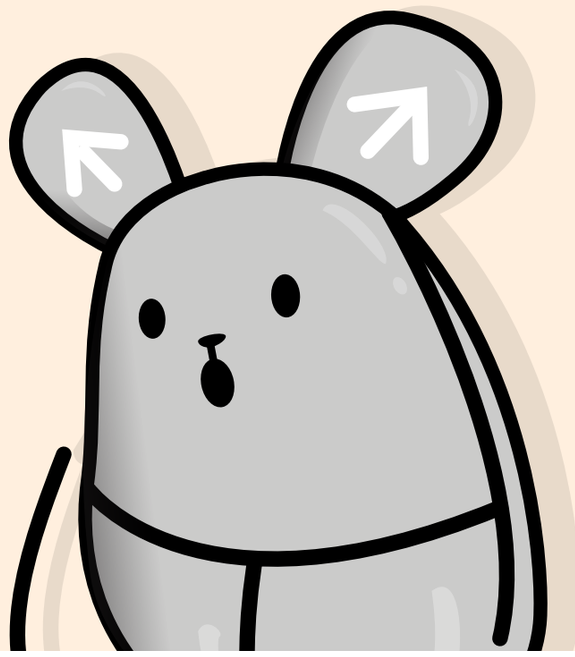
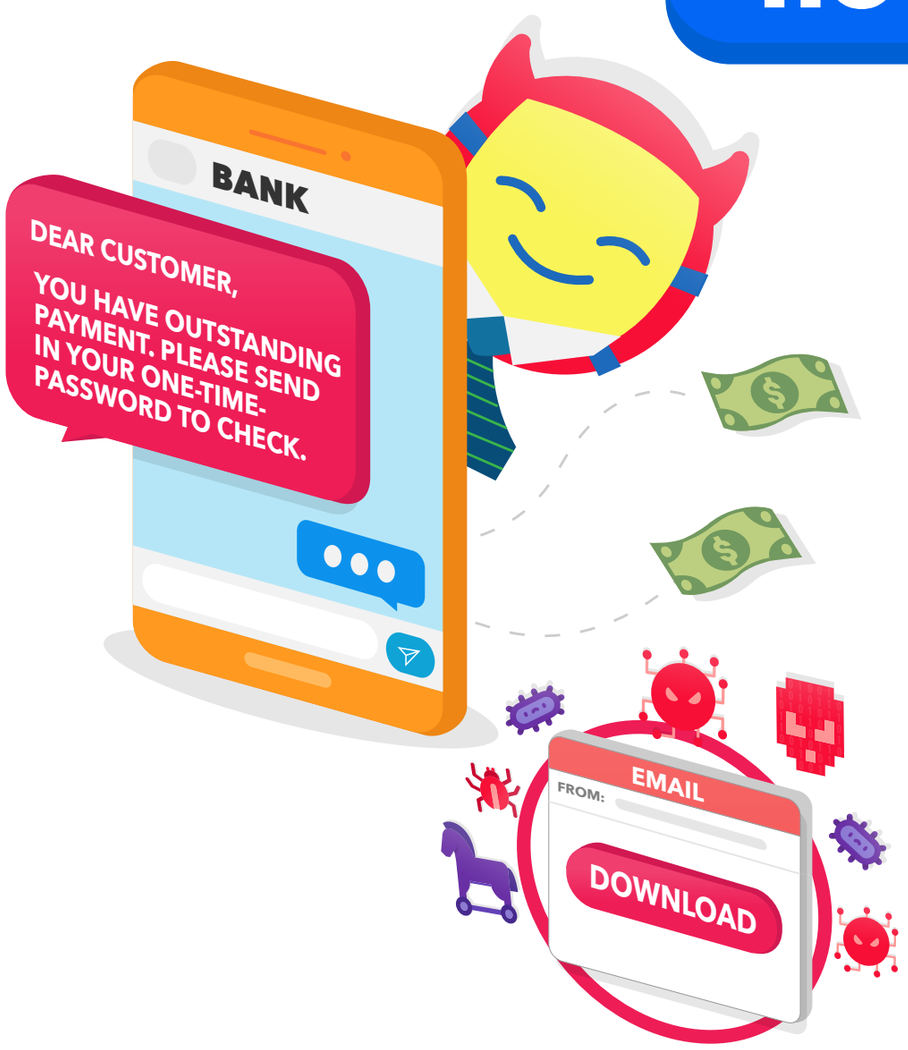
BE SAFE

ONLINE IMPERSONATION SCAMS

Fraud that occurs through fake identities, such as government officials or representatives from banks, credit card companies, or other well-known and trusted companies. Scammers may also use hacked or spoofed social media accounts and pretend to be a family member or a friend.



