விவேகத்தைக் கடைப்பிடிக்கப் பயனுள்ள குறிப்புகள்

இணைய அச்சுறுத்தல்களுக்கு எதிராகப் போராடுவதில் தடுத்தல் முறை முக்கியமானதாக உள்ளது. இணையத்தை ஆரோக்கியமாகப் பயன்படுத்துவது, நாம் நமது சாதனங்களையும் தகவல்களையும் பாதுகாப்பாக வைத்திருப்பதை உறுதிசெய்யும். அவ்வாறு செய்வதன் மூலம், நாம் நமது இணையப் பாதுகாப்புக்காகப் பொறுப்பேற்றுக் கொள்வதுடன், எல்லோருக்கும் ஒரு பாதுகாப்பான இணையவெளியை உருவாக்க நமது பங்கை ஆற்றுகிறோம். இணையப் பாதுகாப்பில் விவேகத்தைக் கடைப்பிடிக்க நீங்கள் செய்யக்கூடிய 10 எளிய பயனுள்ள குறிப்புகள், இதோ.

1. **வலுவான கடவுச்சொற்களைப் பயன்படுத்துவதுடன் சாத்தியமுள்ள இடங்களில் 2FA முறையைச் செயல்படுத்தவும்.**
உங்கள் கடவுச்சொற்களில் பெரிய, சிறிய எழுத்துக்கள், எண்கள், குறியீடுகள் ஆகியவை கலந்து இடம்பெறுவதை உறுதிசெய்து கொள்ளுங்கள். கூடுதல் பாதுகாப்புக்காக, சாத்தியமிருந்தால், உங்கள் கணக்குகளில் 2FA முறையைச் செயல்படுத்தவும்.

2. **இணையத்தில் தகவல்களை மதிப்பிடும்போது விவேகமாக இருக்கவும்.**
நீங்கள் பெறும் தகவல்களின் ஆதாரம் நம்பகமானதா அல்லது நம்பிக்கைக்குரியதா என்பதை எப்பொழுதும் பரிசோதிக்கவும். அது வெறுமனே ஓர் அபிப்பிராயமாக இல்லாமல் நிச்சயமான உண்மைத் தகவல் தானா என்பதைச் சரிபார்க்க நம்பத்தகுந்த இதர ஆதாரங்களுடன் ஒப்பிட்டுப் பார்க்கவும்.

3. **இணையத்தளங்கள் அல்லது இணைப்புகளின் மீது 'கிளிக்' செய்வதற்கு முன் நிறுத்திச் சிந்திக்கவும்.**
வைரஸ், வோர்ம், ட்ரோஜன் ஹார்ஸ் போன்றவற்றை நிறுவுவதற்கு இணையக் குற்றவாளிகள் இணையத்தள மற்றும் மின்னஞ்சல் இணைப்புகளைப் பயன்படுத்துகிறார்கள். அனுப்புநர் ஒரு நண்பராக, உறவினராக அல்லது சக ஊழியராக இருந்தாலும் கூட, அவர்களின் சாதனங்கள் அவர்களுக்குத் தெரியாமலேயே பாதிக்கப்படலாம். மின்னஞ்சல், சமூக வலைத்தளங்கள், மெசேஜிங் செயலிகள் போன்றவற்றில் உள்ள எவ்வித இணைப்புகளையும் திறப்பதற்கு முன் எச்சரிக்கையாக இருக்கவும்.

4. **உங்களது பாதுகாப்பு மென்பொருளைப் புதுப்பித்து வைத்திருக்கவும்.**
உங்கள் சாதனங்களை மிக அண்மைத் தீங்குநிரலிலிருந்து (malware) பாதுகாப்பதில் புதுப்பிக்கப்பட்ட பாதுகாப்பு மென்பொருள் முக்கியப் பங்கு வகிக்கிறது. இணையம் வாயிலாக மற்றவர் உங்கள் கணினிக்குள் அதிகாரமின்றி நுழைவதைத் தடுக்க உங்கள் கணினியின் தீச்சுவரையும் (firewall) நீங்கள் செயல்படுத்த வேண்டும்.

