网络安全工具包

防止网络钓鱼，保护公司资产并创建强健的密码

网络钓鱼

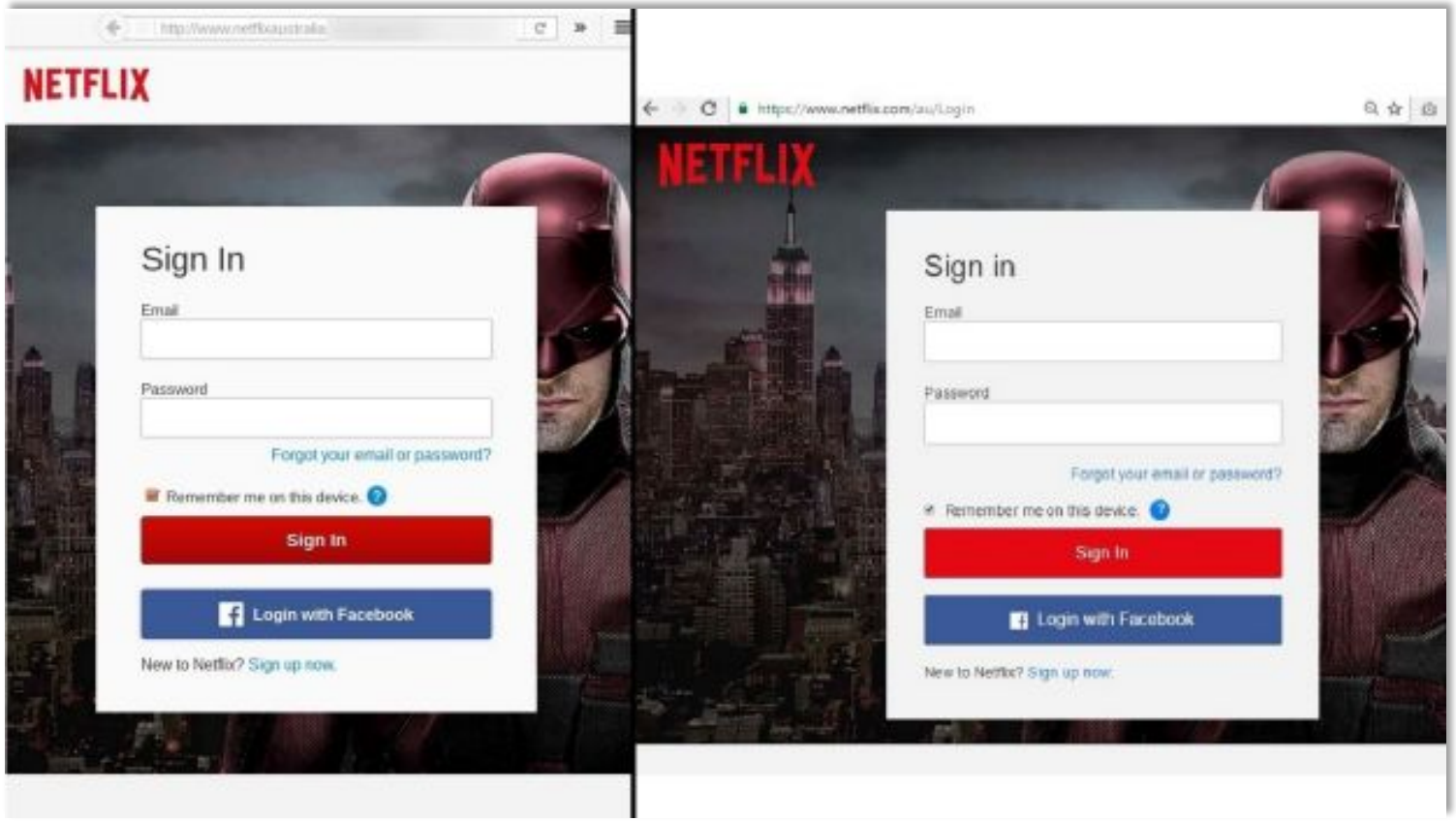
无论在哪里都是各大企业的主要威胁

什么是网络钓鱼？

“网络钓鱼是采取社交工程和技术手段窃取客户的个人身份数据和财务账户证书的一种犯罪机制。”

- 2016年钓鱼攻击的数量高达 1,220,523，比2015年增加了65%。
- 每天平均发现 190,000 个新恶意软件样本。

钓鱼网站：哪个是假冒网站?



