采取适当的
资讯安全措施
以享用互联网

GOsafeonline.sg
Cyber Security Awareness Alliance

https://www.gosafeonline.sg/

ASEAN · JAPAN
Information Security Awareness

了解 保护 坚持

资讯安全

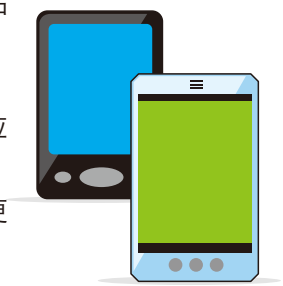
安心使用互联网

智能手机安全

智能手机在全球盛行，它也在流动电话的销售比率中占了绝大部分。

智能手机是拥有尖端科技的器材。它就像是一台电脑，能让我们浏览网页，也能让我们下载并使用各式各样的应用程序。

智能手机的操作系统*1和应用程序*2经常更新*3。有些更新会提供更多的功能、而有些则会加强智能手机的安全。



*1 - OS是操作系统的缩写。它是一个控制电脑或智能手机的软件。在电脑方面，OS管理各种功能，如键盘输入的数据、营光屏输出的画面、和传送到打印机的资料。

*2 - 应用程序是有特定用途的软件，例如文字处理或制造电子表格。用户可以选择把他们需要的应用程式安装在含有基本功能的电脑操作系统。

*3 - 软件更新是指为软件稍作修改、修正错误、或提供功能上的改进。在更新软件之后，用户便能享用最新的软件版本。除了更新电脑软件，用户也应该为网络安全软件更新版本。

风险及威胁

1 专攻智能手机的恶意软件足日增加。若您的器材遭受恶意软件的感染，您储存在器材内的电话簿或其它个人资料便有可能被传送到他人手中。您也可能因此遭受金钱损失。

2 您在下载应用程序前，应先查证它索取的资料。有些应用程序会索取您的器材或电话簿资料，并在您不知情的情况下将其传送给他人。举个例子，某个应用程序表面上的功能可能是增加您器材的电池寿命，但其实它的真正功能是盗取您的电话簿资料！

防范措施

- 确保您智能手机的操作系统、应用程序和防毒软件拥有最新的版本。您的防毒软件也该拥有最新的病毒识别码。既然智能手机储存着联络电话和许多机密资料，在使用时务必要更加小心。
- 在下载应用程序前，您应先确认下载的网址是否可信，而程序供应者是否可靠。另外，您也需详读程序索取的资料的使用协议和服务条款，避免机密资料被盗用。

无线网络安全

近年来，电脑变得轻便，而智能手机也越来越盛行。这股趋势增加了无线网络的使用，而用户无论在家中或职场都能通过无线网络上网。

除了网络供应商所提供的需付费无线网，许多公共场所如机场、购物商场、咖啡座等也有提供免费的无线网络。

风险及威胁

1 我们家中或职场的无线网络所覆盖的范围都可能他人连接至我们的网络。因此，我们应确保无线网络拥有适当的安全措施以避免传送的讯息被截夺。此外，不法之徒也可能通过无线网络盗取个人或机构的机密资料，或通过它来向机构的服务器发动攻击。

2 当您使用公共用无线网络时，您可能会连接至黑客所设置的接入点。一旦连接，即便您的通讯已被加密，您所传送的讯息也可能被截夺。

防范措施

- 您在家中使用的无线网络应该设置如WPA2的数据加密，以确保传送的讯息无法被截夺，以及防止非授权的接入。您也该为无线网络加密选择一个长而随机的密码。
- 当使用公共无线网络时，您该选择浏览拥有SSL*4 加密的网站（“https” 开头）。在上网之前，您也该确保所使用的电脑已将文件共享的功能关闭。

*4 - SSL(Secure Sockets Layer 安全套接层) 是为网络通信提供安全及完整数据的一种安全协议。

点击欺诈

点击欺诈指的是在网页设置图像或影像，而在网页访客点击它时显示需缴付的报名费或服务使用费，骗取款项。

近日来，点击欺诈除了在网页盛行，也在智能手机的应用程序和社交媒体服务*2（例如博客*1）传播开来。

点击欺诈的攻击手法，除了在第一次点击便出现付款屏幕，也有在点击了几个事项如年龄认证、等后出现的。除此之外，攻击者所使用的其它技巧也越来越狡猾和复杂，例如付款屏幕可能在器材被关闭后仍然存在。

