网络钓鱼骗局

深入了解网络钓鱼骗局的攻击工程以及如何防范它们。

1.什么是网络钓鱼骗局?

网络钓鱼骗局从事以下活动:

- 试图骗您分享或泄露重要个人信息
- 试图骗您执行一项任务或操作（如点击某个链接），进而在您的设备上安装恶意软件

黑客们通常会在数据泄露期间获取电子邮箱等信息，然后向这些邮箱发出网络钓鱼邮件，企图对您实施欺诈或诈骗。

2.我如何识别网络钓鱼骗局?

网络钓鱼骗局有多种形式:

- 电子邮件
- 短信
- 电话

它们往往通过调动情绪或利用各种圈套来欺骗您。其中可能包括:

- **恐惧:** 这类骗局声称您欠了一笔钱或有某种麻烦，使您陷入恐慌，然后对其言听计从
- **同情:** 这类骗局向您讲述一个悲伤的故事或博取您的同情，企图说服您去做某件事
- **机会或中奖:** 这类骗局向您提供一个虚假的机会（如免费旅游），让您在兴奋之余满足其提出的要求
- **日常任务或请求:** 这类骗局看似稀松平常，例如来自您工作场所的常规请求

3.我如何发现网络钓鱼骗局?

以下提示有助于您保持谨慎，避免陷入网络钓鱼骗局：

- **务必小心您要点击或打开的内容**

不要立即点击或打开看似奇怪或可疑的内容。如果您在意料之外收到某消息，或者您收到的请求看起来非常急切或令人恐慌，则在采取任何行动之前先慢下来并进行核实

- **检查邮件和任何链接的发件人**

发件人的电子邮件地址看起来可靠吗？在电子邮件网络钓鱼骗局中，发件人的名称可能看似可靠，但电子邮件地址可能与发件人的名称不符。其中的链接也可能是短网址或看起来很可疑。您可以将鼠标悬停在链接上进行检查。记住：在事先检查之前请勿点击任何链接！

- **考虑其中的请求**

您在这个网址有帐户吗？思考其对您提出的要求

- **注意请求的语言**

网络钓鱼骗局可能会使用异常的问候语（例如“你好，亲爱的”而不是您的姓名）或奇怪的措辞。书写错误、语法错误或其他问题也可能预示着该请求并非来自正规组织。此外，还要留意它要求您做什么。例如，正规组织不会要求您在电话中分享敏感信息或透露密码

- **进行搜索**

搜索对方提出的要求可能是关键的一步！大型、常见的网络钓鱼骗局经常见诸各种报道和文章，进行搜索可以帮助您确认这是不是一个骗局

4.我如何避免陷入网络钓鱼骗局?

确保您采取了良好的密码安全和数字安全处理程序!

- 在您的设备上始终保持最新的安全设置
- 对您使用的网站使用多重身份验证，以增加一层安全保护
- 备份您的数据

良好的数据安全处理程序可以帮助您保持数据和信息的安全，避免沦为网络钓鱼骗局的受害者。但请记住，网络钓鱼骗局正变得越来越常见和普遍。要完全避免它们几乎是不可能的，因此识别这类骗局尤为重要。

5.回顾过去的经历

您曾经见到过哪种类型的网络钓鱼骗局？请在此处列出您的一些见闻和遭遇：

6.知识和技能测试

通过以下活动测试您的技能，学会更好地识别网络钓鱼骗局：

- 使用 Google 提供的网络钓鱼测验测试您的技能：https://phishingquiz.withgoogle.com/
- 完成测验后，以小组为单位访问以下网址，查看一些常见的网络钓鱼骗局示例：https://www.phishing.org/phishing-examples
- 看看您从中发现了哪些趋势，在这些示例中使用了哪些操纵手段