网络安全工作简报

2019 年第 1 期

青岛科技大学网信办编 **2019 年 12 月 10 日**

当网络空间成为国家继陆、海、空、天之后的第五疆域，保障网络空间安全就是保障国家主权，保障学校安全，保障师生权利。我校在网络安全与信息化工作领导小组的指挥下，不断完善网络安全保障体系，提升全校师生在网络空间的获得感、幸福感、安全感。但没有攻不破的网络，没有绝对的网络安全，网络安全工作任重道远。

1. 安全动态

1.1. 工信部新规实施：12 月 1 日起办卡需“人脸识别”

根据工信部的相关规定，自 2019 年 12 月 1 日起，电信企业需在实体渠道全面实施人像比对技术措施，人像比对一致方可办理入网手续。

其实早在四年前，为了制止网络不法行为，工信部就曾规定电信企业在销售手机卡时需要查证用户本人身份证件，并当场进行验证。不过，人为检测的“人证比对”并不高效，且精确度不足。

规定还展开了对二次倒卖电话卡的深入治理。要求各电信企业完善电信服务协议条款，明确用户不得二次转售、倒卖电话卡，并充分运用海报、广告、短信等多种方式积极开展宣传提醒，引导用户至正规营业场所购买电话卡。

工信部还在规定中要求，电信企业需通过自有营业厅向用户提供查询名下手机号码的服务，积极防范用户名下不知情办卡，对用户提出存在异议的手机号码应立即组织核查和处理，切实维护群众合法权益。可以想见的是，在手机号码登记之外，人脸识别会越来越成为身份认证不可或缺的一部分。（来源：新浪科技）

1.2. 教育部：专项治理高等院校服务类教育 APP

11 月 26 日消息，近日，教育部网络安全和信息化领导小组办公室关于印发《高等院校管理服务类教育移动互联网应用专项治理行动方案》（下简称《方

案》）的通知。

《方案》指出，加强教育移动应用的统筹协调。各高等院校应加强对教育移动应用的统筹管理，明确本单位的职能部门，与小程序和企业号等其它移动互联网平台统一纳入本单位教育信息化工作予以管理。

《方案》要求，各高等院校应严格控制本单位管理服务类教育移动应用的数量，原则上面向公众提供服务的整合成一个应用；面向教职工提供管理服务的整合成一个应用；面向学生提供办事服务的整合成一个应用。各高等院校应建立“一数一源”的数据共享制度，所有教育移动应用使用个人基本信息应从基础数据库中共享，不得向用户重复采集个人基本信息。

《方案》表示，专项行动分为自查、重点抽查和总结提升等三个阶段。

一、自查阶段（2019 年 12 月 31 日完成）。各高等院校应按照工作任务，逐条对照、排查现存在的问题。

二、重点抽查阶段（2020 年 1 月 31 日前完成）。教育部将根据安全监测和投诉举报发现的问题线索建立问题台账，开展重点检查，针对问题较为严重或整改不力的学校将进行约谈、通报。

三、总结提升阶段（2020 年 3 月 31 日前完成）。各省级教育行政部门和部属高校应及时总结并发掘在教育移动应用治理工作中的典型经验和创新做法，形成 1-2 个可复制、可推广的案例。（来源：搜狐网）

1.3. 三部门联合发布《网络音视频信息服务管理规定》

近日，国家网信办、文化和旅游部、国家广播电视总局联合发布了《网络音视频信息服务管理规定》，自 2020 年 1 月 1 日起正式施行。此次规范的网络音视频信息服务，主要包括网络音频、网络直播、短视频、网络影视剧等所有形式的网络音视频制作、发布、传播等。此外，该规定针对网络音视频信息服务还提出了七点明确要求：资质要求、信息内容安全管理主体责任要求、实名制认证要求、信息安全要求、处罚机制、举报路径、辟谣机制，为网络音视频良性传播提供保障，也为信息安全规范加上了一把安全锁。（来源：网信办）

1.4. 2019 党政机关与关键信息基础设施云服务安全论坛在京举行

12 月 6 日，2019 党政机关与关键信息基础设施云服务安全论坛在北京举

行。本次论坛的主题是宣贯《云计算服务安全评估办法》，推动云计算服务安全评估工作。今年 7 月，国家互联网信息办公室、国家发展和改革委员会、工业和信息化部、财政部联合发布《云计算服务安全评估办法》，建立了云计算服务安全评估工作协调机制，组织对面向党政机关、关键信息基础设施提供服务的云平台开展安全评估。协调机制办公室设在国家互联网信息办公室网络安全协调局。中国网络安全审查技术与认证中心作为支撑单位，承担了云服务安全评估有关具体工作。

通过举办本次论坛，有效提升了参会人员对云服务安全评估工作的认识和了解，推动了相关党政部门、关键信息基础设施运营者、云服务商、专业技术机构之间的交流，对《云计算服务安全评估办法》的落实及安全云服务的采购使用起到了促进作用。（来源：中国市场监管报）

