[FRONTCOVER]

[Start Community Language Document 1]

网络安全意识

国家网络安全中心替代格式版本。

本内容由苏格兰领导组织（Lead Scotland）与合作伙伴共同制作，并由苏格兰政府网络适应性部门（Scottish Government Cyber Resilience Unit）拨款。

本指南根据国家网络安全中心网站上的内容编写。

所含信息分为 7 个社区语言文档，分别是：

- 本文档，包括简介并概述您可以采取的用于提高在线安全性的 6 项措施。
- 然后，关于您可以采取的 6 项措施，分别有单独的详细文档。
- 在国家网络安全中心网站 https://www.ncsc.gov.uk/cyberaware/上，可访问提到的所有链接。

提升您的在线安全性的 6 种方法

由于新冠疫情，今年人们花费了更多时间上网。

这意味着，黑客有更多机会进行网络攻击。他们通常会使用以下方法对人们和企业进行攻击：

- 电子邮件和网站骗局。
- 恶意软件 – 这是指可能会损坏您的设备或让黑客进入的软件。

如果黑客进入您的设备或帐户，他们就可以获取您的资金、您的个人信息，或有关您业务的信息。

您可以采取以下六项措施来提高网络安全性：

措施 1 - 为您的电子邮箱使用一个单独的强密码。

措施 2 - 使用 3 个随机词创建强密码。

措施 3 - 将密码保存在您的浏览器中。

措施 4 - 开启双因素认证（简称 2FA）。

措施 5 - 更新您的设备。

措施 6 - 备份您的数据。

[End Community Language Document 1]

[Start Community Language Document 2]

措施 1：为您的电子邮箱使用一个单独的强密码

如果黑客入侵了您的电子邮箱，他们可以重置您的其他帐户密码，并访问您已保存的关于您或您的业务的信息。

您的电子邮箱应该采用不容易猜到的密码，并且应与所有其他密码不同。这将使它更难被破解或猜到。

使用三个随机词是一个好方法，可创建安全而独特的密码让您记住。我们将在下一个文档中更详细地介绍这一点。

您还应该保护自己的其他重要帐户，例如银行或社交媒体。

为什么电子邮箱如此重要？

电子邮箱是您最重要的帐户之一。但是，为什么黑客会关心您的电子邮箱？

想象一下，如果黑客进入了您的电子邮箱。

他们现在可以访问您保存的有关您自己的信息，

或冒充您与他人联系。

但最糟糕的是，他们可以让您无法登入自己的任何在线帐户。

他们只要前往您的任何帐户，并使用“忘记密码”功能来做到这一点。

这会发送一封电子邮件，其中包含用于重置您密码的链接，

黑客可以使用该链接将您封锁在您的帐户之外。

一旦他们重置了一个密码，他们就可以继续为您的其他帐户重置密码。

那么，您如何能保护您的电子邮箱，并帮助防止黑客进入您的所有在线帐户？

为您的电子邮箱使用一个强密码，并确保电子邮箱密码与您使用的所有其他密码都不相同。

这意味着，如果有人破解了您另一个账户的密码，他们将无法使用该密码进入您的电子邮箱。

请记住，您的电子邮箱是您最重要的帐户之一。请确保它的安全。

如何更改您的电子邮箱密码

如何更改以下网站的邮箱密码：

- Gmail.
- Yahoo!.
- Outlook.
- BT.
- AOL Mail.

如果此处未列出您的电子邮箱，您应在线搜索提供商的建议，以了解如何更改您的电子邮箱密码。

针对个体商户和小型企业的密码建议

如果您是企业主，则您的帐户可能会包含有关您的客户、企业或财务的敏感信息。

如果您的帐户不安全，则您的业务可能存在更容易遭受网络攻击的风险。这可能会使您的业务面临法律或财务风险，并有违反《通用数据保护条例》（简称 GDPR）的风险。

如果您的公司有员工，您应确保他们不要将密码存储在设备附近，并且在不使用设备时将其锁定或关闭。

欲了解更多信息，请参阅国家网络安全中心的《小型企业指南》（Small Business Guide）。

在国家网络安全中心网站 https://www.ncsc.gov.uk/cyberaware/上，可访问提到的所有链接。

[End Community Language Document 2]

[Start Community Language Document 3]

措施 2：使用三个随机词创建强密码。

当您在多个重要帐户中使用不同的密码时，可能很难记住所有密码。

使用三个随机词是创建容易记住的强密码的好方法。

请勿使用容易猜到的词（例如您宠物的名字）。如果需要，可以包含数字和符号。

例如：RedPantsTree4!

