Online Safety

Phishing and Online Safety.

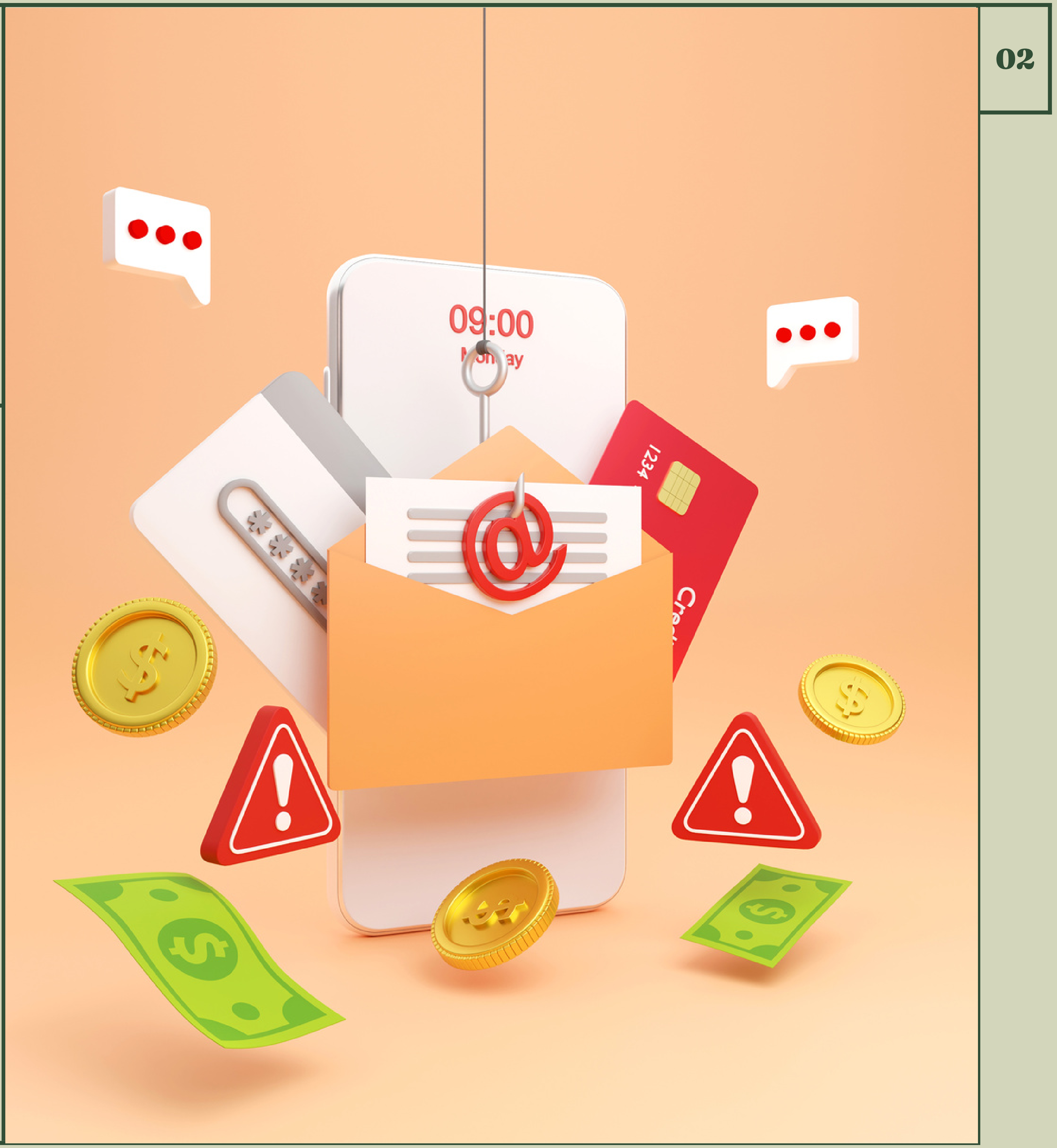
By Rebecca

What is Phishing?

