作，也可能给你带来危险。比如一些直接以 ip 地址访问的链接（有时会加上端口号）绝不可以随便点。

当你发现自己打开了一个空白网页，请务必提高警惕，有时一些危险代码就是在不知不觉间默默运行起来。也许没觉得有什么，但当你点开的那一瞬间，就已经中招了。

如果攻击者使用的是网站自身网页上的漏洞，那么完全可以使用看起来是自家网站的网址来实现恶意行为。

二、钓鱼网站需谨慎判别

如果有时被非正式渠道诱导，或是从非官方页面跳转到某个链接，还需要输入密码时，不如输入错误的密码试试看？如果还能登录成功或是提示再次登录一类的异常情况，那这个链接就有可能是一个钓鱼链接。请时刻保持冷静、保持怀疑，很多骗局都利

用了人的心理弱点把原本并不完美的骗局填补完整。

现在的技术，完全可以轻松地把钓鱼页面做到和原来丝毫不差。不要太过自信去挑战它，有很多人为了完善这项技术付出了努力，我们能做的就是提高警惕保持怀疑。

三、不安全程序别随便运行

不要打开来源不明的 exe 以及其他用途不明的文件，不要在不安全不保险的第三方网站下载软件，一旦这些恶意的可执行文件在你的许可下被运行，后果非常严重！

四、捡到 U 盘不可随意使用

可能大家会想不到，一个小小的常用的 U 盘也可能会是一枚不起眼的“小炸弹”，而且 U 盘，鼠标、键盘、充电宝等 USB 相关设备都有可能是这种攻击的载体。

虽然 USB 相关设备都有可能用来发动攻击，但 U 盘扔到别人面前会让人产生查看的欲望，这种恶意设备“发作”很快，不会给你太多反应时间，最好的避免办法就是不要接触它们。不要捡到什么都想插进电脑看一看，你可能不会发现什么新的“XX 门”。正相反，你更有可能变成下一个“XX 门”。

提醒：BadUSB 会待自己伪装成鼠标键盘等正常的 USB 设备的样子，插入后即运行恶意代码，如果发现有一个 U 盘插入后无法打开，可要小心。

网络安全知识

1. 来源可疑的链接不要点击，不是仅仅浏览就没有一点风险的。
2. 官方渠道的相对而言最可靠，下载软件等需要通过官方渠道满足，其他都有风险。
3. 钓鱼网站如今已经可以做到和真网站一模一样，最好的办法就是别碰它，而不是碰了之后甄别真假。
4. 收到中奖之类的信息时，请辨别信息来源，不要被冲昏了头脑（可以通过多个渠道共同作用来确认信息真假）。
5. 宏功能如果不经常使用做好关闭。
6. 任何设备上的可执行文件都要谨慎使用，不然很有可能是亲自给黑客开了门。
7. 保持重要设备与危险之间的距离，不确定安全的 U 盘、移动硬盘等物品不要轻易与设备连接。

网络安全 手机安全篇

手机是当代人使用频率最高的工具，甚至不用加上“之一”，但实际上，如果使用手机的安全意识能有所提升，就已经可以解决大部分安全问题了。

一、不从非官方渠道安装应用

需要使用的软件尽量从可靠的官方网站下载，而类似于 XX 软件园 XX 软件网的网站，其中的软件来源可能是私人上传，无法保证其安全，可能会存在病毒，以个人名义发给你的软件应用（比如好友私发、微信或 QQ 群内共享），最好不要下载使用，而应该去官网查询下载渠道（有特殊用途或是某些特定功能除外），这些软件极有可能是钓鱼软件，安装微信群中软件导致公司破产的已有先例。

二、手机数据常备份降风险

数据备份是一个好习惯，万一出现意外情况，定期备份可以使你的损失降到最低。如今勒索病毒已经“出圈”，不只是数字货币“圈”内部，它也盯上了普通的互联网用户，勒索病毒的主要运行原理就是加密文件，而这些文件如果没有对应的密钥解密，是无法还原到正常模样的。

