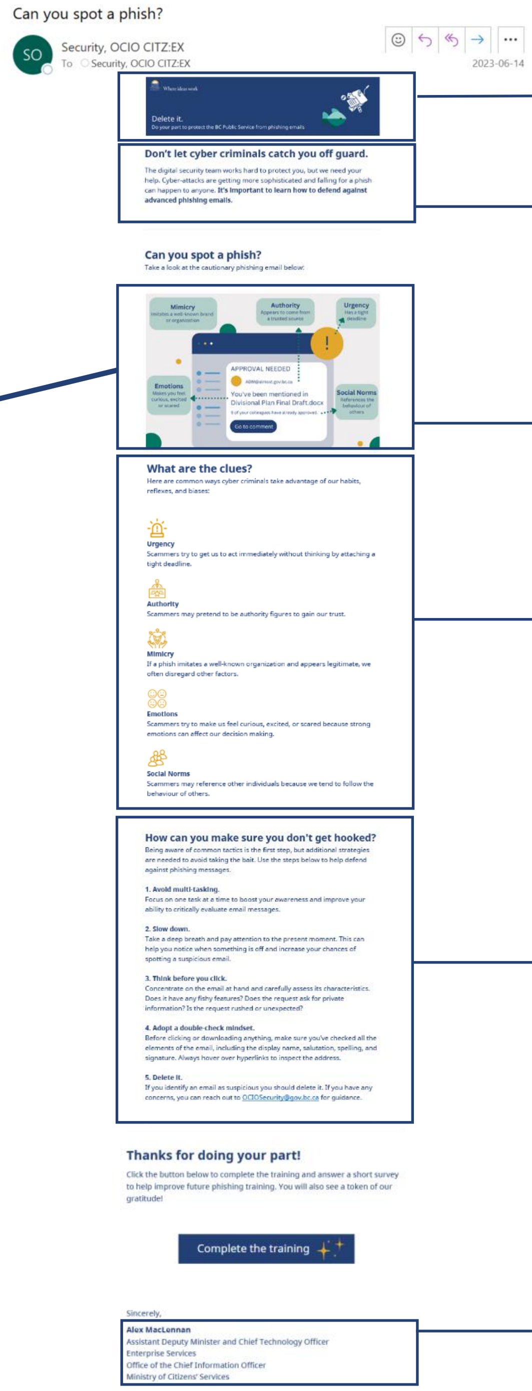
Complete a practice quiz to get points and instant feedback for correctly identifying a phishing email.

Can you spot a phish?

Take a look at the cautionary phishing email below:

Behaviourally Informed Elements


Mimicry
Imitates a well-known brand or organization
Authority
Appears to come from a trusted source
Urgency
Has a tight deadline
!
Emotions
Makes you feel curious, excited or scared
APPROVAL NEEDED
ADM@almost.gov.bc.ca
You've been mentioned in Divisional Plan Final Draft.docx
5 of your colleagues have already approved.
Go to comment
Social Norms
References the behaviour of others



Can you spot a phish?

Security, OCIO CITZ:EX
To Security, OCIO CITZ:EX
2023-06-14

Delete it.
Do your part to protect the BC Public Service from phishing emails

Don't let cyber criminals catch you off guard.

The digital security team works hard to protect you, but we need your help. Cyber-attacks are getting more sophisticated and falling for a phish can happen to anyone. **It's important to learn how to defend against advanced phishing emails.**

Can you spot a phish?

Take a look at the cautionary phishing email below:

What are the clues?

Here are common ways cyber criminals take advantage of our habits, reflexes, and biases:

Urgency
Scammers try to get us to act immediately without thinking by attaching a tight deadline.

Authority
Scammers may pretend to be authority figures to gain our trust.

Mimicry
If a phish imitates a well-known organization and appears legitimate, we often disregard other factors.

Emotions
Scammers try to make us feel curious, excited, or scared because strong emotions can affect our decision making.

Social Norms
Scammers may reference other individuals because we tend to follow the behaviour of others.

How can you make sure you don't get hooked?

Being aware of common tactics is the first step, but additional strategies are needed to avoid taking the bait. Use the steps below to help defend against phishing messages.

1. Avoid multi-tasking.
Focus on one task at a time to boost your awareness and improve your ability to critically evaluate email messages.

