揭秘支付宝暗雷的背后，如何防范此类诈骗

原创HACK学习 HACK学习呀
2020-06-01原文

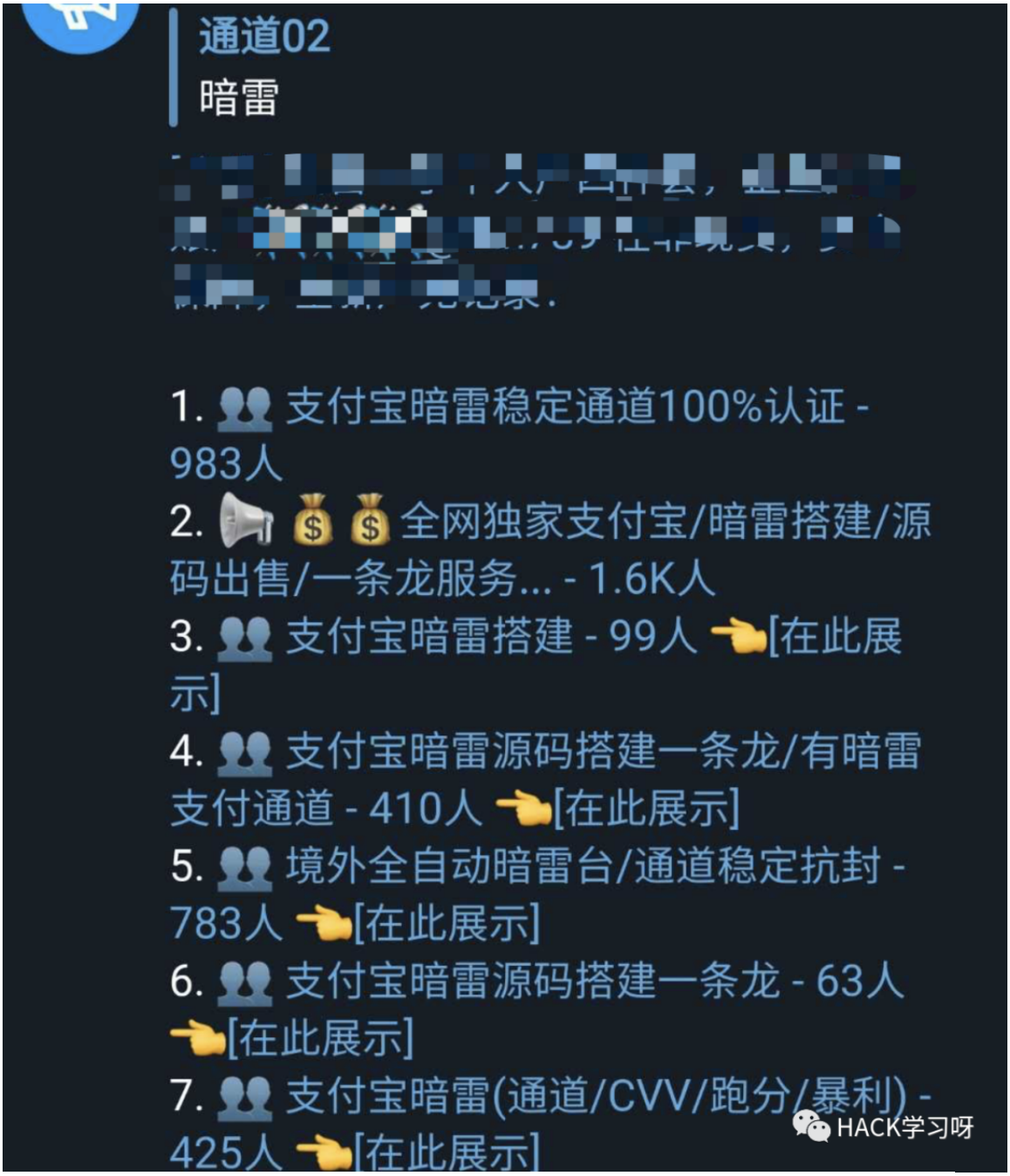
0x00　什么是暗雷

扫码支付1元秒变500元

诈骗分子通过制作假冒色情App、网络交友等信息作为诱饵，当受害者下载后，打开假冒色情App进行开通会员支付的时候，页面显示1元开通，但当确认支付后“1元秒变500元或800元”，此类制作虚假支付页面的障眼法在业内称为“暗雷”。

