2023年国家网络安全宣传周精彩活动抢“鲜”看!

2023年国家网络安全宣传周于9月11日至17日在全国范围内统一开展。其中,开幕式、网络安全高峰论坛、网络安全博览会等重要活动将在福建省福州市举行。今年网安周继续以“网络安全为人民,网络安全靠人民”为主题,通过论坛、研讨、展览、竞赛等形式,实现每一主题日都有主题、有活动,全面营造全社会共筑网络安全防线的浓厚氛围。

开幕式

开幕式于9月11日上午在福州市海峡国际会展中心举行。

网络安全高峰论坛

9月11日

“2023年网络安全技术高峰论坛”以人工智能发展与治理为主题进行交流研讨。

9月12日-17日

围绕关键信息基础设施安全、云计算服务安全、汽车数据安全、网络安全标准与实践、青少年网络保护、网络安全协同治理、网络安全服务产业发展等主题,举办14场分论坛和主题活动。

网络安全博览会

9月10日-16日 福州海峡国际会展中心

展览面积约2万平方米,设置关键信息基础设施保护、数据安全、个人信息保护、网络安全产品与服务等展区;

组织网络安全人才与创新发展、历届网安周回顾等主题展区;

将对特色展览、创新成果等开展导览式网络直播。

主题日活动

9月12日校园日

举办“守护青春网络有你”全国大学生网络安全知识答题活动;

组织大学生网络素养能力提升大课堂。

9月13日电信日

各基础电信企业做好行业网络安全宣传;

电信营业厅开展线下宣传活动。

9月14日法治日

以典型案例发布、论坛研讨、主题宣讲等方式,由公安民警开展网络安全普法宣传教育。

9月15日金融日

举办金融网络安全论坛;

金融机构通过网络渠道及线下营业厅发布网络安全宣传素材。

9月16日青少年日

邀请专家学者、青年网络观察员等开展“明辨”主题网络直播活动。

9月17日个人信息保护日

各级工会、妇联组织网络安全优秀作品、线上微课程展播。

网络安全进基层

开展网络安全进社区、进农村、进企业、进机关、进校园、进家庭等宣传普及活动;

福州市打造网络安全宣传走廊,设置网络安全宣传主题公园、主题街区、主题餐厅、主题校园、主题地铁、主题公交等,建设福州市网络空间安全中心。

网络安全线上知识竞赛

“学习强国”APP将网络安全知识竞赛精选试题纳入平台“挑战答题”模块;

通过“国家网络安全宣传周线上知识竞赛”评选安全达人;

有关互联网企业利用产品平台开展网络安全在线答题活动。

网络安全微视频征集

面向全国征集评选动漫、MV、微电影、公益广告等优秀作品,并通过各大网络平台推广传播。

组织形式

2023年国家网络安全宣传周由中央宣传部、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、全国妇联等部门联合举办。

(来源:2023年国家网络安全宣传周新闻发布会)

什么是电信网络诈骗

电信网络诈骗,是指以非法占有为目的,利用电信网络技术手段,通过远程、非接触等方式,诈骗公私财物的行为。

典型骗术

杀猪盘诈骗。杀猪盘诈骗指通过婚恋平台、社交软件等方式寻找潜在受害者,通过聊天发展感情取得信任,然后将受害者引入博彩、理财等诈骗平台进行充值,骗取受害者钱财的骗局。