HOW DOES IT HAPPEN?



- After gaining your trust, scammers will ask for personal information such as your NRIC number, internet banking log-in details, or One-Time Passwords (OTP).
- Their goal is to access your accounts, make fraudulent purchases and impersonate or blackmail you.
- They may also pressure you into making money transfers.
- Scammers may also trick you into installing malware and viruses, or remote desktop applications on your device through suspicious links or file attachments, to extract your private data or control your device remotely.
- They often do so by getting you to click on suspicious links or download file attachments.

WHY DO I NEED TO KNOW THIS?

- During the COVID-19 pandemic, scammers have come up with new impersonation scams, such as posing as Ministry of Health or Ministry of Finance officers. They may also pretend to be contact tracers to trick their victims into releasing personal information.
- Victims of impersonation scams from Singapore were cheated of at least $38 million from January to November 2019 (according to CNA).

1CLICK AWAY
Be Safe · Be Smart · Be Kind

MEDIA LITERACY COUNCIL

#BeSafe

Check Before You Click

Supported by:

INFOCOMM MEDIA DEVELOPMENT AUTHORITY

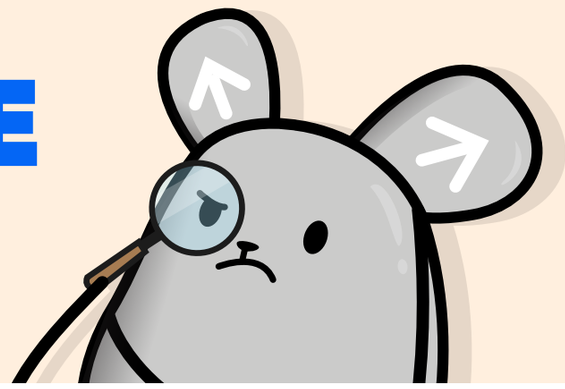
SINGAPORE POLICE FORCE
SAFEGUARDING EVERY DAY

NATIONAL CRIME PREVENTION COUNCIL

In Support of:

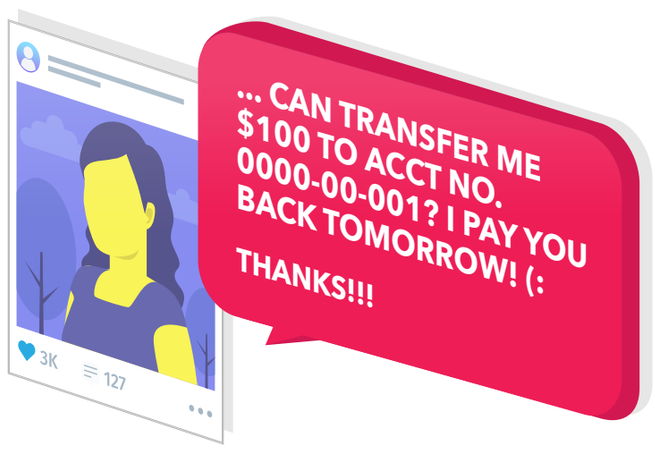
SG:D | GET READY!

HOW CAN I SPOT AN ONLINE IMPERSONATION SCAM?

