2021年10月13日 星期三
责任校对 朱 静 责任编辑 李 鹏
技术编辑 远艾容

沧州晚报

你在微信中“晒娃”，骗子已获取孩子信息……

诸多网络安全漏洞，一定要堵好

当下，每个人都离不开网络，对于网络安全漏洞，每天上网的你，了解多少？以下网络安全知识您一定要了解。

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：不要所有账户使用同一密码；重要的账户应使用更为安全的密码；偶尔登录的论坛可以设置简单的密码；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；不要把论坛、邮箱、网上银行、信息系统账户设置成相同密码。

下面几个窍门要掌握：

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“天生我材必有用”首字母加数字与特殊字符组成密码“tswcbyy@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”转换成密码“wo love work@7”

漏洞三：

使用没有密码的公共Wi-Fi

为了满足网民手机上网需求，现在不少商家都配备Wi-Fi来吸引消费者。“公共Wi-Fi”虽然方便，却有不少安全隐患。黑客们喜欢在“公共Wi-Fi”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Wi-Fi”，以下几招要记牢：

1.手机设置禁止自动连接Wi-Fi。

2.拒绝来源不明的Wi-Fi。

3.使用安全软件检测Wi-Fi。

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Wi-Fi。

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：

扫描来路不明的网站或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，你可能就要付出损失钱财的代价。

常见的几种诈骗伎俩：

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，切不可相信来路不明的二维码，填写账号、密码时，一定要验明对方身份真假，谨防受骗。

据新华网

“领导”让你转账，你会转吗

别大意，这有可能是网络诈骗

“领导”加你微信，关心你的工作和生活，还约你到他办公室安排工作？先别激动，这可能是一场网络骗局。近期，多名基层干部向半月谈记者反映，有犯罪分子冒用部门领导的微信名和头像，通过一些话术诱使受害人向指定账号汇款，达到骗取钱财的目的。

遭遇骗局却“受宠若惊”

去年12月，广西来宾市某单位干部收到一条微信好友申请。看到对方自称该单位领导，受害人通过了申请。随后一段时间，“领导”不时嘘寒问暖，关心其工作生活，与受害人逐渐建立了信任。

12月底的一天，“领导”联系受害人，让他第二天上午到办公室谈工作。在第二天上午约定的时间到来前，这位“领导”再次联系受害人，说正忙着接待上级检查，有一笔比较急的款项需要转给上面“打点关系”，但这么大金额的汇款，自己“不方便直接出面”，让他把钱打到一个指定账号上。为了让受害人放松警惕，“领导”还主动要求受害人提供银行账号，表示自己先把钱转账给他，并出示了一张伪造的银行汇款截图。

看到“领导”如此信任自己，受害人受宠若惊，没有核实相关记录就先后3次将总计68万元的款项汇入指定账号。直到“领导”还在继续要求他汇钱时，受害人才觉得不对劲，向真正的领导询问情况，发现自己已经上当受骗。

无独有偶，今年7月，来宾市某县一工程相关人员也遭遇了相似骗局。诈骗人员冒充该县县长，添加受害人为微信好友，以“预付工程款”的名义，向其索要30万元。受害人看见对方说出了自己的名字就放松了警惕，将工程款转到指定账号。

记者从广西来宾市打击治理电信网络诈骗新型违法犯罪中心了解到，近年来，通过冒充领导微信、QQ账号，以各种借口诈骗的案件呈上升趋势。公职人员、企业财务等岗位成为此类诈骗分子针对的人群。今年1月至7月，该市共发生此类案件49起，涉案金额总量超500万元。

假冒领导有套路

据公安办案人员介绍，实施这类诈骗的犯罪分子都有一些固定的招数和套路。他们一般先通过非法渠道获取受害人及其工作单位领导的个人信息，再用领导的照片注册社交账号，使受害人放下戒心，接受好友申请。

事实上，一些犯罪分子可能并没有完全掌握受害人领导的个人信息，他们不会主动告知自己是谁，而是发一句“这是我的微信，以后方便联系”等类似的消息。等受害人回复“您是某某领导吧”，犯罪分子对号入座，受害人就已经踏进了犯罪分子的圈套。

随后的一段时间里，“领导”会进一步让受害人感受到他的“抬爱”。“最近工作进展得顺利吗”“这周的报告完成得不错”“明天来我的办公室，我给你安排工作”……在“领导”的“殷切关怀”下，受害人一点点放下警惕。一旦建立起足够的信任，犯罪分子就开始以借钱、上级领导要求转账、朋友急用等理由，要求受害人向指定银行账户汇款。

“项目急需资金，你替我转个账，之后还你”“上头来了个领导，帮我包个红包”“这笔款不方便从我这转，过一下你的账户”……犯罪分子还会事先发送一张伪造的转账截图，告诉他钱已经打到受害人账上，让他更“放心”地将钱转出。

广西来宾市反诈中心民警向记者介绍，这类通过冒充领导社交账号要求银行转账的诈骗行为非常难防。诈骗分子打着“领导”的幌子，迅速同下属建立信任。部分受害人即使在转账前产生了疑虑，也不敢找领导多问一句。

新型诈骗为何难防

“诈骗分子太厉害了，我的信息他们都掌握，模仿起来还挺像。”广西某镇党委书记对记者说，有诈骗分子以他的名义添加村干部为好友，随后以碰到困难为由要求转账，很有迷惑性。

这名书记表示，现在诈骗分子信息来源渠道多，甚至会用其下乡的工作照作为头像，让人防不胜防。“遇到拿不准的情况，直接给我打电话核实。”接到村干部的反馈之后，这名书记发布了一条朋友圈来提醒身边的同事朋友。

据民警介绍，这些诈骗分子一般身在国外，使用租借来的银行账户接收受害人汇款，一旦收到汇款，立刻将钱转入专门洗钱的“水房”（犯罪窝点）。反诈中心工作人员告诉记者，诈骗分子租借银行账户的成本很低，而且会通过不知情的第三方刷单转账，案件的资金在中转账号停留的时间一般不超过10分钟。等到受害人报案的时候，诈骗分子早就带着赃款消失得无影无踪。

“我们做了这么多反诈宣传，可很多受害人都觉得自己不会遇到这种事。”当地民警说。警方认为，通过社交软件实施的电信诈骗与电话诈骗不同，公安机关很难及时进行拦截，遇到所谓“领导”“朋友”的转账要求，一定要通过视频电话等方式核实对方身份。

据《半月谈》