

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

EZ-Link Wallet (Possible Inactive Account Alert)



Customers are advised:

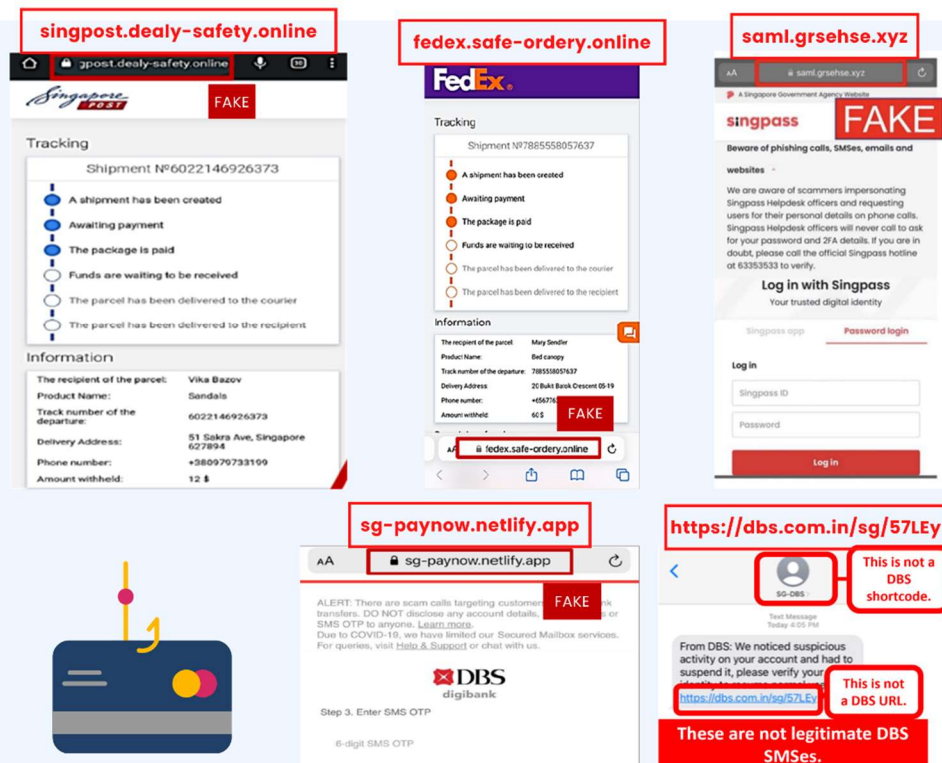
- **To check** that the email domain belongs to EZ-Link (ending with [ezlink.com.sg](mailto:customerservice@ezlink.com.sg)). If unsure, please contact our customer service at customerservice@ezlink.com.sg.
- **NOT TO** click on hyperlinks found on suspicious emails with unknown origins.
- **NOT TO** 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



-  **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