国家安全必修课 毕业季里的

当六月的蝉鸣遇上学位帽的流苏，又一批毕业生褪去青春的稚嫩，奔赴火热的职场，人生新篇正扬帆起航。走出校园，奔赴山海，面对前路的未知，请牢记以下三条国家安全秘籍，将国家安全意识深植心间，助力在新征程上披荆斩棘、行稳致远。

秘籍一：做好个人信息保护

一份履历丰富、内容详实的优秀简历是通往心仪岗位的敲门砖，但同时也会引起别有用心之人的关注。境外间谍情报机关可能会通过非法购买、投放虚假招聘信息、使用网络爬虫软件盗取等方式搜集掌握毕业生简历，并从中筛选“潜力股”，从而有针对性地进行拉拢策反。

提示：毕业生要认真做好个人信息保护，在编写投递简历时，要仔细辨别用人单位资质，注意不随意提供不必要的个人信息；不填写参加涉密科研项目或军工项目等履历、经历，以及亲友在涉密单位任职的相关信息，防止境外间谍情报机关通过上述信息锁定目标。

秘籍二：警惕特殊高薪诱惑

求职过程中，有的毕业生可能会收到一些来路不明的招聘信息，对方以信息咨询、市场调研、设备测试等为名，提供优厚的条件、较低的门槛，要求毕业生搜集涉密敏感信息，或是参加一些看似普通实则可能会泄露国家秘密的调研、咨询工作。而这些不正常的招聘背后，有可能是境外间谍情报机关利用个别毕业生涉世不深、急于求职等特点，以高额报酬物色发展部分学生为其搜集情报，危害我国家安全。

提示：各位毕业生在求职时要留心那些薪酬奇高、门槛极低的“特殊”岗位，防范境外间谍的“局中局”。对于一些境外企业，如其要求提供国内前沿科技研究成果、导师最新研究方向、行业基础数据等涉密敏感信息，毕业生应明确回绝并向国家安全机关进行举报，避免坠入违法犯罪的深渊。

秘籍三：留心异乎寻常的关心

过五关斩六将，毕业生终于收获了自己心仪的工作，有的毕业生可能步入党政机关、科研院所等核心涉密岗位开启新征程。然而，一些不明身份的人士突然“慕名而来”，对工作、生活情况表示高度的关心，并假借提供资源、机会的名义频繁联络，甚至送礼。这异于寻常的关心背后则可能是境外间谍情报机关企图利诱进而胁迫涉世未深的毕业生为其搜集窃取我涉密敏感信息的阴险图谋。

提示：各位毕业生要提高保密意识，不向他人炫耀、透露涉密单位以及涉密人员身份、职务等信息；不向他人透露工作秘密、内部敏感信息或国家秘密，谨防别有用心之人打着“交流近况”“加深感情”的旗号，刺探国家秘密。

毕业启程，亦是守护国家安全的新征程。愿每一位毕业生都能将国家安全意识融入血脉，自觉遵守国家安全法律法规，挺膺担当，护国安宁，为强国建设、民族复兴伟业贡献青春力量。

“刷脸”时代安全不容小觑

刷脸解锁、刷脸支付、刷脸进小区……当前人脸识别技术已被广泛应用于各种工作和生活场景，给人们生活带来诸多便利的同时，也极大提升了社会运行效率。然而，一些“强制刷脸”“无感抓拍”等不当使用乱象以及人脸识别数据滥用等安全风险也日益凸显，应当引起重视和警惕。

个别商家、机构违反个人信息必要原则，过度收集人脸识别数据，甚至通过强迫、捆绑方式收集人脸识别数据，明显超出正常使用需要，导致个人信息存在违法违规收集风险。

人脸图像包含丰富的信息，尤其是高精度图像可能包含虹膜、唇纹等相关信息。因此，非必要存储、传输人脸图像有较高安全风险。特别是如将人脸识别数据与个人身份等敏感个人信息关联存储，还可以关联个人行为和交往规律，重构特定目标的“关系网”，进而带来更大的安全风险。

随着人脸识别技术的广泛应用，部分个人信息处理者所持人脸信息呈指数式增长，因人脸信息等身份信息泄露导致“被贷款”“被诈骗”等问题时有发生。一些不法分子冒充用户身份进行刷脸支付以及网络贷款，导致受骗者财产损失；甚至还有一些不法分子将非法获取的人脸信息用于洗钱、涉黑等违法犯罪活动，导致用户被无辜卷入，给个人财产安全、公共安全甚至国家安全带来损失。

