MediaLiteracyCouncilSG

www.betterinternet.sg

Organised by:

MEDIA LITERACY COUNCIL

Supported by:

INFOCOMM MEDIA DEVELOPMENT AUTHORITY

NATIONAL CRIME PREVENTION COUNCIL

pdpc
PERSONAL DATA PROTECTION COMMISSION
SINGAPORE

In association with:

SG:D | GET READY!

BE SAFE

HOW TO SPOT PHISHING SCAMS

DO WHAT'S RIGHT ONLINE

☑ **CREATE** strong passwords

☑ **PROTECT** personal information

☑ **VERIFY** before clicking

✓ **CHECK Please!**

Be Safe. Be Smart. Be Kind.

Before you trust or click, CHECK PLEASE!

Use our checklist of 5 tips to help you spot and counter a phishing scam.

01 KEEP YOUR DETAILS PRIVATE

A phishing scam involves receiving an email that looks like it was sent by a real organisation. It may ask you to provide your personal information, complete a survey, or pay for a product or service.

02 CHECK THE “FROM” ADDRESS

Emails sent from real organisations will use legitimate email addresses. If in doubt, check directly with the organisation to verify the information.

03 EXAMINE THE EMAIL

Look out for spelling or grammar mistakes, or poor-quality graphics. These are signs that the email could be a phishing scam.

04 BEWARE OF PROMISES AND THREATS

Be suspicious of emails that promise attractive rewards if you respond by clicking on the provided link. Ignore emails that bait or threaten you if you don’t respond. Filter or block these as spam (junk mail) in your email settings.

05 VERIFY THE EMAIL

If you suspect that an email from a certain organisation is a scam, forward the email to the actual organisation to verify it. Use the email address on the official website. Alerting the organisation helps keep you and others safe.