图片来源： *http://www.theage.com.au/business/consumer-affairs/phishing-emails-and-other-online-scams-on-the-rise-as-australians-lose-millions-of-dollars-20161115-gspnar.html*

CSC

影响：泄漏成本

在所有泄漏事件中，48% 是由恶意或犯罪攻击导致的。

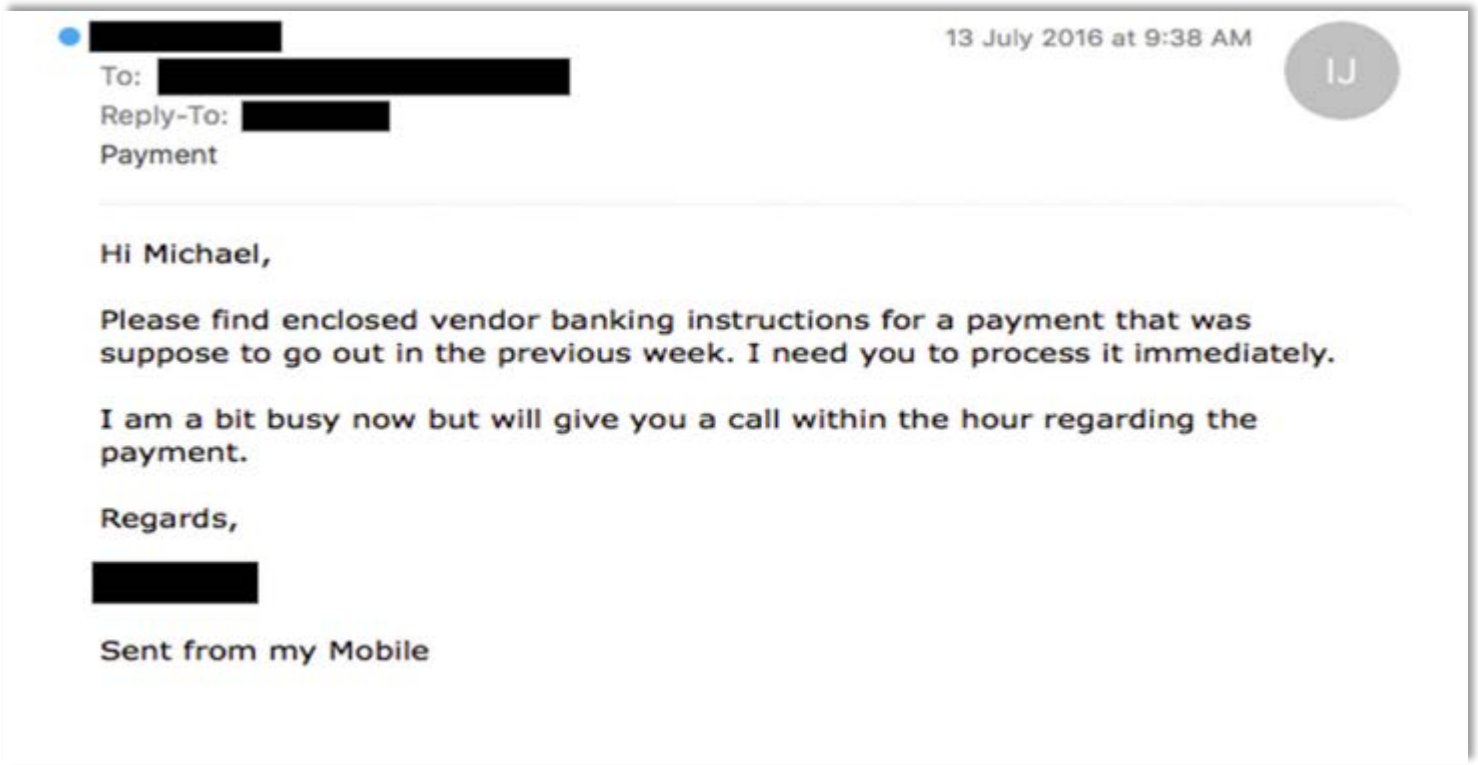
在全球范围内，2013 年到 2015 年之间通过电子邮件进行的网络钓鱼至少造成了总计 31 亿美元的损失。

