CyberSecurity

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 anc others.

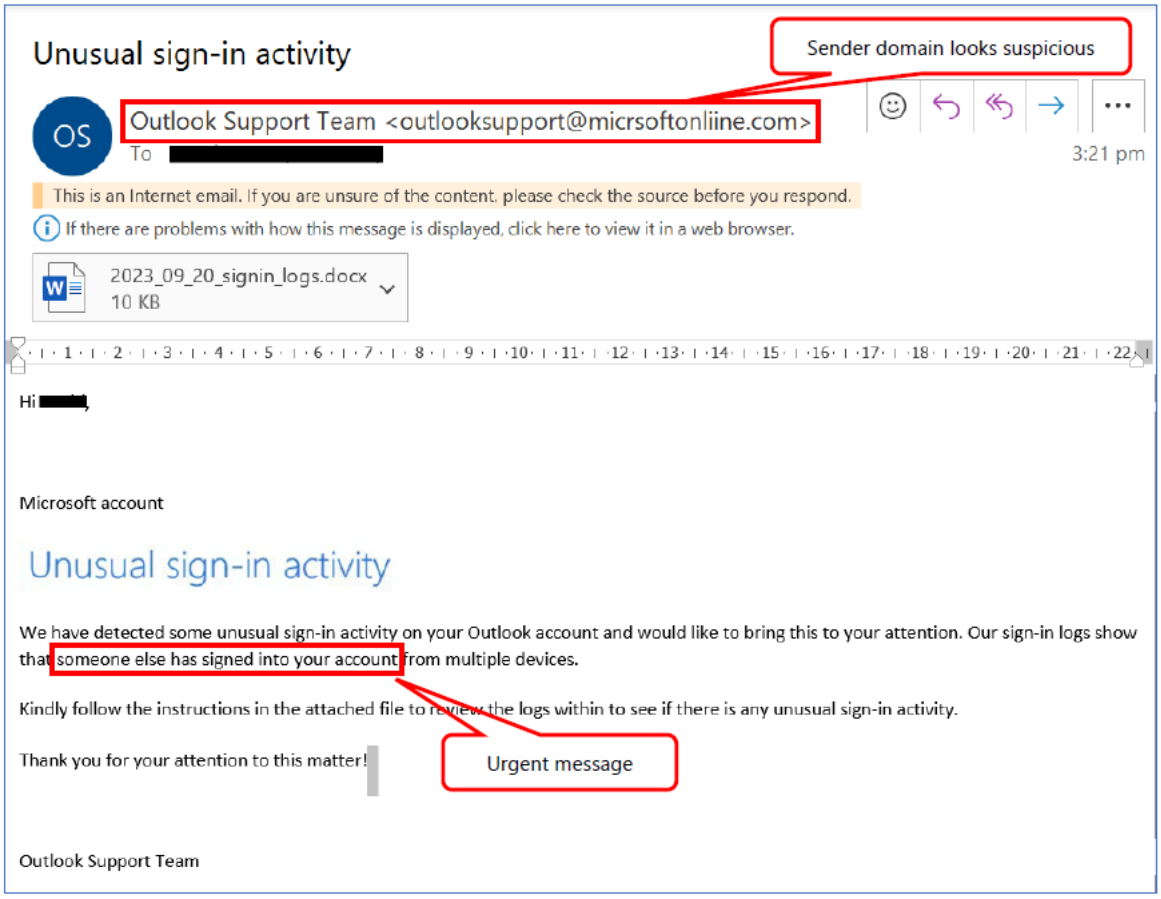
Awareness

FY23 WOG Simulated Phishing Email Scenarios

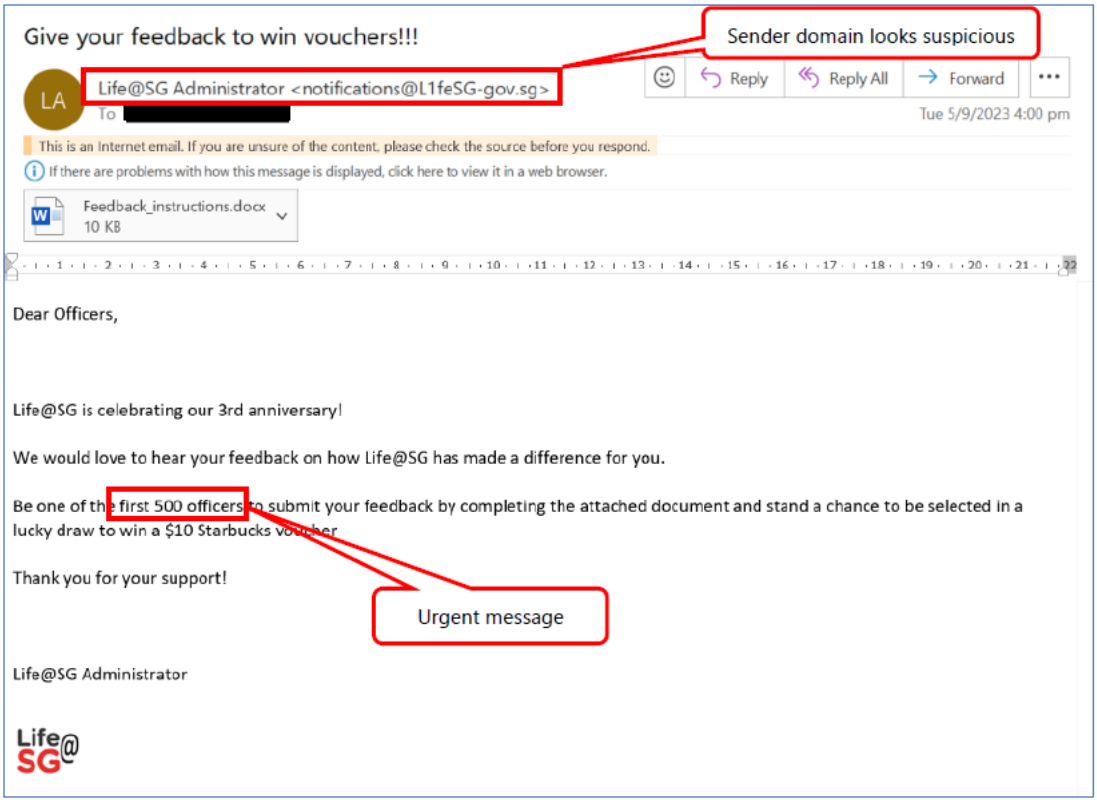
The below shows the emails that were used in the FY23 WOG Simulated Phishing Email Scenaios. The tell-tale signs are highlighted with red outline.

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 sensitve 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 to 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 - 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 ransomwa viruses. The only file type that is always safe to click on is a .txt file.