*1 - 博客是网络日志的简写，用户可以像日记似的叙述自己的观念或意见。博客的访客也可以自由的对内容发表他们的意见。

*2 - SNS是社交网络服务的缩写。社交网络服务拥有许多功能，　例如将我们的网上日记或相簿开放给大众，或让用户能在一个虚拟社区内自由的交换意见。

风险及威胁

1 点击网页上免付费的图像或影像有可能会将用户引致欺诈网站，被威胁缴付款项。

2 在某些情况下，受害者的IP*3地址或网络服务提供商的资料会显示在付款屏幕上，使受害者误以为自己的身份已被辨认，而在畏惧的情况下付款。

*3 - IP地址是电脑等器材连结至互联网时自动分配给器材的登记号码。

防范措施

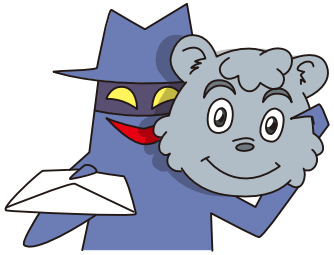
- 使用网页过滤软件或其它最新的网络安全软件阻止电脑连接至恶意网站。在下载智能手机应用程序时，也该确认开发者是否可靠。
- 若您使用电脑上网，请谨记单次点击是不能让网站确认您的身份的。因此，切勿同意让网站向您索取的任何费用。
- 若您已是这些欺诈网站的受害者，请向有关政府部门联络，寻求协助。

针对性电邮攻击/鱼叉式网络钓鱼攻击

针对性电邮的攻击者会冒充成目标所认识的人发送电邮。电邮多半含有恶意附件。一旦收件者打开附件，电脑病毒便会感染电脑系统。

攻击者的目标大多是特定的机构或个人用户。攻击者会冒充成目标所认识的人或同事，将含有电脑病毒附件的电邮发送给目标。

针对性电邮攻击多半会窃取受害者的密码或在受害机构的电脑网络散播电脑病毒。



风险及威胁

1 在最近的攻击中，攻击者所用来掩饰身份的攻击方法已变得越来越复杂和先进。攻击者可能使用确实存在的人或部门名称，和只有相关人士知晓的沟通内容发送电邮。

2 若受害者打开攻击者在电邮中加上的附件，电脑病毒便会自动的连接至攻击者的服务器，将电脑中的资料发送过去。

防范措施

- 不要打开任何可疑的电邮附件或点击电邮中的网络链接。
- 若您打开了可疑的电邮，请别慌张或关闭器材。您应把器材的网络连接断开，并向您的科技部门寻求协助。
- 在您的电脑安装防毒软件，并确保它拥有最新的病毒识别码。
- 确保您电脑的操作系统和软件拥有最新的版本。

分布式拒绝服务攻击

分布式拒绝服务攻击采用设置在多个网络的傀儡机，向特定的服务器发送大量的数据以致其通讯网不胜负荷而中断服务器的服务。

风险及威胁

1 攻击者会暗中将恶意程序安装在和最终目标不相关的电脑中进行攻击。因此用户可能在不知觉的情况下攻击另一台电脑。

2 受感染的电脑可能进行分布式拒绝服务攻击以外的攻击。例如，它可能把电脑病毒散播到其它电脑、发送垃圾邮件或污损网站。

防范措施

- 确保连接至互联网的电脑、智能手机或其它器材的操作系统拥有最新的版本。
- 安装防毒软件并确保它拥有最新的病毒识别码。
- 确保您电脑的操作系统和软件拥有最新的版本。

互联网使用礼仪

随着社交网络服务使用量的增加，以往未曾在互联网想到的问题都出现了。

举个例子，用户可能在互联网刊登诽谤并揭发他人的内容、或是公司在互联网发布道歉的公告。

风险及威胁

1 在社交网络上随意刊登的内容可能导致个人资料被披露、诽谤他人或侵犯隐私。

2 随意刊登在互联网的内容可能会导致索赔、法律谴责、甚至使刊登者被逮捕。

防范措施

- 不要通过博客、微博或其它社交网络服务透露不必要的个人资料。上载图像可能透露您的位置资料，所以您也应该谨慎。
- 即使在互联网上，您也需顾虑他人的隐私和尊严，因此在发布信息之前需确认内容。