它们如何运作

- 网络罪犯使用与被假冒品牌相似的图片、正确语法和关键词组。
- 他们发送的消息引起人们的恐惧，催促他们立即做出回应。
- 网络罪犯假冒权威人物让自己更加有说服力。

网络钓鱼攻击要比我们想的更加精细、更加无处不在且另人深信不疑。

来自权威人士的紧急邮件示例



图片来源： *http://www.mailguard.com.au/blog/whaling-ceo-fraud-business-email-compromise-targeted-spear-phishing-attacks-continue-to-trouble-businesses*

CSC

网络钓鱼的类型：电子邮件网络钓鱼

现在，企业面临的最大威胁就是网络钓鱼，包括鱼叉式网络钓鱼和 CEO 电子邮件欺诈，它们是使用特定个人或企业的相似物来进行的一种电子邮件网络钓鱼尝试。

- 30% 的网络钓鱼电子邮件会被打开，而这些中的 12% 会继续单击链接或附件 。
- 全球 97% 的人们无法正确识别精细的网络钓鱼电子邮件。

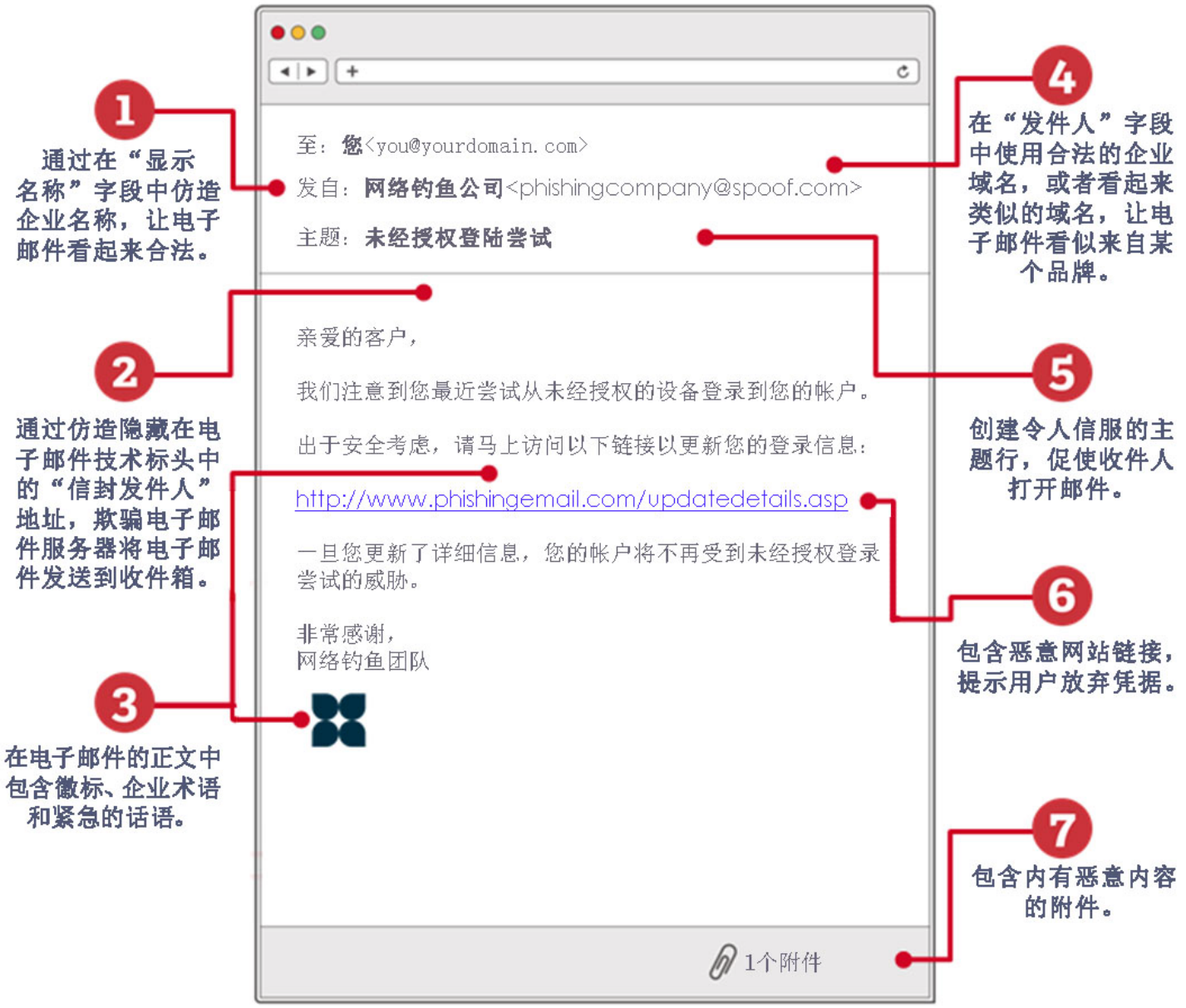
网络钓鱼的类型：电子邮件网络钓鱼

此外：

- 网络罪犯不断进化他们的网络钓鱼电子邮件策略，他们会躲过垃圾邮件筛选器。
- 社交媒体信息的易于获得也使得研究工作变得非常容易，从而可以创作出令人深信不疑的网络钓鱼电子邮件。
- 在一个每个人都在无时不刻地使用智能手机的时代，他们会定期查看电子邮件，这意味着他们会更快地阅读网络钓鱼电子邮件，从而为网络罪犯打开了另一扇漏洞之门，尤其是在员工认为自己收到的是 CEO 在晚上 9 点发出的紧急电子邮件时。

网络钓鱼电子邮件剖析

