



**SINGAPORE  
POLICE FORCE**  
SAFEGUARDING EVERY DAY

# Sharing on Scam Situation March 2021

# Annual Crime Statistics 2020

- ✓ The total amount cheated for the top ten types of scams **increased by almost 65.2% to S\$201.2 million in 2020, from S\$121.8 million in the same period in 2019.**
- ✓ Among the top ten types of scams, the following scams remain key concerns to the Police;
  - E-commerce scams,
  - Social media impersonation scams
  - Loan scams, &
  - Banking-related phishing scams
  - Investment scams



# Re-emergence of Phishing Scams Involving Fake Singtel Website

## What you should lookout for:

- ✓ Victims would receive an e-mail purportedly from 'Singtel' indicating that they have won a cash prize or are eligible to claim a cashback or gift
- ✓ They would be asked to click on the URL link that directed them to a fake Singtel webpage to provide their bank information and One-Time Passwords (OTPs) to claim the prize, cashback or gift

Victims would only realised that they have been scammed when unauthorized transactions were made from their bank accounts.

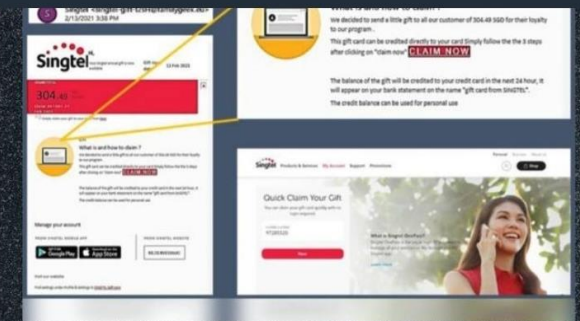
NCPC ScamAlert 📢

Received emails from "Singtel" saying you are eligible for a cashback or cash prize? 📧💰

!! It's a scam! Watch out for suspicious URLs that lead you to fraudulent websites and request for your bank details and OTP! !!

👤 Never disclose your private information to anyone and verify the authenticity of the information with official sources!

🔍 Spot the signs, 🛑 stop the crimes.



RECEIVED EMAILS FROM "SINGTEL" CLAIMING YOU'VE WON A PRIZE OR CASHBACK?

**IT'S A SCAM! ALWAYS VERIFY THE URL LINK BEFORE CLICKING.**

# Re-emergence of Phishing Scams Involving Fake Singtel Website

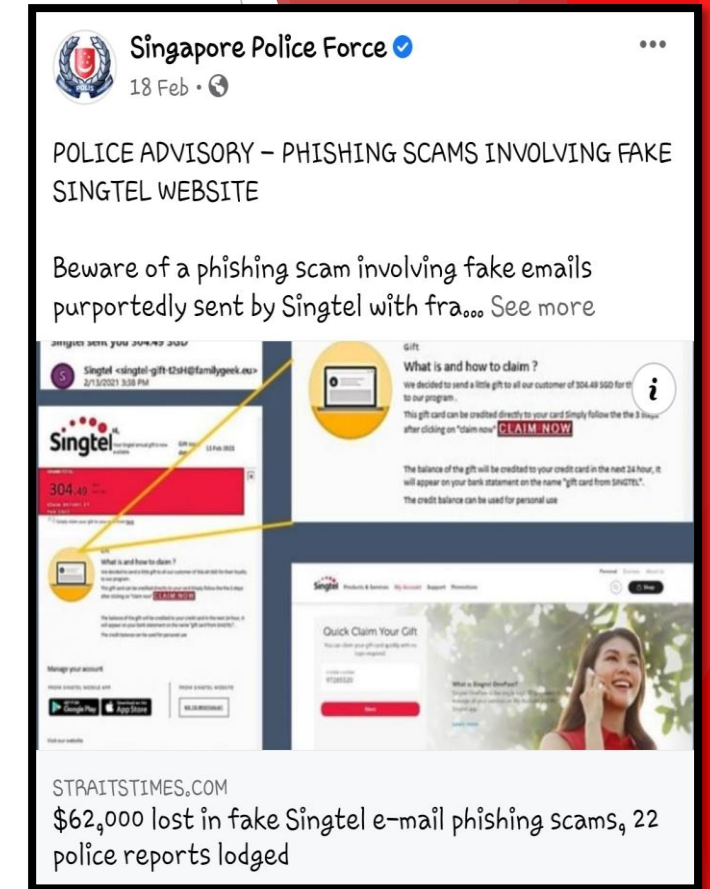
## What you should do:

- ✓ **Be wary** of URL links provided in unsolicited advertisements and text messages, especially those related to deals that seem too good to be true
- ✓ **Always verify** the authenticity of the information with the official website or sources
- ✓ **Never disclose** your personal or internet banking details and OTP to anyone
- ✓ **Report** any fraudulent transaction involving your e-payment accounts to the e-payment service provider immediately