2. 工作专题

2.1. 重大活动期间网络安全保障工作

在全国两会、海军节、跨国公司领导人青岛峰会、中华人民共和国成立 70 周年重大活动期间，我校按照统一指挥、分工负责、协同作战的原则，在网络安全与信息化工作领导小组的领导下，进一步增强网络安全监测预警、应急处置等工作能力，实行 7*24 小时值班制度，制定网络安全保障方案及值班安排和重大活动期间网络安全保障预案，预防和减少重大网络安全事件造成的损失和影响，全面提高应对重大网络安全事件的能力和水平，切实保障重大活动期间网络安全稳定。

2.2. 网络安全宣传周活动

9 月 16 日，2019 年国家网络安全宣传周在我校拉开帷幕。习近平总书记作出重要指示强调，国家网络安全工作要坚持网络安全为人民、网络安全靠人民，保障个人信息安全，维护公民在网络空间的合法权益。我校深入贯彻落实习近平总书记关于网络强国的重要思想，围绕中华人民共和国成立 70 周年，结合 “网络安全为人民，网络安全靠人民”的主题，贯彻落实《网络安全法》以及数据安全管理、个人信息保护等方面的法律、法规、标准，在崂山校区举办一

系列宣传活动，通过知识讲座、网络安全展览、专题网站、教育视频等方式，多形式、多渠道的向师生普及网络安全、数据安全、个人信息保护等方面的法律、法规，提高师生网络安全意识，注重个人信息保护，共同维护和营造网络安全环境，让网络安全不仅走入校园，更走进每位师生心中。

2.3. 网络安全教育和培训工作

网络安全教育和培训工作包含了对“网络安全观”的宣传教育，通过安全专栏（https://nic.qust.edu.cn/aqzl.htm）宣传《习近平：在网络安全和信息化工作座谈会上的讲话》、《中华人民共和国网络安全法》等法律法规及国家政策，学习《网络安全大型专题片<第五空间>》、《安全宣传周系列动漫》等教育视频和科普动漫，了解漏洞信息、漏洞预警等，从而落实“依法加强网络空间治理，加强网络内容建设，做强网上正面宣传，培育积极健康、向上向善的网络文化”。

网络安全教育和培训工作包含了对学生安全知识技能的指导和教育，“2019高校网络信息安全管理运维挑战赛”中我校由网信办徐金云老师领队，徐树洋、闫卓、朱海港三名同学组成的参赛队，最终取得综合成绩全国第 15 名、华东区第 5 名的好成绩，展现了过硬的网络理论知识储备和良好的心理素质、技战素养。

网络安全教育和培训工作包含了对信息安全管理员队伍建设，学校近两年选派关键岗位技术人员，参加网络安全基础培训，提升网络安全专业技能，5 人次获得 CISP 认证、2 人次获得 CIIPT-A 认证、1 人次通过信息安全工程师认证。除此之外，学校组织 8 位队员参加“2019 年全国信息安全管理员知识与技能竞赛活动”，通过本次竞赛，队员们充实了自我，对信息安全有了更深层的认识。

2.4. 网站信息泄露专项检查整改工作

“即知即改、立改立效”为校园网络安全保驾护航，11 月网信办根据上级通报的信息泄露安全事件予以及时通报处置，并对网站群内 144 个网站进行信息泄露专项检查工作，共检查出含有身份证号、银行卡号、手机号等敏感信息的文档共计 153 项，涉及学校二级单位 14 个。通过协同办公系统，及时将检查

整改事项通知到相关单位，监督整改进度，并对整改结果进行全面复查，使学校网站内容信息泄露安全隐患得到有效抑制，切实保障用户个人信息安全。

2.5. 网络安全日常运维工作

要安全可控，必须打好地基，在自家的地基上起高楼，为此我校推动资产识别、基线检查、病毒查杀、边界防护、入侵防范、数据保护、追踪溯源等，保障校园网络安全，更好的服务校内师生。

2.5.1. 落实网络安全等级保护工作

为了贯彻落实《网络安全法》和《教育部办公厅关于开展信息系统安全等级保护工作的通知》，学校制定了《信息化项目建设管理办法》，从制度上规范信息系统建设，明确要求新建设信息系统必须落实网络安全等级保护测评工作。截止到 2019 年 11 月底，我校已通过网络安全等级保护测评的信息系统共 15 个，原有信息系统将按学校规划逐步升级更新。

2.5.2. 厘清学校网络信息资产

全面开展资产清查，摸清家底管好家当，网信办利用技术手段通过 IP 地址安排专人分别清查，进行全面盘点、核对、查实，服务器 IP 段内的一个也不放过，全部落实归属系统及责任人。经过两轮的清查，确认学校信息系统服务器数目，并清理僵尸服务器。

2.5.3. 构建网站安全发布管理体系

为了保障用户隐私安全及校内资源安全，为了提高用户的访问体验，网信办利用 Web 资源发布系统构建了安全可信的网站发布、运维及管理体系。截止到 2019 年 11 月底，全校 188 个网站已全部通过 Web 资源发布系统实现了 IPv4/IPv6 双栈发布；提供公网访问的资源（包括校主页在内的网站和业务系统），基本实现了 HTTPS 安全加密访问与密文传输；情况细化访问控制策略，保障了用户的正常访问的同时确保资源安全；利用 Web 资源发布系统实现负载均衡，提升选课体验。