全球 97% 的人无法正确识别精细的网络钓鱼电子邮件



让收件人单击的前五电子邮件诱骗清单

引自 Proofpoint 的原文， 下一代网络安全企业

“请查看附上的发票”

“单击此处打开您的扫描文档”

“您的包裹已发货”

“我想下单购买所附的清单”

“请确认这笔交易”

关于电邮：请 / 请勿

- 不管来自哪里，都要小心对待所有附件。 特别是可疑格式的附件，例如 .zip、.exe。

- 将鼠标移到链接上（不单击）来验证它们指向的是否是正确的网站 URL。 确保这是您打算访问的网站；您可以看到链接的登录页面是否确实是您要导航至的品牌，还是该品牌的诱骗网站（其中会包含一串不可识别的的字词、字母和字符）。如有疑问，请勿点击。

- 在点击“回复”电子邮件时，始终要确认收件人的电子邮件地址。 选择手动键入，或者从通讯录中插入，同样，您需要检查网站的 URL。

CSC

关于电邮：请 / 请勿

- 使用垃圾邮件筛选器和最新保护。 最新的防病毒、反网络钓鱼和电子邮件欺诈保护解决方案是基本保护形式。确保定期更新这些保护。

- 访问网站时，寻找绿条和 HTTP 末端的 S。 这是为了检查该网站的安全套接字层证书——您正在输入个人可识别信息的页面和表单的安全登录符号。

CSC

关于电邮：请 / 请勿

- 如果您不认识发件人，请谨慎处理链接和附件。即使您确实认识发件人，也请小心。打电话确认电子邮件的内容，或者直接联系该企业，尤其是当您发现任何可疑情况时。

- 绝不要回复要求提供个人身份或访问信息的电子邮件，尤其是在该要求听起来非常紧急时。即使该要求来自您的 CEO 或 CFO。即使您经常与首席级高管通信。不妨先用电话或当面核对这个人的身份。

