西北农林科技大学
NORTHWEST A&F UNIVERSITY

网络安全常识

信息化管理处（网络与教育技术中心）

2024年9月

一、杜绝弱口令

1. 弱口令的危害

弱口令：容易被别人猜测到或被破解工具破解的口令均为弱口令。

2020年7月30日，四川省西昌市公安局网络安全保卫大队接到报警，西昌市某校学生发现自己的中考志愿被篡改！警方侦查发现该学校竟有上百名学生的中考志愿遭到了篡改！

经过走访摸排，警方于次日凌晨锁定了嫌疑人——该校毕业学生吉洛某某。经审讯，吉洛某某因成绩差，升学无望，心理严重失衡。某日，他看见班主任在微信群里发布《2020年度初三毕业生名单》，就用自己的手机登录凉山州中考志愿填报系统，通过猜密码的方式，对照名单逐一尝试登陆，将他人志愿恶意篡改。因多名学生使用的密码都是“12345678”等弱口令，导致账户被并没有什么黑客技术的吉洛某某登入，志愿遭到了恶意篡改。

此次风波最终得到了妥善处置，没有对学生造成损失和伤害。然而此事还是值得广大网民警醒——不要设置弱口令！

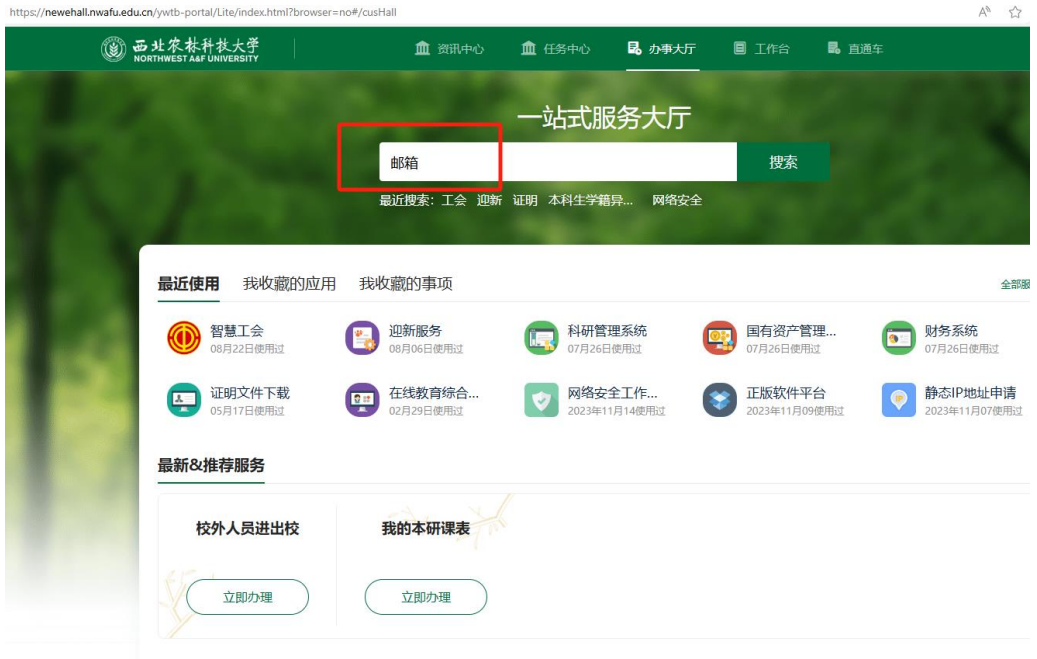
2. 设置适当的口令

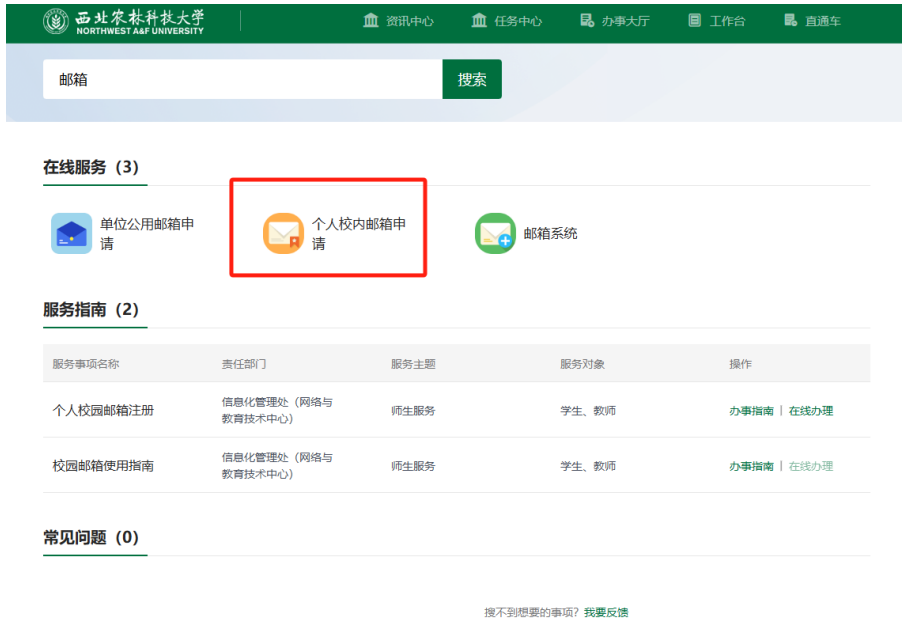
- 绝对不要使用123456、654321、123123、000000、888888、abcabc、123qwe、qaz123等超级弱口令。
- 纯数字或纯字母口令的安全性非常低。建议使用大小写字母+数字+特殊符号，长度不少于8位。
- 密码不要使用账号、生日、手机号码等信息，以防被猜出。
- 不同的系统使用不同的密码，避免连锁反应。