2.5.4. 建设网络安全管理体系

在网络安全与信息化工作领导小组的带领下，网信办协同相关部门陆续发布《网络与信息安全管理细则》、《机房安全管理办法》等安全相关规则制度，

制定《网络安全事件应急响应综合预案》、《重大活动期间网络安全保障预案》、《数据备份与恢复管理制度》，以及重要应用系统专项应急预案共计 12 项，重点岗位工作人员以及第三方人员全部签署保密协议，逐步落实网络安全管理体系。

2.5.5. 加强漏洞和风险管理工作

网信办每年对所有服务器进行两次漏洞扫描和基线检查工作，识别安全漏洞和隐患，对发现的安全漏洞和隐患及时进行修补或评估可能的影响后进行修补。截止到 2019 年 11 月底，已完成对 30 个关键信息系统的渗透测试，漏洞扫描和基线检查工作，完成“Windows 远程桌面服务远程代码执行漏洞”、“跨站脚本漏洞”、“任意文件上传绕过漏洞”、“验证码功能缺陷漏洞”等漏洞的修复工作。

3. 普及专栏

网络购物安全小贴士

预售骗局

活动期间，优惠短信较多，不法分子以“预购”“限时购”“预先降价”等为诱饵，通过即时通讯软件或手机短信发送包含木马病毒的链接。

需警惕：凡是短信中有优惠券或者红包链接的都不要点！因为链接中很可能含有木马病毒，能“秒”盗客户信息和账户资金。

伪“红包”骗局

活动期间，有很多人在微信朋友圈中分享红包，但并不能直接领取，而是要先关注并分享，或转发一定数额的好友或群。

需警惕：需要提供个人信息的、拆红包要求输密码的都不可相信。高额红包也要提高警惕，还要谨防低价拼团陷阱，比如“低价拼团”可能只是为了获取用户隐私信息，甚至有的虚假拼团链接可能带有木马病毒。

假“客服”骗局

活动期间网购订单较多，网银交易很可能出现迟缓的情况。一些不法分子便冒充客服，假借“所购商品出现了卡单、调单或交易失败等情况，若逾期处理，账户资金将被冻结”等理由，要求到银行 ATM 机前操作退款。

需警惕：此类信息容易使人信以为真，但网友们一定要通过电商平台官方热线或客服咨询，多方核实后再行处理，切勿轻信不明短信或电话。

“信用提额”骗局

活动期间，有消费者因现阶段资金无法支撑其购买力，想提升花呗或信用卡额度。不法分子通常会冒充花呗或银行客服，谎称可以提升信用额度，继而以支付“服务费”为由，诱导网友扫其二维码支付，从而实施诈骗。

需警惕：提高透支额度要经过严格审核、提供相关证明，并且不会额外收取费用。切勿轻信网络上关于提高花呗、信用卡等透支额度的信息。

“刷单返利”骗局

不法分子冒充电商，以在活动前提高店铺销量、信誉度、好评度为由，称需要雇人兼职刷单刷信誉。

需警惕：不法分子为了骗取信任，开始会在约定时间连本带利返还，待网友刷的金额越来越大，不法分子将以各种借口拒绝返款，甚至诱导网友继续刷单。这是典型的“刷单返现”骗局，师生一定不要轻易尝试，寻找兼职要通过正规渠道进行，需要交纳定金或先行支付的工作，务必要谨慎对待。

“中奖免单”骗局

在活动期间有不法分子冒充网店客服，声称回馈客户有“中奖免单”活动。

需警惕：活动期间，各种抽奖、免单活动较多，消费者收到这类信息后一定要仔细甄别，详细了解活动规则，跟正规客服求证，不轻易汇款、转账。遇到“账户异常”“缴纳保证金”等情况要谨慎，小心上当。

退款骗局

不法分子以商品有瑕疵、订单失效等各种事由，要求给买家办理退款或赔偿金，使用木马链接或开通买家各种不熟悉功能实施转账，以此诈骗。

需警惕：在得知网购退款、包裹丢失后应当第一时间与平台卖家咨询、核实，切不可在第三方网上平台操作。

小贴士

- 在结算支付时尽量使用第三方支付平台。第三方支付平台有冻结货款的权

利，如果消费者收货后发现有问题，可以申请立即冻结货款。

- 在活动期间各种抽奖、免单活动较多，消费者收到这类信息后一定要仔细甄别，详细了解活动规则，跟正规客服求证，不轻易汇款、转账。遇到“账户异常”“缴纳保证金”等情况要谨慎，小心上当。
- 保留网上购物凭证。一旦产生纠纷，消费者要注意保留聊天记录，妥善保管订货单、发货凭证、发票等购物凭证。
- 经常更新账号和密码，发现被骗后及时报警，并拨打消费者投诉举报专线12315 维权。