网络安全知识

1. 个人信息泄露早就不新鲜了，就算有人能提供准确信息也不要轻易相信对方。
2. 天上不会掉馅饼，时刻保持冷静，失去理智会提高黑客的成功率。
3. 来源未知的软件不要安装，敏感权限不要都给，视情况而定。
4. 手机和软件有更新最好及时安装，也许就省去了一次麻烦。
5. 没有必要获取设备最高权限。
6. 设备数据定时备份，减少损失。
7. 免密支付一类的便捷功能使用时应特别注意安全。

什么是互联网违法和不良信息？

2020 年 3 月 1 日起施行的《网络信息内容生态治理规定》中第六条规定

网络信息内容生产者不得制作、复制、发布含有下列内容的违法信息：

（一）反对宪法所确定的基本原则的；

（二）危害国家安全，泄露国家秘密，颠覆国家政权，破坏国家统一的；

（三）损害国家荣誉和利益的；

（四）歪曲、丑化、亵渎、否定英雄烈士事迹和精神，以侮辱、诽谤或者其他方式侵害英雄烈士的姓名、肖像、名誉、荣誉的；

（五）宣扬恐怖主义、极端主义或者煽动实施恐怖活动、极端主义活动的；

（六）煽动民族仇恨、民族歧视，破坏民族团结的；

（七）破坏国家宗教政策，宣扬邪教和封建迷信的；

（八）散布谣言，扰乱经济秩序和社会秩序的；

（九）散布淫秽、色情、赌博、暴力、凶杀、恐怖或者教唆犯罪的；

（十）侮辱或者诽谤他人，侵害他人名誉、隐私和其他合法权益的；

（十一）法律、行政法规禁止的其他内容。

遇到互联网违法和不良信息如何举报

一、向所在网站平台举报

（一）网站平台内举报

点击右上（下）角，选择“举报 / 投诉”按钮，选定举报类别后提交。举报评论内容可点击或长按，选择“举报 / 投诉”按钮，选定举报类别后提交。

（二）部分常用网站平台举报电话

网站平台	违法和不良信息举报电话
腾讯	4006700700
百度	4009216911
微博	010-60618076
抖音 / 今日头条	4001402108
快手	4000066666
小红书	021-60109904
哔哩哔哩动画	4006262233 转 1

二、向中央网信办举报中心举报

1. 登录举报中心官网 www.12377.cn 举报；
2. 下载安装“网络举报”客户端举报；
3. 关注举报中心官方微博“国家网信办举报中心”，点击“私信举报”；
4. 关注举报中心官方微信公众帐号“国家网信办举报中心”，点击“一键举报”；
5. 拨打 12377 举报热线举报；
6. 发送邮件至邮箱 jubao@12377.cn 举报。

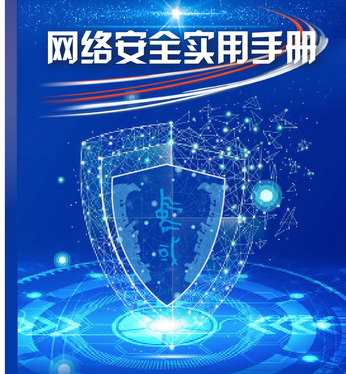
三、陕西省各地违法和不良信息举报电话、邮箱

市（区）	举报电话	举报邮箱
陕西省网信办	029-63907150/63907152	shxiwxb@126.com
西安市网信办	029-86780735	jubao@xawljb.cn
宝鸡市网信办	0917-3263322	bjwxjb001@163.com
咸阳市网信办	029-33210010	xy12377@126.com
铜川市网信办	0919-3158095	sxtcwljb@163.com
渭南市网信办	0913-2936050	wxk109@163.com
延安市网信办	0911-7097286	yaswxb@126.com
榆林市网信办	0912-6662189	ylwljubao@163.com
汉中市网信办	0916-2226631	hz_wxb@163.com
安康市网信办	0915-3288078	akwljb@163.com
商洛市网信办	0914-2866698	slwljb@163.com
杨凌区网信办	029 -87030800 yanglingwangxinban@163.com	

四、举报须知

举报互联网违法和不良信息时，应当遵循以下要求：

1. 对举报的客观性、真实性负责，不得故意捏造事实、伪造证据；
2. 提供明确、具体的举报信息网址或者能够定位举报信息的说明、证明、证据等举报材料；
3. 陈述举报事项，阐明举报理由；
4. 为处置互联网违法和不良信息，确需举报主体提供真实姓名、有效证件和联系方式等信息的，举报人应当予以配合。



