

# HOW TO GO SAFE ONLINE

如何维持良好的  
网络安全习惯



In support of:



In association with:

**SG:D | GET READY!**

Brought to you by:



An initiative of:



Supported by:



Prevention is key in the fight against cyber threats. Just as we lock our doors to keep burglars out, we must secure our devices to keep ourselves safe from cyber criminals.

In this booklet, you'll find 4 simple tips to go safe online.

防患于未然才是对抗网络威胁的制胜之道。正如我们平日会将门上锁以防盗贼，我们也必须采取相应措施，加强电脑、平板电脑和手机以及个人信息安全，防范网络罪犯。

在这本小册子中，您将了解四个简单的网络安全小贴士，让您可以安全上网。

---

### Get more tips at:

欲知更多贴士，请浏览：



[csa.gov.sg/gosafeonline](http://csa.gov.sg/gosafeonline)



[facebook.com/gosafeonline](http://facebook.com/gosafeonline)



[twitter.com/gosafeonline](http://twitter.com/gosafeonline)

---

## **Use anti-virus software on your computer and mobile devices to prevent malware infections.**

Like computers, your mobile devices are vulnerable to malware infections too. Once infected, your devices could slow down and malfunction and your data could be corrupted, stolen or even deleted. Use an anti-virus app downloaded from official app stores to protect your devices.

**At minimum, an anti-virus software should have these features:**



### **AUTOMATIC UPDATE AND SCAN**

Provides up-to-date protection against the latest threats



### **MALWARE REMOVAL**

Removes malware from infected devices

**在电脑、平板电脑和手机安装防毒软件，防止病毒入侵。**

就像电脑，您的手机和平板电脑也可能遭恶意软件侵入。一旦感染病毒，您的电脑、平板电脑和手机可能变得反应慢、发生故障，个人资料也可能遭破坏、盗用，甚至被删除。要避免这种情况，您可以从官方应用程序商店下载防毒应用程序。

**防毒软件应至少具备以下特征：**



### **自动更新和扫描功能**

提供针对最新威胁的实时保护



### **清除恶意软件**

清除受感染电脑、平板电脑和手机中的恶意软件

## **Update your software promptly to keep sensitive information safe from cyber criminals.**

Software updates contain important security fixes that address known vulnerabilities and bugs. Promptly updating your apps limits the amount of time that cyber criminals have to find and use these vulnerabilities.

### **To minimise disruptions to your daily routine:**



Enable automatic updates over Wi-Fi



Schedule updates to install overnight when your device is plugged in

**及时更新软件，避免您的敏感资料落入网络罪犯手中。**

更新后的软件包含可修补安全漏洞和防毒的程式。及时更新您的应用程序能有效限制网络罪犯用来寻找和攻破漏洞的时间。

### **为减低更新软件对日常生活的不便：**



设置仅在连接到Wi-Fi之后自动更新



设置仅在电脑、平板电脑和手机插入电源的情况下，于夜间进行自动更新

**Step 1**



**Step 2**



**Step 3**



## **Use strong passwords of at least 12 characters and enable Two-Factor Authentication (2FA), such as a token, for your online accounts.**

Cyber criminals can easily guess weak passwords. To protect your accounts, it is essential to use a strong password. A strong password is long (at least 12 characters) and random.

### **Here's how to create a strong and memorable password:**

**1** Pick five or more words that relate to a memory that is unique to you.

Don't use information about yourself such as your name, mobile number and birthdate, in your passwords.

**使用含有至少12个字符的安全性高的密码，并启动双重认证功能(2FA)，例如密码生成器。**

网络罪犯能轻易猜到安全性低的密码。为了保护您的账户，请务必使用安全性高的密码。安全性高的密码应当足够长（含有至少12个字符）并且是随机组合的。

### **以下介绍如何创建一个安全性高又能容易记住的密码：**

挑选至少5个与您独特的记忆相关的单词。

在创建密码的过程中，不要使用您的个人信息，例如名字、电话号码和生日日期。



**Learnt to ride a bicycle at five**

- 2** Use a mix of uppercase and lowercase letters, numbers or symbols.

