HOW TO GO SAFE ONLINE

Cybercrime is on the rise and it is important for us to protect ourselves so we do not become the next victim. Just as we lock our doors to keep burglars out, we must secure our devices and information to keep ourselves safe from cyber criminals.

Prevention is key in the fight against cyber threats.
Here are 4 simple tips to GO SAFE ONLINE.

USE AN ANTI-VIRUS SOFTWARE

Install anti-virus solutions on your computer and mobile devices to prevent malware infections, which can cause persistent pop-ups, battery drain or data loss.

Anti-virus solutions can scan and remove malware and block unsafe websites. They are not costly and do not take up much memory. Be wary of fake apps and only install anti-virus software from official app stores.

SPOT SIGNS OF PHISHING

Scammers use phishing emails or websites to get you to disclose your personal information. Clicking on unknown links or attachments could infect your computer with malware.

Look out for mismatched information such as website addresses that are misleading. Be wary of emails that ask for your confidential information, emails you are not expecting (e.g. winning a contest you didn't join), and emails with urgent 'calls to action' (e.g. Your account will be closed).

USE STRONG PASSWORDS AND ENABLE 2FA

Cyber criminals can easily guess or obtain your passwords if they are weak, so don't use personal information (e.g. your name, birthdate, NRIC, etc.) as passwords.

Create long and random passwords by using 'passphrases' that you can remember (e.g. IhadKAYAtoastAT8am) and use different passwords for different accounts. Enable 2-factor authentication whenever it's available. It provides an additional layer of verification, which makes it harder for cyber criminals to access your accounts.

UPDATE YOUR SOFTWARE ASAP

Software updates keep your computer and devices safe from known security vulnerabilities.

Enable automatic updates if the option is available.

Watch the videos on these cyber tips!

facebook.com/gosafeonline
twitter.com/gosafeonline
www.csa.gov.sg/gosafeonline

Brought to you by: CSA SINGAPORE

An initiative of: GOsafeonline Cyber Security Awareness Alliance

In association with: SG:D EMPOWERING POSSIBILITIES

Supported by: Ministry of Communications and Information

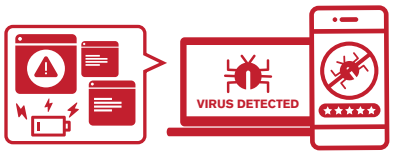
CARA-CARA UNTUK **SELAMAT DALAM TALIAN**

Jenayah siber kini semakin berleluasa dan ianya penting untuk melindungi diri kita sendiri supaya kita tidak menjadi mangsa siber seterusnya. Situasinya sama seperti kita mengunci pintu rumah kita untuk mengelak pencuri menceroboh ke dalam rumah kita, kita perlu memastikan peranti dan maklumat kita sentiasa selamat daripada pencerobohan penjenayah siber.

Pencegahan merupakan kunci untuk memerangi ancaman siber ini. Berikut adalah 4 panduan mudah untuk kekal selamat dalam talian.

GUNAKAN PERISIAN ANTI-VIRUS

Pasang perisian anti-virus pada komputer dan peranti mudah alih anda untuk mengelak daripada jangkitan perisian hasad yang boleh menyebabkan tetingkap yang timbul (pop-ups) secara berterusan, kehabisan bateri atau kehilangan data.



Perisian anti-virus boleh mengimbas dan membuang perisian hasad dan menyekat lelaman web yang tidak selamat. Perisian anti-virus ini tidak mahal dan tidak menggunakan banyak memori komputer dan peranti anda. Berwaspadalah dengan aplikasi palsu dan hanya memasang perisian anti-virus dari stor aplikasi rasmi.

PERHATIKAN TANDA-TANDA PERCUBAAN MEMANCING DATA (PHISHING)

Penipu menggunakan e-mel atau lelaman web memancing data untuk membolehkan anda mendedah maklumat peribadi anda. Mengetik pautan atau lampiran yang tidak dikenali dapat menyebabkan komputer anda dijangkiti perisian hasad.

Perhatikan maklumat yang tidak sepadan seperti alamat laman web yang mengelirukan. Berwaspadalah dengan e-mel yang meminta maklumat peribadi anda, e-mel yang tidak anda jangkakan (contohnya memenangi satu peraduan yang anda tidak sertai), dan e-mel yang memerlukan 'hubungi untuk tindakan' segera (contohnya: Akaun anda akan ditutup).

GUNAKAN KATA LALUAN-KATA LALUAN YANG KUKUH DAN AKTIFKAN 2FA

Penjenayah siber boleh meneka atau mendapatkan kata laluan-kata laluan anda dengan mudah jika ia terlalu mudah, oleh itu, jangan gunakan maklumat peribadi (contohnya: nama, tarikh lahir, kad pengenalan anda dan lain-lain) sebagai kata laluan-kata laluan anda.

