

**Note:**

Information and data shared in this site may be classified or sensitive. These publications and documents are intended for NYP Staff only. Please do NOT download and others.

## Awareness

### FY23 WOG Simulated Phishing Email Scenarios

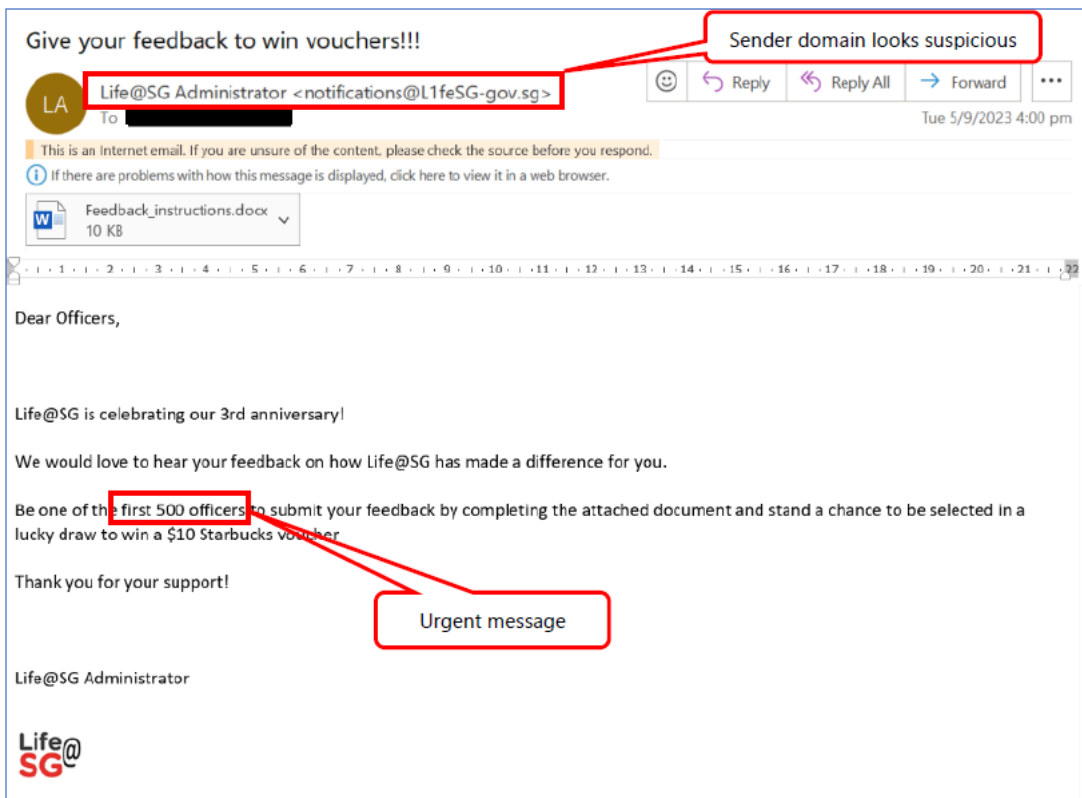
The below shows the emails that were used in the FY23 WOG Simulated Phishing Email Scenarios. The tell-tale signs are highlighted with red outline.

Remember: Always think and verify before you click. [Report](#) if in doubt!

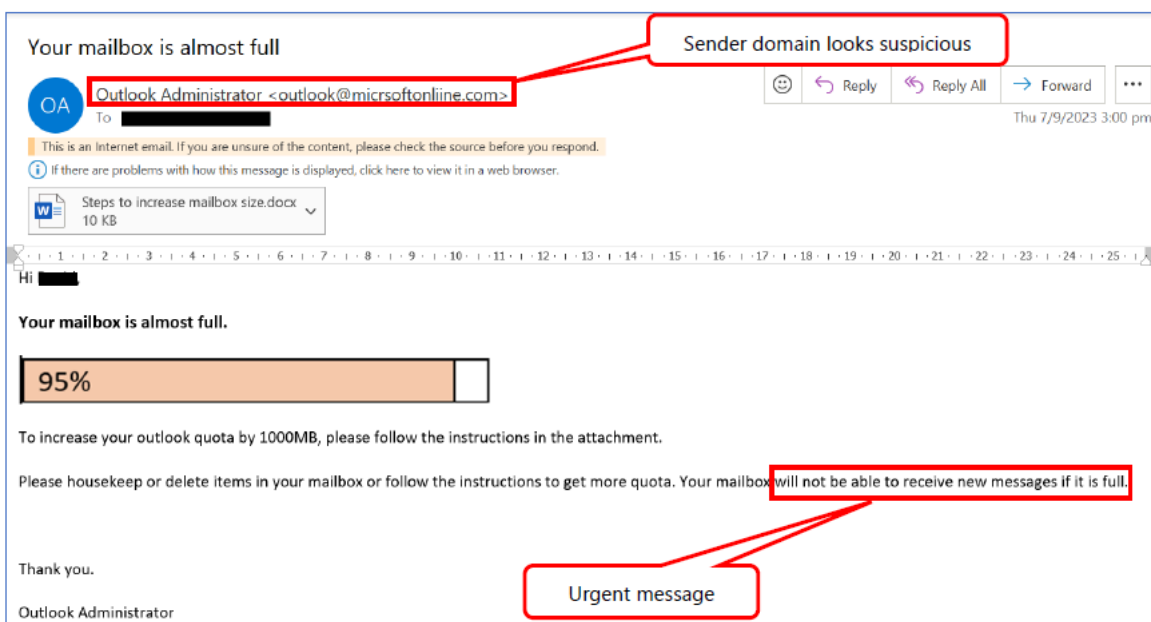
#### Scenario 1 - Unusual sign-in activity