- 请勿点击弹出窗口，它可能会将您重定向到欺诈网站或下载恶意软件。

- 也请谨慎对待实时聊天窗口，尤其是在他们要求提供个人证书时。

CSC

网络钓鱼的类型：电话

也称为语音网络钓鱼或“vishing”，可以使用电话来索要个人信息。

呼叫人 ID 可以假冒，使用复杂的自动电话系统可让人相信该呼叫来自您的银行（关于您的信用卡或银行活动），并且该呼叫非常紧急！！！

也可以使用通常包含一个立即采取行动呼吁的短信（短信网络钓鱼，或“smishing”），如可单击的链接或可呼叫的号码，以“确认”您的个人信息。

如果您单击或呼叫，则可能会在您的手机上安装可窃取密码的恶意软件。

关于电话：请 / 请勿

- 始终应确认呼叫人的身份。 如果您接起电话，请要求提供回拨号码及分机号，或者要求提供他们应该已存档的有关您的一段信息。

- 在互联网上调查对同一号码的报告。 不熟悉的呼叫人 ID 格式或国家代码可能指示来自自动系统的 IP 语音呼叫或短信。

- 查找该组织的客户服务号码。 不直接呼叫电话或短信中给出的号码，而是应通过查看您的信用卡、银行账单或者起码上网确认过的正确号码。

CSC

关于电话：请 / 请勿

- 绝不要回复 smishing 短信。 并且绝不要单击链接，尤其是没有透露其目的地的缩短的链接。

- 绝不要透露您的个人银行信息。 一定要保密保管您的支付密码和 CVV 号码；银行绝不会要求提供此类信息，因为这些信息已在您的帐户中存档。

CSC

网络钓鱼的类型：社交媒体

社交媒体几乎没有安全控制，从而网络罪犯可以很轻松地设置欺诈帐户模仿真实的企业（而且免费），逼真的徽标、内容、促销信息等一应俱全。罪犯有时也自称是这家被模仿企业的员工，帐户链接到实际的企业，从而获得用户对社交环境的信任。

- 现在，每 5 次网络钓鱼尝试中就有 1 次是通过社交媒体进行的。

- 在社交媒体上联系客户服务获取帮助时，请务必谨慎；发送到 *@customerservice* 的社交媒体推文很容易就会被来自的 *@customer-service* 的回复所拦截。

关于社交媒体：请 / 请勿

- 注意社交媒体评论以及对您询问的回复。 它们可能来自欺诈帐户。相反，请使用官方渠道联系企业。

- 注意您将社交资料链接到哪些网站和应用程序。

关于社交媒体：请 / 请勿

- 请勿将未经验证的联系人添加到社交媒体帐户，即使它们声称来自您的企业。在您做好功课之前，请务必谨慎添加陌生人，例如招聘人员。

- 请勿单击不受信任来源中的链接。 许多社交渠道都使用缩短的链接，掩盖了真实 URL；该链接可能是垃圾邮件或恶意软件。

- 请勿回复可疑电子邮件或消息。 即使来自朋友，如果看起来可疑或出乎意料，则他们的帐户很可能已经被黑。立即通过其他方式通知他们。

- 绝不要分享机密和财务信息。即使社交媒体保护对话隐私，也不要在社交媒体上分享机密信息，甚至包括账单的照片。

CSC

保护企业资产

降低内在风险

流动劳动力

- 到 2020 年为止，美国的全部劳动力中将近四分之三 的人预计将成为流动人员。
- 到 2018 年为止，预计需要使用 121 亿台移动设备。
- 高德纳咨询公司预测，到 2017 年底，全球超过一半的雇主需要员工“带上自己的设备”。
- 在员工设备上下载的最受欢迎的应用是电子邮件、日历和联系人管理 (84%)，后跟文档和编辑应用 (45%)，然后是内联网 (43%)。

固有的安全风险

持续连接有其固有的风险：

- 在一次信息安全调研中，五分之一的组织由于员工的移动设备而曾遭到过安全威胁，主要是因为连接到恶意软件下载和恶意 WiFi[2]。
- 在调查的组织中，39% 报告 BYOD 或企业自有设备在过去的某个时刻下载过恶意软件[2]。
- 平均来说，员工始终拥有 2 台以上设备，通常人们需要使用 WiFi 进行连接， 很少人仍然使用以太网[3]。
- 很大比例的 WiFi 热点使用的是过时的安全措施或者根本没有采用安全措施[4]。