2. Slow down.
Take a deep breath and pay attention to the present moment. This can help you notice when something is off and increase your chances of spotting a suspicious email.

3. Think before you click.
Concentrate on the email at hand and carefully assess its characteristics. Does it have any fishy features? Does the request ask for private information? Is the request rushed or unexpected?

4. Adopt a double-check mindset.
Before clicking or downloading anything, make sure you've checked all the elements of the email, including the display name, salutation, spelling, and signature. Always hover over hyperlinks to inspect the address.

5. Delete it.
If you identify an email as suspicious you should delete it. If you have any concerns, you can reach out to OCIOSecurity@gov.bc.ca for guidance.

Thanks for doing your part!

Click the button below to complete the training and answer a short survey to help improve future phishing training. You will also see a token of our gratitude!

Complete the training

Sincerely,

Alex MacLennan
Assistant Deputy Minister and Chief Technology Officer
Enterprise Services
Office of the Chief Information Officer
Ministry of Citizens' Services

Salience: The desired action to complete is clear and visible.

Reciprocity: Employees are encouraged to help in return.

Simplification: Key takeaways are easy to understand.

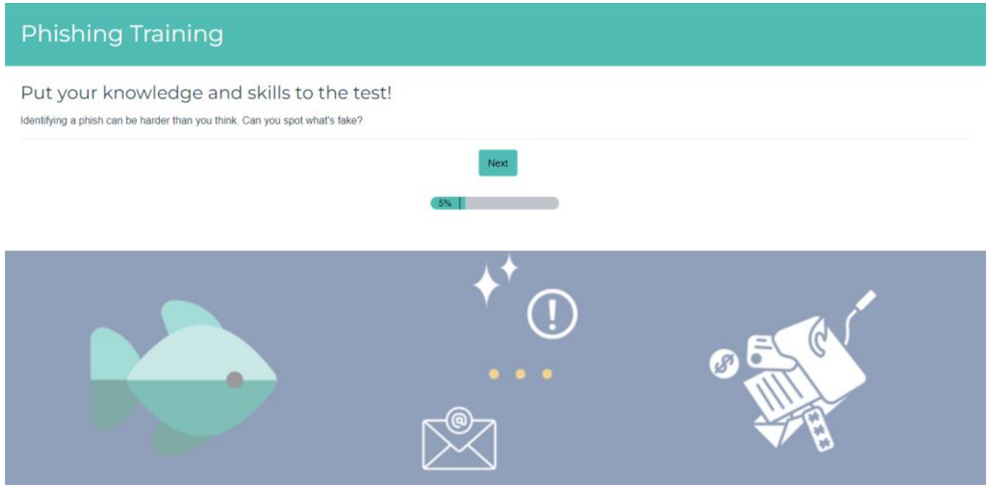
Chunking: Information is broken into manageable and digestible parts.

Counterstrategies: Provided tactics are designed to support phishing identification through slowing down, allocating cognitive resources, and knowing how to respond in a potentially emotional situation.

Influential Messenger: A trusted messenger is used.

Gamified Quiz

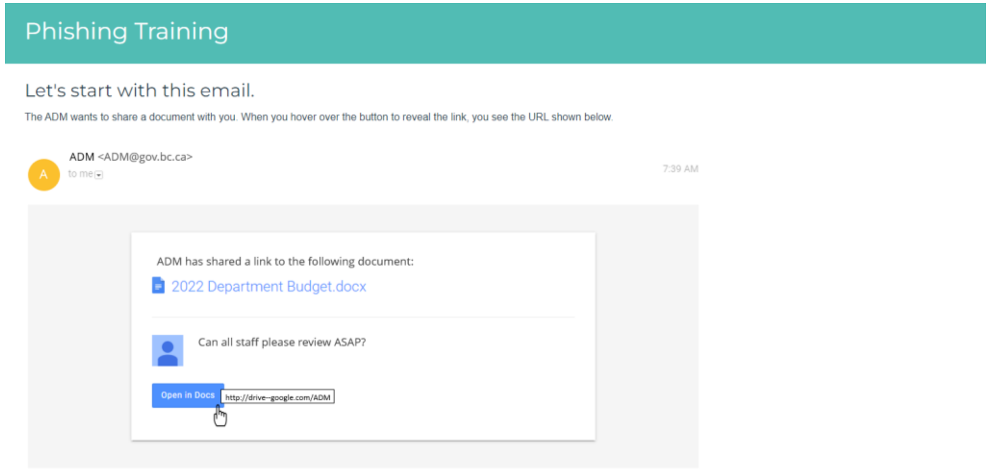
- Rewards practicing skills and experiential learning
- Points and badges
- Immediate feedback
- Fosters motivation, engagement, enjoyment



Phishing Training

Put your knowledge and skills to the test!