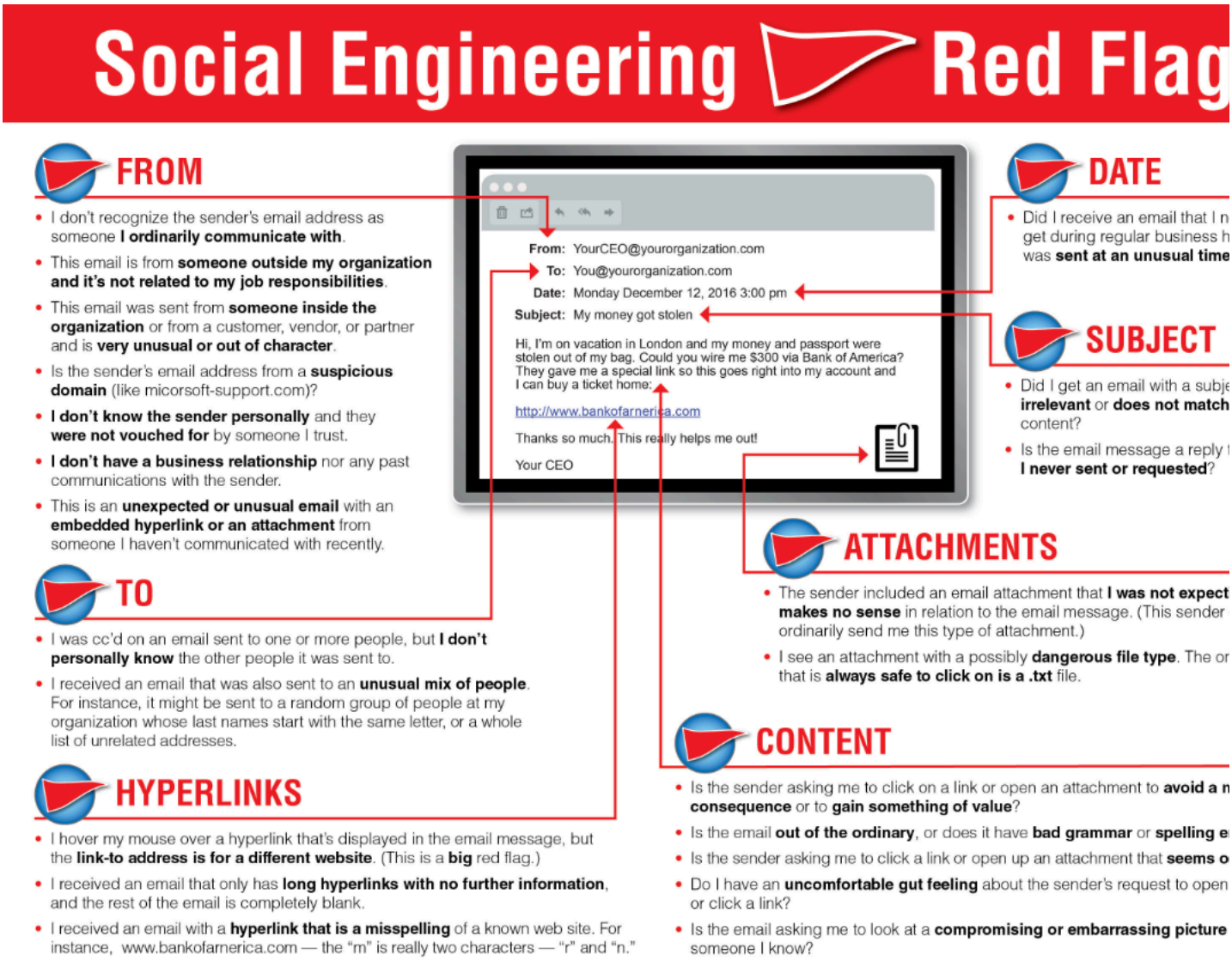
5. **Unusual Sender** - Whether it looks like it's from someone you don't know or someone you do know, if anything seems out of the ordinary, unexpected, out of c suspicious in general don't click on it!

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!

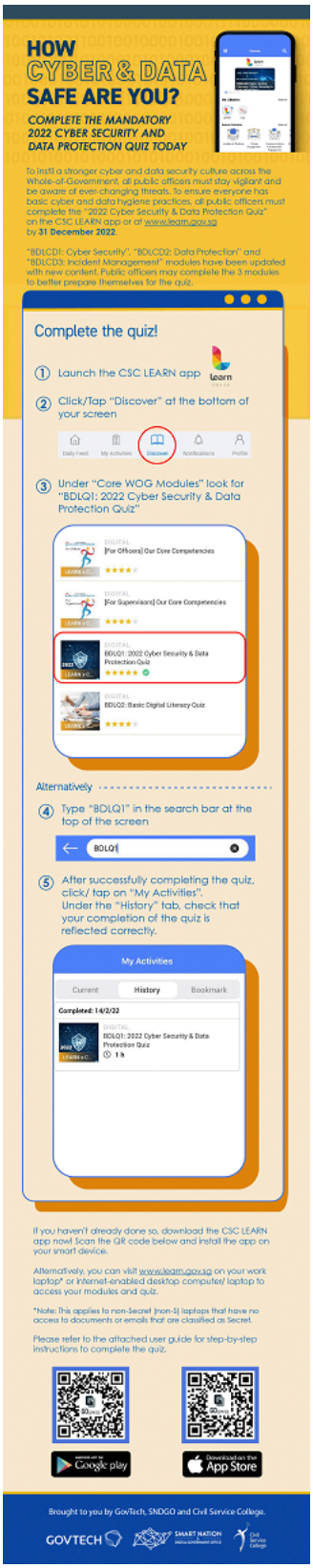


Cyber Security Training

Click image below to access www.learn.gov.sg to complete BDLCD1: Cyber Security, BDLCD2: Data Protection, BDLCD3: Incident Management modules. You are strongl
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 atte



- 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 anc others.