2024年陕西省第十一届国家网络安全宣传周

网络安全实用手册

中共陕西省委网信办
陕西省互联网信息办公室 宣

网络安全 线上社交篇

如今，网络世界已经变成了人们第二个生活场所，越来越多的网民喜欢在虚拟的世界里展现自己的现实生活，但是，人们展现现实生活的同时，也暴露出了更多的自身信息。一个技术全面的黑客可以轻易地在各类动态、相片中捕捉与之相关的蛛丝马迹，从而发起一场具有针对性的攻击活动。

一、社交账号莫凭手机可查

微信、QQ 等社交软件具有“可通过其他相关信息（如手机号\QQ 号等）搜索到我”的功能，如果不是日常需要，完全可以关掉该功能！它使社交更加容易的同时，也会加大在黑客面前的暴露面积！

二、社交空间勿显个人信息

谁都想把自己的生活在朋友圈中展现得美美站，但朋友圈等社交媒体软件往往也是黑客收集信息的最佳渠道之一，在展现美丽生活的同时，也要注意个人信息安全。

信息时代，很多大家想不到的地方，都会暴露个人隐私，哪怕是在家对着窗户发一张自拍，都有暴露居住地的风险！（某国外女星就经历过这样的事件：在家里面向窗户发了一张自拍照后，被某“粉丝”依照睫孔里映照出来的窗外画面，找到了该女星的住址。）

网络安全知识

1. 对陌生人设置社交媒体浏览权限，加了不明身份的好友时也应限制浏览权限。
2. 照相机原图可能存有机器型号，拍摄时间拍摄地经纬度信息，不要发原图。
3. 不要在社交媒体中每一处（留言板、个性签名朋友圈背景、生活照片、微信号、昵称）留下有关自己的真实敏感信息（真实姓名、个人资料、家庭、工作地址定位、证件号码、个人履历、关系网络、房间场景、好友备注），如果有请及时删除或管理。
4. 关闭他人可通过手机号或其他非微信号、QQ 号渠道查询到你的功能。
5. 新好友确认对方真实身份前，不要先提供自身敏感信息或产生资金往来，可多渠道确认身份，如打电话、询问私密问题等。
6. “附近的人”功能可被人用来确认上一次开启定位时的具体位置。

网络安全 办公安全篇

在惯性的思维习惯中，办公室是一个只有同事出入的地方，相对而言更加私密、安全，因而有人把一些账号密码写在便利贴上贴在能看见的地方；有人离开工位不锁屏；有公司只有一个 WiFi，办公会客都用这一个，但实际上办公室并不如此安全。黑客的特长之一就是跳出思维惯性，不按套路出牌，他们经常会利用人们的思维习惯做一些意料之外的事情以达成目的。

网络安全知识

1. 将办公和访客使用的网络分离开。
2. 对外部防御严格的同时，加强内网防御。
3. 妥善保管各种密码，可使用密码管理工具或写在纸上藏好，不要在便利贴上记录太多敏感信息。
4 . 不可私自启动热点。
5. 严防各种身份不明确的人进入敏感的办公区，即使进来了也不能深入。
6. 有访客前来时，及时将具有敏感信息的废弃物销毁。
7. 离开工位时，随手将电脑锁屏（记得设置密码）。
8. 及时安装各种安全补丁。

一、办公访客无线网络分离

如果情况允许，可以将网络分为工作用和访客用两个部分，并对网络 SSID（无线网的名字）进行隐藏。另外，不要使用易取得的信息（如公司联系电话或贴在墙上的信息等）作为密码，对访客只需提供对应级别的信息即可，保护内网安全更重要。

