关于口令安全的三个误区

简译版

非官方中文译文·安天技术公益翻译组 译注

文档信息			
原文名称	3 Myths About Threat Actors and Password Safety		
原文作者	苏·波伦巴（Sue Poremba）	**原文发布日期**	2021 年 7 月 16 日
作者简介	苏·波伦巴是一位专注网络安全和技术领域的作家。		
原文发布单位	Security Intelligence		
原文出处	https://securityintelligence.com/articles/3-myths-password-safety/		
译者	安天技术公益翻译组	**校对者**	安天技术公益翻译组
分享地址	请浏览创意安天论坛 bbs.antiy.cn 安天公益翻译板块		
摘要	毫无疑问，口令安全对企业至关重要。包括口令在内的访问凭证是进入企业网络的网关。因此，口令仍然是一个安全热点。员工通常是凭证遭窃的薄弱环节，这可能是因为他们缺乏对“攻击者如何获取口令信息”的认识。企业应向员工说明关于口令安全的误区，并改善围绕口令的安全意识培训。		
免责声明	本译文不得用于任何商业目的，基于上述问题产生的法律责任，译者与安天集团一律不予承担。		

关于口令安全的三个误区

苏·波伦巴

2021 年 7 月 16 日

我们已经被警告社交媒体的危险性——回答有关生活史的问题会破坏用户的口令安全。这会给攻击者提供他们需要的信息，帮助他们猜出用户口令并获得安全问题的答案。

这是真的吗？攻击者真得会潜伏在社交媒体上，等着我们透露“最喜欢的老师”和“舞会日期”等信息吗？实际上，对你怀恨在心的人可能会使用这些信息来造成一些损害，但一般来说，网络犯罪分子并不会针对个人。相反，他们更有可能使用社会工程攻击手段，例如基于你的社交媒体算法的恶意视频或网络钓鱼电子邮件，来访问你的网络和数据。

任何人都不应分享自己的敏感信息，因为这些信息可能会被用于恶意目的。但是，这是围绕口令安全的众多误区之一。

毫无疑问 ,口令安全对企业至关重要。包括口令在内的访问凭证是进入企业网络的网关。因此，口令仍然是一个安全热点。员工通常是凭证遭窃的薄弱环节，这可能是因为他们缺乏对“攻击者如何获取口令信息”的认识。企业应向员工说明关于口令安全的误区，并改善围绕口令的安全意识培训。

误区 1：不要写下口令

事实：几十年来，关于口令安全的最常见建议是不要将口令写下来。我们当然不想将口令粘贴到计算机屏幕上，然后在社交媒体上分享屏幕截图（就像某位国会议员所做的那样），但是写下口令并将其存储在安全的地方是可以的。攻击者通常会使用更复杂的方法来获取口令，例如键盘记录或暴力破解攻击。要知道，大多数网络犯罪分子都希望尽可能轻松地访问尽可能多的系统，在本地一次使用一个口令对他们来说无关紧要。

误区 2：使用文本消息作为多因子身份鉴别（MFA）口令是最好的

事实：对于大多数人来说，使用文本消息作为多因子身份鉴别（MFA）口令无疑是最简单的，但这并不是确保口令安全的最佳方式。手机号码就是一种新的攻击向量，攻击者可以通过“SIM 卡交换”（SIM swapping）窃取我们的手机号码。

执行“SIM 卡交换”攻击的攻击者会伪装成用户，联系电话提供商。之后，他们就可以将自己的 SIM 卡与用户的手机号码相关联。然后，他们将可以访问以文本形式发送到用户手机的所有 MFA 口令，以及用户手机上的所有个人身份信息。鉴于此，诸如生物识别或身份验证器等 MFA 措施是更好的选择。

误区 3：我的口令独一无二且安全

事实：目前存在着数十亿个口令，因此任何口令都不太可能是真正独一无二的。大多数用户通过更改字母大小写或添加符号来创建“独一无二的”口令，并且通常是在被警告“旧”口令被窃取时才会这样做。攻击者会使用“口令喷洒”（password spraying）等技术，尝试使用数百万个常用口令来访问网络。因此，即使你的口令确实独一无二且难以破解，但攻击者只要获得一个弱口令即可访问整个系统。

让更多的用户了解攻击者如何获取口令，有助于提升口令安全，而了解上述三个误区是第一步。

安天简介

安天是引领威胁检测与防御能力发展的网络安全国家队，始终坚持自主先进的能力导向，依托下一代威胁检测引擎等先进技术和赛博超脑大平台工程能力积累，研发智甲、探海、镇关、捕风、追影、拓痕等系列产品，为客户构建端点防护、流量监测、边界防护、导流捕获、深度分析、应急处置的安全基石。安天致力于为客户建设实战化的态势感知体系，依托全面持续监测能力，建立系统与人员协同作业机制，指挥网内各种防御机制联合响应威胁，实现从基础结构安全、纵深防御、态势感知与积极防御到威胁情报的有机结合，协助客户开展深度结合与全面覆盖的体系化网络安全规划与建设，支撑起协同联动的实战化运行，赋能客户筑起可对抗高级威胁的网络安全防线。

安天是全球基础安全供应链的核心赋能方，全球近百家著名安全企业、IT 企业选择安天作为检测能力合作伙伴，目前，安天的威胁检测引擎为全球超过八十万台网络设备和网络安全设备、超过十七亿部智能终端设备提供了安全检测能力。安天的移动检测引擎获得国际知名测试机构颁发的 2013 年度权威评测奖项。

安天是中国应急响应体系中重要的企业节点，在“红色代码”、“口令蠕虫”、“心脏出血”、“破壳”、“魔窟”等重大安全威胁和病毒疫情方面，实现了先发预警和全面应急响应。安天针对“方程式”、“白象”、“海莲花”、“绿斑”等几十个高级网空威胁行为体（如 APT 组织）及其攻击行动，进行持续监测和深度解析，协助客户在“敌情想定”下形成有效防护，通过深度分析高级网空威胁行为体的作业能力，安天建立了以实战化对抗场景为导向的能力体系。

安天被行业管理机构、客户和伙伴广泛认可，已连续六届蝉联国家级安全应急支撑单位，是中国国家信息安全漏洞库六家首批一级支撑单位之一，亦是国家网络与信息安全信息通报机制技术支撑单位，国家信息安全漏洞共享平台成员单位。

2016 年 4 月 19 日，在习近平总书记主持召开的网络安全和信息化工作座谈会上，安天创始人、首席架构师作为网络安全领域发言代表，向总书记进行了汇报。2016 年 5 月 25 日，习近平总书记在黑龙江调研期间，视察了安天总部，并对安天人说，“你们也是国家队，虽然你们是民营企业”。

安天实验室更多信息请访问： http://www.antiy.com（中文）

http://www.antiy.net（英文）

安天企业安全公司更多信息请访问： http://www.antiy.cn

安天移动安全公司（AVL TEAM）更多信息请访问： http://www.avlsec.com