

浅析账号体系安全

携程信息安全部

个人简介

Wooyun id : 小胖胖要减肥

Weibo: 小胖胖_要减肥

Weixin号&qq: 676931473

2015年8月加入携程,负责业务安全,产品安全,移动安全相关



[首页](#) | [羊毛福利](#) | [返现任务](#)

携程



前海理想金融 送1万体验金 14元利息 可提现



前海理想金融，信誉一直很好，这次的活动也比较简单，这次的活动，新老用户都可以参加（限没投资过的老

余额E贷注册送10000体验金（3天收益9.8

活动介绍： 活动期间注册余额E贷送10000元体验金，投资3天提现收益9.86元，可提现。邀请人送里程

招财猫 投资90元5天标 赚10元



招财猫之前就举办过送红包活动，挺靠谱的，现在这个活动大家可以参与下，注册即送70元红包，其中有10

唐小僧 投100撸8元（投资1天）



唐小僧 投100撸8（投资1天），仅限新用户。当日投资，平台次日会送5元现金奖励。扫下面二维码注册，亲

风筝银行 充1元送15元话费 活动结束后到账，



风筝银行的活动，通过手机APP或者网页版注册风筝银行，并完成充值（金额≥1元），得15话费，话费将

推荐新闻

广发银行 月光宝盒APP，注册绑卡送10元话费

之前向大家介绍过广发银行直销银行注册绑卡送10元的活动(点击直达)，10元奖励已经到账...

百度钱包 1分钱5元话费

百度钱包，有1分钱充话费活动，都是针对新用户，百度钱包1分钱充5元话费，没有做过的...

腾讯理财通，新用户投资500元，得10元现金

理财通，新用户体验理财通并支付500元，可最少得10元现金 活动时间：截止到2015年6月...

阳光动力 投资1元 3天17.26元收益 可以提现

阳光动力注册认证，只需1元投资，即获30000元体验金，享7%固定年化收益，3日后收益返...

平安陆金所，200起投，最高撸300+大羊毛(别用手

陆金所，即上海陆家嘴国际金融资产交易市场股份有限公司，是中国平安保险（集团）股份...




前海理想金融 送1万体验金 14元利息

前海理想金融，信誉一直很好，这次的活动也比较简单，这次的活动，新老用户都可以参加...

[关于我们](#)

[网站概况](#)

[会员登录](#)

撸羊毛（luyangmao.cc），免费收集、分享最新银行，基金及名企商家的羊毛信息，致力于为财富们提供真实有效的信息，踏出理财的第一步。如果觉得网站不错，请按 Ctrl+D 收藏本站！喜欢聊天的请进群：213643331  加入QQ群

 [RSS订阅](#)

 [微信关注](#)

 [新浪微博](#)

 [邮箱订阅](#)

热门活动

ppmoney, 10元话费 + 25元现金

羊毛标签

薅羊毛

账号体系与业务安全相关性

直接相关:

1 营销活动

----马甲，羊毛党，黄牛

2 金融安全

----盗号，盗卡，欺诈，诈骗（支付，卡券，积分，理财产品，用户个人资产）

直接影响

- 1 营销没有达到预期
 - 2 大量刷单浪费成本
 - 3 用户信息泄露
 - 4 用户资金损失
- 。 。 。 。

较大影响:

- 1 公司直接资金损失（自身营销费用，用户赔偿）
- 2 信誉损失
- 3 金融产品强制关停

如何防止-营销活动

营销防刷—核心：同一个人的判断（同一批）

- 1 注册限制：图片验证码，短信验证码，语音验证码
- 2 注册数据收集，建模，针对马甲账号打标示(指纹，行为识别，生物识别等)
- 3 用户价值体系，从注册开始，通过维度数据建立不同用户价值
- 4 行为点控制，通过维度数据控制黄牛行为，增加验证项提高其成本