二、安全使用电子邮件

1. 自助申请我校电子邮箱

登录我校一网通办平台（地址：https://newehall.nwafu.edu.cn），搜索“邮箱”，进入“个人校内邮箱申请”即可自助申请校内电子邮箱。





2. 使用电子邮件的注意事项

- 不轻易点击不明邮件中的链接、图片、文件，不给恶意程序或病毒可趁之机。
- 适当设置找回密码的提示问题或绑定手机号。
- 收到与个人信息或金钱相关（如中奖、集资等）的邮件时要提高警惕，校园邮箱收到可疑邮件时，可咨询信息化管理处，电话：87082057、87082976。

三、谨防钓鱼网站

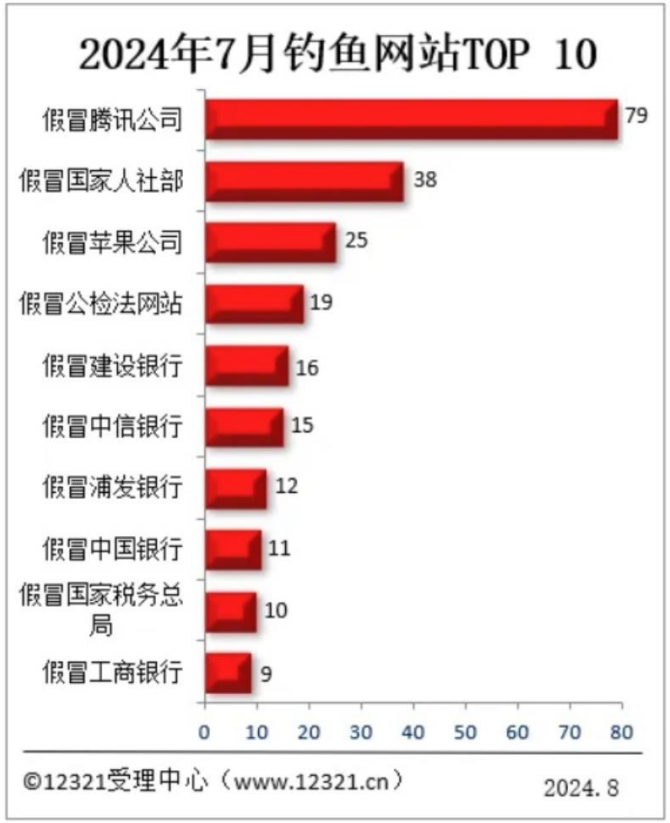
1. 什么是钓鱼网站

钓鱼网站：欺骗用户的虚假网站，与真实网站的界面基本一致，欺骗消费者或者窃取访问者提交的账号和密码信息。

- 钓鱼网站一般只有一个或几个页面，和真实网站页面极为相似。通常伪装成银行及电子商务、窃取用户提交的银行账号、密码等私密信息的网站。
- 钓鱼网站的网址通常与真实网站的地址非常相似。
- 钓鱼网站通常通过电子邮件、即时通讯工具（例如QQ、MSN、Google talk、旺旺等）等发送虚假的钓鱼链接；在论坛、贴吧、博客、微博等开放性的网上社区发布虚假钓鱼链接；通过假冒银行、购物网站或第三方支付平台等正规机构名义发送短信传播钓鱼网站链接。

2. 如何防范钓鱼网站

- 通过查询网站备案信息等方式核实网站资质的真伪。
- 注意防护软件弹出的警告和提示信息。
- 要警惕中奖、修改网银密码，以及貌似苹果账户、支付宝等的通知邮件、短信，以及即时通讯工具发送的莫名链接，这很可能是钓鱼网站设置的陷阱。



