关于网络安全 这些防范知识要牢记

在今天，一个APP，就能让手机里的信息如同“裸奔”；一条链接，就能让网络电信诈骗肆无忌惮……数据显示，截至2022年6月，我国网民规模已达10.51亿，人均每周上网时长为29.5个小时。网信事业越是繁荣发展，越不能忽视与日俱增的风险挑战。

9月5日至11日是2022年国家网络安全宣传周，主题为“网络安全为人民，网络安全靠人民”。我们能做哪些事来避免个人信息的泄露？如何规避可能遭受的财产损失？

这些陷阱不要踩

你扫过恶意二维码吗？

随着电子支付的发展，无现金支付已经深入到每个人的生活当中，但有些不法分子将木马病毒、钓鱼软件植入二维码，威胁着人们的信息安全。

奇安信科技集团天津技术总监崔宗福介绍，目前恶意二维码主要可能带来信息泄露、人身财产损失、木马病毒传播等方面的风险。

对此他建议，不要随意扫来源不明的二维码，扫码后认真核对相关信息，也可以下载一些知名度高、安全性强的安全软件来规避风险。“要增强安全意识，遇到来源不明的二维码多一些防范心理，不要给不法分子可乘之机。”崔宗福说。

公共场所蹭Wi-Fi？小心“被钓鱼”

点上一杯咖啡，连上咖啡厅的免费Wi-Fi看个剧，不少年轻人喜欢在工作之余用这样的方式放松心情。深信服科技股份有限公司天津区产品专家井雨晴提醒，公共场所需警惕“钓鱼Wi-Fi”。

“公共场所的开放Wi-Fi大多不止一个，一些不法分子通过设置移动基站的方式诱导大家连接，所发布的信息、网站访问记录甚至登录密码都会被不法分子窃取。除此之外，一些恶意软件会在连入网络的同时获取用户的通讯录、相册、支付信息等。公共场所连接Wi-Fi时一定要多加小心。”井雨晴说。

你的密码安全吗？

“一组密码走天下”是很多人的习惯，但这种设置密码的方式在方便、好记的同时也增加了个人信息泄露的风险。崔宗福介绍，一般不法分子会采用四种方式尝试破解用户密码，一是暴力破解，即用一定的频率尝试破解密码。二是以用户的生日等个人信息尝试破解。三是使用弱口令尝试破解。四是根据已获得用户密码在其他平台进行“撞库”。

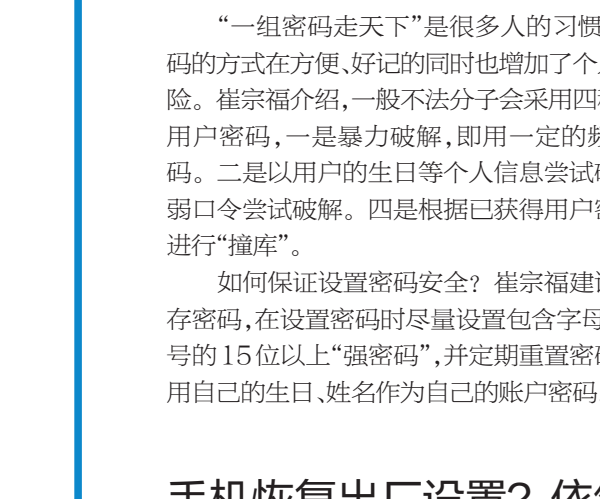
如何保证设置密码安全？崔宗福建议不要用文本储存密码，在设置密码时尽量设置包含字母、数字和特殊符号的15位以上“强密码”，并定期重置密码。“尽量不要使用自己的生日、姓名作为自己的账户密码。”

手机恢复出厂设置？依然有风险

为了更好保护个人隐私，越来越多人在出售旧手机前点击手机自带的“恢复出厂设置”，或一一删除文件。

“恢复出厂设置和删除文件，并不等于彻底删除信息。”中国电子技术标准化研究院网安中心测评实验室副主任何延哲介绍，在手机上删文件，其实系统只是将该文件的指示路径删除，一般人找不到该文件了，但实质内容信息仍存储于手机内部。

何延哲说，目前恢复数据的技术门槛不高，恢复手机中以前的内容信息并非难事。从技术层面讲，即便用户先前做了一些简单的数据清除，删除的信息仍可恢复，可能只是需要多花一些时间和精力，个人信息泄露甚至被兜售的风险依然存在。



这些案例要警惕

刷单返利诈骗

邹奶奶退休后想找个轻松的兼职赚外快，经过网络查询，找到刷单兼职招聘。起初，她尝试支付1.9元，马上得到4.9元返现。看到资金入账后，邹奶奶放松警惕，根据招聘方指示下载指定App，先小额刷单返现，后来金额越来越大，返现却没有了。邹奶奶想退出，要求对方退款，结果又被对方以验证账户安全等各种理由骗取7万余元。醒悟后，邹奶奶报警。

