

# MONTHLY SCAMS BULLETIN

## Phishing: Don't get hooked!

Victims receive SMSes/emails from scammers impersonating government agencies or banks that inform them of urgent payments or account renewals.

These messages contain links to fake webpages mimicking PayNow, bank sites, and government portals that steal victims' personal and banking details.

### Remember:

- Never click on links from unsolicited text messages/emails
- Do not share your personal/banking details with anyone
- Text messages from banks will come with their official sender ID and will never include clickable links
- Text messages from government agencies will be sent from 'gov.sg' sender ID.
- Messages will appear in a single conversation (i.e., part of the gov.sg message thread), instead of separate conversations.

**For other messages you receive that are not in a single conversation, contact the agency directly or call and check with the 24/7 ScamShield Helpline at 1799.**

**You can also check suspicious numbers, messages and links with the ScamShield app.**

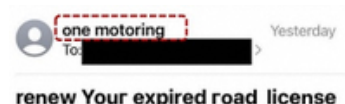
PayNow: Your PayNow certificate has expired.

Update it on <https://paynow.help/?BbemaPjJnz> now to avoid any blocking of your services.

07:16

### Spot the Signs of Phishing!

1. Random Emails: Criminals often test their luck by sending mass emails. Never click on unsolicited links and attachments. Delete the email immediately.
2. Discrepancies in Sender ID: Substitute or additional letters to trick you. Watch for mistakes in email addresses and URLs that resemble official links.
3. Unsolicited requests for your One-Time passwords (OTPs), personal or banking details.



**SINGAPORE  
POLICE FORCE**  
SAFEGUARDING EVERY DAY



Scan for  
SPF Scam Resources

# 诈骗月刊

## 钓鱼骗局：别上钩！

骗子会冒充政府机构或银行向受害者发出短信/电邮，通知他们有紧急付款或更新户口的情况。

这些信息包含链接引导受害者至模仿PayNow、银行和政府机构网站的假网页以便窃取受害者个人和银行信息。

### 切记：

- 切勿点击未经请求短信/电邮内的链接
- 切勿与他人分享您的个人/银行资料
- 银行发出的短信只来官方发送者身份，并肯定不会包含可点击链接
- 来自政府机构的短信将来自'gov.sg'发送者身份。
- 信息将出现在同一个对话中（即包含在gov.sg信息的一部分），而不是单独的对话中。

如果您所收到的其他信息不在同一个对话中，请直接联系该部门或拨打1799查询ScamShield的全天候援助热线。

您也能通过ScamShield应用程序查看可疑号码、信息和链接。

### 注意钓鱼迹象！

1. **随意发送电邮：**罪犯经常通过发送大量电邮来试探运气。切勿点击未经请求的链接和附件，并立即删除该电邮。
2. **发送者身份的差异：**替换或附加字母鱼目混珠。注意类似官方链接的电邮地址和网址中的错误。
3. **未经请求**向您索取一次性密码（OTPs）、个人或银行资料。

PayNow: Your PayNow certificate has expired.

Update it on <https://paynow.help/?BbemaPjJnz> now to avoid any blocking of your services.

07-16

one motoring Yesterday

renew Your expired road license



SINGAPORE  
POLICE FORCE  
SAFEGUARDING EVERY DAY



Scan for  
SPF Scam Resources

# BULETIN PENIPUAN BULANAN

## Pancingan Data: Jangan terperangkap!

Mangsa menerima SMS/e-mel daripada penipu yang menyamar datang daripada agensi pemerintah atau bank yang memaklumkan kepada mereka pembayaran segera atau pembaharuan akaun.

Mesej ini mengandungi pautan ke laman web palsu yang menyerupai PayNow, laman web bank, dan portal pemerintah yang mencuri butir-butir peribadi dan perbankan mangsa.

### Ingat:

- Jangan klik pada pautan daripada mesej/e-mel yang tidak diminta
- Jangan kongsi butir-butir peribadi/perbankan anda dengan sesiapa
- Mesej teks daripada bank akan datang bersama dengan identiti (ID) pengirim rasmi mereka dan tidak akan sekali-kali mengandungi pautan yang boleh diklik.
- Mesej teks daripada agensi pemerintah akan dihantar daripada ID pengirim 'gov.sg'.
- Mesej akan muncul dalam satu perbualan (iaitu sebahagian daripada urutan mesej 'gov.sg' tersebut), dan bukannya perbualan berasingan.

PayNow: Your PayNow certificate has expired.

Update it on <https://paynow.help/?BbemaPjJnz> now to avoid any blocking of your services.

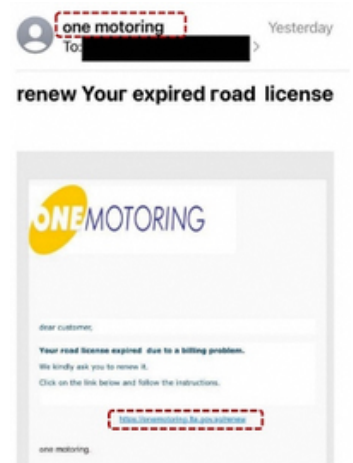
07-16

**Untuk mesej lain yang anda terima yang bukan dalam satu perbualan, hubungi agensi secara langsung atau telefon dan periksa dengan Talian Bantuan ScamShield 24/7 di 1799.**

**Anda juga boleh memeriksa nombor, mesej dan pautan yang mencurigakan dengan aplikasi ScamShield.**

Perhatikan Tanda-Tanda Pancingan Data!