5. **ஒரு மொபைல் பாதுகாப்புச் செயலியை நிறுவவும்.**
நீங்கள் பதிவிறக்கம் செய்யும் ஒவ்வொரு செயலியிலும் தீங்குநிரல் மற்றும் உளவுநிரல் (spyware) இருக்கின்றதா என்பதை ஸ்கேன் செய்து, பாதுகாப்பற்ற இணையத்தளங்களிலிருந்து உங்களைப் பாதுகாக்கின்ற ஒரு மொபைல் பாதுகாப்புச் செயலியை நிறுவவும். அவற்றின் விலை அதிகமில்லை. மேலும் அதிகமான சேமிப்பிடத்தையும் எடுத்துக்கொள்ளாது.

6. **அதிகாரப்பூர்வ இணையத்தளங்கள் மற்றும் செயலிக் கூடங்களிலிருந்து (app stores) மட்டுமே மென்பொருளையும் செயலிகளையும் பதிவிறக்கம் செய்யவும்.**
அதிகாரப்பூர்வமற்ற ஆதாரங்களிலிருந்து பதிவிறக்கம் செய்யப்படுகின்ற மென்பொருளும் செயலிகளும் பல தீங்குநிரலைக் கொண்டிருக்கக்கூடும். அதே நேரம், அதிகாரப்பூர்வ ஆதாரங்களிலிருந்து பதிவிறக்கம் செய்யப்படுகின்ற மென்பொருளும் செயலிகளும் பாதுகாப்பு வல்லுநர்களின் கடுமையான மதிப்பாய்வுகளுக்கு உட்படுத்தப்படுவதால், தீங்குநிரல் தொற்றுகளுக்கான வாய்ப்பு குறைக்கப்படுகிறது.

7. **உங்கள் கணினியில் சேமிக்கப்பட்டுள்ள தகவல்களைக் காப்புப்பிரதி (back up) எடுத்துக்கொள்ளவும்.**
வன்தட்டு (hard disk) செயலிழக்கும்போதோ அல்லது உங்கள் கணினியில் கோளாறு ஏற்படும்போதோ உங்களுடைய தரவு இழக்கப்படாமலிருப்பதை உறுதிசெய்வதற்கு எப்பொழுதுமே முக்கியமான தரவுகளை வெளிப்புறச் சேமிப்புச் சாதனங்களில் (ஃப்ளாஷ் டிரைவ், வெளிப்புற வன்தட்டு போன்றவை) காப்புப்பிரதி எடுத்துக்கொள்ளுங்கள். முதலில் வெளிப்புறச் சேமிப்புச் சாதனத்தை ஸ்கேன் செய்யவேண்டும் என்பதை நினைவில் கொள்ளுங்கள் - நீங்கள் நினைப்பதுபோல அதற்கு அதிக நேரம் எடுக்காது.

8. **பகிரப்பட்ட சாதனங்களில் மற்றும் பாதுகாப்பற்ற கம்பியில்லாத் தொடர்பு (Wi-Fi) வாயிலாக இணையவழிப் பரிவர்த்தனைகளை மேற்கொள்ளாதீர்கள்.**
பகிரப்பட்ட அல்லது பொதுக் கணினிச் சாதனங்கள் தீங்குநிரலால் பாதிக்கப்பட்டிருக்கக்கூடும். இதனால் உங்களது கடனட்டை (credit card) தகவல்களை மற்றவர் மீட்டெடுக்க முடியும். பாதுகாப்பற்ற கம்பியில்லாத் தொடர்புகளைப் பயன்படுத்துவதையும் நீங்கள் தவிர்க்கவேண்டும், ஏனெனில் அவற்றின் வாயிலாக அனுப்பப்படுகின்ற உங்களுடைய வங்கிக் கணக்கு விவரங்கள் உள்ளிட்ட தகவல்களை இணையக் குற்றவாளிகள் கண்டுபிடிக்க இயலும்.

9. **இணையவழிக் கொள்முதல் மோசடிகள் குறித்து எச்சரிக்கையாக இருக்கவும்.**
இணையவழி விளம்பரங்களை எப்பொழுதும் நம்பவேண்டாம். இணையம் வழி பொருள் விற்பவர் உங்களுக்கு அறிமுகமில்லாதவர் என்பதை எப்பொழுதும் நினைவில் கொள்ளவும். எனவே, பணம் செலுத்துவதற்கு முன் அவரது நம்பகத்தன்மையை நீங்கள் சரிபார்த்துக் கொள்ளவேண்டும். கூடுமானவரை, பொருளை உங்கள் கையில் நீங்கள் பெறும்போது மட்டுமே பணம் செலுத்தவும்.