Identifying a phish can be harder than you think. Can you spot what's fake?



Phishing Training

Let's start with this email.

The ADM wants to share a document with you. When you hover over the button to reveal the link, you see the URL shown below.

ADM <ADM@gov.bc.ca>

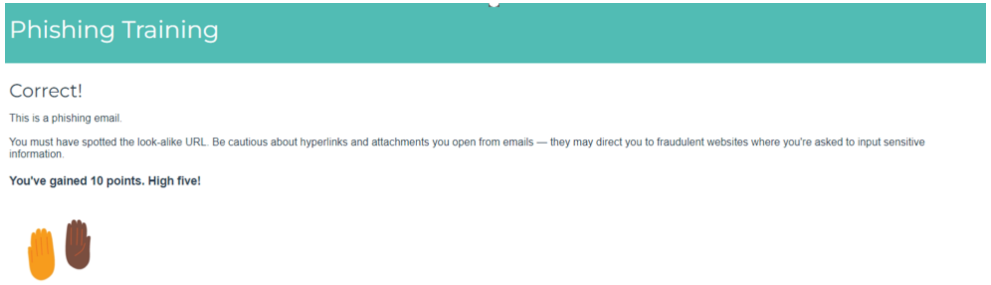
to me

7:39 AM

ADM has shared a link to the following document:

2022 Department Budget.docx

Can all staff please review ASAP?



Phishing Training

Correct!

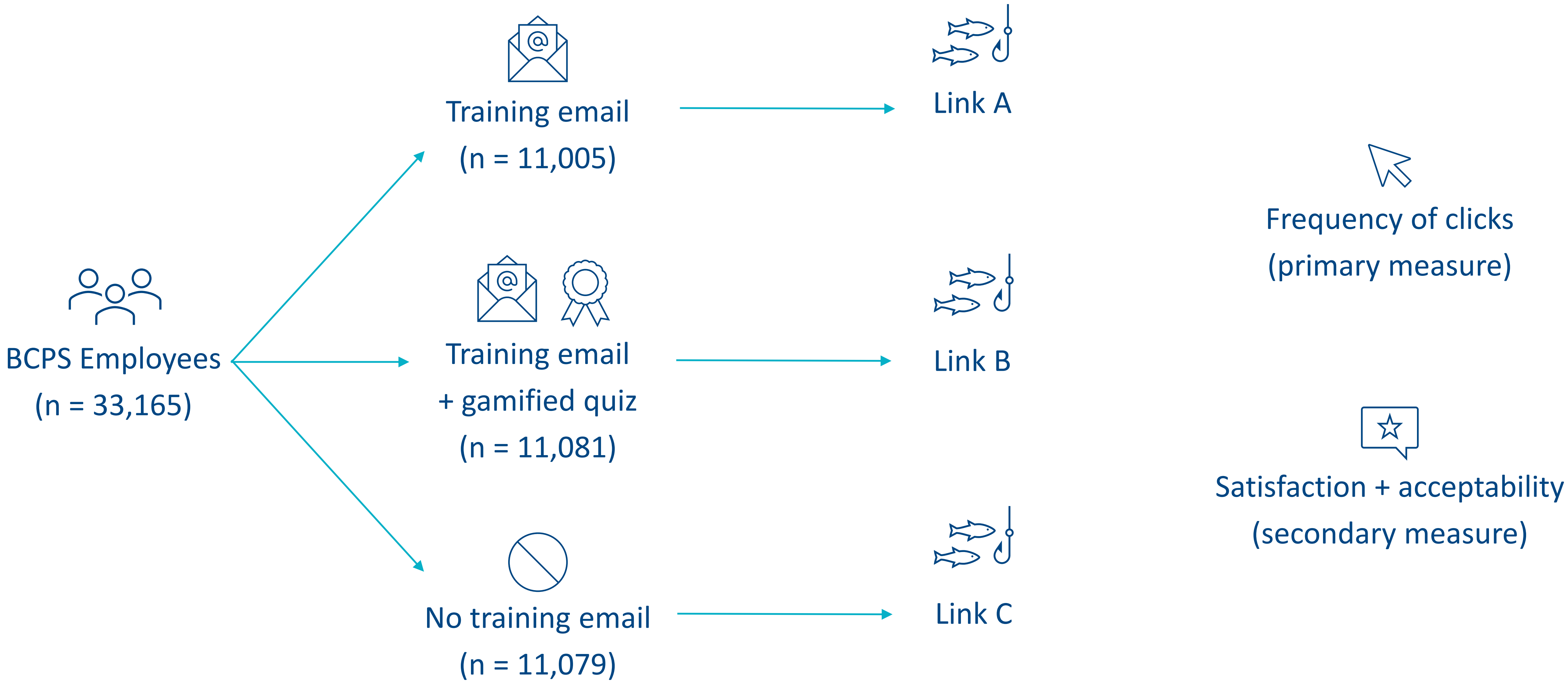
This is a phishing email.

