

# 如何在办公室内外确保组织的安全

无论您是居家工作或是在办公室工作，确保组织的安全必须是您的首要任务之一。虽然在这两个地方可能让人感觉大为不同，但无论您是在办公室还是居家工作，都可以应用同样的预防措施。让我们查看一些重要的网络安全规则，以及它们如何在办公室和居家工作的环境中发挥作用。

## 仅使用安全的设备

- 请记住，要想确保设备的安全，设备上运行的应用必须是安全的。在未事先与 IT 部门核实之前，切勿安装应用或插件。
- 仅将工作设备用于工作。如果要将自己的电脑用于工作，建议另外创建一个具有唯一用户名和密码的用户帐户。
- 在办公室，网络安全可能由 IT 部门负责。为确保家庭互联网连接的安全，请为路由器设置复杂的密码。如果您的组织提供虚拟专用网络 (VPN) 的访问权限，请同时连接至 VPN。

## 保护您的实际工作空间

- 在办公室，需要留意不要捎带他人进入或被他人尾随进入。捎带者是指声称是您所在组织的成员，并在不使用工牌或门禁密码的情况下跟随您进入安全区域的人。尾随者是指等待您进入或离开安全区域，然后趁着门还开着的时候偷偷溜进去的人。对任何不认识的人持怀疑态度，应主动询问对方身份。
- 在家中，找到一个私密而舒适的工作空间，确保工作时没人能看到您的屏幕。必须将所有敏感信息置于任何未经授权人员的视线范围之外，包括您的伴侣、孩子和朋友。
- 每次离开办公桌时都要锁定电脑。如果电脑处于未锁定状态，任何人都可以利用它来访问敏感数据、窃取您的登录凭据，甚至安装恶意软件。

## 点击前务必三思

- 对于意外收到的电子邮件，切勿点击其中的链接或下载其中的附件。即便发件人看起来像是来自某个真实的组织，电子邮件地址也有可能是假冒的。
- 当电子邮件要求您登录某个帐户或在线服务时，请通过浏览器访问相应服务。切勿点击电子邮件中的链接。直接访问该网站可确保您登录的是真实网站，而非外观相似的仿冒网站。
- 如有疑问，请致电电子邮件的发件人，以确保请求、链接或附件均是真实有效的。请勿拨打电子邮件中提供的电话号码，因为有可能是虚假号码。



KnowBe4 安全团队