杀鸟盘诈骗。杀鸟盘诈骗指刷单诈骗、兼职诈骗,骗子通过发高薪兼职信息吸引受害者参与,再通过套路不断鼓动受害者投钱代刷,最终骗取所有投资钱财的骗术。

AI换脸 新型AI诈骗。AI换脸是一种基于人工智能技术的图像处理应用,可以将一个人的面部特征和表情应用到另一张照片或视频中,实现快速、高效的人脸替换。

防范建议

保护个人信息:不向陌生人提供身份证号码、家庭住址等重要信息;尽量减少个人照片、视频的泄露。

不透露密码:为银行卡、网上银行、手机银行设置复杂程度较高的密码,不向任何人透露或转发短信验证码或其它形式动本密码。

官方渠道办业务:办理银行信用卡及额度提升等业务,一定要通过银行官方微信平台、官方网站等可靠渠道进行申请。在网购平台办理退款、退货要通过官方App渠道。

建议将转账汇款到账时间设定为“2小时到账”或“24小时到账”,以预留处理时间。

不要与他人共享屏幕;不要听信陌生人的转账汇款请求;遇熟人借款等情形,尽量通过多种方式(如主动拨打电话等)确认对方是否为本人。

个人信息保护

个人信息是以电子或者其他方式记录的与已识别或者可识别的自然人有关的各种信息,不包括匿名化处理后的信息。

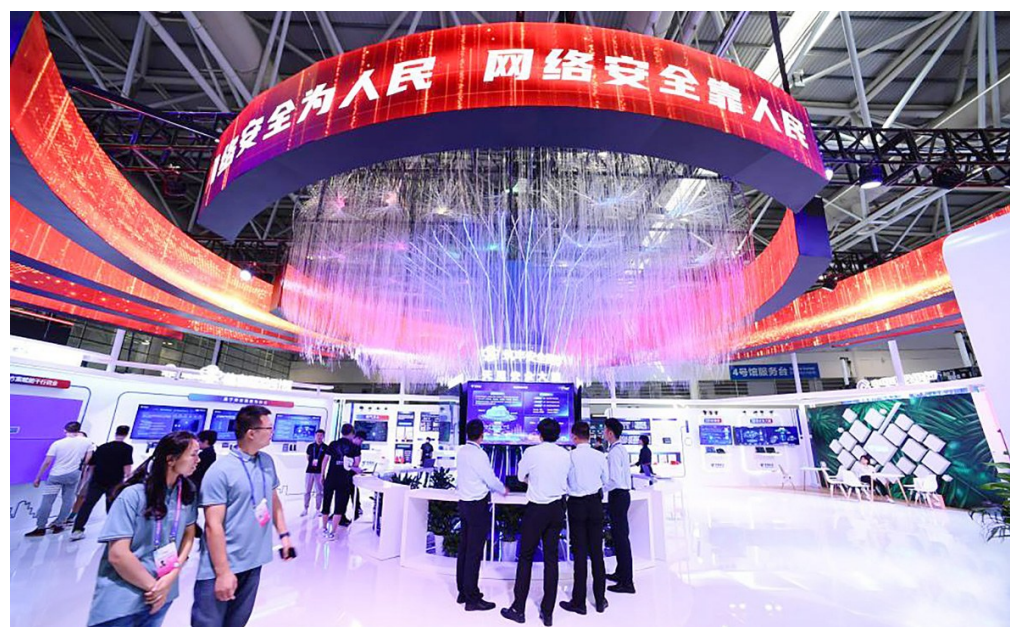
个人信息的处理包括个人信息的收集、存储、使用、加工、传输、提供、公开、删除等。

敏感个人信息是一旦泄露或者非法使用,容易导致自然人的人格尊严受到侵害或者人身、财产安全受到危害的个人信息,包括生物识别、宗教信仰、特定身份、医疗健康、金融账户、行踪轨迹等信息,以及不满十四周岁未成年人的个人信息。

泄露途径:非法披露、非法买卖、非故意泄露、攻击手机、攻击网站。

信息泄露危害:垃圾短信源源不断;骚扰、诈骗电话接二连三;垃圾邮件铺天盖地;大数据“杀熟”“人肉搜索”等恶意披露特定对象的个人信息事件。

防护建议:要优先选择尊重个人信息保护的产品、服务;要审核App要求的权限,并谨慎授权;要在身份证复印件上标注“仅限办理某业务时使用”;要对重要信息进行加密保护;要设置他人对自己所分享信息的访问权限。不要随意连接免费Wi-Fi热点;不要随意点击进入短信、邮件中的网站,提交个人敏感信息;不在网上晒车票、证件,以及含有孩子学校、家庭住址、个人收入情况的照片。



2023年国家网络安全宣传周网络安全博览会在福建省福州市举办。本次博览会展览面积约2万平方米,全国70余家单位、企业参加展览。图为9月10日拍摄的2023年国家网络安全宣传周网络安全博览会现场。(来源:新华社)

如何防范病毒或木马的攻击?