密码应由大小写字母、号码或符号组成。

learntto**RIDE**abicycleat**5**



Use different passwords for your online accounts.

为不同的网络账户使用不同的密码。

**For an additional layer of security, enable 2FA for your online accounts, including email and social media.**

This means that you have to identify yourself by providing:

**为了提高安全, 请为您的网络账户(包括电子邮件和社交媒体)启动双重认证功能(2FA)。**

这表示您必须提供以下信息来验证身份:



**OR 或**



**SOMETHING YOU KNOW**

(Password)

**您知道的**

(密码)

**SOMETHING YOU HAVE**

(One-time password from a 2FA token)

**您拥有的**  
(双重认证密码生成器发出的一次性密码)

**SOMETHING YOU ARE**

(Biometrics)

**您的生理特征**

(指纹等生物特征)

## **Spot signs of phishing, such as suspicious links, to protect yourself from cyber criminals.**

Phishing is a method which cyber criminals use to fraudulently obtain your personal and financial information such as your login details, bank account and credit card numbers. They disguise themselves as a legitimate individual or reputable organisation, through channels such as email and instant messaging. Once cyber criminals obtain your personal information, they could access your online accounts, and even impersonate you to scam others.

To prevent yourself from becoming a victim of phishing attacks, learn to spot the tell-tale signs. When in doubt, contact the company directly to clarify, but don't use the contact information provided in the email. Otherwise, delete the email immediately.

**留意任何网络钓鱼迹象，  
例如可疑链接，以免掉入  
网络罪犯的陷阱。**

网络钓鱼是网络罪犯用来骗取个人和财务信息（例如登录信息、银行账户和信用卡号码）的一种手法。网络罪犯会通过电邮和简讯等管道，假扮成他人或信誉良好的机构来骗取资料。一旦得到您的个人资料，他们就能登录您的网络账户，甚至冒充您去诈骗他人。

为了避免让自己成为网络钓鱼攻击的受害者，就要学会识别这些蛛丝马迹。如有疑问，请直接与相关公司联系，但不要使用电子邮件中提供的联系信息。否则，请立即删除该电子邮件。

# Anatomy of a phishing email

## 分析钓鱼电子邮件

Can you spot the signs of phishing?  
您能识别电邮中的钓鱼迹象吗?

The screenshot shows an email window with the following details:

- Subject: [URGENT] CLAIM YOUR GIFT CARD OR ACCOUNT WILL BE DEACTIVATED
- From: SGSHOPPING <sgshopping@s1231.net> (1)
- Date: 11 April 2018, 12:42 AM
- To: John Tan (5)
- Subject: [URGENT] CLAIM YOUR GIFT CARD OR ACCOUNT WILL BE DEACTIVATED (2)
- Attached: Gift-Card-Redemption.exe (150kb) (6)

The body of the email contains the following text:

Dear John,

Congratulations! We are pleased to inform you that you have won a \$100 gift card for our monthly lucky draw! ([www.253749.co/d43lFK](http://www.253749.co/d43lFK)) (1)

(4) Simply log on to ([www.sgshopping.com](http://www.sgshopping.com)) (1) fill up the attached document with your NRIC, address and bank account details (2) to claim your gift card.

Failure to claim your prize within 24 hours will result in the permanent deactivation of your account.

Sincerely,  
Customer Service

1



**Mismatched and misleading information**  
不协调和具误导性的信息

2



**Use of urgent or threatening language**  
使用语调急迫或带威胁性的字眼

3



**Promises of attractive rewards**  
诱人奖品

4



**Requests for confidential information**  
向您索取个人机密资料

5



**Unexpected emails**  
由陌生人发出的电邮

6



**Suspicious attachments**  
可疑的附件

# CARA-CARA MEMASTIKAN KESELAMATAN DALAM TALIAN

எவ்வாறு இணையத்தில்  
பாதுகாப்பாக இருப்பது



In support of:



In association with:

**SG:D | GET READY!**

Brought to you by:



An initiative of:



Supported by:



Pencegahan penting dalam memerangi ancaman siber. Sama seperti kita mengunci pintu rumah kita untuk menghalang pencuri daripada menceroboh masuk, kita harus memastikan peranti-peranti kita selamat daripada penjenayah siber.

