提高在家办公安全性的几个意见

目前，许多公司都要求其工作人员远程工作。 远程工作可能会带来一些新的安全问题，尤其是对于不熟悉 office 的人而言。

下面是一些有关如何使用家庭更安全的提示。

1.1 选择一个好的工作区

有很多关于挑选 ergonomically 舒适的空间的建议，以及可以最大限度地减少干扰的地方，但也有一些安全注意事项。

1. 选择一个私人空间。 如果您正在家里工作，这可能比在咖啡店或图书馆工作时更容易。 选择用户无法 "肩冲浪" 的位置;在你的屏幕上查看你的肩。

   如果找不到要使用的私人位置，请考虑获取隐私筛选器。 这是一种可附加到你的屏幕的防护板，因此很难阅读屏幕上的内容，除非你在它前面。

2. 如果你有电话会议或视频会议，请注意其他人是否可以 eavesdrop，即使是无意间也可以。 即使在戴上耳机) (有时也是如此。 讲话时，其他人可能仍然能够听到您的声音。 请确保您使用的是视频会议软件和高级安全功能（如 Microsoft Teams ）。 了解详细信息
3. 不允许家庭成员使用您的工作设备。 如果你必须离开设备才能转到厨房或卫生间，请锁定你的设备，以防其他人看到你正在处理的内容。 在 Windows 设备上按 Windows 徽标键 + L，或在 Mac 上 Control + Command + Q，快速锁定你的屏幕。 当您返回时，您必须进行快速登录，一切都应位于您离开时的位置。
4. 仅使用已加密的 Wi-fi for business。 使用 WPA 加密的 wi-fi 比 Wi-fi 加密更安全，但对于所有访问都开放。 如果您在家工作，请确保您的家庭 Wi-fi 网络是安全的-所有家庭路由器都支持加密。 了解详细信息
5. 如果需要访问在公司位置实时的资源（如服务器），请使用 VPN (虚拟专用网络) 连接到您的 office 网络。 VPN 为你的网络流量创建加密隧道，使其流过并使其他人更难截取你的流量。 如果您不确定您的公司是否提供 VPN 或如何连接到它，请与您的 IT 支持人员联系。 了解如何在 Windows 10 中连接到 VPN。

1.2 确保数据安全

如果您的设备已被访问或被盗，您可以采取一些措施来帮助减少他们可以获取的数据。

1. 使用强身份验证访问你的设备，例如 Windows Hello。 如果你的设备支持，则为 PIN、指纹或面部认可。 了解详细信息

2. 使用多因素身份验证（MFA）访问任何基于云的资源。 MFA 利用多个 "因素"，如发送到移动设备的 PIN 和密码;或 PIN 以及面部或指纹扫描，以便对您进行身份验证。 通常，首次从特定设备登录时，您只需要使用多个因素。 MFA 使其他人可以更轻松地登录。 了解更多信息

3. 现在，我们来思考您使用的密码是个好时机。 如果你使用简单的密码（如 "可爱" 或 "password1"），则最好将其升级为更安全的密码。 长度比复杂程度更重要，尽管这两个角色都有一个角色。 密码长度至少应为 12 个字符，而不能是英文单词或狗的名称。 请考虑使用喜欢歌曲 lyric、电影引述或的短语来创建长而复杂但易于记忆的密码。 了解详细信息
4. 请确保已启用本地驱动器加密，如 BitLocker。 这样，如果设备丢失或被盗，任何本地数据都将很难访问。 了解详细信息
5. 请确保你的设备是最新的安全更新，并且你有一个反恶意软件程序，如 Microsoft Defender 防病毒软件，正在运行。 了解详细信息
6. 使用新式浏览器（如 Microsoft Edge），确保您运行的是最新版本。
7. 将文件存储在安全的云位置，而不是在本地驱动器或可移动媒体上。 安全的云存储（如 SharePoint 或 工作或学校 OneDrive ）意味着即使你的物理设备丢失或被盗，你的数据仍可供你和你的公司使用。 了解详细信息
8. 尽可能使用应用的 web 版本，例如 Word 、 Outlook 或 Excel 。 将文件存储在安全的云位置的另一个好处是，当你使用应用的 web 版本时，你的数据会保留在服务器上，并且不会下载到你的本地设备。 了解详细信息

1.3 保持联络

1. 在远程工作时，请与您的公司保持联系。 您的 IT 部门可能有特殊请求或向您提供新的工具。 如果你怀疑你的设备或数据已受到任何影响，请立即通知 IT 人员，以便他们能够调查情况并采取措施来防止不必要的损坏。
2. 现在，您可以在公司资源之外抵御使用未经批准的工具或存储数据的诱惑。 如果您需要一些内容才能完成工作，请咨询 IT 部门或通过管理链进行升级。 当您不在办公室时，您可能会发现无法正常工作的系统。 现在是让它知道的好时机，这样你就可以一起处理这些问题。
3. 请通知网络钓鱼电子邮件或电话通话。 罪犯通过发送看似来自机构或公司官员的电子邮件来尝试利用恐惧和不确定性，以尝试引诱您单击恶意链接或提供您的私人信息。

   千万不要单击不需要的附件，即使它看起来来自您认识的人。 在打开附件之前，最好始终与该用户核对以确保附件合法。

   如果您收到一封电子邮件，要求您登录到网站，请在浏览器中打开新的选项卡，然后在自己的 URL 中键入 URL (或通过受信任书签访问它) 而不是单击电子邮件中的链接。 了解详细信息

   如果您从您的公司的技术支持部门处收到意外电话呼叫，而您不认识的是您公司的技术支持，请获取其名称，然后挂断并直接拨打公司的技术支持。 如果您收到来自声称来自 Microsoft 支持的意外电话呼叫，您应该立即挂断。 Microsoft 支持从不直接呼叫客户，除非您已与我们联系以寻求支持。

NOVATECH

我们传递价值 / We Deliver Values

联系我们

上海 +86 021-22065380　　北京 +86 010-53605669　　香港 +852 94019304