暗雷，指的是那些来路不明的APP，经过底层代码修改之后，就变成了地雷：一点就炸。比如，你在这些APP里发起支付，界面显示只扣1块钱，就可以买到XX网站的会员。

我们前往telegram调查了一番，找到了支付宝暗雷的背后的技术原理，当你在机器人上一搜，就能找到很多此类的群组。



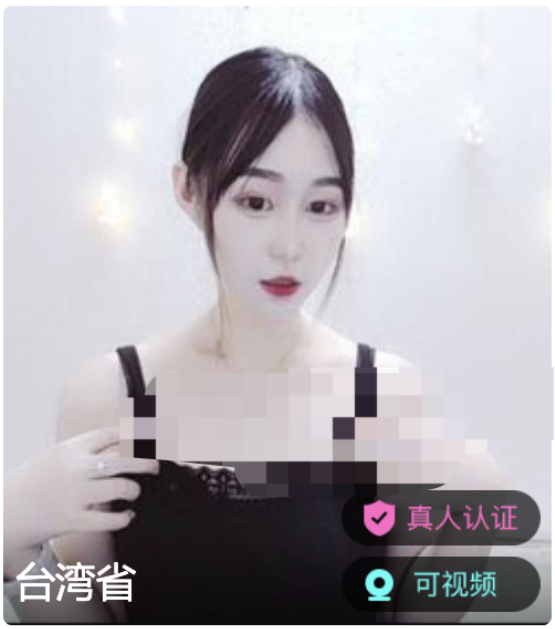
0x02　新型诈骗-支付宝暗雷

可能会是一个色情App或者一个网页，还会有不同的模板和网站类型
比如，下面这种，打开App，就是这种漏骨的画面，当你想点进去看，会提示你支付1元开通会员

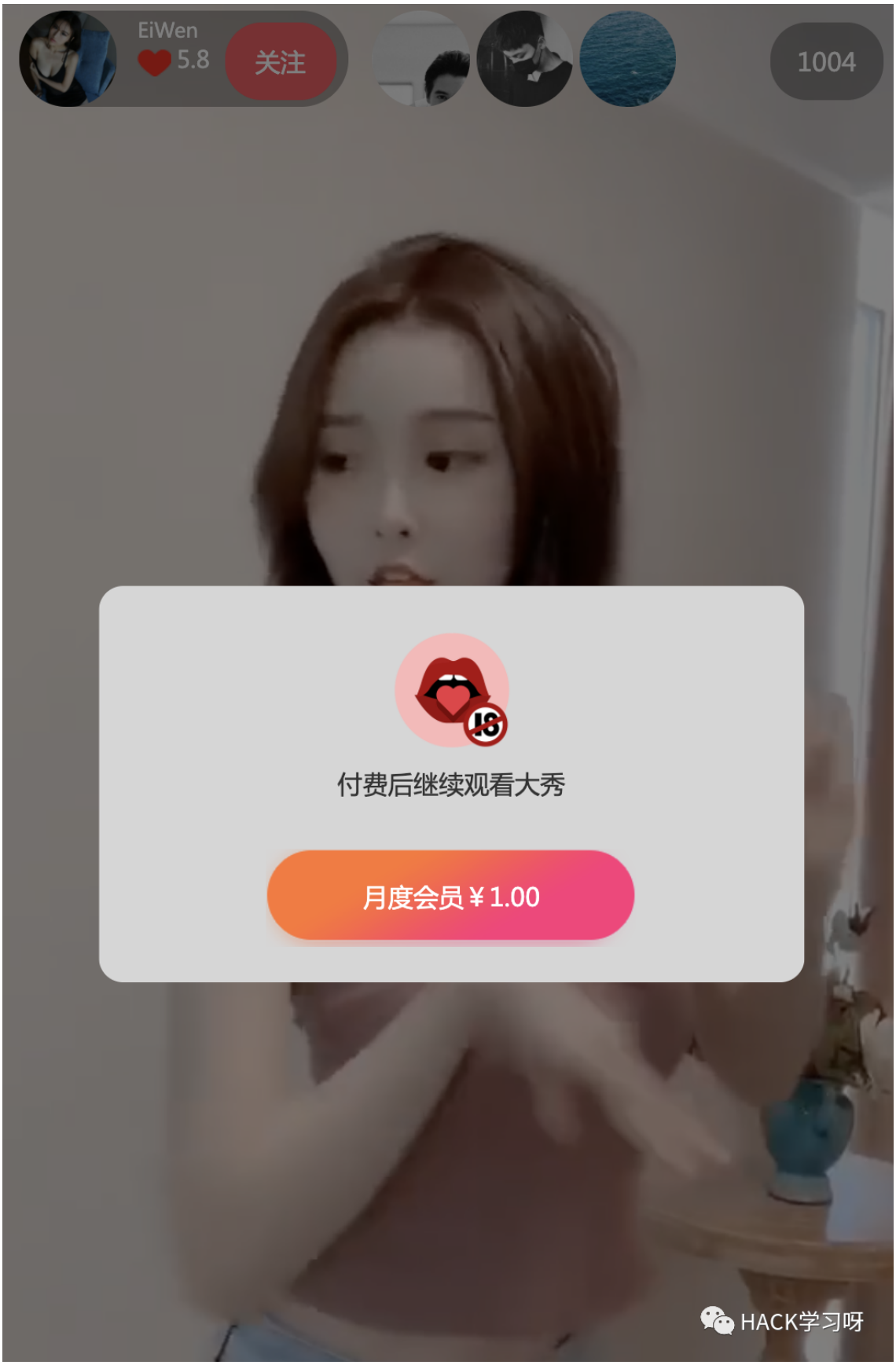
