#

**安全在家办公的 5 个首要步骤**

我们知道在家办公对你们中的某些人来说很陌生，可能难以适应这种新环境。我们的目标之一就是尽量使你能够安全在家办公。以下是安全工作的五个简单步骤。最重要的在于，这些步骤不仅能保障工作安全，还能使你创造安全的家用网络，让你和你的家庭更加安全。



**你**：首先，仅凭技术无法完全保护你，你才是最强的防御。攻击者明白，比起针对你的电脑或其他设备，以你为目标是获得他们所需的最简单方式。如果他们想要获取你的密码、工作资料或控制你的电脑，他们通常会制造紧迫感试图诱骗你交出这些信息。例如，他们伪装成微软的技术支持打电话，声称你的电脑受到了感染。或是给你发送邮件，警告你包裹无法送达，欺骗你点击恶意链接。社会工程学攻击的最常见迹象包括：

* 某人制造巨大的紧迫感，让你恐惧、被恐吓、感到危机或使用重要的最后期限。网络攻击者很擅长制造令人信服的消息，使其看上去似乎来自可信任的组织机构，例如银行、政府或国际组织。
* 迫使你绕过或忽视安全政策或程序，或是提供好的难以置信的东西（不，你没有中大乐透！）
* 看似是朋友或同事发送的消息，但是签名、语气或措辞又不像是他们。

说到底，你才是对抗这些攻击的最佳防御。

**家庭 网络：** 几乎每个家庭网络都是从无线（常被称为Wi-Fi）网络开始的。你可以使用它将所有设备接入互联网。家用无线网络大多是由你的网络路由器或独立的专用无线接入点控制的。二者运作形式相同：传播无线信号使家中设备联网。这意味着，保障无线网络安全是保护家庭安全的重要部分。我们建议采取以下步骤保护它：

* 更改控制无线网络设备的默认管理员密码。管理员账户使你能够配置无线网络设置信息。
* 确保只有你信任的人连接你的无线网络。开启高安全性来保证这一点。开启后，人们需要输入密码来连接你的无线网络，且一旦连接，其在线活动都将被加密。
* 确保人们用来连接无线网络的密码为强密码，并且与管理员密码不同。记住，你只需要在每个设备上输入一次密码，它们会储存和记录密码。

不确定如何实施这些步骤？询问你的互联网服务提供商，查看他们的网站、查看无线接入点所附的资料，或参考供应商的网站。

****

**密码：**当网站要求你创建密码时 ，创建强密码，字符越多，密码就越强。确保拥有强密码最简单的方式之一就是使用密文。密文是多个词组成的密码，例如“ mifengfengmiboben”。使用独一无二的密文意味着针对每个设备或在线账户使用不同的密码。这样，如果你的一个密文被盗用，你所有其他的账户和设备仍然是安全的。记不住所有的密文？

使用密码管理器，这是一个以加密形式安全储存你所有密文（并且还具有许多其他功能！）的专用程序。最后，尽可能开启两步验证（又名双因素认证或多因素认证）功能。它使用的仍是你的密码，但增加了另一个步骤，例如发送至你智能手机的一个验证码或由一个应用生成的验证码。两步验证可能是你用来保护在线账户的最重要步骤，它比你想象的要容易得多。

**更新：**确保你的每一台电脑、移动设备、程序和应用都运行最新版本的软件。网络攻击者会不断寻找的设备中软件的新漏洞。当他们发现漏洞时，会使用特殊程序通过漏洞入侵你所使用的设备。同时，为设备制造软件的公司也在通过不断发布更新努力修复这些漏洞。确保你的电脑和移动设备及时安装这些更新，他人就更难以入侵了。保持更新，只需要尽可能开启自动更新即可。这一原则适用于几乎任何连接网络的技术，不仅包括你的工作设备，还有联网的电视、婴儿监视器、安全摄像头、家用路由器、游戏机，甚至你的汽车。



**孩子/客人**：在办公室工作时，你可能不必担心你的孩子、客人或其他家庭成员使用你的工作笔记本电脑或其他工作设备。确保家人和朋友明白他们不能使用你的工作设备，因为他们可能意外清除或变更信息，或者甚至更糟的情况是，不小心使你的设备受到感染。