Dalam buku kecil ini, anda akan mendapati 4 panduan mudah untuk selamat semasa dalam talian.

இணைய அச்சுறுத்தல்களுக்கு எதிரான போராட்டத்தில் தடுப்பு நடவடிக்கைகள் முக்கியம். திருடர்கள் நமது இல்லத்திற்குள் வராமல் தடுப்பதற்காக நம் கதவுகளைப் பூட்டுவது போல, இணையக் குற்றவாளிகளிடம் இருந்து நம்மைப் பாதுகாப்பாக வைத்துக்கொள்வதற்கு நமது சாதனங்களையும் தரவுகளையும் பாதுகாப்பாக வைத்திருப்பது அவசியம்.

இச்சிற்றேட்டில், நீங்கள் இணையத்தைப் பாதுகாப்பாக பயன்படுத்துவதற்கான 4 எளிய வழிகளைப் பார்க்கலாம்.

---

### Dapatkan panduan selanjutnya di:

மேலும் குறிப்புகள்  
பெற, பின்வரும்

இணையத்தளங்களை  
நாடுங்கள்:



[csa.gov.sg/gosafeonline](http://csa.gov.sg/gosafeonline)



[facebook.com/gosafeonline](https://facebook.com/gosafeonline)



[twitter.com/gosafeonline](https://twitter.com/gosafeonline)



**Gunakan perisian anti-virus pada komputer dan peranti mudah alih anda untuk mengelak daripada jangkitan perisian hasad (malware).**

Seperti komputer, peranti mudah alih anda juga terdedah kepada jangkitan perisian hasad. Sebaik sahaja dijangkiti, peranti anda boleh menjadi perlahan dan rosak, malah data anda boleh dicemari, dicuri atau dipadam. Gunakan aplikasi anti-virus yang dimuat turun daripada kedai aplikasi rasmi untuk melindungi peranti anda.

**Perisian anti-virus harus sekurang-kurangnya mempunyai ciri-ciri berikut:**



#### **KEMAS KINI DAN IMBASAN AUTOMATIK**

Menyediakan perlindungan terkini terhadap ancaman-ancaman terbaru



#### **PENYINGKIRAN PERISIAN HASAD**

Menyingkirkan perisian hasad daripada peranti yang telah dijangkiti

**நச்சு நிரல் தாக்குதலைத் தடுப்பதற்கு, உங்கள் கணினி மற்றும் கைப்பேசி சாதனங்களில், நச்சு நிரல் எதிர்ப்பு மென்பொருட்களைப் பயன்படுத்துங்கள்.**

கணினிகளைப் போலவே, உங்கள் கைப்பேசி சாதனங்களும் நச்சு நிரல்களால் பாதிக்கப்படலாம். அவ்வாறு, பாதிப்பு ஏற்பட்டதும், உங்கள் சாதனங்கள் செயல்படும் வேகம் குறைந்து, அவை தவறாகச் செயல்படக்கூடிடும். மேலும், உங்களின் தரவுகள் சேதமடையலாம், களவுடைப்படலாம் அல்லது அழிக்கவும் படலாம். உங்கள் சாதனங்களைப் பாதுகாப்பதற்கு, அதிகாரப்பூர்வச் செயலி அங்காடிகளில் இருந்து பதிவிறக்கம் செய்யப்பட்ட நச்சு நிரல் எதிர்ப்புச் செயலியைப் பயன்படுத்துங்கள்.

**குறைந்தபட்சம், ஒரு நச்சுநிரல் எதிர்ப்பு மென்பொருளில் பின்வரும் அம்சங்கள் இருக்கவேண்டும்:**



**தானியக்க அடிப்படையில் புதுப்பித்தல் மற்றும் அலகிடுதல்**

ஆக அண்மைய அச்சுறுத்தல்களுக்கு எதிரான, புதுப்பிக்கப்பட்ட பாதுகாப்பை வழங்குதல்



**நச்சுநிரலை அகற்றும் மென்பொருள்**

பாதிக்கப்பட்ட சாதனங்களிலிருந்து நச்சுநிரல்களை அகற்றுதல்

**Kemas kini perisian anda dengan segera untuk memastikan maklumat sensitif selamat daripada penjenayah siber.**

Kemas kini perisian mengandungi pembetulan keselamatan penting yang menangani kelemahan dan pepijat yang dikenali. Mengemaskini aplikasi anda dengan segera membataskan jumlah masa yang penjenayah siber punyai untuk mencari dan mempergunakan kelemahan ini.