结果：羊毛党，黄牛，以利益驱动为基础，在防御上采用纵深防御，拉长战线

- 1 提高获利难度
- 2 适当结合业务，降低获利程度（太大的利益不是技术能够解决的）

如何防止-金融安全（账号体系）

账号安全（浅析账号）-核心：人机识别

- 1 防撞库，人机识别（规则，模型等）
- 2 数据搜集，账号标签（指纹，行为，生物信息等）
- 3 用户价值体系（信用，行为频度等）

应用功能点：

- 1 提示高危账号进行密码修改（推送，登陆后，使用功能时）
- 2 各关键功能调用账号标签数据，过滤用户及提升不同难度挑战

。 。 。

海量密码被盗，被拖库网站众多，用户信息随手可得

除大麦网本次的密码泄露外，其实近年来网站用户数据库被盗屡见不鲜，其中不乏天涯社区、当当网、腾讯QQ等知名网站。通过搜索引擎搜索发现有各类黑产论坛明码标价公开售卖，数量庞大，种类繁多，亦有网友收集制作的网站泄露数据库密码查询网站，通过简单的搜索，密码、邮箱、手机号等个人信息直接暴露在外，网络安全现状堪忧。

近日，站长之家编辑也从某社工库网站上看到了一份“泄露网站列表”数据清单，涉及网站数量众多，令人咋舌。编辑同时测试了自己常用的用户名，竟然发现有14个网站存在泄漏账号密码的情况，而且部分密码还是目前仍在使用的密码。

目前该社工库网站已有20.97亿条共133G密码数据，并且还在持续不断添加中。据了解，相关内容数据均已在互联网公开，可在多个社工库、论坛网盘自由下载。虽然属于N年前的旧信息，但对网络用户来说，仍有很大的“杀伤力”。

编辑不禁感慨，已经曝光的就有如此众多，没有曝光的又会有多少呢？

WooYun.org

已关注 14.8万

[首页](#)[厂商列表](#)[白帽子](#)[乌云榜](#)[团队](#)[漏洞列表](#)[提交漏洞](#)[乌云招聘](#)[乌云集市](#)[知识库](#)[公告](#)

当前位置：WooYun >> 搜索结果

搜索关键字：密码泄露 (共 512 条记录) [将未公开漏洞纳入搜索结果](#)

事件起因--密码

- 1 用户密码较弱，123456，88888等
- 2 用户帐号密码各站一样，其他网站密码泄漏
- 3 访问钓鱼网站输入帐号密码
- 4 用户中木马帐号密码被窃取

。 。 。 。

帐号密码泄漏影响

- 1 用户信息泄漏，舆论风险
- 2 用户帐号资金余额卡券盗用风险
- 3 账户欺诈风险（金融产品，快捷等）
- 4 账户诈骗风险（飞单，退款钓鱼等）

。 。 。

为何不去密码?

怎么做?

- 1 用户信息识别
- 2 登陆方式完善
- 3 用户主动选择,提升安全感知
- 4 自助信息验证,流程优化
- 5 减少密码使用场景

假如没有了登陆密码,会发生什么?

事件影响

1 **网站几千万账号密码泄露
----和我们好像关系不大

2 **售卖账号密码,含卡券
----和我们关系又不大

3 **批量领取优惠
----好像没法批量登陆,刷不到啊

4 **相关恶意行为(下单,购物车等)
----没有账号密码,成本高,无法批量

我们将面临新的挑战

- 1 新技术的探索,指纹意外的声纹,红膜等生物技术在设备上的普及
- 2 在全新模式下的流程规划（技术之外的业务流程是新模式的重点）
- 3 同时会带来攻击的变革，新的攻击模式在新技术的广泛普及后势必应运而生

前进还是原地踏步？

- 1 流媒体引发的群体效应,信息安全已成为互联网的核心之一
- 2 用户资金安全在账号密码泄露的巨大风险
- 3 马甲账号，刷单，羊毛党带来的具体大损失
- 4 用户质疑账号的安全性，便捷性

但是，大部分都是围观的群众，
他们在等待什么？

第一个吃螃蟹的人!

Q&A
Thank you !