

# WELCOME TO PHISHING TEST REVIEW!



Reply All Forward



If you want to learn more about phishing indicators or are curious about the last phishing test you clicked on, you're in the right place.

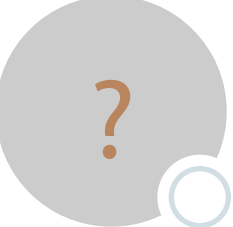
The emails in this document are for phishing tests from **January 2021 to June 2021**. This document will be updated monthly.

Phishing Indicators in Emails

Test 10: Tax Refund

Can you spot the phishing indicators?

Tax Refund



Tax Refund <noreply@taxinfo.com>  
To ● Ahmad Zaini (CS-DO/DIGITAL)

Reply Reply All Forward

Wed 3/17/2021 10:36 AM

We could not verify the identity of the sender. Click here to learn more.  
Click here to download pictures. To help protect your privacy, Outlook prevented automatic download of some pictures in this message.

Dear myPasport User,

You have received a tax refund payment of MYR309.35 from i-Sinar into your respective Banking Account.

Please click on [Sign In](#) to i-Sinar to accept your incoming funds.

The money will appear in your account in 3-5 working days. A refund can be delayed for a variety of reasons. For example submitting invalid, out of date records or applying after the end of the application deadline.

Best Regards,  
Inland Revenue



Here are the indicators showing that this could be a potential phishing email

Tax Refund



Tax Refund <noreply@taxinfo.com>  
To ● Ahmad Zaini (CS-DO/DIGITAL)

Reply Reply All Forward

Wed 3/17/2021 10:36 AM

We could not verify the identity of the sender. Click here to learn more.  
Click here to download pictures. To help protect your privacy, Outlook prevented automatic download of some pictures in this message.

Dear myPasport! User,

You have received a tax refund payment of MYR309.35 from i-Sinar into your respective Banking Account.

Please click on [Sign In](#) to i-Sinar to accept your i

The money will appear in your account in 3-5 working days. A refund can be delayed for a variety of reasons. For example submitting invalid, out of date records or applying after the end of the application deadline.

Best Regards,  
Inland Revenue

Unofficial email sender - not from PETRONAS

Spelling error - myPassport instead of myPasport

Hover on "here" shows the suspicious link

Sense of urgency; creates panic



Social engineering tactic:

This message plays into financial gain - a lot of people like getting money! If you weren't expecting this and/or don't recognize why, it's always wise to verify the sender and the link before clicking and providing any information.



## Phishing Indicators in Emails

# Test 11: Mobile Promotion

Can you spot the phishing indicators?

### Pavillion Special Offer

 Pavillion Special Offer <info@pavipromo.com>  
To ● Ahmad Zaini (CS-DO/DIGITAL)


Reply

Reply All

Forward

...

Wed 3/17/2021 10:36 AM

 We could not verify the identity of the sender. Click here to learn more.  
Click here to download pictures. To help protect your privacy, Outlook prevented automatic download of some pictures in this message.

Exclusive offer!

This is a one time offer of 25% off the latest Oppa phone of your choice. Grab this opportunity while you can! Limited to 500 registrants only, first come first serve basis (terms and conditions apply).

Click [here](#) to register.

Oppa Marketing Pte. Ltd.

Here are the indicators showing that this could be a potential phishing email

### Pavillion Special Offer

 Pavillion Special Offer <info@pavipromo.com>  
To ● Ahmad Zaini (CS-DO/DIGITAL)

Reply

Reply All

Forward

...

Wed 3/17/2021 10:36 AM

 We could not verify the identity of the sender. Click here to learn more.  
Click here to download pictures. To help protect your privacy, Outlook prevented automatic download of some pictures in this message.

Exclusive offer!

Sense of urgency

Spelling error and disguised as Oppa instead of Oppo

This is a one time offer of 25% off the latest Oppa phone of your choice. Grab this opportunity while you can! Limited to 500 registrants only, first come first serve basis (terms and conditions apply).

Click [here](#) to register.

[https://www.onlineservicetec.com/link/i/ivr57o64d52mb-lb9hstarws\\_2tifmr3gjvbf2ggijr6ybf1v\\_zhcvudc3cnwtv](https://www.onlineservicetec.com/link/i/ivr57o64d52mb-lb9hstarws_2tifmr3gjvbf2ggijr6ybf1v_zhcvudc3cnwtv)

Click or tap to follow link.

Oppa Marketing Pte. Ltd.