#### **Untuk mengurangkan gangguan kepada rutin harian anda:**



Aktifkan kemas kini automatik melalui Wi-Fi



Jadualkan kemas kini untuk dipasang semalam semasa peranti anda sedang dicas

Step 1



Step 2



Step 3



உங்களின் முக்கியமான தகவல்களை இணையக் குற்றவாளிகளிடமிருந்து பாதுகாப்பதற்கு, உங்கள் மென்பொருளை உடனடியாகப் புதுப்பித்துக்கொள்ளுங்கள்.

மென்பொருள் புதுப்பிப்புகளில், அறியப்பட்ட பாதிப்புகள் மற்றும் பிழைகளைச் சரிசெய்யும் முக்கியமான பாதுகாப்பு அம்சங்கள் இருக்கும். உங்கள் செயலிகளை உடனடியாகப் புதுப்பிக்கும்போது, இணையக் குற்றவாளிகள் இத்தகைய பாதிப்புகளைக் கண்டுபிடித்து, அவற்றைப் பயன்படுத்துவதற்கான கால அவகாசம் கட்டுப்படுத்தப்படுகிறது.

#### **உங்களுடைய அன்றாட நடவடிக்கைகளில் இடையூறு ஏற்படுவதைக் குறைப்பதற்கு:**



கம்பியில்லா இணையச் சேவையின் (Wi-Fi) மூலம் தானியக்கப் புதுப்பிப்புகளைச் செயல்படுத்துங்கள்



உங்கள் சாதனம் இரவில் மின்னேற்றம் செய்யப்படும் வேளையில், புதுப்பிப்புகளைப் பொருத்துவதற்குத் திட்டமிடுங்கள்

**Gunakan kata laluan yang kukuh yang terdiri daripada sekurang-kurangnya 12 karakter dan aktifkan Pengesahan Dua Tahap (2FA), seperti token, untuk akaun-akaun dalam talian anda.**

Penjenayah siber boleh meneka kata laluan yang lemah dengan mudah. Untuk melindungi akaun anda, penting untuk menggunakan kata laluan yang kukuh. Kata laluan yang kukuh seharusnya panjang (sekurang-kurangnya 12 karakter) dan rawak.

**Berikut adalah cara untuk mereka kata laluan yang kukuh dan mudah diingat:**

- 1 Pilih lima atau lebih perkataan berkaitan suatu memori yang unik kepada anda.

Jangan gunakan maklumat peribadi anda seperti nama, nombor telefon bimbit dan tarikh lahir, dalam kata laluan anda.

இணையத்தில் உள்ள உங்களுடைய கணக்குகளுக்கு, குறைந்தது 12 எழுத்துருக்களைக் கொண்ட வலிமையான கடவுச்சொற்களைப் பயன்படுத்துவதுடன், இரட்டை மறைச்சொல் முறையையும் (2FA) செயல்படுத்துவங்கள்.

இணையக் குற்றவாளிகளால், பலவீனமான கடவுச்சொற்களை எளிதில் ஊகிக்க முடியும். இணையத்தில் உள்ள உங்கள் கணக்குகளைப் பாதுகாப்பதற்கு, வலிமையான கடவுச்சொல்லைப் பயன்படுத்துவது அவசியமாகும். வலிமையான கடவுச்சொல்லானது, நீளமாகவும் (குறைந்தபட்சம் 12 எழுத்துக்கள்) சீரற்றதாகவும் இருக்கவேண்டும்.