12321网络不良与垃圾信息举报受理中心2024年7月份数据

四、防范挖矿木马

1. 什么是挖矿木马

挖矿木马：网络黑客通过各种手段将挖矿程序植入受害者的计算机中，在受害者不知情的情况下利用其计算机进行挖矿，从而获取利益，这类非法植入用户计算机的挖矿程序就是挖矿木马。

- “挖矿”实质上是用计算机解决一项复杂的数学问题，来保证比特币网络分布式记账系统的一致性。挖矿本身需要大量计算机高速运算，一部分人并不通过自己投入成本来挖矿，而是通过挖矿木马控制其他人的计算机挖矿。
- 挖矿木马最早出现于2013年，2017年披露的挖矿木马攻击事件数量呈现出爆发式的增长。其原因在于，比特币等虚拟数字货币交易火爆，有人利用虚拟数字币交易大发横财，吸引大量黑产从业人员进入挖矿产业。
- 此类病毒行为隐蔽、更新频繁、病毒文件特征不明显，一旦感染，很难通过传统杀毒软件发现并彻底清除。

2. 为什么会中挖矿木马

- “挖矿木马”和病毒一般因为疏于安全防护而感染：

  垃圾邮件：用户运行了钓鱼邮件中的附件。

  软件捆绑：用户下载运行来历不明的破解软件。

  漏洞传播：用户没有及时修补漏洞，目前大部分挖矿木马都会通过漏洞传播。

  网页挖矿：用户访问了植入挖矿脚本的网页，浏览器会解析脚本进行挖矿。

3. 感染症状

- 早期的挖矿木马，并没有对系统资源消耗做限制，当挖矿木马运行时，计算机的资源消耗就会增加，CPU占用明显增加，电脑变热，运行速度变慢，重启也不能解决问题。这些明显的症状使得早期的挖矿木马更容易被用户发现、清除。

- 后期，挖矿木马为了避免被用户发现，对挖矿行为做了调整，当检测到用户电脑上CPU占用较高时，会自动暂停挖矿，当用户电脑闲置时，全力挖矿。这样一来，进化后的挖矿木马就能在用户电脑上存活更长的时间，导致即便电脑已经中毒了，也不会有明显异常。

3. 如何防范

- 避免使用盗版、破解或者来源不明的软件，建议从可信的来源安装软件。目前，我校正版软件管理与服务平台（网址：https://software.nwafu.edu.cn）提供Windows、Office、Visio、MATLAB等正版软件，附带详细的安装、激活说明，操作过程中如遇问题，可联系信息化管理处。
- 不随意打开来自聊天工具或邮件传输的不明文件。
- 避免使用非官方网站下载的向日葵、TeamViewer等远程控制软件，避免将远程控制软件的密码传给不信任的人。
- 开启系统自动更新功能，防止因为漏洞感染病毒。

4. 如何处置

- 先使用独立的外置移动硬盘或者网络存储备份当前系统的个人数据和文件。
- 重新安装操作系统，建议从我校正版软件管理与服务平台（网址：https://software.nwafu.edu.cn）下载安装、激活。如遇问题，可联系信息化管理处。

五、安全使用移动终端

1. 安全使用手机

- 为手机设置锁屏密码，防止手机遗失后，通信录、文件等信息泄露。
- 经常为手机数据做备份，手机遗失后，要及时向运营商挂失SIM卡，若手机绑定了支付软件，还需及时向支付服务商冻结相关业务。
- 在QQ、微信等应用程序中关闭地理定位功能，防止泄露个人隐私，仅在需要时开启蓝牙。

2. 安全使用Wi-Fi

- 勿见到免费Wi-Fi就用，要用可靠的Wi-Fi接入点，关闭手机和平板电脑等设备的无线网络自动连接功能，仅在需要时开启。
- 警惕公共场所免费的无线信号为不法分子设置的钓鱼陷阱，尤其是一些和公共场所内已开放的Wi-Fi同名的信号。在公共场所使用陌生的无线网络时，尽量不要进行与资金有关的银行转账与支付。

3. 防范病毒、木马

- 安装安全防护软件，开启实时监控功能，并定期升级病毒库。
- 到安全可靠的应用商店下载手机应用软件。
- 不轻易点击陌生人发送的链接、图片、压缩包等，不随意扫描二维码，以免感染木马病毒，泄露手机号、卡号、密码等信息。

4. 保护手机支付安全

- 建议手机支付客户端与手机绑定，使用数字证书，开启实名认证。
- 登录手机支付应用、网上商城时，勿选择“记住密码”选项。

网络安全为人民　网络安全靠人民

西北农林科技大学
NORTHWEST A&F UNIVERSITY