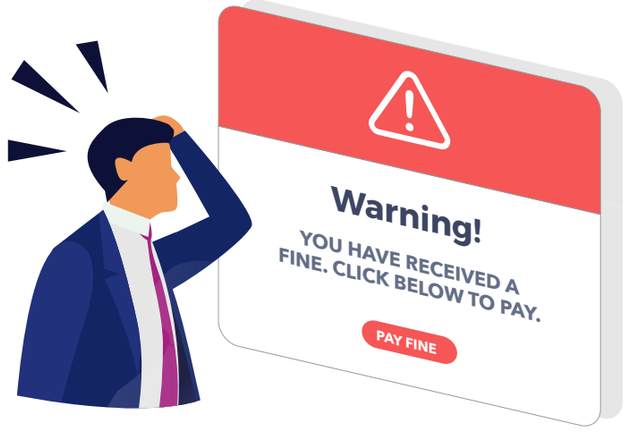


HERE ARE SOME THINGS TO LOOK OUT FOR!

- Scammers often impersonate official authorities to gain your trust.
- They can also impersonate telecommunications, banks or courier companies, claiming that there are urgent issues with your bank account, phone subscription or a problem with a parcel delivery.
- Be wary if you receive requests supposedly from government officers or corporate representatives asking for sensitive information such as personal details via email or messages.



- Scammers may hack your friends' or family members' social media accounts and use them to ask you for information or money.
- Be wary if your friend or family member makes unusual requests over social media.



- Scammers often try to put you in a stressful situation such as threatening you with a fine, legal costs, cancellation of service or even arrest if you do not comply.
- Be wary if you are pressured into making a rushed decision or giving up personal information.

NEED SCAM-RELATED ADVICE?

Call the Anti-Scam Helpline at 1800-722-6688

1CLICK AWAY
Be Safe · Be Smart · Be Kind

MEDIA LITERACY COUNCIL

#BeSafe

Check Before You Click

Supported by:

INFOCOMM MEDIA DEVELOPMENT AUTHORITY

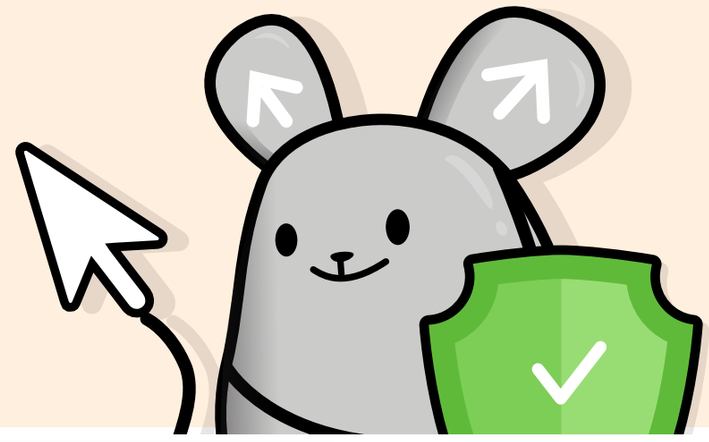
SINGAPORE POLICE FORCE
SAFEGUARDING EVERY DAY

NATIONAL CRIME PREVENTION COUNCIL

In Support of:

SG:D | GET READY!

HOW CAN I GUARD AGAINST ONLINE IMPERSONATION SCAMS?



HERE ARE SOME WAYS YOU CAN PROTECT YOURSELF WHILE ENGAGING OTHERS ONLINE!

- Do not disclose important information such as your bank details or passport numbers.
- A government agency or trusted business will never ask you for such information over the phone or through social messaging platforms.

- Be cautious of requests for payment via unusual methods, such as gift cards, prepaid cards, wire transfers or bitcoin.
- Do not follow instructions to download attachments or click on links before the source is verified.
- Never give anyone remote access to your devices, unless they have proven to be an official representative of the company or organisation.

- If at any point you feel uncertain about the nature of the call or the caller's identity, stop all communications and verify if the source is reliable.
- Do not give in to the caller's demands if you feel pressured or rushed to make a quick decision.
- Verify the request by calling the organisation's or business' main phone line.

THINK YOU'VE FALLEN FOR AN IMPERSONATION SCAM?

For urgent police assistance, call 999.

#BeSafe

Check Before You Click

1CLICK AWAY
Be Safe · Be Smart · Be Kind

MEDIA LITERACY COUNCIL

Supported by:
INFOCOMM MEDIA DEVELOPMENT AUTHORITY
SINGAPORE POLICE FORCE
SAFEGUARDING EVERY DAY
NATIONAL CRIME PREVENTION COUNCIL

In Support of:
SG:D | GET READY!