网络安全速查表

我们生活的世界虚拟化程度越来越高，网络犯罪增长的速度令人担忧，但这种现象并非意外。事实上，**网络犯罪在 2021 年产生了大约 6 万亿美元的收入**，成为仅次于美国和中国的世界第三大经济体。[*]攻击者变得越来越狡诈，但只要您意识到最新的威胁并采取适当的保护措施，就很容易实现在线安全。**下面介绍了戴尔网络安全专家一直在努力防御的一些威胁，以及有关如何确保工作区和家庭安全的提示。**

偷渡式泄露攻击

提示：
及时更新浏览器和插件程序

当您无意间进入不安全或被入侵的网站时，恶意方会获取访问您系统的权限。

如何发现：

系统上出现您未添加的新文件或网络连接

收到来路不明的请求，需要您提供配置信息

不安全的硬件

提示：
从获得授权的销售方进行购买

威胁行为体将漏洞直接嵌入到硬件和配件中。

如何发现：

所谓“好得难以置信”的交易

社会工程

提示：
政府机构（IRS 等）会首先通过 USPS 进行联系

诈骗者伪装成法人实体或其他权威机构来操纵受害人，窃取他们的敏感的**个人或财务信息**（又称为网络钓鱼）。以链接或附件形式，通过电子邮件、私信和文本方式发送恶意代码。

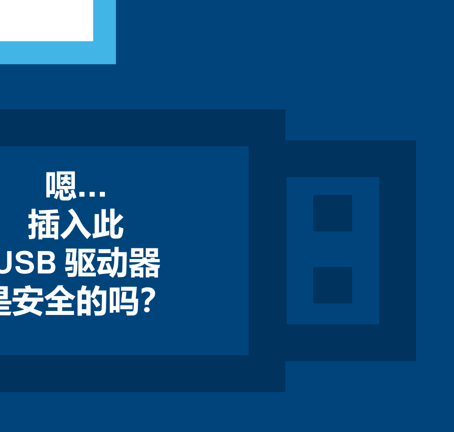
如何发现：

收到来路不明的电子邮件或文本，通过指示您打开链接和附件，要求您提供个人信息

奇怪的发件人电子邮件地址、措辞、拼写

USB 恶意软件攻击

提示：
警惕未知的 USB 驱动器，即使是来自好友的分享



罪犯使用 USB 驱动器、移动硬盘、智能耳机、音乐播放器、SD 卡和光介质（CD、DVD、BluRay）等可移动存储设备感染计算机或网络。

如何发现：

对设备上的文件或新创建的文件的非预期访问

信赖的关系

提示：
使用独特的强密码

黑客入侵一个受信任的第三方，例如医生的办公室，并利用其声誉来欺骗和利用患者。

如何发现：

反常的登录行为

如何确保网络安全：

正确做法

在您的所有帐户中使用多因素身份验证和独特的强密码。

任何连接到互联网的设备都容易遭受攻击。
因此，要及时更新软件。

保持警惕，心存疑惑。了解如何识别诈骗者的伎俩。

不要保持沉默。向 IT 报告攻击事件，并通知同事、家人和朋友。

错误做法

不要懒惰。始终遵守所有安全协议。

不要单击未经请求的电子邮件或私信中嵌入的任何链接。

不要忽略浏览器警告，例如，“您的连接不安全”或“您的连接不是私密连接”。

提示：
有关详细信息，请访问：
Dell.com/Endpoint-Security

---

[*] Cybersecurity Ventures：《2022 Cybersecurity Almanac: 100 Facts, Figures, Predictions and Statistics》