You must have spotted the look-alike URL. Be cautious about hyperlinks and attachments you open from emails — they may direct you to fraudulent websites where you're asked to input sensitive information.

You've gained 10 points. High five!

Trial Design

Sample → Random assignment → Simulated phishing email → Key outcome measures



BCPS Employees
(n = 33,165)

Training email
(n = 11,005)

Training email
+ gamified quiz
(n = 11,081)

No training email
(n = 11,079)

Link A

Link B

Link C

Frequency of clicks
(primary measure)

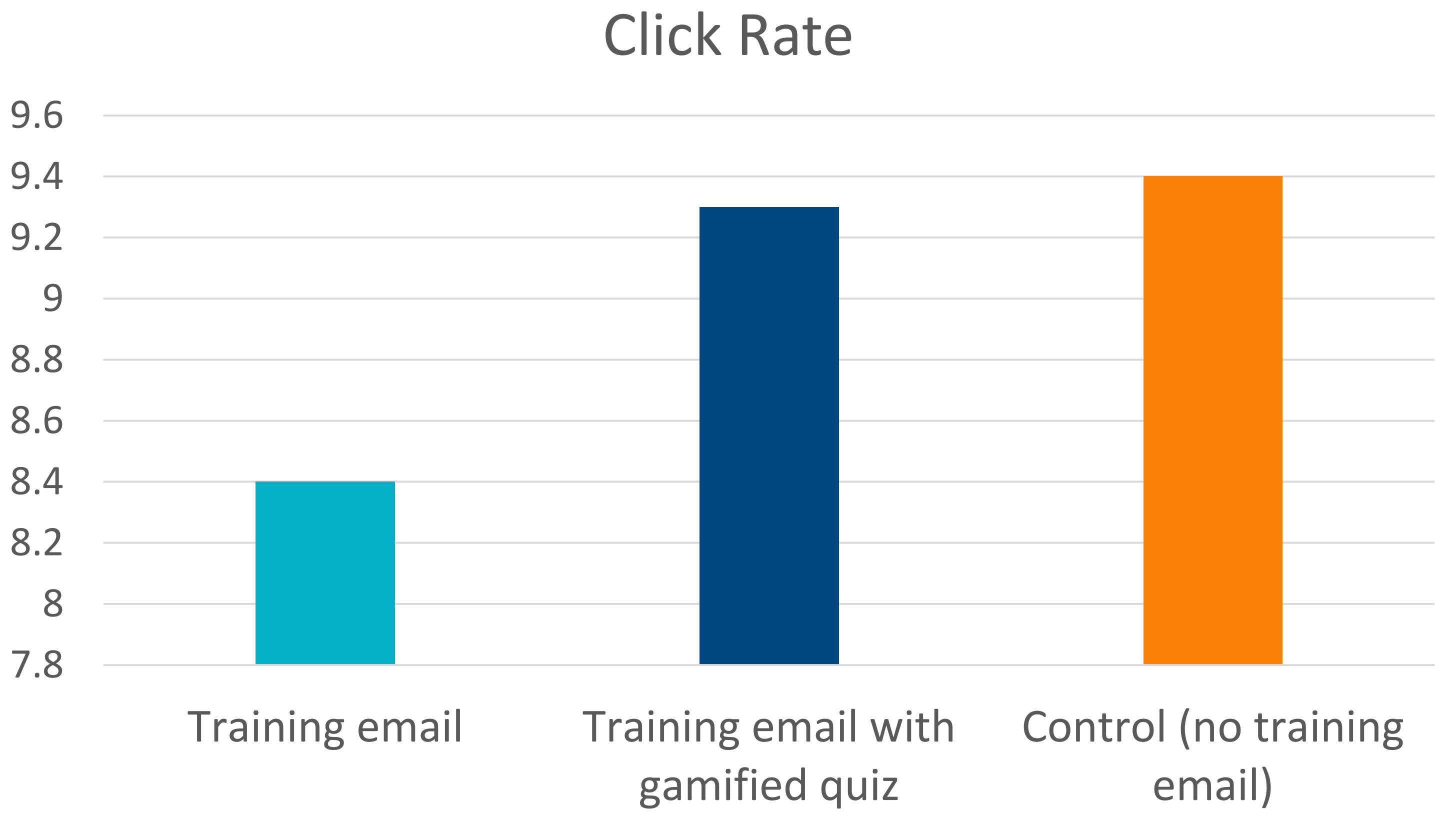
Satisfaction + acceptability
(secondary measure)