Reka kata laluan-kata laluan yang panjang dan rawak dengan menggunakan 'frasalangkau' ('passphrases') yang anda boleh ingat (contohnya: IhadKAYAtoastAT8am) dan gunakan kata laluan-kata laluan yang berbeza untuk akaun-akaun yang berbeza.

Aktifkan pengesahan 2-faktor pada bila-bila masa ianya tersedia. Pengesahan 2-faktor ini memberikan satu lagi peringkat pengesahan yang membuatkan penjenayah siber ini lebih sukar untuk mencerobohi ke akaun-akaun anda.

MENGEMASKINI PERISIAN ANDA DENGAN SEGERA

Mengemaskini perisian memastikan komputer dan peranti anda selamat daripada kelemahan keselamatan terkenal.

Aktifkan kemas kini automatik jika pilihan tersebut tersedia.

Saksikan video-video ini untuk panduan siber!

facebook.com/gosafeonline
twitter.com/gosafeonline
www.csa.gov.sg/gosafeonline

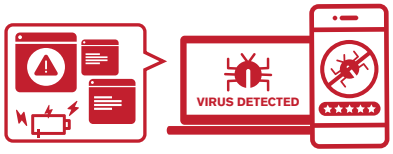
如何维持良好的网络安全习惯

随着网络罪案的上升，我们更要保护自己，避免成为网络罪案的受害者。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，加强电子设备和信息安全，防范网络罪犯。

防患于未然才是对抗网络威胁的制胜之道。这里有4个简单的小贴士来指导您维持良好的网络安全习惯。

使用防毒软件

在您的电脑和电子设备上安装防毒软件，能够有效地防止例如连续弹窗，电池耗尽，文件损失的电脑病毒感染迹象。



防毒软件能够扫描和移除恶意软件，也能够屏蔽不安全的网站。这些防毒软件价格低廉，也不占据太多的储蓄空间。警惕盗版的手机应用程序，只从官方的应用商店下载防毒软件。

时时警惕电邮以及网页的钓鱼迹象

网络罪犯通过钓鱼电邮或者网页来骗取您的重要个人信息。点击未知的链接或者附件有可能会让您的电脑感染恶意软件。

注意电邮是否具有可疑信息，例如网址域名是否像是仿冒域名。警惕那些向您索取个人机密信息的电邮、陌生可疑的电邮（例如赢得您未参加的竞赛）以及发出紧急“号召行动”的电邮（例如您的帐户将被关闭）。

观看网络安全贴士视频！

使用安全性高的密码并启用双重认证功能

如果您的密码强度很弱，网络罪犯将可以轻松地猜到或者获取您的密码。因此，不要使用个人信息作为密码（例如您的名字、生日日期、身份证号码等等）。

使用您能够记住的“短语”创建长而且随机组合的密码（例如 IhadKAYAtoastAT8am ），并且确保不同的账号使用不同的密码。如果账户设置包含启动双重认证的选项，请立即启动双重认证功能。这是为了添加多一层验证，让别人更难进入你的账户。

及时更新您的软件

最新版本的软件可以保护您的电脑和电子设备，以免受网络攻击。

如果设置包含让软件自动更新的选项的话，请启用这项选项。

facebook.com/gosafeonline
twitter.com/gosafeonline
www.csa.gov.sg/gosafeonline

இணையத்தை எவ்வாறு பாதுகாப்பாகப் பயன்படுத்துவது

இணையக் குற்றங்கள் அதிகரித்து வருவதால், அவற்றால் பாதிக்கப்படப்போகும் அடுத்த நபராக ஆகாமல் இருக்க நம்மை நாமே பாதுகாத்துக் கொள்ளவேண்டியது முக்கியம். திருடர்கள் வராமல் தடுக்க நம் கதவுகளைப் பூட்டுவது போன்று, இணையக் குற்றவாளிகளிடம் இருந்து நாம் நமது சாதனங்களையும், தகவல்களையும் பாதுகாத்திட வேண்டும்.

இணைய அச்சுறுத்தல்களுக்கு எதிரான போரில் தடுப்பு நடவடிக்கைகள் மிக முக்கியம். இணையத்தைப் பாதுகாப்பாகப் பயன்படுத்த 4 எளிய குறிப்புகள் இதோ.

நச்சுநிரல் எதிர்ப்பு (ANTI-VIRUS) மென்பொருளைப் பயன்படுத்துங்கள்

தொடர்ச்சியான பாப்-அப்கள், அதாவது மேல்விரித் திரைகள், மின்கலத் திறன் இழப்பு அல்லது தரவு இழப்பை ஏற்படுத்தக் கூடிய தீங்குநிரல் (malware) தாக்குதல்களிலிருந்து தடுப்பதற்கு, உங்கள் கணினி மற்றும் கைபேசி சாதனங்களில் நச்சுநிரல் எதிர்ப்பு மென்பொருள்களை நிறுவவும்.