10. **உங்கள் தனிப்பட்ட தகவல்களைப் பிறருடன் பகிர்ந்துகொள்ளாதீர்கள்.**
உங்கள் முகவரி, தொலைபேசி எண் அல்லது இதர தனிப்பட்ட தகவல்களை இணையத்தில் பகிர்ந்துகொள்ள வேண்டாம், அல்லது அவற்றை உங்கள் கடவுச்சொற்களில் பயன்படுத்த வேண்டாம். உங்கள் உண்மையான இருப்பிடத்தையோ அல்லது நீங்கள் எங்குச் செல்லத் திட்டமிட்டுள்ளீர்கள் என்பதையோ வெளிப்படுத்த வேண்டாம்.

இறுதியாக, ஆக அண்மை இணையப் பாதுகாப்புச் செய்திகளுக்கும் உதவிக் குறிப்புகளுக்கும் எமது GoSafeOnline ஃபேஸ்புக் பக்கத்தில் (www.facebook.com/gosafeonline) எங்களைப் பின்தொடருங்கள்.

Live Savvy Tips

Prevention is key in the fight against cyber threats. Practising good cyber hygiene will ensure that we keep our devices and our information safe. By doing so, we are taking responsibility for our cybersecurity and doing our part to create a safer cyberspace for everyone. Here are 10 simple tips you can do today to live savvy with cybersecurity.

1. **Use strong passwords and enable 2FA where possible.**
Ensure that your passwords consist of a combination of uppercase and lowercase letters, numbers and symbols. For an extra layer of security, enable 2FA for your accounts when available.

2. **Be smart when assessing information online.**
Always check the source of your information, whether it is reliable or trustworthy, and cross-check against other reliable sources to verify whether it is indeed a fact and not just an opinion.

3. **Stop and think before you click on links or attachments.**
Cyber criminals use links and email attachments to install viruses, worms and Trojan horses. Even if the sender is a friend, relative or colleague, their devices could be infected without their knowing. Exercise caution before opening any attachment or links on emails, social networking sites or messaging apps.

4. **Keep your security software up-to-date.**
Up-to-date security software is vital in defending your devices against the latest malware. You should also enable your computer's firewall to protect your computer from unauthorised access over the Internet.

5. **Install a mobile security app.**
Install a mobile security app that scans every app you download for malware and spyware, and protects you from unsafe websites. They are not costly and do not take up much storage space.

6. **Only download software and apps from official websites and app stores.**
Software and apps from unofficial sources may come bundled with malware, while software and apps from official sources undergo strict reviews by security experts, thereby reducing the chances of malware infections.

7. **Back up information stored in your computer.**
Back up important data to external storage devices (such as flash drives or external hard disks) regularly to ensure that your data will always be available in the event of a hard disk failure or if your computer becomes compromised. Remember to scan your external storage devices first – it is not as time consuming as you think.

8. **Do not perform online transactions on shared devices, and over unsecured Wi-Fi.**
Shared or public computing devices can be potentially infected with malware, allowing others to retrieve your credit card information. You should also avoid using unsecured Wi-Fi networks as cyber criminals can capture information passing through them, including your bank credentials.

9. **Watch out for online purchase scams.**
Don't always trust online advertisements. Always bear in mind that the online party is a stranger so you should check his or her credibility before making payment. Whenever possible, pay only upon delivery of items.

10. **Keep personal information to yourself.**
Don't share your address, phone number or other personal information online, or use them in your passwords. Don't reveal your actual location or when you plan to be somewhere.

Last but not least, follow us on our GoSafeOnline Facebook page (www.facebook.com/gosafeonline) for the latest cybersecurity news and tips.