Results

Intervention Impact on Simulated Phish Click Rate

- **The training email was effective compared to control**
    - 8.4% vs. 9.4% click rate
    - Z = -2.65, *p = 0.024
    - Odds-ratio [95% CI]: 0.88 [0.79, 0.99]

- **The training email with gamified quiz was not effective compared to control**
    - 9.3% vs. 9.4% click rate
    - Z = -0.35, p = 0.726
    - Odds-ratio [95% CI]: 0.98 [0.88, 1.10]



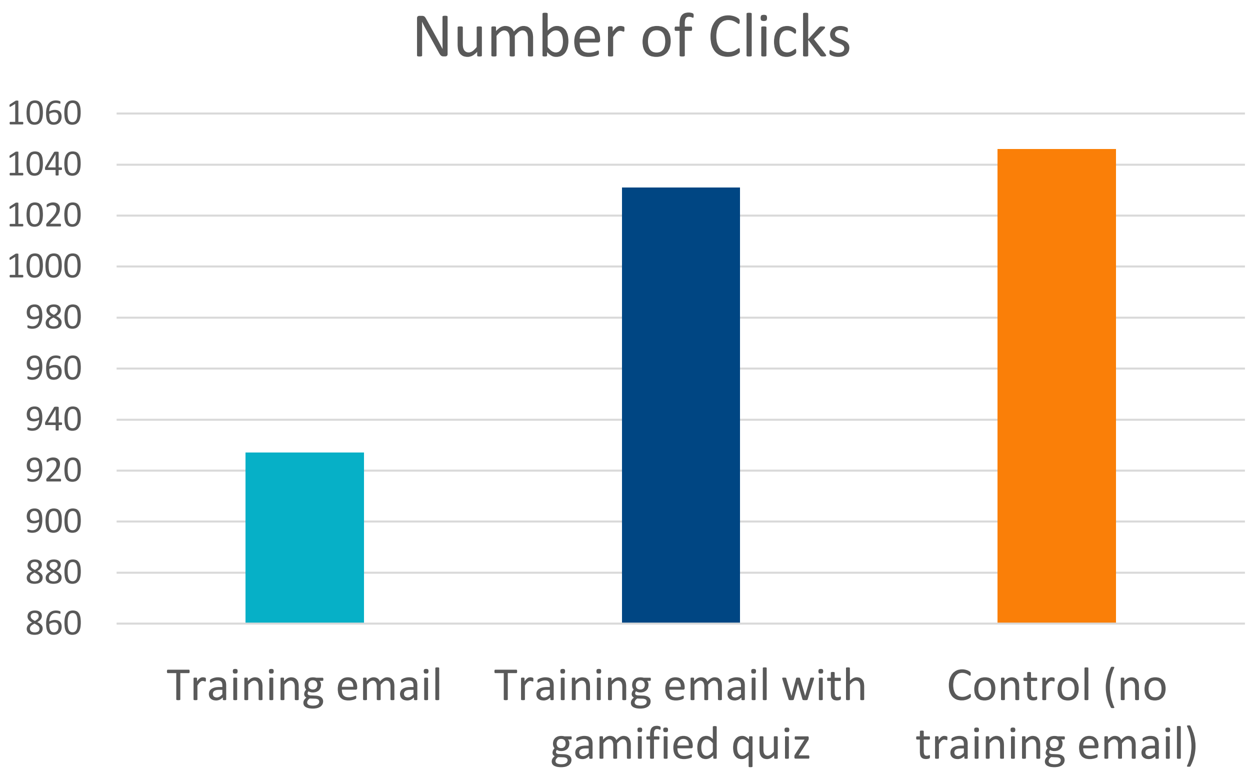
Are These Results Meaningful?

