讯息/短信钓鱼攻击

概述

网络攻击者最常见的骗人方法之一便是电子邮件攻击（通常称为网络钓鱼）或电话诈骗。不过随着技术的进步，坏人也在不停地尝试新的招数，包括利用讯息技术实施诈骗，比如文本讯息、iMessage/Facetime、WhatsApp、Slack或Skype。这里介绍几个简单的方法，帮助你保护你自己并识别/终止这些常见的攻击。

什么是讯息攻击?

讯息攻击（有时称为短信钓鱼，是网络钓鱼的变种）是指网络攻击者利用短讯服务、文本或讯息技术来接触你并试图骗你采取不应该的行动。他们可能想骗你点击一个恶意链接，或让你拨打一个电话以便获取你的银行信息。就像传统的电子邮件攻击，坏人常常会利用你的情绪来作恶。但是，讯息攻击之所以如此危险是因为跟邮件相比，它们通常显得更日常化或者私人化，更可能让你落入圈套成为受害者。另外，讯息攻击中的信息和线索更少，你从中更难发现有问题或可疑的地方。当你收到一条看起来奇怪或者可疑的消息，先问问你自己，这条消息说得通吗？我为什么会收到它？这里有一些最常见的线索，你可以用来辨别攻击行为。

如果有人试图让你匆忙采取行动，那么会表现出一种强烈的紧迫感。

这条短讯是否在索要个人信息、密码或者其他他们不应该获取的敏感信息？

这条短讯的内容是否看起来好到令人难以置信？不，你并没有中彩票，特别是你从来没买过的彩票。

短讯看起来是同事或者朋友的账户或手机号发来的，但是措辞却不像他们会用的。他们的账户可能被攻击者盗用了，或者攻击者试图冒充他们，骗你采取行动。

如果你收到一条让你反应强烈的短讯，稍等一下，让自己冷静下来，在回复前要深思熟虑。

有时候，坏人甚至会把电子邮件攻击和短讯攻击结合起来对付你。比如，礼品卡便是这种套路。网络攻击者会冒充你的朋友或同事给你发送一封紧急电子邮件，索要你的手机号码。然后他们就可以不停地给你发送文字短信，向你施加压力，让你购买礼品卡。一旦购买，攻击者会让你刮掉卡背面的代码涂层，然后拍照发给他们。另一种常见的攻击方式会劝你打开一段视频或一张图片（措辞包括：“你肯定不敢相信！”）。它激起了你的好奇心。如果这条消息看起来是你认识的人发送的，在回应前最好给这个人打电话进行核实。

如果你收到官方组织的警告消息，请直接与他们进行核实。例如，如果你收到一条你的银行发给你的文字讯息，说你的银行账户或者信用卡出了问题，请直接访问他们的网站或者拨打银行卡或信用卡背面的电话联系他们。记住，大部分政府机构，比如税务或执法机构，不会通过文字讯息联系你。

在短讯攻击面前，你本人就是你自己的最佳防御。

特邀编辑

Jen Fox 持有第23届DEF CON社会工程学类别的黑色奖章，她作为Domino's公司的安全项目专家提供安全意识教育。你可以在Twitter上关注她 @j_fox。

资源

社会工程学：	http://www.sans.org/u/XAQ
阻止网络钓鱼：	http://www.sans.org/u/XAV
电话诈骗：	http://www.sans.org/u/XB0
报告欺诈短信：	https://www.consumer.ftc.gov/articles/0350-text-message-spam