

10月11日至17日,2021年国家网络安全宣传周在全国范围内统一开展。本届网安周主题为“网络安全为人民,网络安全靠人民”,由中央宣传部、中央网信办、教育部、工业和信息化部、公安部、中国人民银行、国家广播电视总局、全国总工会、共青团中央、全国妇联等十部门联合举办。本届国家网络安全周期间,将陆续举办网络安全技术高峰论坛主论坛、青少年网络保护论坛、网络安全产业发展论坛、“长安杯”网络安全极客挑战赛、零信任安全实践论坛、全国青少年网络安全竞赛决赛等多项主题活动。

家长注意! 小朋友也可能 成为电信诈骗对象

作为家长,你是不是有以下想法:小朋友没有钱,不会被骗。事实上,从今年以来,多地已有多起未成年人被诈骗案件发生,被骗人中年龄最小的仅8岁。

【案例】

今年暑假,君君随父母到一家火锅店参加聚会。午饭后,家长们聊天打牌,无聊的君君像往常一样,拿过妈妈的手机玩。君君最开始刷的某视频平台,看到好几个视频主播称关注他完成任务后就能免费得到游戏“迷你世界”的外观皮肤。君君按照操作,依次关注了6个主播,最后一个让君君加了一个“迷你世界暑假皮肤领取群”的QQ群。

第二天,群中的“派送员”联系君君,让其扫描二维码领取皮肤。君君扫描二维码后,屏幕上却弹出一句:“检测到此微信使用期间存在风险,导致兑换失败,请在30分钟内联系警官解除风险,超时将会导致此微信永久封号,及使用人面临罚款10万元判刑坐牢!”

年幼的君君一下子吓蒙了!他马上问“派送员”这是怎么回事?而对方则立即又推送了一个二维码,叫君君找警官解决。君君听话地扫描了对方为好友。自称“警官”的对方让君君下载一个社交联系APP,以会议的方式教他操作,并警告君君不要告诉其他人。

按照对方指挥,君君打开手机上的支付宝,但他不知道妈妈的支付密码,这点却并没有难住对方。“警官”教君君通过手机短信改密码的方式,把其妈妈的登录密码、支付密码给更改了。然后在对方的教唆下,君君通过二维码支付的方式付了好几笔钱,共计被骗12083元。

【反诈提醒】

1、家长对孩子应做好“规范使用手机”的教育,特别是对社交账号、游戏账号的使用,不要擅自添加陌生好友,短信验证码不能随意给到网上陌生人,也不要轻易和陌生人进行屏幕共享,避免个人信息的泄露。

2、公安机关不会在网上远程“办案”,更不会需要当事人“转账”了事,要提醒未成年人,不管是网络中还是现实中,如果遭遇不明情形,不要擅自处理,当面求助师长或民警,或者拨打110报案是最稳妥的办法。

@所有人 网络安全绝招,你值得拥有

对网络安全“漏洞”,每天上网的你,了解多少? 知道怎样保护自己的个人信息吗?

今天就为大家科普网络安全知识,向安全漏洞、风险隐患说“不”!

漏洞一:个人敏感信息随意外泄

一张照片就能泄露全部家庭成员信息,容易给不法人员创造行骗、行窃的机会,尤其是老人、小孩的信息,更要注意保护,包括姓名、幼儿园和学校的地址等。

1、晒娃要注意

有些爱晒孩子的家长没有关掉

微信中“附近的人”这个设置,骗子通过微信搜索“附近的人”,轻易就能获取孩子的信息。

2、行程要保密

外出时,日程安排、行踪等信息要注意保密,不要给犯罪分子行窃的机会。所以,外出期间能够显示

姓名、身份证号的车票、护照、飞机票等不要“晒”。

3、保护好隐私

尽量不要在照片中出现特征明显的东西,例如你的家门钥匙、车牌号码,以及身份证、驾照和护照等证件。

漏洞二:密码过于简单或所有账户使用同一密码

对于密码我们都不陌生,每当我们登录论坛、邮箱、网站、网上银行或在银行取款时都需要输入密码,密码的安全与否直接关系到我们的工作资料、个人隐私及财产安全。

以下几点要注意:

- 1、不要所有账户使用同一密码
- 2、重要的账户应使用更为安全的密码
- 3、偶尔登录的论坛可以设置简单的密码
- 4、日常使用的电子邮箱、网上银

行、公司信息系统需设置复杂的密码

5、不要把论坛、邮箱、网上银行、信息系统账户设置成相同密码

下面几个窍门教给大家:

第一式 短语拼接

自己熟悉的短语,最好有数字有字母,大小写结合,如“5G时代@”转换为密码“5Gshidai@”。

第二式 整句化散词

使用喜爱的诗词拼音首字母加上数字与特殊符号组成密码,如“天生我才

必有用”首字母加数字与特殊字符组成密码“tswcbuyy@6”。

第三式 数字换文字

可以将汉字替换成对应的阿拉伯数字,如“二月春风似剪刀”转换成密码“2ycfsjd@”。

第四式 中英文匹配

选择熟悉的一句话,部分用拼音其余用英文单词代替,并加上数字与特殊字符进行组合,如“我爱工作”“wo love work@7”。

漏洞三:使用没有密码的公共WiFi

为了满足网民手机上网需求,现在不少商家都配备WiFi来吸引消费者。“公共WiFi”虽然方便,但也有不少安全隐患。黑客们喜欢在“公共WiFi”里设置埋伏,网民一不小心就会

中招,轻则损失钱财,重则个人信息全泄露。

手机如何安全使用“公共WiFi”?下面几招教你:

- 1、手机设置禁止自动连接WiFi

- 2、拒绝来源不明的WiFi
- 3、使用安全软件检测WiFi
- 4、不使用陌生Wi-Fi进行网购
- 5、警惕同一地区多个相同或相似名字的WiFi

漏洞四:放松对“熟人”钓鱼邮件的警惕

钓鱼邮件是指黑客伪装成同事、合作伙伴、朋友、家人等用户信任的人,诱使用户回复邮件、点击嵌入邮件的恶意链接或者打开邮件附件以植入木马或恶意程序,进而窃取用户敏感数据等的一种网络攻击活动。

防范钓鱼邮件要做到“五要”:杀毒软件要安装;登录口令要保密;邮箱账号要绑定手机;公私邮箱要分离;重要文件要做好防护。

另外,不要轻信发件人地址中显示的“显示名”。因为显示名实际上是

可以随便设置的,要注意阅读发件邮箱全称;不要轻易点开陌生邮件中的链接;不要放松对“熟人”邮件的警惕。如果收到了来自信任的朋友或者同事的邮件,你对邮件内容表示怀疑,可直接拨打电话向其核实。

漏洞五:扫描来历不明的网站或APP上的二维码

移动支付时代,扫描二维码已经成为我们生活中最稀松平常的事儿。可是,这些二维码看起来方便,但是一不小心,你可能就要付出钱财损失的代价。

以下是常见的几种二维码诈骗伎俩:

1、在商场购物时,遇到称“扫二维码”就能免费赠送商品的“推销员”,大家决不能抱着“不要白不要”的想法顺手扫码。有些不法分子利用了这种心

理,通过各种方式诱导受害者扫描二维码。受害人在不知情的状态下登录预设网站自动下载木马病毒,导致个人信息、网银密码被窃取。

2、有不法分子会通过微信向大家发送一个二维码,谎称扫描二维码帮忙刷一下淘宝店的信誉,还能得到佣金。市民一旦输入了手机号和银行账号,不久后微信钱包里的余额会被转走。

3、有人在车窗上看到“违法停车

单”,单子底部附有一个二维码,如果车主扫描二维码进入,屏幕上就会出现一个200元的转账界面。该手段比传统诈骗有较强的迷惑性,群众容易上当受骗,社会危害相当大。

所以,一定要慎重甄别网络虚拟身份,切不可相信来历不明的二维码,填写账号、密码时,一定要验明对方身份真假,谨防受骗。一旦发现钱款被转走,及时报警。

中国 西安 2021.10

Xi'an, China October, 2021

