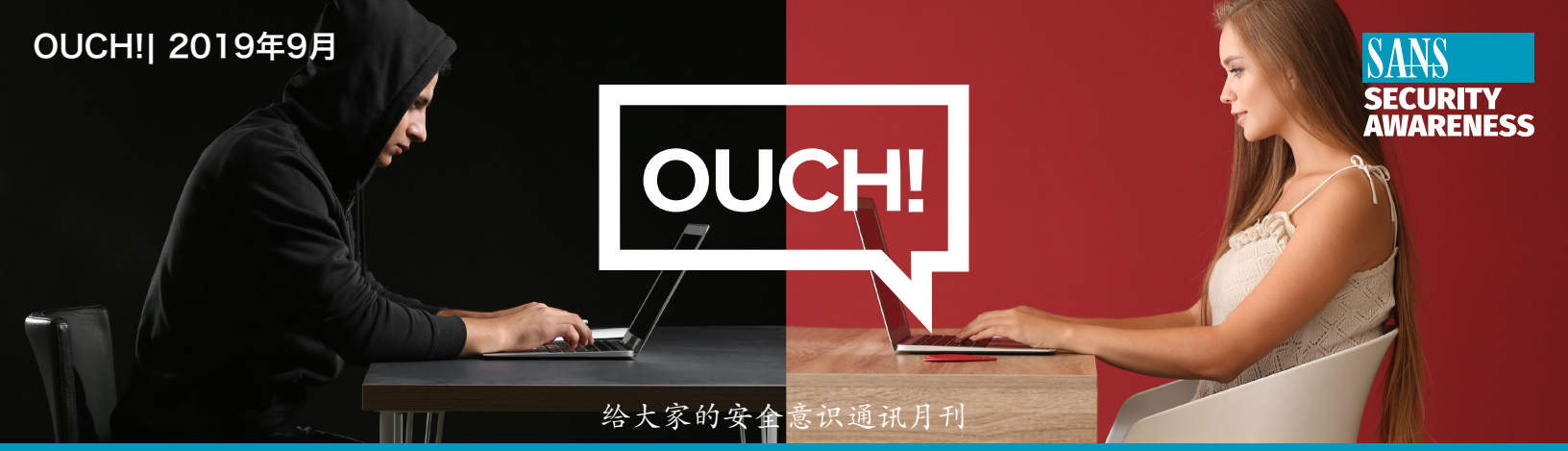

通过社交媒体实施欺诈

概述

我们中有很多人都遭遇过电子邮件形式的网络钓鱼攻击，无论是在单位还是家中。这些电子邮件看似合法，比如像是由您的银行、上司或喜爱的网店所发送的。但这其实是一种网络攻击手段，目的是促使或诱骗您采取不当措施，比如打开被病毒感染的电子邮件附件，共享您的密码或进行转账汇款。道高一尺魔高一丈，挑战在于即使我们加大识别和阻止电子邮件攻击的力度，网络罪犯仍然会尝试通过其他方式与用户取得联系并实施诈骗。

这种欺诈和欺骗行为可能发生在您所使用的任何通信渠道中，从 Skype、WhatsApp 和 Slack 到 Facebook、Snapchat、Instagram，甚至是游戏应用。在这些平台和渠道上进行交流，可以更加随意，或者更容易取得信任。正因如此，攻击者使用它们实施欺诈。此外，借助当今技术，世界各地的攻击者更容易伪装为他们所需的其他身份。请谨记，眼见不一定为实，您收到的任何通信以及遇到的任何人都是这样。

关键要点

您可以利用以下常见线索来判断您收到的邮件或者阅读的博文是否为网络攻击。

紧迫感：邮件为您带来某种巨大的紧迫感，要求您立即采取行动，以免发生严重后果， 比如威胁要关闭帐户或将您送进监狱。攻击者想催促您犯错误。

压力：迫使您绕过或忽略正在实施的安全程序或政策。

好奇心：一种强烈的好奇心或有些东西好得令人难以置信。（不，您并没有中彩票。）

敏感性：要求提供极其敏感的信息，例如您的银行卡号或密码，或者您愿意提供的任何信息

官方邮件：邮件声称是由官方组织所发送，但存在语法和拼写错误。大多数政府组织不会使用社交媒体与您进行直接沟通。如果您不确定邮件是否合法，请使用可靠的电话号码（例如官方网站上的电话号码）致电相关组织。

冒充他人：您收到了朋友或同事的邮件，但口吻和措辞却不像他们本人。如果您有疑问，可以打电话核实他们是否发送了邮件。网络攻击者很容易伪造一封看起来像发自您朋友或同事的邮件。在某些情况下，他们还可能盗用了您朋友的帐号，然后冒充您的朋友与您联系。对短信、Twitter 和其他短消息格式应格外谨慎，从这类消息中很难判断发送人的语气。

要预防此类诈骗和攻击，您本人的行动最有效。如果帖子或邮件看起来很奇怪或可疑，只需将其忽略或删除即可，或者如果它来自您个人认识的人，请打致电相关人士进行核实。

特邀编辑

Jessica Barker 博士(@drjessicabarker) 是研究网络安全中的人性方面的专家。她是 Cygenta 的联合首席执行官，她热衷于提高全球的网络安全意识、行为和文化。她是 ClubCISO 的主席，也是一位颇受欢迎的主题发言人。

资源

社会工程：https://www.sans.org/u/Uz6
电话诈骗：https://www.sans.org/u/Uzb
停止此网络钓鱼：https://www.sans.org/u/Uzg
个性化诈骗：https://www.sans.org/u/Uzl