Subjectline：网络安全提示，帮助您保持安全

致 NYCHA 居民：

现正值开展网络安全宣传月，我们想向您介绍一些有助于您在家和工作中使用网络时保持网络安全的信息。 感谢您帮助我们的世界保持网络安全。

做好本分。#BeCyberSmart.

保障网络安全是每个人应尽的责任。 您可尽自己的努力，报告任何可疑现象，采取更强的安全措施，并帮助提高警惕。

如何明智使用網絡

去年，针对美国企业的网络攻击导致的破坏情况上升了百分之 17。 全国共有 1,474 起系统被成功入侵的案例。 网络罪犯不仅仅是使用技术偷窃资料 -他们还利用人类的错误和我们的本性行为分享我们生活中所使用的信息。

保持警惕：只因一个错误。 数据泄露很少是由于犯罪分子通过机构的基础设施进行黑客攻击的结果。 通常，他们利用一个简单的弱点开始。 用户只要被诱骗泄露了其密码和其它信息，那么所有关于这个用户所使用的信息和数据将会被暴露。 时刻保持警惕，防止网络钓鱼和社会工程的攻击。 时刻谨慎处理不寻常的信息来源，不要点击陌生的链接，并立刻通过发送邮件 (邮址：phish@nycha.nyc.gov) 举报与 NYCHA 相关的可疑信息或邮件。

保持网络安全的简单技巧

1. **如果您看到什么，就说出来**

   如果您发现 NYCHA 的网页或 NYCHA 的应用程序有任何异常，请致电 NYCHA 客户服务中心（CCC）举报，电话：718-707-7771。

2. **商业信息就是个人信息** 很多人在工作中处理敏感的资料或数据。 这些数据不一定是信用卡或社会安全号码 -可以是任何职员或客户的数据，特别是任何属于某个特定用户的数据。 不要向机构以外的任何人泄露公司数据。

3. **保持密码智能和安全** 用户所设置的密码应该是容易记住但难以被猜测的。 您可使用一个词组或一系列单词，但记得包括足够多的随机元素让人无法猜测您的密码。 谨记，尤其是当您在家办公，保持所使用的路由器，网络，和所连接设备的正确备置。

4. **随时更新** 确保您的软件定期使用最新的版本更新。 确保您用于办公的电脑都安装了病毒/恶意软件保护程序，并定期进行病毒扫描。

5. **工作结束后，仍要明智使用网络** 社交媒体也属于诈骗工具的一部份。 网络攻击者可以通过谷歌（Google），脸书（Facebook）或任何网站查找有关您的信息。 避免在社交

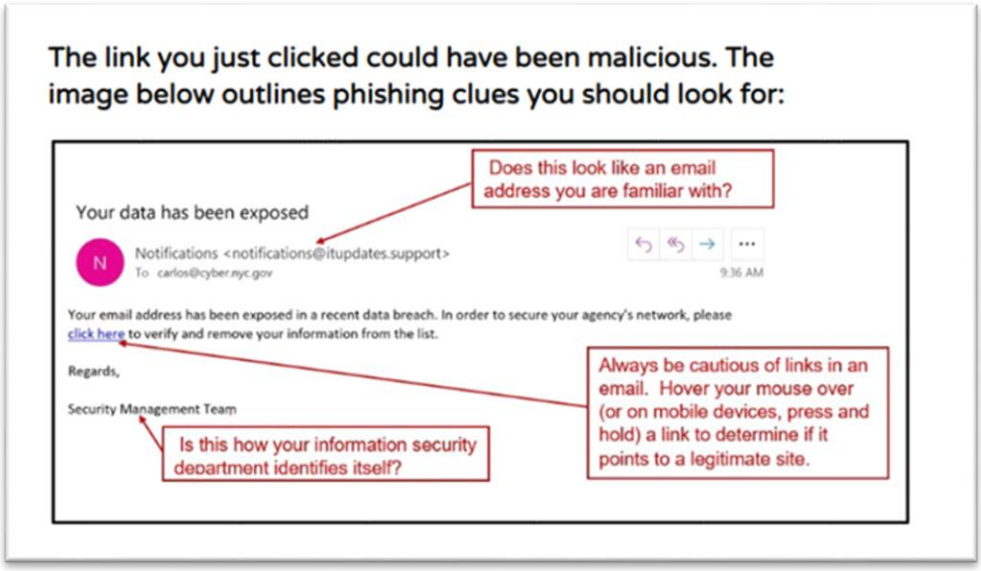
媒体或任何网络分享潜在的敏感信息，切勿使用社交平台进行与工作相关的业务或交换敏感信息。

了解更多

点击观看这些互动视频了解更多如何 ##BeCyberSmart 明智使用网络的详情

什么是网络钓鱼(Phishing)？

您在邮件，社交媒体帖子，短信和网上广告中所看到的链接通常都是网络罪犯试图窃取您的个人资料的手段。 即使您知道其来源，如果这些链接可疑，请删除。 不要点击陌生人发送的链接。 下图是辨别企图网络钓鱼的方法：



什么是勒索软件（ Ransomware）？

勒索软件是一种流氓软件，或恶意软件，阻止您进入您的电脑文件，连接系统或网络并要求您支付赎金才能再次进入或连接。 您可通过打开邮件的附件，点击广告，关注链接，或浏览恶意软件关联的网站，在不知不觉中将勒索软件下载至您的电脑上。 一旦下载了勒索软件，它将锁定您电脑或所存储的资料和文件。 当您发现您无法再打开您的资料或文件或看到电脑显示的受到攻击并要求您支付赎金的提示信息时，您才会发现您的电脑已受到病毒感染。

避免下载勒索软件-或任何类型的恶意软件的最好方法是做一个谨慎和尽责的电脑用户。 恶意软件的经销商越来越精明，您需要格外谨慎您所下载和点击的链接或程序。

谢谢合作！

格雷戈里·罗斯（Greg Russ）
主席兼行政总监