#### Scenario 2 - Free vouchers



## Scenario 3 - Mailbox Full



## How to spot a phishing email?

Phishing is a cybercrime in which a target or targets are contacted by email, telephone or text message by someone posing as a legitimate institution to lure individual sensitive data such as personally identifiable information, banking and credit card details, and passwords. The information is then used to access important accounts an identity theft and financial loss.

### Common Features of Phishing Emails

1. **Too Good To Be True** - Lucrative offers and eye-catching or attention-grabbing statements are designed to attract people's attention immediately. For instance, you have won an iPhone, a lottery, or some other lavish prize. Just don't click on any suspicious emails. Remember that if it seems too good to be true, it probably
2. **Sense of Urgency** - A favorite tactic amongst cybercriminals is to ask you to act fast because the super deals are only for a limited time. Some of them will even have only a few minutes to respond. When you come across these kinds of emails, it's best to just ignore them. Sometimes, they will tell you that your account w unless you update your personal details immediately. Most reliable organizations give ample time before they terminate an account and they never ask patrons t personal details over the Internet. When in doubt, visit the source directly rather than clicking a link in an email.
3. **Hyperlinks** - A link may not be all it appears to be. Hovering over a link shows you the actual URL where you will be directed upon clicking on it. It could be com or it could be a popular website with a misspelling, for instance [www.bankofarnerica.com](http://www.bankofarnerica.com) - the 'm' is actually an 'r' and an 'n', so look carefully.
4. **Attachments** - If you see an attachment in an email you weren't expecting or that doesn't make sense, don't open it! They often contain payloads like ransomwv viruses. The only file type that is always safe to click on is a .txt file.

5. **Unusual Sender** - Whether it looks like it's from someone you don't know or someone you do know, if anything seems out of the ordinary, unexpected, out of context or suspicious in general don't click on it!

The example below was an email that was being used in the recent WOG Simulated Phishing Exercise. The email was crafted to look like a genuine request to check for activity' and sent using a masqueraded authority source - Microsoft Cloud 365 Security.

The tell-tale signs are highlighted in **red**.



It can be really difficult to spot a phishing email as technologies and techniques of malicious actors improve. Below are more red flags that you should look out for.

Remember: Always think and verify before you click. [Report](#) if in doubt!

# Social Engineering Red Flag



## FROM

- I don't recognize the sender's email address as someone I **ordinarily communicate with**.
- This email is from **someone outside my organization and it's not related to my job responsibilities**.
- This email was sent from **someone inside the organization** or from a customer, vendor, or partner and is **very unusual or out of character**.
- Is the sender's email address from a **suspicious domain** (like micorsoft-support.com)?
- I **don't know the sender personally** and they **were not vouched for** by someone I trust.
- I **don't have a business relationship** nor any past communications with the sender.
- This is an **unexpected or unusual email** with an **embedded hyperlink or an attachment** from someone I haven't communicated with recently.



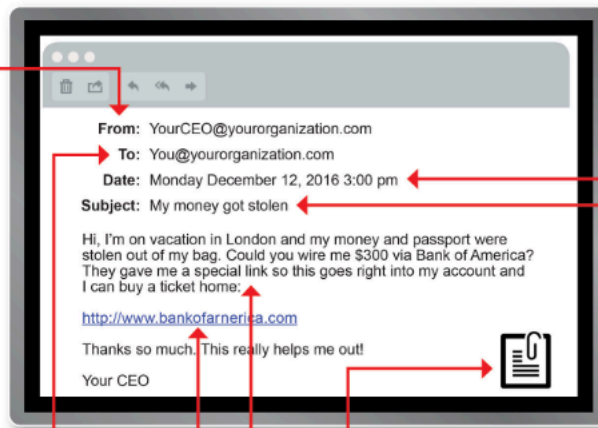
## TO

- I was cc'd on an email sent to one or more people, but I **don't personally know** the other people it was sent to.
- I received an email that was also sent to an **unusual mix of people**. For instance, it might be sent to a random group of people at my organization whose last names start with the same letter, or a whole list of unrelated addresses.