国家安全机关提示

人脸信息暗藏身份密码，非法使用触碰的是法律红线。人脸信息安全关系数据安全和广大人民群众切身利益，要构建全方位安全保障体系。

强化法治规范。我国《数据安全法》《网络安全法》《网络数据安全管理条例》等法律法规相继出台，为我国网络数据安全，以及包括人脸识别技术应用在内的网络应用提供了制度保障。《人脸识别技术应用安全管理办法》作为上述法律、行政法规的关键配套制度，明确了人脸识别技术的应用边界、使用规则，是对上位法中关于个人信息处理原则的具体细化落实，增强了法律法规的可操作性和执行力，有利于保障新技术合规应用，提升个人信息保护水平。

强化技术防范。建立严格的访问控制机制，定期对人脸识别系统进行安防检查，采用防火墙、入侵测试系统、入侵防御系统等网络安全设备，保护人脸识别系统免受网络攻击。数据采集要遵循最小必要原则，仅采集实现特定目的所必需的人脸数据，避免过度采集，采用先进的加密算法对采集到的人脸数据进行加密存储，且对不再需要的人脸数据及时清理和删除，降低数据泄露风险。

强化自我防范。个人应提高对人脸识别技术安全风险的防范意识，谨记“非必要不提供”原则，除了必要人脸认证之外，在授权使用面部识别前应确保其用途、范围以及信息保护措施，核准正规网络平台和软件，减少个人人脸信息泄露风险。如发现个人人脸信息被非法使用，应寻求法律帮助，维护自身合法权益。

“断舍离”不能把这些宝贝丢了

当下，“断舍离”正成为一门精致的生活哲学，即时舍弃不必要的物品和执念，用低成本的方式，拥抱高质量的生活。但是有些东西却不能随意处置，稍有不慎可能产生危害国家安全的风险。

垃圾桶内值“千金”

接群众举报，某单位门口的垃圾桶内有大量疑似涉密图纸资料。经查发现，该单位曾承担某重要涉密工程项目，在一次办公场所搬迁过程中，工作人员将项目图纸草稿误作废品清理，丢在了单位门口的垃圾桶内，造成了失泄密隐患。

回收站里现“珍品”

某市一废品回收站点，发现大量某单位涉密文件资料。经查，该单位在清理历史涉密文件时，没有及时送销，而是随意存放在储藏室内。清洁工在打扫储藏室时，将这批涉密文件资料误作一般图书资料出售给废品回收站，导致大量涉密信息被泄露。

旧书摊上有“秘密”

军迷张大爷在旧书摊上淘到4本军事书籍，回家翻阅时发现封面上赫然标注着“机密”“秘密”字样。经查，这些书籍原本属于某涉密单位，因未按规定销毁而被当做废品出售，造成国家秘密泄露。

国家安全机关提示

近年来，因未严格执行保密规定遗弃涉密载体等情况时有发生，不仅造成失泄密事件，还为境外间谍人员渗透窃密提供可乘之机。广大人民群众亟需引起重视，提高保密意识，共同筑牢国家安全防线。

知其意。涉密载体是指以文字、数据、符号、图形、图像、视频和音频等方式记载国家秘密信息的纸介质、光介质、磁介质、半导体介质等各类物品，是国家秘密的主要存在形式，也是境外间谍情报机关和反华敌对势力窃密活动的主要目标。

明其责。《中华人民共和国保守国家秘密法》明确国家秘密载体的制作、收发、传递、使用、复制、保存、维修和销毁的全生命周期管理应当符合保密规定；国家秘密载体应当按照国家有关保密规定配发或者装备，任何组织和个人不得私自买卖、转送；机关、单位应当按照国家有关保密规定和标准销毁国家秘密载体，任何组织和个人不得私自销毁。

行其道。国家秘密载体的保密管理应遵循严格管理、严密防范、确保安全、方便工作的原则；应当指定专门机构或人员负责国家秘密载体的日常管理工作，并接受监督检查。在涉密载体处置工作中，要认真执行涉密载体管理规定，严守国家秘密，织密安全防线。广大人民群众如发现相关可疑线索，可通过12339国家安全机关举报受理电话、网络举报平台（www.12339.gov.cn）、国家安全部微信公众号举报受理渠道或直接向当地国家安全机关进行举报。

（均转自国家安全部微信公号）

责任编辑/王睿卿 E-mail:fzbfyzk@126.com