关于移动设备：请 / 请勿

- 访问安全的网站（检查 URL 中是否有 HTTPS，是否为绿色 URL，是否有加密锁），并尽量不在公共网络上进行财务交易。
- 使用虚拟专用网加密您的在线流量，尤其是在连接到企业网络时。
- 使用安全性强的密码保护您的设备。
- 启用双重认证以增加安全性。

CSC

关于移动设备：请 / 请勿

- 保持软件处于最新状态，使其具有最新安全补丁、防病毒保护、垃圾邮件拦截器和间谍软件检测。
- 在查看电子邮件时注意网络钓鱼威胁和恶意软件链接。
- 将 Bluetooth®蓝牙设备与手机或笔记本电脑进行配对时，确保不在个人身份号码或支付密码可能会受到威胁的公共场所，并将蓝牙设备切换为隐藏（不可发现）模式。

CSC

关于移动设备：请 / 请勿

- 请勿连接到不安全的开放 WiFi 热点（检查是否已启用密码保护作为一个加密指标）。

- 请勿下载您不信任的程序或应用程序。

密码安全

最后一道防线

密码安全的重要性

一个好的密码是用于保护您自己不会遭到数据泄漏的一种简单方式，而且完全免费。

- 经分析，80% 的数据泄漏已确认是为了获得经济利益，
- 并且 63% 的泄漏涉及到默认、较弱的密码或密码被盗。

密码泄漏

密码可以说是挡在网络罪犯染指您的数据之前的最后一道防线。密码可能会通过以下方式泄漏：

- 诈骗分子通过网络钓鱼获取个人的信息，例如用户名和密码证书、网上银行信息等。
- 黑客采用暴力破解攻击系统地计算所有可能密码组合和模式。
- 已经遭到黑客攻击的企业或网站上发生数据泄漏，导致数百万的帐户信息泄漏。

密码通病

在发生数据泄漏的前后，复杂密码最安全。请将密码设置成您可以记住，但是网络罪犯需要花很大心思才能弄明白的组合——因此您不应该使用自己的狗狗的名字。下面列出了您应该避免的一些密码通病：

- 前 3 种最容易受黑客攻击的密码是 *Password1*、*Welcome1* 和 *P@ssword*。
- 在密码中最常用的关键字包括儿女、宠物和城市的名字。
- 在排名前 10 的字符序列中，接近 30% 采用以下格式： 大写字母 (U) 后跟一系列小写字母 (l)，末尾附加数字 (#)，即“Ullllll##”这样的的形式；比如：*Hello11*。

关于密码：请 / 请勿

- 虽然复杂性很重要，但是密码长度是关键。使用长密码（至少 10 个字符）会让网络罪犯更难破解。

- 使用暴力破解技术，8 字符密码在 1 天之内就可以破解；10 字符密码则需要大约 591 天，接近 600 倍的工作量！ 使用您可以记住，而任何其他人看上去却杂乱无章的词组，形成一个短语或句子，例如：*TW2gsi2QT&bd*，它其实是华特 · 迪士尼的名言“The way to get started is to quit talking and begin doing.”（将想法付诸实践，少说多做）的英文缩写形式。 始终使用一个主密码和一个密码管理器。

- 除了安全密码，双重认证也可以帮助您限制威胁。攻击者会将注意力转移到更容易的目标上，而不会花精力破解这两种认证模式。

CSC

关于密码：请 / 请勿

- 避免使用容易被人猜到的密码，例如 Ullll##，或者相邻的键位，例如“qwerty”和“asdf”。
- 请勿在密码中使用词典中的单词、家人或宠物的名字、地址、身份证号码、出生日期、社会安全号或电话号码等机密信息。
- 请勿为多个网站使用相同的密码。如果在多个帐户上重复使用，那么任何一个帐户上出现数据泄漏时，即使最复杂的密码也会变得没用。绝不在任何在线网站上使用您的电子邮箱的密码。
- 请勿以纯文本形式将密码存储在任何计算机上。

CSC

谢谢！