二、痕迹泄露信息一定销毁

开会结束时记得擦除小白板上你们留下的机密信息，不要把这些直接地提供给攻击者，一些打印出的纸制品，在使用过或已失效后，请不要保留，及时销毁，不要留下痕迹。

网络安全 WiFi 安全篇

目前 WiFi 已经不仅仅出现在家庭中，商场、办公室、餐厅等公共场所都已经有它的身影出现，而这样普及且看管并不严格的技术很容易带来严重又不可控的安全问题。

一、公共无线网不必要勿用

如今 WiFi 普及，在很多公共场所都有公共 WiFi 供大家使用，比如商场、餐厅，纵然是会带来很多便利的，但不要随随便便什么 WiFi 都使用，尤其是进行一些付款之类的敏感操作时，更不要使用公共 WiFi。不甚安全的公共 WiFi 很容易被人做手脚。

二、用他人网刷做敏感操作

不要在别人的网络上做一些登录、付款之类的敏感操作。付款、登录或是传输敏感文件 / 信息类的操作，建议使用自己的手机移动数据，耗费流量并不多。

网络安全知识

1. 公共 WiFi 不要轻易使用，如果要使用请仔细辨别真假。
2. 不是使用自己的数据网络时，不要做一些敏感操作。
3. 含有重要文件、数据的设备不要随便连接不可靠的网络。
4. 隐藏 SSID 也是保护无线网络安全的好法。

网络安全 密码保护篇

密码的进化经历比较传奇，有些古老的密码由于某些密码审核机制并不严格的原因，依然沿用到现在。虽然，这些古老的密码（比如123123）仍然可以发挥基本作用，但技术与时代都在发展，那与之搭配的东西也要紧跟发展，不然就会变成被淘汰的老古董。

一、勿用个人信息组成密码

不要使用个人信息作为密码的组成部分！最经典的例子就是“重要的人的生日”挖到这些信息并进行随机组合不是什么难事。

二、使用多位多种字符密码

目前大多数的服务提供机构都会强制要求密码长度在 6 位或 8 位以上，除了长度以外还有一个增加密码复杂度的方法，就是大小写字母，数字和特殊字符混用。仅以 8 位大小写字母和数字混用的情况来算，就有 218340105584896 种可能，非常不好猜解。

三、定期更换密码防止撞库

在互联网刚刚兴起的初期，互联网的从业者，使用者们普遍安全意识不强，企业安全也并非做的尽善尽美，有很多企业的用户信息数据库被黑客“脱裤”流传在网上，如果大家没有定期更换密码的习惯，就可能被黑客用手里的古老数据抢走你的账户。（友情提示！私自储存这一类的个人信息以及社工库是违法行为！）

注：“脱裤”，意指恶意攻击者违法攻击后获取目标数据库大量信息的行为。

注：撞库是指黑客通过收集互联网已泄露的用户和密码信息，生成对应的字典表，尝试批量登录其他网站后，得到一系列可以登录的用户的操作。很多用户有多个账号共用同一个密码的习惯，所以往往用某某一账号的密码也可以登上其他账号。

除了各个账户的密码不共用以外，也要记得定期更换密码。万一常用网站的数据库被人“脱裤”，黑客拿到的也是过时密码。

网络安全知识

1. 不要使用个人信息设置密码（因为易猜解）。
2. 密码长度应在 8 位以上，使用大小写字母数字符号等多项内容组成。
3. 定期更换密码。
4. 不同的账户使用不同密码，分级管理。
5. 私钥手抄，不要导入浏览器或第三方网站，写在纸上藏好。
6. 不要使用社交网络或邮件传输私钥，也不要截图，可能会被上传同步到云端。
7. 不要在越狱或者拿到 root 权限的安卓机器上安装资产类 App，不要明文存储在电脑上，这二者都有可能被潜在的木马控制。root 过的设备上木马往往拥有更高权限。

网络安全 反钓鱼篇

钓鱼攻击也可以算是社会工程学攻击的一种，主要通过伪装与欺骗的手段引诱受害者掉入陷阱，达成目的。除了常见的“撒网式”钓鱼（即以量补质只要发的信息足够多，总会有人上钩的）以外，还有具有针对性的“鱼叉式”钓鱼。完成“鱼叉式”钓鱼需要攻击者对受害者的信息进行挖掘分析，最后依照受害者的心理，设定出成功概率较大的针对性陷阱进行钓鱼攻击。

一、来源可疑不可随意点击

有一些链接不要随便打开，即便是仅仅打开网页不做其他操