1. 为计算机安装杀毒软件,定期扫描系统、查杀病毒;

2. 及时更新病毒库、更新系统补丁;

3. 下载软件时尽量到官方网站或大型软件下载网站,在安装或打开来历不明的软件或文件前先杀毒;

4. 不随意打开不明网页链接,尤其是不良网站的链接,陌生人通过QQ给自己传链接时,尽量不要打开;

5. 使用网络通信工具时不随便接收陌生人的文件,若接收可取消“隐藏已知文件类型扩展名”功能来查看文件类型;

6. 对公共磁盘空间加强权限管理,定期查杀病毒;

7. 打开移动存储器前先用杀毒软件进行检查,可在移动存储器中建立名为autorun.inf的文件夹(可防U盘病毒启动);

8. 需要从互联网等公共网络上下载资料转入内网计算机时,用刻录光盘的方式实现转存;

9. 对计算机系统的各个账号要设置口令,及时删除或禁用过期账号;

10. 定期备份,当遭到病毒严重破坏后能迅速修复。

钓鱼邮件及防护建议

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,通过发送电子邮件的方式,诱使用户回复邮件、点击嵌入邮件正文的恶意链接或者打开邮件附件以植入木马或间谍程序,进而窃取用户敏感数据、个人银行账户和密码等信息,或者在设备上执行恶意代码实施进一步的网络攻击活动。

防护建议:要将公私邮箱分开,不要轻易泄露邮箱地址;要仔细辨认发件人地址,不要轻易点击陌生邮箱发来的邮件;多渠道核实来自熟人的转账汇款请求;提前安装杀毒软件,不轻易下载来历不明的邮件附件;要绑定邮箱账户和手机,便于必要时找回密码,接收“异地登录提醒”掌握状态。

网络安全和个人隐私防范措施

1. **使用强密码:**使用包含大小写字母、数字和特殊字符的强密码,并定期更改密码。同时,不要在多个网站或应用程序使用相同的密码,以免一个账户的泄露影响到其他账户。

2. **保持软件和操作系统更新:**安装所有可用的安全补丁和更新,以确保您的操作系统和软件保持最新的安全状态。及时更新软件和操作系统,安装最新的安全补丁,以防止黑客利用已知漏洞入侵系统。

3. **安装杀毒软件:**安装可信赖的杀毒软件,并定期更新病毒库以保护您的设备免受病毒和恶意软件的攻击。

4. **使用防火墙:**使用防火墙保护您的网络不受攻击。

5. **禁用远程桌面:**禁用远程桌面和远程访问,除非您确实需要这些功能。

6. **谨慎使用公共Wi-Fi:**避免使用公共Wi-Fi网络来处理敏感信息,如果必须使用,使用VPN保护数据传输安全。

7. **注意电子邮件附件:**不要打开未知发件人的电子邮件附件,即使您认识发件人,也要小心处理可能包含恶意软件的附件。

8. **定期备份:**定期备份重要数据,以便在遭受攻击或意外数据丢失时可以恢复数据。

9. **设置隐私选项:**设定文件隐私,不要所有内容公开。

10. **不要轻易相信陌生人:**在互联网上不要轻易相信陌生人,不要随便点击陌生人发送的链接,更不要向陌生人提供个人敏感信息。

11. **使用加密连接:**不要随意打开未知来源的链接,特别是电子邮件中的链接,因为它们可能是欺诈性的或包含恶意软件,使用HTTPS加密连接,在网络传输过程中保护数据不被窃听。

12. **注意公共Wi-Fi网络:**在使用公共Wi-Fi网络时,避免使用敏感账户或进行敏感操作,因为这些网络可能不够安全,使您的账户信息容易被盗。

13. **保护个人信息:**不要在社交媒体或其他公共场合发布过多的个人信息,例如家庭地址、生日等,以免被不法之徒利用。

14. **注意电子邮件的伪装:**不要相信您不认识的人或机构发来的电子邮件,特别是那些需要您提供个人信息或密码的邮件,因为它们可能是欺诈性的。