网络安全周信息安全意识漫谈

——手机安全

**-工作交流群-**

****

**隐患分析**

一些企业使用专门的工作沟通软件，这些软件通常会接入人事信息，可以保证已离职或外部人员无法加入。但是，如果使用日常生活中的即时通讯软件，则无法保证人员调整后自动同步，也无法保证用户不添加外部人员进入群组中，会产生信息外泄风险。

**安全建议**

在互联网上运行的工作交流群，严禁讨论、传输国家秘密；进行相关工作交流时，建议优先使用企业指定的工作沟通软件；如果需要使用即时通讯软件（例如：QQ、微信）建群，管理员应该做好群组成员维护，禁止非管理员邀请其他用户入群，及时移出离职人员；重要文件建议优先选择邮件发送或单点发送，避免直接发送到外部群里。

**-短信恶意链接-**

****

**隐患分析**

案例中，攻击者通过短信方式，引诱用户点开链接，从而导致感染木马。一些用户收到此类短信后会抱着“点开没事，只要我不填写就行”的心态，这种认识是不正确的。点击恶意链接后，手机会自动在后台下载恶意软件，也可能立即在手机上运行恶意代码。

**安全建议**

在收到可疑短信后，不要点击短信中的链接；在手机中安装移动安全软件，防范此类短信诈骗风险；及时更新手机系统版本，防止攻击者利用漏洞感染手机。

**-双因素认证**-



**隐患分析**

攻击者常常会利用病毒木马、暴力破解、撞库等方式，来获取用户的账号并尝试登录。为了防范这种风险，越来越多的平台都开始支持“双因素认证”，即在登录时除验证密码之外，还验证另外的一个信息。

**安全建议**

针对比较重要的平台，应该开启双因素认证，可以绑定常用的手机；手机上收到的验证码，在绝大多数情况下都不能提供给其他人；在更换手机后，应该及时更改收取验证码的手机号，以免无法正常登录。

**-应用安装-**

****

**隐患分析**

随着智能手机的普及，各类APP接连涌现，其中出现了一些存在恶意行为的应用程序。并且，由于每天都要审核大量APP上架，应用商店平台也难免会出现一两只“漏网之鱼”，这时就需要用户加强安全防范意识。

**安全建议**

下载APP时，请从官方认证的应用商店中下载，或前往应用程序的官网扫码下载；在下载游戏辅助、系统优化、手机安全、身份信息管理类型的APP 时，由于这些APP通常需要较高权限，需谨慎选择信誉较好的产品，并从官方途径下载。

**-SIM卡安全-**



**隐患分析**

目前，许多平台都会使用短信验证码的方式进行用户身份验证。一旦手机丢失，如果没有及时挂失SIM卡，就给了攻击者可乘之机。除了收取验证码之外，攻击者还可能拨打亲友电话进行诈骗。

**安全建议**

在丢失手机后，应及时拨打运营商电话远程挂失SIM卡； 为SIM卡设置PIN密码，在重启手机或更换手机后，必须输入PIN码才能使用SIM卡。

**-号码注销-**



**隐患分析**

注销手机号后，一般间隔 6个月左右，运营商就会重新发放已经注销的老号码。如果前一个用户没有及时将老号码绑定的支付软件、银行卡、应用程序解绑，新用户在拿到号码后，有可能通过短信验证码获取上一个用户的私人信息。

**安全建议**

在换号前，务必修改银行卡、支付软件、常用应用程序绑定的手机号码； 注销手机号后，如果发现有平台未更换预留号码，通常可以通过联系人工客服的方式，在验证身份信息后进行修改。

（供稿：绿盟科技）