# Re-emergence of Phishing Scams Involving Fake Singtel Website

## What have we done:

- ✓ The Police News Release was issued and published on The Straits Times news
- ✓ Singtel was alerted of the cases and an email notification has been sent to their customers in phases to alert them to be vigilant
- ✓ Police have cross shared the advisory and news release on social media platforms



The image shows a screenshot of a social media post from the Singapore Police Force, dated 18 Feb. The post is titled "POLICE ADVISORY – PHISHING SCAMS INVOLVING FAKE SINGTEL WEBSITE" and contains the text: "Beware of a phishing scam involving fake emails purportedly sent by Singtel with fra... See more". Below the text is a collage of images. On the left is a screenshot of a fake Singtel email with a subject line "Singtel <singtel-gift-2544@familynet.sg>" and a body that says "304.49". On the right is a screenshot of a fake Singtel website with a "What is and how to claim?" section and a "Quick Claim Your Gift" button. At the bottom of the collage is a screenshot of a woman smiling on a phone. Below the collage, the text "STRAITSTIMES.COM" is visible, followed by the headline "\$62,000 lost in fake Singtel e-mail phishing scams, 22 police reports lodged".



# Re-emergence of Police Impersonation Scams

## What you should lookout for:

- ✓ Scammers would call the victims through messaging applications such as WhatsApp, imo and Viber, or via normal phone calls, and claim to be Police officers
- ✓ Used publicly available photographs of actual Police officers as their profile picture on the messaging applications
- ✓ Victims would be informed that there are issues with their bank accounts
- ✓ Scammers would then trick victims into revealing their bank account or credit card details and One-Time Password (OTP) on the pretext of assisting them to resolve issues with their bank accounts or credit cards

Victims would only realised that they have been scammed when unauthorized transactions were made from their bank accounts.



# Re-emergence of Police Impersonation Scams

## What you should do:

- ✓ **Ignore** the instructions. No government agency will obtain personal information through telephone call
- ✓ **Never disclose** your personal or internet banking details and OTP to anyone
- ✓ **Report** any fraudulent credit/debit card charges to your bank and cancel your card immediately

# Re-emergence of Police Impersonation Scams

## What have we done:

- ✓ The Police News Released was issued to the media.
- ✓ Police have cross shared the advisory and news release on social media platforms

## SCAM ALERT

### Re-Emergence of Police Impersonation Scams

- ❑ The Police have observed a re-emergence of the **Police impersonation scam** and would like to alert the public to be vigilant
- ❑ Scammers would call the victims through messaging applications such as WhatsApp, imo and Viber, or via normal phone calls, and claim to be police officers and use publicly available photographs of actual police officers as their profile picture on the messaging applications
- ❑ The victims were then informed that there were issues with their bank accounts. Scammers would then trick victims into revealing their bank account or credit card details and one-time password (OTP) on the pretext of assisting them to resolve issues with their bank accounts or credit cards
- ❑ The victims only discovered that they had been scammed when they noticed unauthorised transactions made to their bank accounts or credit cards



- Ignore the instructions. No government agency will obtain personal information through telephone call.
- Never disclose your personal or Internet banking details and OTP to anyone.
- Report any fraudulent credit/debit card charges to your bank and cancel your card immediately.



**POLICE**

**FOR SCAM-RELATED ADVICE,  
PLEASE CALL 1800-722-6688 OR  
VISIT WWW.SCAMALERT.SG**



# NCPC Anti-Scam Advisories

## IMPERSONATION SCAM

Scammers pretend to be a trusted source, authority, or even a friend to lower your guard. They then make up 'emergencies' to threaten and get you to share your personal details or do money transfers.

For the next quarter, we will be spotlighting impersonation scams and the signs that public can look for to protect themselves from falling prey.

*Watch this space!*

KNOW THE ESSENTIALS TO  
PROTECT YOURSELF FROM AN

### IMPERSONATION SCAM



Spot the signs, stop  
the crime

[Learn More](#)



### VERIFY CALLER

Verify the caller ID and  
organisation

[Learn More](#)



### KEEP PRIVATE

Keep your personal  
details to yourself

[Learn More](#)



