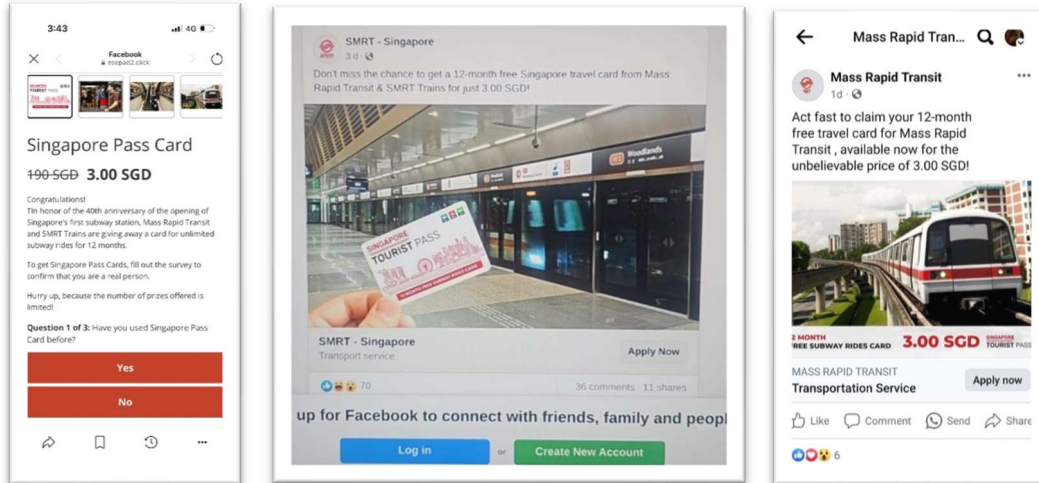


Examples of **scams** utilizing EZ-Link's product name and images



Customers are advised:

- **To check** that the website links belong to the official EZ-Link domain (ending with ezlink.com.sg). If unsure, please contact our customer service at customerservice@ezlink.com.sg.
- **NOT TO** click on hyperlinks found on suspicious social media posts from dubious accounts.
- **NOT TO** reveal personal information/log-in credentials or credit card details to purchase or take part in any promotions. EZ-Link **will never ask** for such information over a web form.

For more information on common signs of phishing, please visit bit.ly/CSA-tips.

Example of a **phishing email** impersonating EZ-Link

EZ-Link Wallet (Possible Inactive Account Alert)



Possible Inactive Account Alert.

It seems that you had no activity with EZ-Link last months .

EZ-Link has determined your account as inactive , when the owner of the inactive account doesn't top up before the given deadline the account and all its data will be permanently deleted.

In order to keep your ezlink wallet please top up at least 1 SGD

[Top-up Wallet](#)

Customers are advised:

- **To check** that the email domain belongs to EZ-Link (ending with [ezlink.com.sg](mailto:customerservice@ezlink.com.sg)). If unsure, please contact our customer service at customerservice@ezlink.com.sg.
- **NOT TO** click on hyperlinks found on suspicious emails with unknown origins.
- **NOT TO** reveal personal information/log-in credentials or credit card details. EZ-Link will never ask for such information over a web form.

For more information on common signs of phishing, please visit bit.ly/CSA-tips.

You can also refer to the following notice from the Singapore Police Force:

BEWARE OF PHISHING SCAMS

THESE ARE THE TYPICAL SCAM MESSAGES

singpost.dealy-safety.online (FAKE)

fedex.safe-ordery.online (FAKE)

saml.grsehse.xyz (FAKE)

sg-paynow.netlify.app (FAKE)

https://dbs.com.in/sg/57LEy (This is not a DBS shortcode. This is not a DBS URL.)

These are not legitimate DBS SMSes.

 **Do not click on dubious URL links provided in unsolicited text messages or emails!**
Banks do not send SMSes containing links!

 **Always verify with the bank or business about the claims of problems!**

 **Never disclose your banking details, SingPass ID, password or OTPs to others!**



For scam-related advice,
please call 1800-722-6688 or visit www.scamalert.sg