推荐

正在直播

EiWen 5.6万



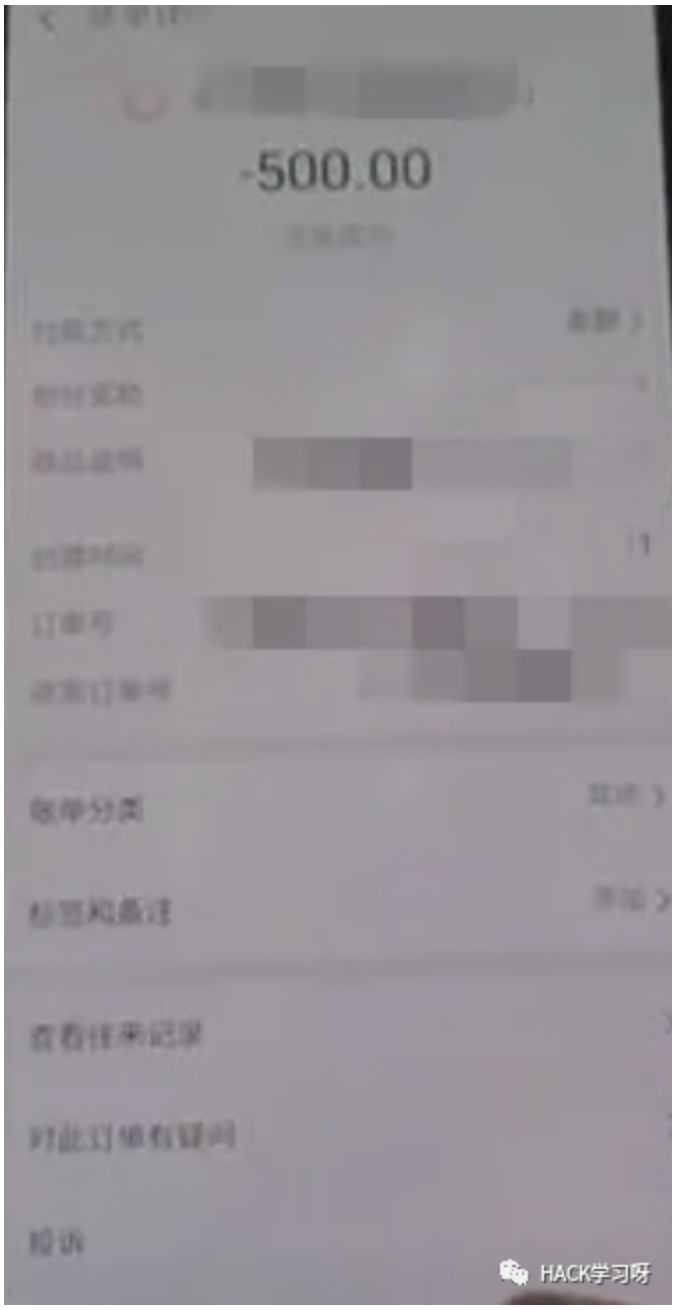
我爱台妹 1.5万


EiWen
5.8
关注
1004
付费后继续观看大秀
月度会员￥1.00
HACK学习呀

点击后会跳转到支付宝的wap端登录，这是真的支付宝，也不是钓鱼

当你使用继续浏览器付款，就会出现下面这种情况

显示1元，实际上扣费500元或者其他金额



大家可能就会很好奇，这是支付宝的漏洞吗，还是Android/IOS系统的漏洞

大家接着看技术原理就明白了，这是障眼法

0x03　技术原理

这既不是钓鱼网站，也不是支付宝的漏洞，而且障眼法