Reduction in the number of clicks

- Training email with no quiz resulted in 119 fewer clicks (11.4% reduction) compared to control

Fewer employees interacting with phishing

- Email with no quiz would represent 332 fewer clicks across the BC Public Service (practical significance)



Intervention Satisfaction and Acceptability

Well-received + promising

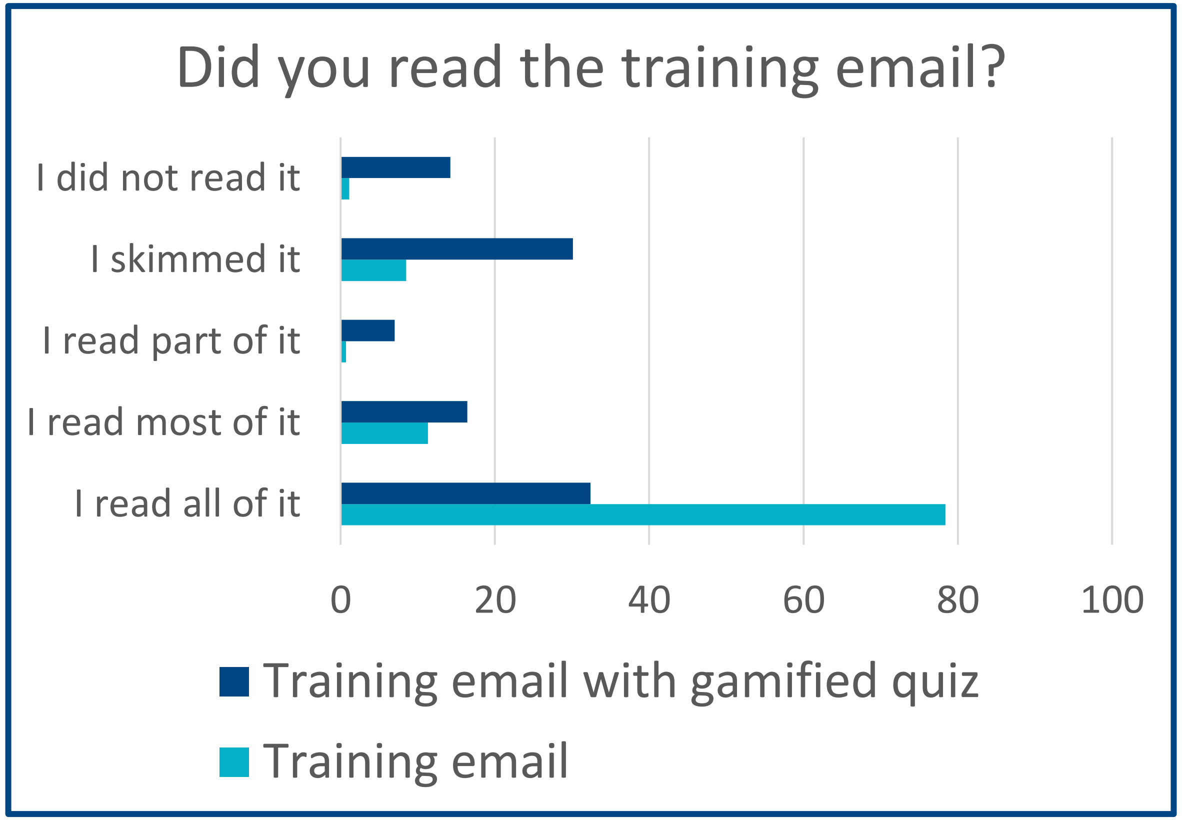
- Over 90% of respondents in both conditions reported feeling better equipped to identify suspicious emails after receiving the training.

