DSBC
Financial Group

#DSBCsecured Guide

"Knowledge is the best defense against cybercrime and fraud"

A brief guide to help you reinforce your knowledge on cybercrime, scam and protect yourself, your business from phishing attacks

Version 01.2020

1 Phishing email usually slightly misspells the official company name/ website address/ domain of email.

Fraudsters may use a slightly different name from the authentic company. These fake brands can lie to users and encourage them to disclose their confidential information.

Some scams attack users by email with fake domains that victims could recognise like "@gmail.com".

To stay safe when encountering the suspicious, you should carefully check the spelling of phishing emails and immediately report to DSBC Financial Europe.

2 Official DSBCnet Internet banking and mobile banking app

Official DSBC*net* Internet Banking

To log into your DSBC*net* account on web browsers you can visit https://www.dsbcf.com/ or https://www.dsbcnet.com/ and follow below steps:

1

Click the **"Online banking"** button on the top right corner.

2

Or click the **"DSBC*net*"** option at the **"Useful links"** on the footer website.

3

Then you will see DSBC*net* landing page: https://www.dsbcnet.com/ and after that click to the **"Log on"** button.

4

The official Login DSBC*net* page is: https://secure.dsbcnet.com/login

Official DSBC*net* Mobile Banking App

To avoid fraudsters from scam mobile applications in stores, DSBC Financial Europe would like to help you recognize the authentic DSBC*net* mobile banking app icons that are available on iOS and Android and the right links to download.

To install the official DSBC*net* mobile banking app, you can download from:

Available on the App Store

The DSBC*net* App Store icon preview

GET IT ON Google Play

The DSBC*net* Google Play icon preview

3 Hoax SMEes that stimulate victimes take action.

Several people may be cheated into providing their personal information and payment card details on phishing SMSes or over the phone, after responding to advertisements via SMSes purposely sent out by DSBC with the content like earning a big number of money, getting great value of promotion, becoming a billionaire and they do attach a link or download file which calls to action.

DSBC Financial Europe sends our clients SMSes with three purposes:

1/ OTP message

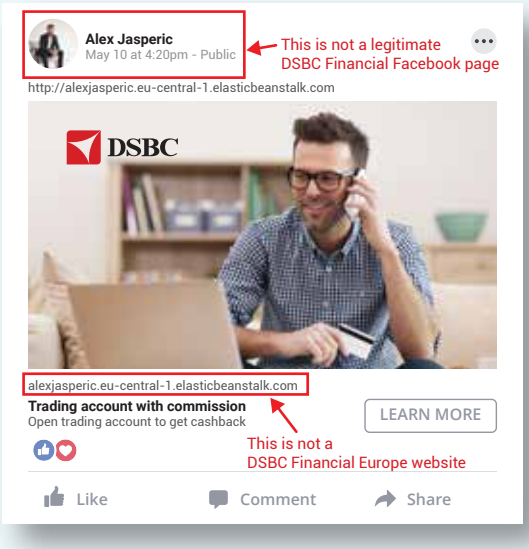
2/ Password changing

3/ Referral Link

If you receive SMSes that claim to be sent from DSBC with content different from the 3 purposes above, please report directly to DSBC Financial Europe hotline.

4 Be caution on social media

There are various advertisements across Facebook, LinkedIn and other channels with promotion content from one of the banks regarding an investment opportunity, fund transfer and huge discount for account opening. Upon clicking the link provided, victims will then be directed to a website that either promoted a new investment product or bank account.



You should be conscious about the host of these advertisements and check the hyperlink whether or not it is the official website of DSBC Financial Europe: www.dsbcf.com or www.dsbc.eu.

Cybercrime evolves their practice continuously, we should stay up-to-date with the new financial secure information to protect ourselves as the first line of defence.