风险提示

骗子以兼职刷单的名义，先以小额返利为诱饵，诱骗投入大量资金后，再拉黑。切记不要被蝇头小利迷惑。

冒充“公检法”诈骗

薛爷爷接到一个自称民警的陌生电话，对方告知薛爷爷涉嫌某洗钱案，要求他添加QQ号。添加好友后，对方发来警官证和含薛爷爷身份信息的刑事拘捕令，并要求薛爷爷找个安静的地方接受远程调查，不能挂断通话。随后对方声称需要验证经济能力、信用能力证明其无罪，让其在网络平台及银行贷款后汇款到某账号上，称结案后会退回。薛爷爷向对方提供的账号转账62万元人民币，之后才发现被骗并报警。

风险提示

公检法机关会当面向涉案人出示证件或法律文书，不会提出远程转账汇款或验证经济能力等要求。

“杀猪盘”诈骗

小李在社交软件上认识一名自称在国外做军医的人，经过一段时间聊天接触，两人感情逐渐升温。某日，“国外军医”声称获得100万美元任务津贴，放在他那里不安全，要快递给小李，小李答应了。随后“国外军医”开始以运费、保险费、被海关扣留等各种理由向小李索要了超28万元。之后，“国外军医”突然失去了联系，此时小李才恍然大悟。

风险提示

素未谋面的网友、网恋对象推荐网上投资理财、炒数字货币（虚拟币）、网购彩票、博彩赚钱或通过各种借口直接索要钱财的要当心。

虚假票务诈骗

赶上寒暑假小张都会出去旅游，正因是临近旺季，这次小张未订到心仪的机票，最后通过搜索引擎找到一个小网站，上面的机票价格低廉但库存紧张。小张赶忙预订，但付款成功后，页面显示“出票失败”，并建议购买更高等级舱位。小张见其建议售价仍低于市场价，便再次付款。但依然显示“出票失败”。这时小张察觉到不对，想要退款，却发现没有退款通道，这才意识到自己被骗。

风险提示

务必通过正规渠道购买车（机）票，不要轻易点击、扫描任何来历不明的网址链接、二维码。

这些防护要做足

手机、电脑使用

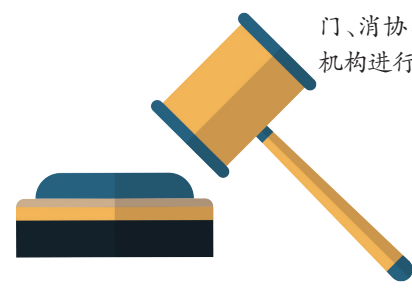
- 为电脑安装安全软件并开启防火墙。
- 及时更新操作系统和软件版本。
- 下载软件必须通过正规渠道。
- 不随意丢弃、出售旧手机、平板、智能手表等电子设备。
- 软件安装过程中，谨慎开启敏感权限（如定位、录音录像等）。
- 定期清除浏览器Cookie，防止浏览行为被追踪。
- 定期检查电子设备的运行情况，防止数据“偷跑”。

个人信息保管

- 不在网络过度分享家人、住址等敏感信息。
- 尽量不在网络留存身份证号、手机号等重要资料。
- 收快递时要撕毁快递箱上的面单。
- 不随意向外提供手机收到的验证码。
- 不随意在网上参与小测试、小调查。

投诉举报

- 个人信息一旦被泄露，可以向互联网管理部门、工商部门、消协、行业管理部门和相关机构进行投诉举报。



这些法规要学习

《中华人民共和国网络安全法》

2016年11月7日，第十二届全国人民代表大会常务委员会第二十四次会议通过《中华人民共和国网络安全法》，自2017年6月1日起施行。

- 明确个人、组织不得危害网络安全，不得利用网络从事危害国家安全、荣誉和利益，传播暴力、淫秽色情信息，编造、传播虚假信息扰乱经济秩序和社会秩序，以及侵害他人名誉、隐私、知识产权和其他合法权益等活动。
- 明确社会公众对危害网络安全行为有举报权，可向网信、电信、公安等部门举报。
- 明确网络运营者开展经营和服务活动，需履行网络安全保护义务，接受政府和社会的监督，承担社会责任。

《中华人民共和国数据安全法》

2021年6月10日，第十三届全国人民代表大会常务委员会第二十九次会议通过《中华人民共和国数据安全法》，自2021年9月1日起施行。

- 明确非经中华人民共和国主管机关批准，境内的组织、个人不得向外国司法或者执法机构提供存储于中华人民共和国境内的数据。
- 明确数据处理活动以及研究开发数据新技术，应当有利于促进经济社会发展，增进人民福祉，符合社会公德和伦理。

《中华人民共和国个人信息保护法》

2021年8月20日，第十三届全国人民代表大会常务委员会第三十次会议通过《中华人民共和国个人信息保护法》，自2021年11月1日起施行。

- 明确任何组织、个人不得非法收集、使用、加工、传输他人个人信息，不得非法买卖、提供或者公开他人个人信息。
- 明确信息处理者利用个人信息进行自动化决策，应当保证决策的透明度和结果公平、公正，不得对个人在交易价格等交易条件上实行不合理的差别待遇。

（综合自新华网、2022年国家网络安全宣传周指挥部办公室、中国支付清算协会、中国普法微信公众号等）

整理/珠江时报记者 黎国栋