Positive + constructive feedback

- Feedback was largely positive with some suggestions for improvement and recommendations for additional training.

Differences in read rates

- Very few (1%) reported not reading the email with no quiz as compared to 14% who did not read the email with gamified quiz.



Discussion

Conclusions

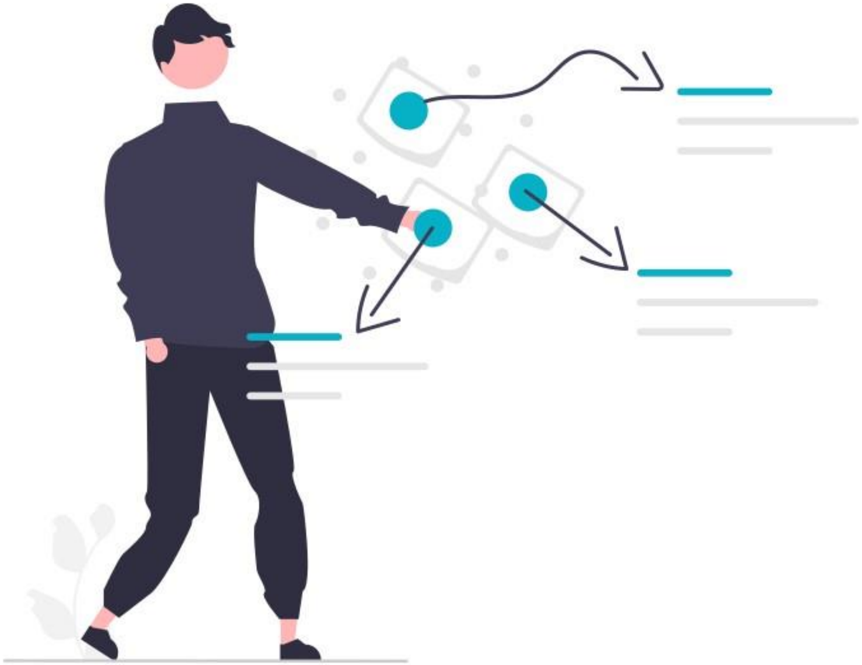
- The training email with no quiz was effective

- Improved employees’ ability to identify possible threats and may reduce phishing interaction in the near-term

- Intervention satisfaction was high

- Support for implementation of email-based training

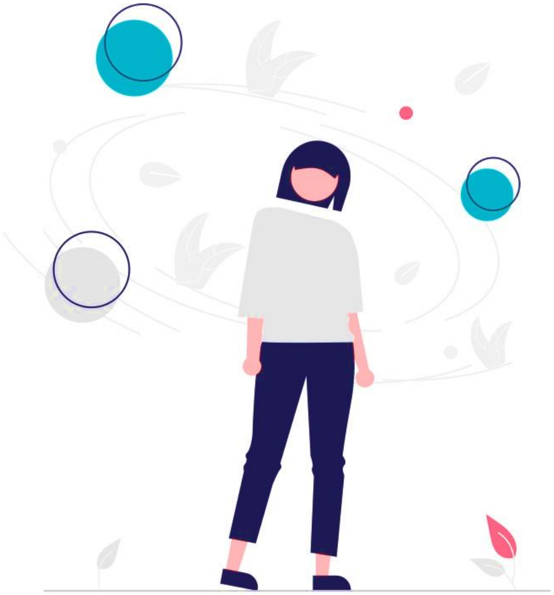
- Findings can inform future anti-phishing efforts



Interesting Findings

- **The optional gamified quiz activity was not effective**
  - Hesitancy around clicking the link
  - Recipients may be busy
  - Game-based learning might perform better in a different context
  - More sophisticated gamification may be necessary

- **Differences in read rates**
  - Placement of quiz link likely contributed to this pattern
  - Plausible participants did not receive key info and tactics



Future Directions

- Intervention exposure
- Duration of the effects
- Optimal frequency of training
- Protection against phishing of varying difficulty
- Additional strategies to combat phishing

Thank You!

Contact: Stina Grant – stina.grant@gov.bc.ca