Phishing is an attack that attempts to steal and gain your personal information like: your money, bank details or even your passwords.
Many people around the world are tricked daily into giving out sensitive infomation. But this can all be changed.

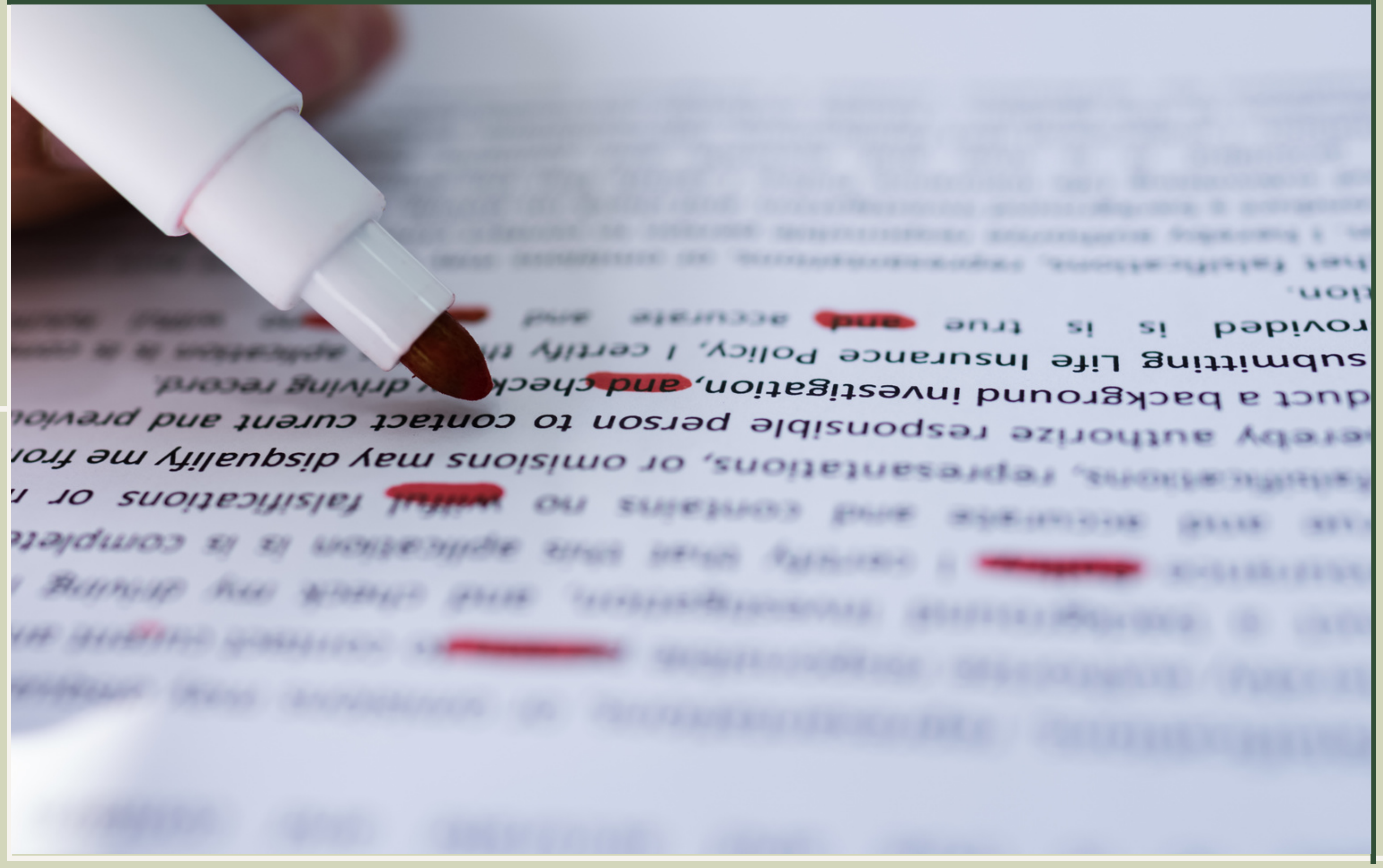
Signs of Phishing

1. The website/email that is sent to you has spelling errors
2. The website/email has suspicious links
3. A email that is sent to you gives a sense of urgency
4. The form asks a lot of personal infomation
5. There is a mismatch between the email and the website