### DON'T TRANSFER

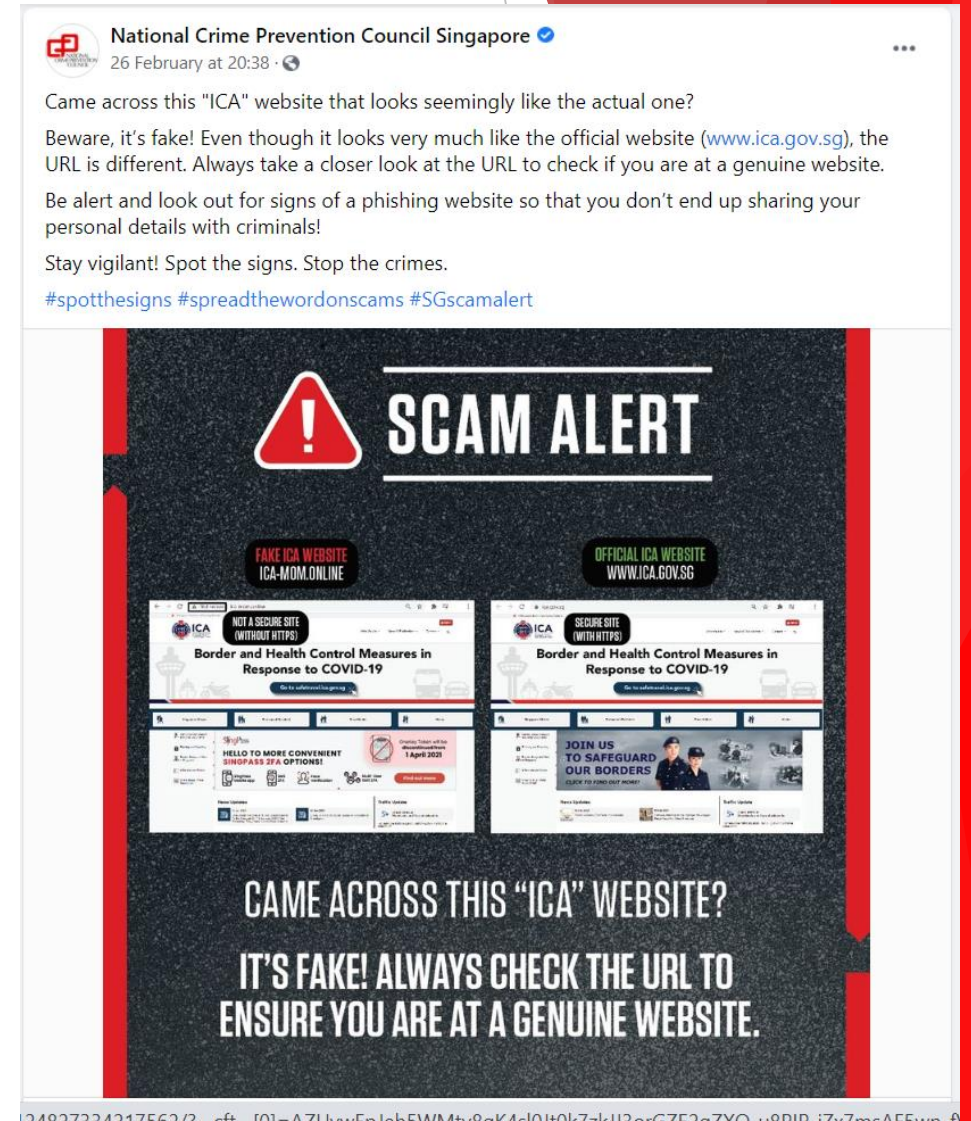
Know that government  
agencies do not...

[Learn More](#)

## SPOT THE SIGNS, STOP THE CRIMES.

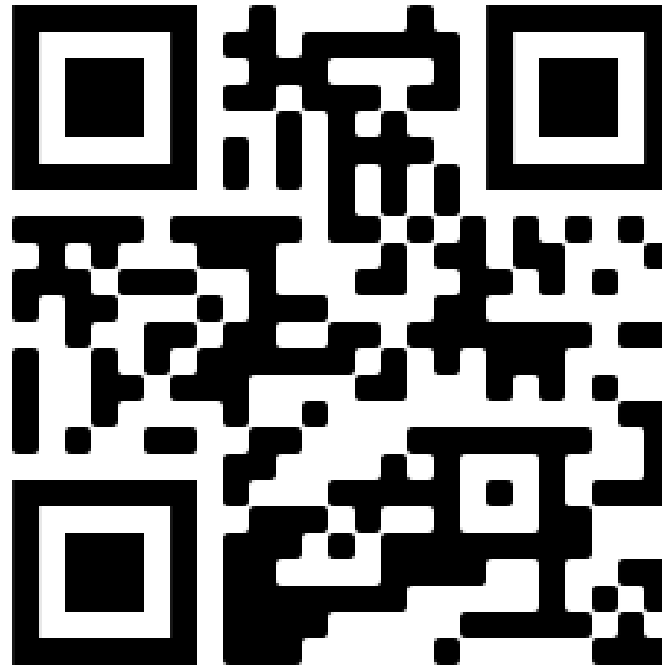
# NCPC Anti-Scam Advisories

- ✓ Advisories have been put out to educate people to look out for phishing websites.
- ✓ Posted on 26 Feb 2021 touched on a fake ICA website.



# Join the “Let’s Fight Scams!” Movement

- Join our Whatsapp or Telegram channels to get the latest scam alerts!



Telegram



Whatsapp

# Thank you



**SINGAPORE  
POLICE FORCE**  
SAFEGUARDING EVERY DAY