利用IOS以及安卓系统可以嵌入网页和JS的原理

在APP端覆盖了原有的金额和一些内容，将其覆盖为1元以及其他内容
从而欺骗大家，利用人们贪小便宜的心理进行诈骗

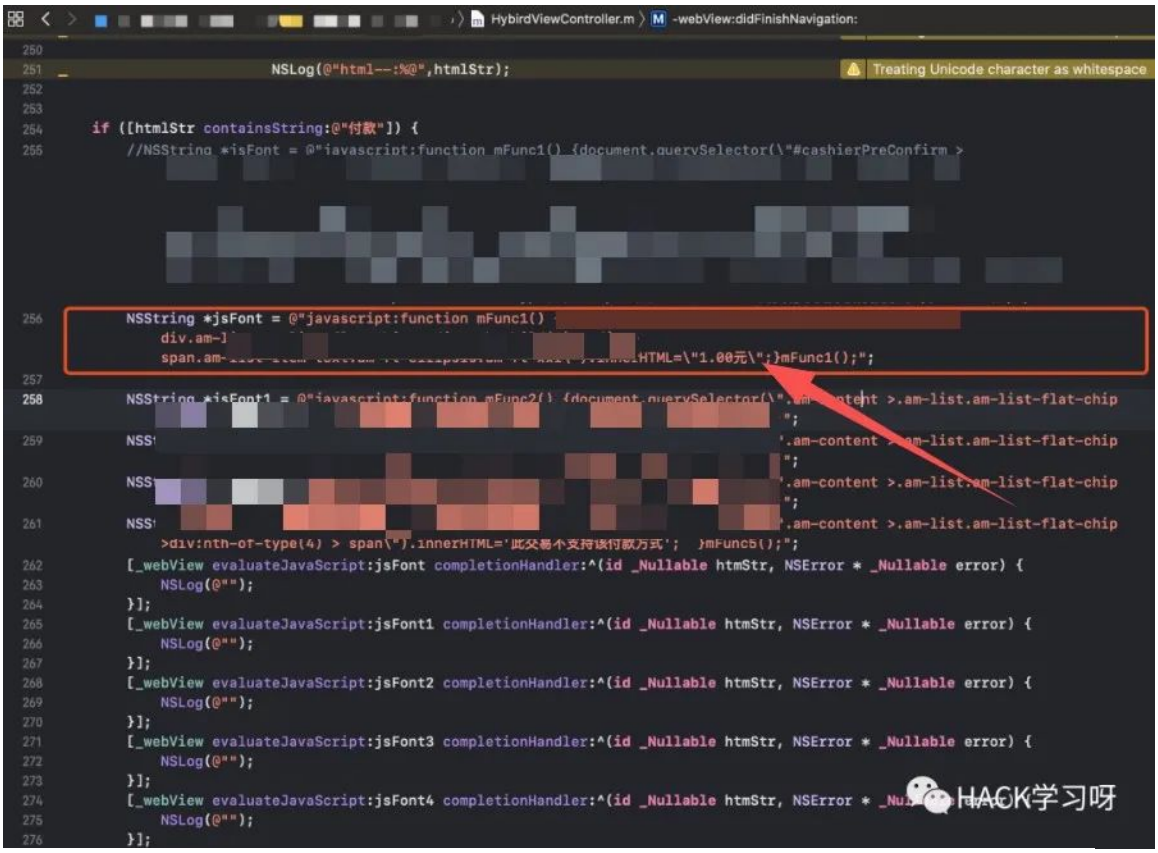
Android端

通过在telegram上找到一个自称买源码的，拿到apk脱壳后，拿到了android端的源码

注意看红色的箭头处和上述的支付的时候显示的数字　　1

这个订单信息就会被覆盖为显示直播间充值，细心的人可以看的出来，其实这个　1
看起来上很别扭的，字体和大小和上面上默认的字体不一样

IOS端