வலிமையான, நினைவில் வைத்துக்கொள்வதற்கு எளிதான் கடவுச்சொற்களை எப்படி உருவாக்குவது என்பதை இப்போது கற்றுக்கொள்வோம்:

உங்களுக்குத் தனித்துவமாக இருக்கின்ற, உங்கள் நினைவிற்கு எளிதில் வருகின்ற ஐந்து அல்லது அதற்கு மேற்பட்ட சொற்களைத் தேர்ந்தெடுங்கள். உங்கள் பெயர், கைப்பேசி எண் மற்றும் பிறந்த தேதி போன்ற தனிப்பட்ட தகவல்களை, கடவுச்சொற்களில் பயன்படுத்தாதீர்கள்.



Learnt to ride a bicycle at five

- 2** Gunakan campuran huruf besar dan huruf kecil, nombor atau simbol.

பேரெழுத்துகள் மற்றும் சிற்றெழுத்துகளின் கலவை, எண்கள் அல்லது சின்னங்களைப் பயன்படுத்துவங்கள்.

learntto**RIDE**abicycleat**5**



Gunakan kata laluan berbeza untuk akaun-akaun dalam talian anda.

பேரெழுத்துகள் மற்றும்  
சிற்றெழுத்துகளின் கலவை,  
எண்கள் அல்லது சின்னங்களைப்  
யென்பதுக்காங்கள்.

**Untuk langkah keselamatan tambahan, aktifkan 2FA untuk akaun dalam talian anda, termasuk e-mel dan media sosial.**

Ini bermakna bahawa anda perlu mengenalpasti identiti anda dengan memberi:

மின்னஞ்சல், சமூக ஊடகக் கணக்கு உட்பட இணையத்தில் உள்ள உங்களுடைய கணக்குகளுக்குக் கூடுதல் பாதுகாப்பு அம்சமாக, இரட்டை மறைச்சொல் முறையையும் (2FA) செயல்படுத்துங்கள்.

அப்படியென்றால் நீங்கள்  
உங்களைப் பின்வரும் வழியில்  
அடையாளப்படுத்திக் கொள்ள  
வேண்டும் என்று அர்த்தம்:



## **SESUATU YANG ANDA KETAHUI**

## உங்களுக்குத் தெரிந்த அம்சங்கள் (கடவுச்சொல்)



## **SESUATU YANG ANDA PUNYA**

(Kata laluan sekali daripada token 2FA)

**உங்களிடம் இருக்கக்கூடியது**  
 (இரட்டை மறைச்சொல்  
 முறைக்கான சாதனத்திலிருந்து  
 பெறப்படும், ஒரு முறை மட்டுமே  
 பயன்படுக்கக்கூடிய கடவுச்சொல்)



ATAU  
அல்லது

# **SESUATU TENTANG DIRI ANDA** (Biometrik)

## உங்களுடைய அங்க அடையாளம் (உயிரளவியல்)

**Kenal pasti tanda-tanda percubaan memancing data (phishing), seperti pautan-pautan yang mencurigakan, untuk melindungi diri anda daripada penjenayah siber.**

Pemancingan data adalah kaedah yang digunakan oleh penjenayah siber untuk mendapatkan maklumat peribadi dan kewangan anda menerusi penipuan, seperti butir-butir pengesahan, nombor-nombor akaun bank dan kad kredit anda. Mereka menyamar sebagai individu yang boleh dipercayai atau pertubuhan yang bereputasi baik melalui saluran seperti e-mel dan aplikasi mesej segera. Sebaik sahaja penjenayah siber mendapatkan maklumat peribadi anda, mereka boleh menggunakan akaun-akaun dalam talian anda, bahkan juga menyamar sebagai diri anda untuk menipu orang lain.

Untuk mengelak diri anda daripada menjadi mangsa serangan percubaan memancing data, belajar mengenali tanda-tandanya. Sekiranya anda berasa ragu, hubungi syarikat yang berkenaan secara langsung untuk mendapatkan penjelasan, tetapi jangan gunakan maklumat hubungan yang diberi dalam e-mel tersebut. Jika tidak, padam e-mel tersebut dengan segera.