Hover on "here" shows the suspicious link – URL not related to sender, subject & content (Pavillion & Oppo) at all

### Social engineering tactic:

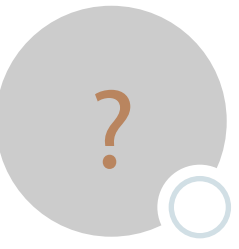

This message plays into free stuff - a lot of people like getting free phones! Remember - if it sounds too good to be true, it probably is - especially if it comes out of nowhere! More often than not, these are scams designed to either get personal information for other (often nefarious) purposes.




# Test 12: Survey (Return to Office)

Can you spot the phishing indicators?

## Survey - Return to Office

 PETRONAS Survey <info@petronassurvey.com>  
To  Ahmad Zaini (CS-DO/DIGITAL)

 We could not verify the identity of the sender. Click here to learn more.  
Click here to download pictures. To help protect your privacy, Outlook prevented automatic download of some pictures in this message.

Dear Employee,

Is has been a year since we embarked on this joruney of working from home.  
With the new arrangements in place, how eager are you to return to work in office?



We would like to hear from you! Participate in the survey below to voice out your opinion  
by login with your enterprise ID,


Your voice matters to us.

[Complete your survey here.](#)

Here are the indicators showing that this could be a potential phishing email

## Survey - Return to Office

 PETRONAS Survey, <info@petronassurvey.com>  
To  Ahmad Zaini (CS-DO/DIGITAL)

 We could not verify the identity of the sender. Click here to learn more.  
Click here to download pictures. To help protect your privacy, Outlook prevented automatic download of some pictures in this message.

Dear Employee,

Is has been a year since we embarked on this joruney of working from home.  
With the new arrangements in place, how eager are you to return to work in office?

We would like to hear from you! Participate in the survey below to voice out your opinion  
by login with your enterprise ID,

Your voice matters to us.

[Complete your survey here.](#)

Unofficial Email sender –  
not from PETRONAS

Generic greeting - PETRONAS comms seldom/  
do not use "Dear Employee"

Spelling error -  
journey instead of jorney

<https://www.solutionfun.info/link/l/h4qyhms24z4dds3soklf1nw63vuzbsc2hy6-i0odbgwo4xwdhqx438i7v7bpklwj>

Click or tap to  
follow link.

Hover on "here" shows the suspicious link –  
URL not related to sender,  
subject & content to PETRONAS at all

## Social engineering tactic:

This message plays into personal emotions. In today's situation, work-from-home can trigger feelings of worry, anxiety, excitement or even annoyance - as a result, sometimes readers will click on the link without pausing to check for phishing indicators. If you are ever faced with this type of email, some immediate checks you can do is to validate the sender and the link - official PETRONAS emails will typically use the PETRONAS email domain and use approved tools or sites (i.e. NOT www. solutionfun.info!).




# Test 13: Update Banking Info

Can you spot the phishing indicators?

## Update Banking Information

Update Banking Info <info@petronassupdate.com>  
To ● Ahmad Zaini (CS-DO/DIGITAL)  
Wed 3/17/2021 10:36 AM

 We could not verify the identity of the sender. Click here to learn more.  
Click here to download pictures. To help protect your privacy, Outlook prevented automatic download of some pictures in this message.

Hi,

Due to the recent system corruption, we have lost your banking information with us.


Do update and confirm your latest banking informtaion with us to avoid unnecessary delay in your salary payment immediately!

Click [here](#) to update and login with your enterprise ID.

Here are the indicators showing that this could be a potential phishing email

## Update Banking Information

Update Banking Info <info@petronassupdate.com>  
To ● Ahmad Zaini (CS-DO/DIGITAL)  
Wed 3/17/2021 10:36 AM

 We could not verify the identity of the sender. Click here to learn more.  
Click here to download pictures. To help protect your privacy, Outlook prevented automatic download of some pictures in this message.

Hi,

Due to the recent system corruption, we have lost your banking information with us.

Do update and confirm your latest banking informtaion with us to avoid unnecessary delay in your salary payment immediately!

Click [here](#) to update and login with your enterprise ID.

<https://www.solutionfun.info/link//h4qyhms24z4dds3soklf1nw63vuzbsc2hy6-i0odbgwo4xwdhqx438i7v7bpklwj>  
Click or tap to follow link.  
Hover on "here" shows the suspicious link – URL not related to sender, subject & content to PETRONAS at all

## Social engineering tactic:

This message plays into panic - nobody likes having their salary delayed. However it's important to remember that emails asking for employee information for company use should always come from a company email - that's the first sign there is something wrong with this message. Knowing to check for the phishing indicators may also help you to identify what is a valid request for information vs. one that is phishing you for your personal information.



# Test 14: Employee Evaluation

Can you spot the phishing indicators?