An initiative of:
GOsafeonline
Cyber Security Awareness Alliance

Brought to you by:
CSA SINGAPORE

Supported by:
MEDIA LITERACY COUNCIL
NATIONAL CRIME PREVENTION COUNCIL
pdpc PERSONAL DATA PROTECTION COMMISSION SINGAPORE

简单贴士，让您做个精明的网民

在防患于未然才是对抗网络威胁的制胜之道。维持良好的网络安全习惯能保障我们的电子设备和个人信息，而维护本身的网络安全也能为打造更安全的网络空间尽一份力。以下列举一些简单的贴士，让您从即日起做个精明的网民。

1. **尽量使用强度高的密码并启用双重认证功能。**
   请确保您的密码组合拥有大小写英文字母、数字和符号。为增加多一道安全防线，尽量为您的账户启用双重认证功能。

2. **在核实网络信息时保持机警。**
   时刻检查您的信息来源是否可靠可信，并参照其他可靠来源的信息进行比对，以核实所得信息是否确有其事或只属个人意见。

3. **在点击链接或打开电邮附件前，请三思而后行。**
   网络罪犯经常利用链接和电邮附件来安装病毒、蠕虫和特洛伊木马程式。即便发送者是您的亲朋好友或同事，他们的电脑或移动设备也可能在他们毫不知情的情况下遭到入侵。因此，在打开或点击电邮、社交网站或通讯程序上的任何附件或链接时，请三思而后行。

4. **及时更新您的安全防护软件。**
   为防止最新型的恶意软件攻击您的电脑或移动设备，最新版本的安全防护软件是必不可少的。您也应该启用电脑的防火墙，以避免有人通过网络非法入侵您的电脑。

5. **为手机和移动设备安装安全防护应用程序。**
   为手机和移动设备安装安全防护应用程序。这类程序会扫描您所下载的每个应用程序，防止恶意及间谍软件的入侵，让您能避开不安全的网站。这些安全防护程序价格低廉，也不会占据移动设备太多的储存空间。

6. **只从官方网站和应用商店下载软件及应用程序。**
   非官方来源的软件和应用程序可能附带恶意软件，而官方来源的软件和应用程序则经过安全防护专家的严格审查，因此遭到恶意软件入侵的风险较低。

7. **对电脑里保存的信息进行备份。**
   请定期将重要资料备份到外置储存设备（如闪存盘或外置硬盘）。这将确保即便您的硬盘发生故障或电脑遭到入侵，您还能保有这些资料。请先扫描您的外置储存设备，确保储存设备没有被病毒入侵才备份信息。其实，扫描过程并不如您想象中耗时。

8. **请勿使用未加密的无线网络，或在共享设备上进行网络交易。**
   共享或公共电脑设备很有可能会遭到恶意软件的入侵，让不法之徒有机会盗取您的信用卡信息。您也应该避免使用未加密的无线网络，因为网络罪犯能够透过这类无线网络获取包括您的银行验证信息在内的资料。

9. **慎防网络购物诈骗伎俩。**
   别轻易相信网络广告，要切记网络上的卖方是素不相识的陌生人，在付费前应确认对方的可信度，尽量采用货到付款的支付方式。

10. **绝不公开您的个人资料。**
    别在网上公开您的地址、电话或其他个人资料，或在密码中透露这些信息。请也不要公开您的具体位置或出行计划。

最后欢迎关注我们的GoSafeOnline面簿主页（www.facebook.com/gosafeonline），了解有关网络安全的最新资讯与贴示。

Nasihat Cara-cara untuk Menjadi Orang Bijak Siber

Pencegahan merupakan kunci untuk memerangi ancaman siber. Mengambil langkah keselamatan semasa melungsuri ruang siber akan memastikan peranti dan maklumat kita kekal selamat. Dengan berbuat demikian, kita bersikap bertanggungjawab terhadap keselamatan siber dan memainkan peranan kita untuk mewujudkan ruang siber yang lebih selamat untuk semua. Berikut adalah 10 nasihat mudah yang anda boleh amalkan sekarang untuk menjadi seorang yang bijak dengan keselamatan siber.

1. **Gunakan kata laluan-kata laluan yang kukuh dan gunakan 2FA jika boleh.**
   Pastikan kata laluan-kata laluan anda terdiri daripada gabungan huruf besar dan huruf kecil, nombor-nombor dan simbol-simbol. Untuk langkah keselamatan tambahan, gunakan 2FA untuk akaun anda jika ia disediakan.

