诈骗和网路安全术语须知

- 防毒软体 - 用于预防、侦测，甚至移除恶意软体的电脑程式。
- 自带设备政策（BYOD） - 由企业实施的政策，允许员工将自己的个人电子设备作公务用途。
- 常见漏洞与揭露（CVE） - 罗列已发现资安弱点及漏洞的清单，并提供独有的ID编号、描述和参考资料以便供公众查阅。
- 加密货币 - 可像商品一样交易的端对端去中心化电子货币。
- 网络攻击 - 对电脑系统、网络、基础设施或设备的恶意攻击。
- 网络事件 - 国家网络安全中心（NCSC）定义为「违反系统安全政策以影响其完整性或可用性和/或未经授权访问或试图访问系统的行为；符合《滥用电脑法》（1990年）」。
- 暗网 - 网路的其中一部分，但无法在搜寻器搜索出来，仅能透过特殊权限或软体访问。
- 数码足迹 - 使用网路后留下的数据踪迹，可能包括被动信息，如存储的Cookie，或者被主动在网络上发表的资讯，如社交媒体帖子。
- 加密 - 使用数学算法将数据打乱的过程。这些数据可以是静态加密，例如储存在硬碟中的数据，亦可以是传输中的数据，例如透过 HTTPS 从您的网页浏览器传送到银行伺服器的资料。加密了的资料并不能代表网络上的不法份子无法截取，只是已被转换为无用的和无法理解的乱码，让不法份子得物无所用。
- 防火墙 - 根据特定规则，监控网路进出流量的网路安全系统。
- 骇客 — 专门从事电脑网路攻击的人士。黑帽骇客进行恶意攻击，而白帽骇客则进行有助于网路防御的行动。
- 恶意软体— 以达成不法或恶意目标的程式，涵盖多个方面，例如提供远端存取、载入或植入其他恶意程式、窃取银行资讯、加密并拒绝存取资料，或盗用设备的运算能力。
- 安装补丁 — 安装修补程式以更新现有软体或硬体，修复已发现错误和漏洞的过程。
- 渗透测试（pen testing） - 机构利用骇客的攻击手段来检测自身网络的安全性，通常由「红队」或专业的白帽骇客团队负责。

- 钓鱼 - 通常透过电子邮件欺骗收件人泄露敏感资料、点击恶意连结和/或打开恶意附件。不法份子常用钓鱼以取得设备或网络上初始入侵管道。
- 勒索软体 - 封锁或限制使用者存取资料的恶意软体，并要求受害者支付赎金才能解除限制。
- 短讯钓鱼 — 透过短讯/简讯传送的钓鱼讯息。
- 社交工程 — 操控他人的心理而作出某种行为，通常用于骗取个人资料。
- 鱼叉式网路钓鱼 — 针对特定人士或群体所发出的钓鱼讯息。
- 特洛伊木马 — 伪装成看似无害的档案或程式，让受害者以为可安心开启。特洛伊木马十分常见，通常透过钓鱼邮件传送，或者由其他称为「载体」的恶意软体传送。
- 双重要素验证（2FA） — 一种要求用户提供两种身分识别要素的验证过程，例如已知密码和一次性密码（OTP）。一般来说，这些要素可分为：「认知要素」（密码）、「生物特征」（指纹）或「持有物件」（密匙卡）。
- 虚拟私人网路（VPN） — 允许在公共基础设施上建立安全私人的连线，最初由机构开发，以对访问内部网络资源，例如电邮伺服器或共享文件夹等的员工进行身份验证。现在，越来越多的人使用消费者VPN来作为建立及选取VPN伺服器的加密连线，并使用该伺服器连接到其他互联网资源。
- 语音钓鱼 — 透过电话进行并大量利用社交工程的钓鱼攻击。
- 零日漏洞 — 在补丁或更新发布之前所发现到的漏洞。利用此类漏洞的恶意软体通常被称为零日漏洞攻击。