**இணையக் குற்றவாளிகளிடமிருந்து உங்களைப் பாதுகாத்துக்கொள்வதற்கு, சந்தேகத்திற்குரிய இணைய இணைப்புகள் உள்ளிட்ட, தகவல்களைத் திருடும் மோசடிச் செயல்களுக்கான அறிகுறிகளைக் கண்டுகொள்ளுங்கள்.**

இணையக் குற்றவாளிகள், உங்களின் புகுபதிகை விவரங்கள், வங்கிக் கணக்கு, கடன் பற்று அட்டை என் முதலான தனிப்பட்ட மற்றும் நிதி சார்ந்த தகவல்களைத் திருடும் மோசடிச் செயலே, ‘Phishing’ என அழைக்கப்படுகிறது. மின்னஞ்சல், உடனடிச் செய்தி அனுப்புதல் போன்ற வழிகளில், அவர்கள் தங்களை முறையான தனிநபர்கள் அல்லது மதிக்கத்தக்க அமைப்பிலிருந்து வந்தவர்களைப் போன்று காட்டிக் கொள்வார்கள். இணையக் குற்றவாளிகள் உங்களின் தனிப்பட்ட தகவல்களைப் பெற்றுக்கொண்டதும், உங்களின் இணையக் கணக்குகளைப் பயன்படுத்தலாம்; உங்களைப் போல் ஆளுமாறாட்டம் செய்து மற்றவர்களையும் ஏமாற்றலாம்.

தகவல்களைத் திருடும் மோசடிச் செயல்களில் இருந்து உங்களைப் பாதுகாத்துக்கொள்வதற்கு, மோசடிச் செயல்களுக்கான அறிகுறிகளைக் கண்டுகொள்ளுங்கள். சந்தேகம் ஏற்படும்போது, நிறுவனத்தை நேரடியாகத் தொடர்புகொண்டு சந்தேகத்தை நிவர்த்தி செய்துகொள்ளுங்கள். ஆனால், மின்னஞ்சலில் கொடுக்கப்பட்டுள்ள தொடர்புத் தகவலைப் பயன்படுத்தாதீர்கள். இல்லையென்றால், உடனடியாக மின்னஞ்சலை அகற்றி விடுங்கள்.

# Anatomi e-mel memancing data

## தகவல்களைத் திருடும் மோசடி மின்னஞ்சல் பற்றி

Bolehkah anda mengenali tanda-tanda percubaan memancing data? உங்களால் தகவல்களைத் திருடும் மோசடி செயல்களுக்குரிய அறிகுறிகளைக் கண்டறிய முடிகிறதா?

[URGENT] CLAIM YOUR GIFT CARD OR ACCOUNT WILL BE DEACTIVATED

From: SGSHOPPING <sgshopping@s1231.net> 1  
Date: 11 April 2018, 12:42 AM  
To: John Tan 5  
Subject: [URGENT] CLAIM YOUR GIFT CARD OR ACCOUNT WILL BE DEACTIVATED 2

Attached: 6

Dear John,

Congratulations! We are pleased to inform you that you have won a \$100 gift card for our monthly lucky draw! 1 [www.253749.co/d431fk](http://www.253749.co/d431fk)

4 Simply log on to [www.sgshopping.com](http://www.sgshopping.com) 2 fill up the attached document with your NRIC, address and bank account details to claim your gift card.

Failure to claim your prize within 24 hours will result in the permanent deactivation of your account.

Sincerely,  
Customer Service

1



Maklumat yang tidak sepadan dan mengelirukan

பொருந்தாத மற்றும் வவறாக வழிநடத்தக்கூடிய தகவல்கள்

2



Bahasa yang mendesak atau mengugut

அவசரமான அல்லது அச்சுறுத்தும் வகையிலான மொழியைப் பயன்படுத்துதல்

3



Janji ganjaran yang menarik

கவர்ச்சிகரமான வெகுமதிகளைத் தருவதாக உத்திரவாதம் அளித்தல்

4



Permintaan maklumat peribadi

இரகசியத்தன்மை வாய்ந்த தகவல்களைக் கோருதல்

5



E-mel yang tidak dijangkakan

எதிர்பாராத மின்னஞ்சல்கள்

6



Lampiran yang mencurigakan

சந்தேகத்திற்குரிய பின்னிணைப்புகள்