原理和Android端上一样的，也是利用JS和HTML元素进行覆盖原有的显示金额和付款信息，从而诱导你支付

0x03　如何防范此类新型诈骗

1.警惕各类色情App的下载以及凡是涉及支付和转账的操作一定要谨慎

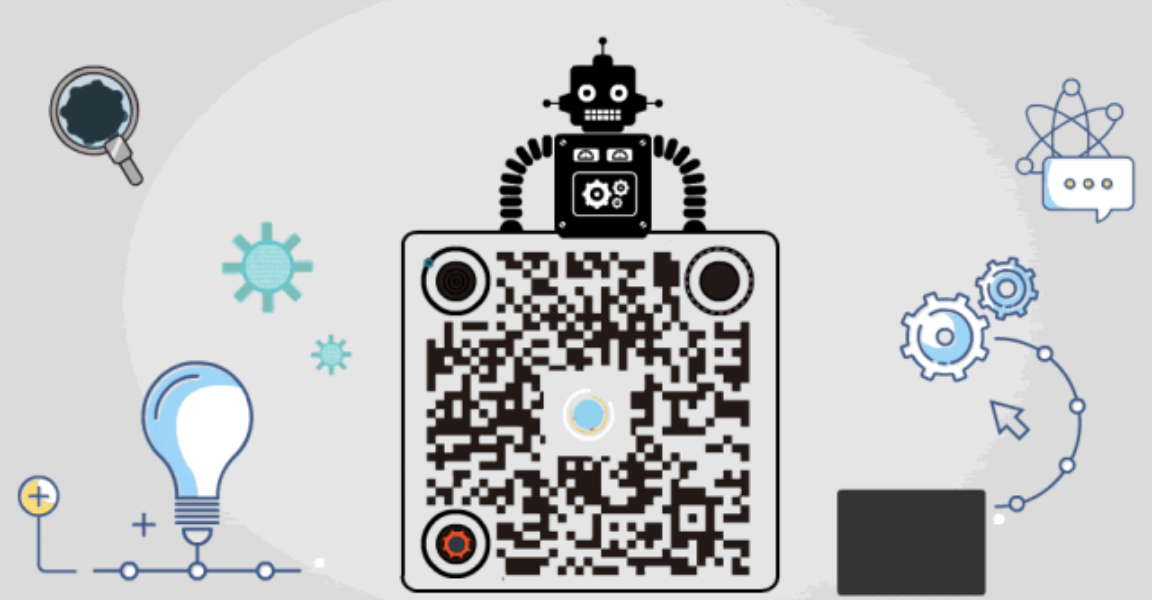
2.管好自己的二弟，有时候往往就是一时的JING虫上脑，才会破财又伤身

3.陌生人发来的链接不要随便乱点，还有就是App，极有可能上木马或者其他恶意软件

4.wx和支付宝能扫码支付就扫码支付，扫码就会暴露真实的金额，不会被障眼法所蒙蔽

5.遇到此类诈骗，记得第一时间报警

点赞，转发，在看



精选留言

用户设置不下载评论