社交工程

了解如何识别社交工程操纵伎俩并避免受其影响。

1.社交工程攻击如何运作?

社交工程是指骗子利用一些手段和伎俩，企图欺骗您做一些不该做的事，例如泄露您的个人信息或汇款。社交工程已存在数百年的时间，随着互联网时代的到来也演化出新的形式。

社交工程的主要目的是操纵您。以下是社交工程攻击的运作方式:

- 攻击者识别受害者并发现他们的信息
- 然后他们决定要使用哪种社交工程伎俩
- 攻击者接触受害者，并使用不同的伎俩来操纵他们
- 攻击者说服受害者泄露他们的信息或汇款
- 攻击者结束表演并销声匿迹

2.常见的社交工程伎俩有哪些?

社交工程攻击企图操纵您。以下是一些常见的手段和伎俩:

- **诱饵攻击**：这类攻击企图用虚假承诺引诱受害者上钩，例如承诺提供免费下载、免费服务或奖品
- **恐吓软件**：通常形式为带有警报信息的弹出式广告，试图吓唬您，迫使您泄露自己的信息或数据
- **网络钓鱼骗局**：这是一类非常常见的社交工程形式，通过短信或电子邮件操纵您的情绪，企图说服您点击或下载某个内容，或者发送信息或汇款。网络钓鱼骗局通常会利用紧迫感作为触发点，但有时也会试图恐吓您，利用您的同情心或者用奖品引诱您
- **冒名攻击**：在这一伎俩中，攻击者会冒充某个您信任的人或权威人物来骗取您的信任，使您泄露自己的信息

- **鱼叉式网络钓鱼**：这类网络钓鱼骗局针对的是某一个人或一小群人，行骗信息通常看似由某个他们认识的人发出。

请注意，社交工程攻击也可能在线下发生，通过骚扰电话或现场形式。例如，犯罪分子可能会通过搜索垃圾箱来获得您的个人信息，或者试图进入某栋大楼以窃取数据或技术。

3.社交工程攻击有哪些迹象?

警惕以下迹象：

- 意外的请求或消息
- 请求非常急迫
- 您感觉自己迫于压力，需要立刻去做某件事
- 事情听起来美好得令人难以置信
- 您注意到奇怪的拼写或语法错误
- 信息看似恐吓或威胁

记住，社交工程师们正千方百计地操纵您，企图使您不加思索地立即采取行动。切勿迫于压力做任何事！

4.如何避免社交工程攻击?

- 警惕此类骗子所使用的伎俩
- 调查其请求，切勿马上回应或直接配合
- 思考自己的情绪反应 — 您是否感到很仓促或是受到了威胁?
- 运用数据最小化原则，留意您在互联网上发布和提供给他人的信息
- 采用密码安全做法，使用多重身份验证和密码管理器
- 不要打开或点击未知来源的附件或链接
- 管理您的帐户安全设置，清理您的社交媒体个人简介信息，确保其中没有包含隐私或敏感信息

- 保持设备更新，并始终安装最新的安全更新
- 销毁敏感文件
- 始终备份数据，以防黑客或勒索软件攻击

5.制定计划

考虑您可以采取哪些措施来更好地保护您的帐户和信息，并避免陷入社交工程骗局。将您思考的结果写在下方空白处：