2. **Anda mesti bijak ketika memperolehi maklumat dalam talian.**
   Sentiasa periksa sumber maklumat anda, sama ada ia boleh dipercayai atau tidak, dan semak dengan sumber-sumber lain yang boleh dipercayai untuk mengesahkan sama ada maklumat tersebut benar atau tidak dan bukan sekadar pendapat.

3. **Perhatikan dan fikir dahulu sebelum anda klik pautan atau lampiran.**
   Penjenayah siber menggunakan pautan dan lampiran e-mel untuk memasang virus, cecacing dan kuda Trojan. Walaupun pengirimnya ialah rakan, saudara atau rakan sekerja anda, peranti mereka mungkin telah dijangkiti tanpa pengetahuan mereka. Berhati-hati sebelum membuka sebarang lampiran atau pautan dalam e-mel, laman rangkaian sosial atau aplikasi pesanan ringkas.

4. **Pastikan perisian keselamatan anda sentiasa dikemas kini.**
   Perisian keselamatan yang dikemas kini penting untuk melindungi peranti anda daripada perisian hasad yang terkini. Anda juga harus membolehkan tembok api (firewall) yang ada pada komputer anda untuk melindungi komputer anda daripada dicerobohi melalui Internet.

5. **Pasang aplikasi keselamatan alat mudah alih.**
   Pasang aplikasi keselamatan alat mudah alih yang mengimbas setiap aplikasi yang anda muat turun untuk mengesan perisian hasad dan perisian intip, dan melindungi anda daripada lelaman web yang tidak selamat. Ia tidak terlalu mahal dan tidak memerlukan ruang penyimpanan data yang banyak.

6. **Hanya muat turun perisian dan aplikasi daripada lelaman dan kedai aplikasi rasmi sahaja.**
   Perisian dan aplikasi daripada sumber tidak rasmi mungkin mengandungi perisian hasad, manakala perisian dan aplikasi daripada sumber-sumber rasmi diperiksa secara ketat oleh pakar-pakar keselamatan, dari itu ia mengurangkan kemungkinan jangkitan perisian hasad.

7. **Buat salinan maklumat yang disimpan dalam komputer anda.**
   Buat salinan data yang penting pada peranti penyimpanan luar (seperti pemacu kilat atau cakera keras luar) secara kerap untuk memastikan data anda sentiasa boleh didapati sekiranya cakera keras gagal berfungsi atau jika komputer anda diceroboh. Jangan lupa untuk mengimbas peranti penyimpanan luar anda terlebih dahulu - ia tidak mengambil masa yang panjang seperti yang anda fikirkan.

8. **Jangan lakukan transaksi dalam talian di peranti yang dikongsi, dan menerusi Wi-Fi yang tidak dikawal.**
   Peranti yang dikongsi atau komputer awam berkemungkinan besar dijangkiti perisian hasad yang membolehkan orang lain mendapat kan butir-butir kad kredit anda. Anda juga harus elakkan daripada menggunakan rangkaian Wi-Fi yang tidak dikawal kerana penjenayah siber boleh mendapatkan maklumat dengan melalui masuk termasuk maklumat peribadi perbankan anda.

9. **Awas terhadap penipuan pembelian dalam talian.**
   Jangan selalu percayakan iklan dalam talian. Sentiasa ingat bahawa pihak dalam talian adalah orang yang tidak dikenali, oleh itu anda harus periksa sama ada mereka boleh dipercayai atau tidak sebelum membuat pembayaran. Seberapa yang boleh, buat pembayaran hanya selepas anda menerima barangan anda.

10. **Jangan dedahkan maklumat peribadi anda.**
    Jangan berikan alamat, nombor telefon atau maklumat peribadi anda yang lain dalam talian, atau menggunakan alamat, nombor telefon atau maklumat peribadi anda sebagai kata laluan anda. Jangan beritahu lokasi sebenar anda atau bila anda merancang untuk berada di sesuatu tempat.

Akhir sekali, ikuti kami di halaman Facebook GoSafeOnline kami (www.facebook.com/gosafeonline) untuk mendapatkan berita dan nasihat tentang keselamatan siber yang terkini.