1.Spelling Errors

One of the most common ways to see if there is a phisher is to always check for spelling errors . This is because when there are spelling errors, the website or email. is more likely to be illegitimate.
When on a real website, there would be no grammar mistakes and spelling errors.



Mia was playing on her I-pad when she got a email which read:

You have singed out of ur gnail acount and lost all ur ebails in oreder to log hack in. Click in that link to revibe ur emails.
hppw.gnail.log.in.com
From Ceo of gmails

Should Mia click on the link?
Answer: No, because of all the spelling and grammar mistakes, the website and email is not a legit website

Online Safety

2.Suspicious Links

When one recieves a email including links that are out of the ordinary and seem suspicious, you shouldn't click on the link and instead you should block and report the user.
Real websites will have the format:
https://_______.com.au

While scrollling through Jason's email account, he comes to this email which read:
Want to win a Ihone for free? Click on the link below and recieve the Ihone in 2 days!
hssc.}}hackchildren.com.nz
Should Jason click on the link to get his dream phone?
Answer: No, the link says it all. The word "hackchildren" has shown that it is not a legit website and the link is not in a formal format.

Online Safety

3. Urgency

A sense of urgency encourages, or even demands, immediate action from the person that they are phishing. It will cause the reader to think that the object is only on for a limited time.

For a limited time only, FitnessPlus will have no joining fee and will also will have a two week fitness club for 5 dollars for two days!
Go to https://www.fitnessplus.com.au/ and enrol now to get the limited time offer!

Should you click on it?
Answer: Yes you can, as there are no errors nor any suspicious links.

4.Personal Infomation

Phishers use forms in order to get personal infomation and to gain ones details. Instead of filling out all the questions, one should close the website and report.

While walking down the street, Sarah has been asked to fill out a form. On it read:

1. What is your full name?
2. When are you born?
3. What is your bank number and password?
4. What is your email?

Sarah was told that the imfomation was used to get more infomation about how people lived in the city. Should she fill the form or ignore it?

Answer: No, when questions start to envade your privacy, you should:

1. ignore the form
2. write false infomation

5. A Mismatch

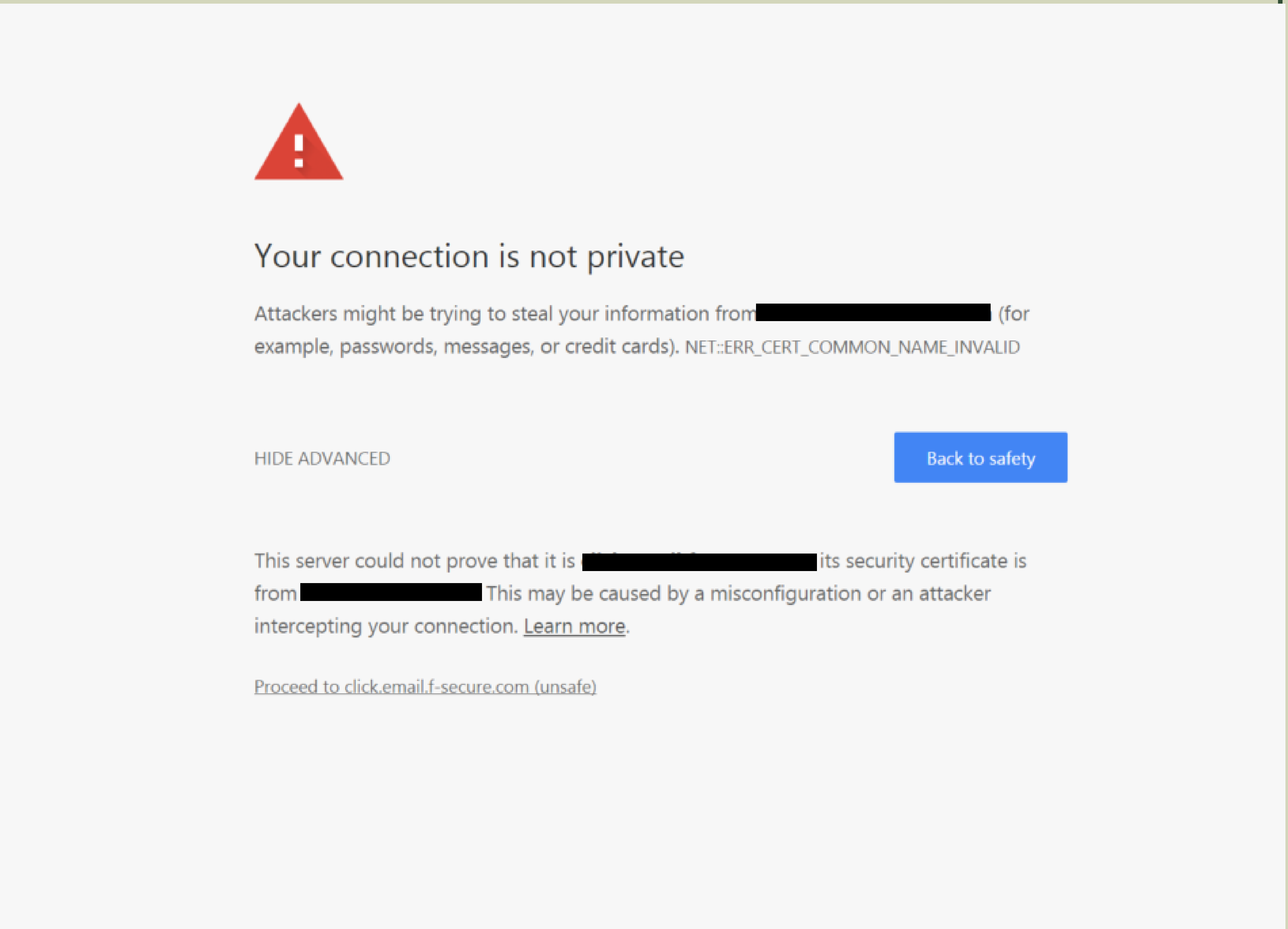
Online Safety

When there is an mismatch between the infomation and the email address you know that it is not trustworthy. For example you recieve a email from paypal but when you click on the link, the domain name has nothing to do with paypal. You should immediately close the tab and do not provide any details.

When Fred recieved an email, it had attachment with it but before checking, Fred looked at the link which wrote Oreo Factory but when he put the mouse on the link, it read faketimtams.nz.hppt.au

Should Fred click on the link?

Answer: No, this is because there is a mismatch between the infomation which may cause suspicion



Your connection is not private

Attackers might be trying to steal your information from [redacted] (for example, passwords, messages, or credit cards). NET::ERR_CERT_COMMON_NAME_INVALID

This server could not prove that it is [redacted] its security certificate is from [redacted] This may be caused by a misconfiguration or an attacker intercepting your connection. Learn more.

Proceed to click.email.f-secure.com (unsafe)

An Overview

In order to prevent phishing, you need to consider:

- Are there any spelling error?
- Does the email have any suspicious links?
- If the email sent to you gives a sence of urgency
- If the form asks a lot of personal infomation
- If here is a mismatch between the email and the website

Remember, always think before you act. When you think that you are being phished, you should block report to an adult. Always think, look and ask before you click.