## HYPERLINKS

- I hover my mouse over a hyperlink that's displayed in the email message, but the **link-to address is for a different website**. (This is a **big red flag**.)
- I received an email that only has **long hyperlinks with no further information**, and the rest of the email is completely blank.
- I received an email with a **hyperlink that is a misspelling** of a known web site. For instance, [www.bankofamerica.com](http://www.bankofamerica.com) — the "m" is really two characters — "r" and "n."



## DATE

- Did I receive an email that I **never get** during regular business hours that was **sent at an unusual time**?



## SUBJECT

- Did I get an email with a subject that is **irrelevant or does not match** the content?
- Is the email message a reply to an email that I **never sent or requested**?



## ATTACHMENTS

- The sender included an email attachment that I **was not expect** and it **makes no sense** in relation to the email message. (This sender does not ordinarily send me this type of attachment.)
- I see an attachment with a possibly **dangerous file type**. The one that is **always safe to click on is a .txt file**.



## CONTENT

- Is the sender asking me to click on a link or open an attachment to **avoid a negative consequence** or to **gain something of value**?
- Is the email **out of the ordinary**, or does it have **bad grammar or spelling errors**?
- Is the sender asking me to click a link or open up an attachment that **seems odd**?
- Do I have an **uncomfortable gut feeling** about the sender's request to open up or click a link?
- Is the email asking me to look at a **compromising or embarrassing picture** of someone I know?

## Cyber Security Training

Click image below to access [www.learn.gov.sg](http://www.learn.gov.sg) to complete BDLCD1: Cyber Security, BDLCD2: Data Protection, BDLCD3: Incident Management modules. You are strongly encouraged to watch BDLCD4: Cyber Tips on How to Spot Phishing (2 mins)

and BDLCD5: Cyber Tips on Strong Passwords and Enabling 2FA (1 min), for useful cyber hygiene tips.

Tips: You may wish to refresh your knowledge on cyber security and data protection, click [here](#) for the 3 e-learning modules that will bring you up to speed before attending the training.

## HOW CYBER & DATA SAFE ARE YOU?

COMPLETE THE MANDATORY 2022 CYBER SECURITY AND DATA PROTECTION QUIZ TODAY

To instil a stronger cyber and data security culture across the Whole-of-Government, all public officers must stay vigilant and be aware of ever-changing threats. To ensure everyone has basic cyber and data hygiene practices, all public officers must complete the "2022 Cyber Security & Data Protection Quiz" on the CSC LEARN app or at [www.learn.gov.sg](https://www.learn.gov.sg) by 31 December 2022.

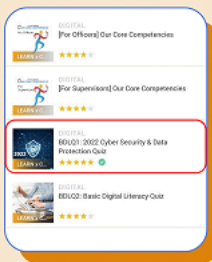
"BDLQ01: Cyber Security", "BDLQ02: Data Protection" and "BDLQ03: Incident Management" modules have been updated with new content. Public officers may complete the 3 modules to better prepare themselves for the quiz.

### Complete the quiz!

- 1 Launch the CSC LEARN app
- 2 Click/tap "Discover" at the bottom of your screen

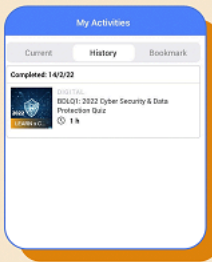


- 3 Under "Core WOG Modules" look for "BDLQ1: 2022 Cyber Security & Data Protection Quiz"



### Alternatively

- 4 Type "BDLQ1" in the search bar at the top of the screen
- 5 After successfully completing the quiz, click/tap on "My Activities". Under the "History" tab, check that your completion of the quiz is reflected correctly.



If you haven't already done so, download the CSC LEARN app now! Scan the QR code below and install the app on your smart device.

Alternatively, you can visit [www.learn.gov.sg](https://www.learn.gov.sg) on your work laptop\* or internet-enabled desktop computer/ laptop to access your modules and quiz.

\*Note: This applies to non-Secret (non-S) laptops that have no access to documents or emails that are classified as Secret.

Please refer to the attached user guide for step-by-step instructions to complete the quiz.



Brought to you by GovTech, SINGO and Civil Service College.



- Using Data Securely 2019
- Cyber and Data Security Awareness Briefing 2019

- Cyber and Data Security Awareness Briefing 2020
- Cyber and Data Security Awareness Briefing 2021
- Information Protection & Security Awareness 2021
- Advisory on Using Commercial Messaging Platforms for Work Collaboration and Coordination 2021

## Advisories and Alerts



- GITSIR's Security Announcements for Last and Prevailing Months
- NRIC Advisory Guidelines for Public Sector Agencies

## How to Go Safe Online



- <https://www.csa.gov.sg/gosafeonline>
- <https://facebook.com/gosafeonline>
- <https://twitter.com/gosafeonline>

### Note:

Information and data shared in this site may be classified or sensitive. These publications and documents are intended for NYP Staff only. Please do NOT download and others.