用户名和密码的正确设置与管理

在互联网使用电邮、购物、进行银行交易和其它服务的身份认证方案有很多种类，而最流行的是用户名和密码组合。

盗取用户帐户信息（例如用户名和密码）的网络攻击日益增加。

风险及威胁

1 如果用户密码使用非常简单的组合（例如4位数的生日日期、“9999”、等等），或用户没小心管理用户密码（例如将密码贴在荧光屏上、等等），不法之徒可能会乘机冒充用户以透露信息或造成金钱损失。

2 如果您在多个网站使用相同的用户名和密码，当其中一个网站的信息被泄露，您其于网站的户口被侵入的可能性会增加。

防范措施

- 设置不易破解的密码，采用至少8个字符长，包含数字、大小写字母和符号的字符串。另外，您的密码也需定期更改。
- 不要与其他人分享您的密码或在多个网站使用相同的密码。若有任何网站通知您的密码被泄漏，您该立即在该网站及其它使用相同密码的网站更换密码。
- 避免在公共场所（例如网吧）的电脑输入个人资料。

垃圾电邮 1

电邮是一种相当方便的通信工具，不论收件人在何处或有多远的距离都可接送邮件。然而，这样的便利可能会造成很多不必要的电邮和垃圾邮件。

电邮服务供应商若需处理大量的垃圾邮件，它们的器材设施可能因无法复核而延误其它邮件的发送和接收。

风险及威胁

1 在有一些情况下，受病毒感染的电脑会随机生成大量的电邮地址，并发送电邮。因此，使用简短和普遍的电邮地址名称可能会使接收垃圾邮件的可能性增大。通过注册伪造的免费服务或虚构的退订程序都能收集成立的电邮地址发送垃圾邮件。

2 此外，打开电邮的附件或点击链接都可能会使接收者登陆黑客网站或使其电脑受到病毒感染。

防范措施

- 电邮地址应该包含多个字符，包括随机数字，使其难以猜测。
- 若非必要，不要随便将您的电邮地址输入到网站或将您的电邮地址显示在网站上。
- 如果非要浏览可疑网站，与其使用网络服务供应商所提供的电邮地址，您可考虑注册另一个免费的电邮地址。

垃圾电邮 2

发放垃圾邮件的方法越来越多样化，意图也越来越恶劣。有些垃圾邮件可能会通过垃圾邮件过滤器的检测进入收件人的电邮信箱。而垃圾邮件不仅会让收件人觉得厌烦和干扰工作，它的内容也可能引导收件人点击意图想骗取钱财的恶意网站。

与电脑相同，智能手机也可能受到垃圾邮件附件中的病毒感染，而在用户不知情之下被遥控而传送大量的垃圾邮件。

风险及威胁

1 在一些情况下，受病毒感染的电脑会随机生成大量的电邮地址，并发送电邮。因此，用户若使用简短和普遍的电邮地址名称可能会使接收垃圾邮件的可能性增大。

2 通过注册伪造的免费服务或虚构的退订程序都能收集成立的电邮地址发送垃圾邮件。此外，打开电邮的附件或点击链接都可能会使接收者登陆黑客网站或使其电脑受到病毒感染。

防范措施

- 您可使用互联网服务供应商或电邮过滤软件所提供的垃圾邮件应对措施服务阻挡垃圾邮件。
- 若收到垃圾邮件，您立即删除即可，无需将其打开。此外，不要打开可疑电邮中的附件或点击其链接。您也可将垃圾邮件转发到您的电邮供应商或相关的政府执法部门寻求协助。
- 您的智能手机和电脑都该采取防范措施。

保护您的智能手机和电脑。

智能手机和电脑都是有用的工具，
但它们却面临着许多威胁，
像是遭受病毒感染。
记得遵守三大资讯安全贴士
以便安全的使用您的电脑和智能手机。

资讯安全的三大贴士

小心的处理重要的个人资料。

确保您的电脑拥有最新的版本。

切勿登陆可疑的网站或打开不熟悉的电邮。

采取资讯安全措施就象在车上需系上安全带一样重要。它是我们在使用智能手机或电脑时绝不能忘记的。