நச்சுநிரல் எதிர்ப்பு மென்பொருள்களால் தீங்குநிரல்களை அகற்றவும், பாதுகாப்பற்ற இணையத்தளங்களுக்குச் செல்வதைத் தடுக்கவும் முடியும். இவை விலையுயர்ந்தவை அல்ல. மேலும், இவை நினைவகத்தில் அதிக இடத்தை எடுத்துக்கொள்வதுமில்லை. போலிச் செயலிகள் குறித்து எச்சரிக்கையுடன் இருங்கள். மேலும், அதிகாரபூர்வ செயலிக்கூடங்களிலிருந்து (app stores) மட்டுமே நச்சுநிரல் எதிர்ப்பு மென்பொருளைப் பதிவிறக்கம் செய்யுங்கள்.

ஃபிஷிங்கின் (மோசடி மின்னஞ்சல்களின்) அறிகுறிகள்

உங்கள் தனிப்பட்ட தகவல்களை நீங்களே வெளிப்படுத்தும்படி செய்ய, ஃபிஷிங் மின்னஞ்சல்கள் அல்லது இணையத்தளங்களை இணைய மோசடிக்காரர்கள் (Scammers) பயன்படுத்துவர். அறிமுகமில்லா இணையத்தள அல்லது கோப்பு இணைப்புகளைச் சொடுக்குவது, உங்கள் கணினியில் தீங்குநிரல் பாதிப்பை ஏற்படுத்தக்கூடும்.

சந்தேகத்துக்குரிய இணையத்தள முகவரிகள் போன்ற பொருந்தாத் தகவல்கள் குறித்துக் கவனமாக இருக்கவும். உங்கள் தனிப்பட்ட தகவல்களைக் கேட்கின்ற மின்னஞ்சல்கள், நீங்கள் எதிர்பார்க்காத மின்னஞ்சல்கள் (உதாரணத்திற்கு, நீங்கள் பங்கேற்காத போட்டியில் வெற்றி பெற்றதாக அறிவித்து) மற்றும் அவசர 'நடவடிக்கை அழைப்பு' கொண்ட மின்னஞ்சல்கள் (உதாரணத்திற்கு, உங்கள் கணக்கு மூடப்படும்) போன்றவை குறித்து எச்சரிக்கையாக இருக்கவும்.

வலுவான கடவுச்சொற்களைப் பயன்படுத்துவதுடன் 2FA முறையையும் செயல்படுத்துங்கள்

உங்கள் கடவுச்சொற்கள் பலவீனமாக இருந்தால், இணையக் குற்றவாளிகள் அவற்றை எளிதில் ஊகிக்கவோ பெறவோ முடியும். எனவே, உங்கள் பெயர், பிறந்தநாள், அடையாள அட்டை எண் போன்ற தனிப்பட்ட தகவல்களைக் கடவுச்சொற்களாகப் பயன்படுத்த வேண்டாம்.

உங்களால் நினைவில் வைத்துக்கொள்ளக்கூடிய நீண்ட, எளிதில் யாரும் ஊகிக்க முடியாத 'தொடர்களைக் கொண்ட' கடவுச்சொற்களை உருவாக்குங்கள் (எ.கா. IhadKAYAtoastAT8am). மேலும், வெவ்வேறு கணக்குகளுக்கு வெவ்வேறு கடவுச்சொற்களைப் பயன்படுத்துங்கள். இயன்றபோதெல்லாம் இரட்டை மறைச்சொல் முறையைச் செயல்படுத்துங்கள். உங்கள் கணக்குகளில் மற்றவர்கள் அத்துமீறி நுழைவதை இது மேலும் கடினமாக்கி, சரிபார்ப்பில் ஒரு கூடுதல் படியைச் சேர்க்கும்.

உங்கள் மென்பொருளை உடனுக்குடன் புதுப்பியுங்கள்

முன்னரே அறியப்பட்ட பாதுகாப்பு பாதிப்புகளிலிருந்து மென்பொருள் புதுப்பித்தல்கள் உங்கள் கணினியைப் பாதுகாப்பாக வைத்திடும்.

தானியக்கப் புதுப்பித்தல்களுக்கான தெரிவு இருக்குமாயின், அதனைச் செயல்படுத்தவும்.

இணைய பாதுகாப்புத் தொடர்பான உதவிக்குறிப்புகளின் காணொளியைக் காணுங்கள்!

facebook.com/gosafeonline
twitter.com/gosafeonline
www.csa.gov.sg/gosafeonline