1. **E-mel Rawak:** Penjenayah selalunya mencuba nasib mereka dengan menghantar e-mel secara beramai-ramai. Jangan sekali-kali klik pada pautan dan lampiran yang tidak diminta. Padam e-mel tersebut dengan segera.
2. **Percanggahan dalam ID Pengirim:** Ada huruf pengganti atau tambahan untuk menipu anda. Perhatikan kesilapan dalam alamat e-mel dan URL yang kelihatan seperti pautan rasmi.
3. **Permintaan yang tidak diminta** untuk Kata Laluan Sekali Sahaja (OTP), butir-butir peribadi atau perbankan.



**SINGAPORE POLICE FORCE**  
SAFEGUARDING EVERY DAY



Scan for  
SPF Scam Resources

# மாதாந்திர மோசடிகள்

## தூண்டிலிடல்: சிக்கிக்கொள்ளாதீர்கள்!

உடனடியாகக் கட்டணம் செலுத்த சொல்லியோ கணக்கைப் புதுப்பிக்கவோ அறிவுறுத்தும் அரசாங்க அமைப்பு அல்லது வங்கி போன்று ஆள்மாறாட்டம் செய்து மோசடிக்காரர்களிடமிருந்து குறுஞ்செய்திகள்/மின்னஞ்சல்களைப் பாதிக்கப்பட்டோர் பெறுவர்.

இந்தச் செய்திகளில் PayNow, வங்கி இணையத்தளங்கள், அரசாங்கத் தளங்கள் கொண்ட போலி இணையத்தளங்களின் இணைப்புகள் இருக்கும்.

### நினைவில் கொள்ளுங்கள்:

- அடையாளம் தெரியாத குறுஞ்செய்திகள்/மின்னஞ்சல்களில் வரும் இணைப்புகளைச் சொடுக்கவேண்டாம்.
- உங்கள் தனிப்பட்ட/வங்கித் தகவல்களை எவரிடமும் பகிரவேண்டாம்.
- வங்கிகளிலிருந்து வரும் குறுஞ்செய்திகளில் அதிகாரபூர்வ அனுப்புநர் அடையாளம் இருக்கும். மேலும் சொடுக்கக்கூடிய இணைப்புகள் அதில் இருக்காது.
- அரசாங்க அமைப்புகளிலிருந்து வரும் குறுஞ்செய்திகளில் 'gov.sg' அனுப்புநர் அடையாளம் இருக்கும்.
- குறுஞ்செய்திகள் ஒரே உரையாடலில் காணப்படும் (i.e., gov.sg குறுஞ்செய்தித் தொடரின் அங்கமாகவே). தனித்தனி உரையாடல்களாக இருக்காது.

தொடர்ச்சியான உரையாடலில் இல்லாமல் வேறு குறுஞ்செய்திகள் பெறப்பட்டால் அமைப்பை நேரடியாகத் தொடர்புக்கொள்ளுங்கள். அல்லது 24/7 ஸ்கேம்ஷீல்டு உதவித்தொடர்பை 1799 எண்ணில் அழைத்து சரிபார்த்துக்கொள்ளுங்கள்.

ஸ்கேம்ஷீல்டு செயலி வழி சந்தேகத்திற்குரிய எண்களை, குறுஞ்செய்திகளை, இணைப்புகளை நீங்களே சரிபார்த்துக்கொள்ளலாம்.

தூண்டிலிடல் மோசடிகளின் அறிகுறிகளை அடையாளம் காணுங்கள்!

1. **தொடர்பில்லாத மின்னஞ்சல்கள்:** குற்றவாளிகள் பெரும்பாலும் பேரளவில் மின்னஞ்சல்களை அனுப்பி தங்களின் அதிர்ஷ்டத்தை சோதிப்பார்கள். அடையாளம் தெரியாத இணைப்புகளையோ இணைக்கப்பட்ட பதிவுகளையோ சொடுக்காதீர்கள். அந்த மின்னஞ்சலை உடனடியாக அழித்துவிடுங்கள்.
2. **அனுப்புநர் அடையாளத்தில் முரண்பாடுகள்:** உங்களை ஏமாற்ற மாற்று அல்லது கூடுதல் எழுத்துகள். மின்னஞ்சல் முகவரிகளிலும் இணையத்தள முகவரிகளிலும் அதிகாரபூர்வ இணைப்புப் போலவே காட்சிதந்தாலும் தவறுகள் இருக்கிறதா என்று கூர்ந்து கவனிக்கவும்.
3. ஒருமுறை பயன்படுத்தப்படும் கடவுச்சொற்கள், தனிப்பட்ட அல்லது வங்கித் தகவல்களுக்கு அடையாளம் தெரியாதவரிடமிருந்து வரும் கோரிக்கைகள்.

PayNow: Your PayNow certificate has expired.

Update it on <https://paynow.help/?BbemaPjJnz> now to avoid any blocking of your services.

07-16

one motoring Yesterday  
To [redacted]  
renew Your expired road license



SINGAPORE  
POLICE FORCE  
SAFEGUARDING EVERY DAY



Scan for  
SPF Scam Resources