将密码保存在浏览器中将有助于您进行管理，我们将在下一个文档中对此进行详细介绍。

测试您对于创建强密码的知识

在这些密码中，您能猜出有哪些没有出现在最易被破解的前 10 万个密码中吗？

- arsenal22
- 1v&upjw3nt
- p@55w0rd
- RedPantsTree
- Victoria!
- 2011977

答案是 RedPantsTree。

黑客们会分享包含数百万个已泄露的密码的在线列表。

3 个随机词可以简便地创建新密码，该密码更有可能只为您所知，并且不太可能被猜中。

在国家网络安全中心网站 https://www.ncsc.gov.uk/cyberaware/上，可访问提到的所有链接。

[End Community Language Document 3]

[Start Community Language Document 4]

措施 3：将密码保存在您的浏览器中

在浏览器中保存您的密码是指让您的网络浏览器（例如 Chrome、Safari 或 Edge）记住您的密码。

这可以有助于：

- 确保您不会丢失或忘记您的密码。
- 保护您免受某些网络犯罪的侵害，例如假冒网站。

相比使用弱密码或在多个地方使用相同的密码，在浏览器中保存密码更安全。请确保保护好您已保存的密码，以防万一您的设备遗失或被盗。

如何保护您已保存的密码

可以访问您的设备的人可能也可以使用您保存的密码来访问您的帐户。

与通过特定软件破解密码的互联网远程攻击相比，这种网络犯罪要普遍得多。

为了确保您受到保护，您应该：

- 在不使用设备时将其关闭或锁定。
- 使用强密码保护您的设备。
- 对所有设备和帐户启用双因素认证。
- 如果您的设备支持，则开启生物特征识别（脸部识别或指纹识别）。

您还应该定期备份您的数据。如果设备遗失或被盗，这将帮助您恢复重要信息。

如何在浏览器中保存您的密码

了解如何在以下浏览器中保存您的密码：

- Google Chrome.
- Microsoft Edge.
- Firefox.
- Safari.

您知道吗？

您可以从任何使用同一浏览器登录的设备访问您已保存的密码。

增加额外的保护

一旦您已为所有设备和服务设置了单独的强密码后（措施 1 到 3），您可以采取其他措施来降低被黑客入侵的风险（措施 4 到 6）。

在国家网络安全中心网站 https://www.ncsc.gov.uk/cyberaware/上，可访问提到的所有链接。

[End Community Language Document 4]

[Start Community Language Document 5]

措施 4：开启双因素认证（简称 2FA）

双因素认证（2FA）有助于阻止黑客进入您的帐户，即使他们已经获得您的密码。

某些网上银行会自动使用 2FA。它通过询问更多信息来证明您的身份，例如，将验证码发送到您的手机。

如何开启双因素认证（2FA）

对于您的大多数帐户而言，您将需要手动开启 2FA。并非所有帐户都提供 2FA。网上银行会自动使用 2FA。

2FA 也称为两步验证，或多因素认证。

视频：2FA 的工作原理

在 YouTube 上可以观看有关 2FA 的工作原理的视频。

为电子邮箱开启 2FA

- Gmail.
- Yahoo.
- Outlook.
- AOL.

为社交媒体开启 2FA

- Instagram.
- Facebook .
- Twitter.
- LinkedIn.

在国家网络安全中心网站 https://www.ncsc.gov.uk/cyberaware/上，可访问提到的所有链接。

[End Community Language Document 5]

[Start Community Language Document 6]

措施 5：更新您的设备

过时的软件、应用程序和操作系统都存在缺陷。这使它们更容易被黑客入侵。

公司通过发布更新来修复这些缺陷。当您更新设备和软件时，这有助于防止黑客入侵。

在您的设备和提供更新的软件中开启自动更新。这意味着您不必记住手动更新。

某些设备和软件需要手动更新。您可能会在手机或电脑上收到提醒。不要忽略这些提醒。更新将有助于确保您上网时的安全。

如何开启自动更新

了解如何在以下系统中开启自动更新：

- Apple - Mac
- Apple - iPhone 和 iPad
- Microsoft Windows 10. – 在 Windows 10 中搜索更新
- Windows 7 不再受支持。您应该升级到 Windows 10。
- 安卓智能手机和平板电脑
- 安卓 app 应用

问：公司如何解决他们软件中的缺陷？

- 绷带
- 补丁
- 修复

答：当某个公司发现他们软件中的缺陷时，会发布一个“补丁”进行修复。这有助于确保您的信息安全。

在国家网络安全中心网站 https://www.ncsc.gov.uk/cyberaware/上，可访问提到的所有链接。

[End Community Language Document 6]

[Start Community Language Document 7]

措施 6：备份您的数据

备份是指为您的信息创建一个副本，并将其保存到其他设备或在线存储到云存储中。

定期备份意味着您将始终存有您的信息的最新版本。如果您的数据丢失或被盗，这将有助于您更快地恢复。

您也可以开启自动备份。这将定期将您的信息保存到云存储中，而您无需自己操作。

如果您将信息备份到 USB 记忆棒或外接硬盘上，请在不进行备份时将其与电脑断开连接。

您知道吗？

在更新设备之前，您应该始终备份数据。

这是因为更新有时可能会删除或更改文件。

如何开启自动备份

如何在以下系统中开启自动备份：

- Apple – Mac.
- Apple - iPhone 和 iPad.
- 安卓
- Microsoft Windows 10 和 Windows 8 OneDrive.

为个体商户和小型企业提供的备份建议

备份数据意味着，如果的确发生网络攻击事件，您的企业仍能继续运营。
首先找出对您的业务最重要的那些数据。这可能是财务、合同、客户或供应商信息。确保对其定期备份。
您还应该知道在数据丢失的情况下如何还原备份。

欲了解更多信息，请参阅国家网络安全中心的《小型企业指南》（Small Business Guide）。

在国家网络安全中心网站 https://www.ncsc.gov.uk/cyberaware/上，可访问提到的所

有链接。

[End Community Language Document7]

[END OF DOCUMENT]