## Employee Evaluation Q1

Employee Evaluation <update@petronas-performance.com>  
To Ahmad Zaini (CS-DO/DIGITAL)

We could not verify the identity of the sender. Click here to learn more.  
Click here to download pictures. To help protect your privacy, Outlook prevented automatic download of some pictures in this message.

Dear Employee,

PETRONAS takes employee performance seriously.  
As part of a new initiative, all managers will conduct routine evaluations of all team members quaterly.

Your supervisor has just uploaded your evaluation for Q1.  
Please use your company ID and password to access the [secure website](#) and add your comments.

Thanks,  
Human Resources Team

Here are the indicators showing that this could be a potential phishing email

## Employee Evaluation Q1

Employee Evaluation: <update@petronas-performance.com>  
To Ahmad Zaini (CS-DO/DIGITAL)

We could not verify the identity of the sender. Click here to learn more.  
Click here to download pictures. To help protect your privacy, Outlook prevented automatic download of some pictures in this message.

Dear Employee,

PETRONAS takes employee performance seriously.  
As part of a new initiative, all managers will conduct routine evaluations of all team members quaterly.

Your supervisor has just uploaded your evaluation for Q1.  
Please use your company ID and password to access the [secure website](#) and add your comments.

Thanks,  
Human Resources Team

Unofficial email sender - not from PETRONAS

Generic greeting – PETRONAS does not address users as 'Dear Employee'

Spelling error – routine instead of rote and quarterly instead of quaterly

https://www.onlinefreemedia.com/link/le\_kwltjefv2y-u7kqv\_ohynfrs9skhdc5lkqeyanxhj6pqnlrdl3mamsoqt3jvn

Click or tap to follow link.

Hover on "here" shows the suspicious link – URL not related to sender, subject & content to PETRONAS at all

## Social engineering tactic:

This message plays into both curiosity and perhaps panic - what did my supervisor say? Similar to queries for personal information, this type of company-related process should come from a company email address. Alongside other common indicators, it's also worth noting that most company systems have a name - 'secure website' is a little suspicious, so it's always worth hovering over the link to check if it really is a PETRONAS website.



Phishing Indicators in Emails

Test 15: Outlook Mails (On-hold)

Can you spot the phishing indicators?

You have 7 Incoming Messages on Hold

Office 365 Outlook <notification@out-look.com>  
To ● Ahmad Zaini (CS-DO/DIGITAL)

Reply Reply All Forward ...  
Wed 3/17/2021 10:36 AM

We could not verify the identity of the sender. Click here to learn more.  
Click here to download pictures. To help protect your privacy, Outlook prevented automatic download of some pictures in this message.

Microsoft Office 365 Outlook

Dear Recipient,

Office 365 Outlook has prevented the delivery of 7 new emails to your inbox as of 22 Apr 2021 and they are awaiting your approval for delivery.

Review your email storage here and restore delivery of pending messages to [ahmad.zaini@petronas.com.my](#).

Review Storage

© 2020 Microsoft Corporation. All rights reserved | [Acceptable Use Policy](#) | [Privacy Notice](#)

Here are the indicators showing that this could be a potential phishing email

You have 7 Incoming Messages on Hold

Office 365 Outlook <notification@out-look.com>  
To ● Ahmad Zaini (CS-DO/DIGITAL)

Reply Reply All Forward ...  
Wed 3/17/2021 10:36 AM

We could not verify the identity of the sender. Click here to learn more.  
Click here to download pictures. To help protect your privacy, Outlook prevented automatic download of some pictures in this message.

Microsoft Office 365 Outlook

Dear Recipient,

Generic greeting – PETRONAS does not address users as 'Dear Recipient'

Office 365 Outlook has prevented the delivery of 7 new emails to your inbox as of 22 Apr 2021 and they are awaiting your approval for delivery.

Sense of urgency

Review your email storage here and restore delivery of pending messages to [ahmad.zaini@petronas.com.my](#).

Review Storage

[https://www.onlinefreemedia.com/link/U/e\\_kwtjtjefv2y-u7kqv\\_ohynfrs9skhdc5lkqeyanxhj6pqnlrdrl3mamsoqt3jvn](https://www.onlinefreemedia.com/link/U/e_kwtjtjefv2y-u7kqv_ohynfrs9skhdc5lkqeyanxhj6pqnlrdrl3mamsoqt3jvn)

Click or tap to follow link.

Hover on "here" shows the suspicious link – URL not related to sender, subject & content to PETRONAS at all

Social engineering tactic:

This message plays into both curiosity and maybe some level of panic/annoyance/FOMO (oh no, I have more emails??). If you're unsure whether something is official and yet sounds urgent, your go-to checks are the accompanying link and the sender.