共筑网络安全防线 护航高质量发展新鞍钢

如今，人们的生活越来越离不开互联网，网络安全重要性日益凸显。2022年第九届国家网络安全宣传周将于9月5日至11日举办，主题为“网络安全为人民，网络安全靠人民”。

鞍钢集团深入学习贯彻习近平总书记关于网络强国战略、国家大数据战略和发展数字经济的重要论述，全面落实党中央、国务院决策部署，在集团范围内开展网络安全宣传活动。

本版今日刊发工作生活中常见的网络安全要点，希望全体职工提高警惕，注意防范。

职工网络安全保护基本要求

（一）账户口令管理

个人办公终端及业务系统必须设置登录口令，要求口令长度8位以上，并由大小写字母、数字、特殊字符三种以上混合构成，避免任何弱口令登录形式。办公桌上禁止粘贴账户密码，废弃纸质文档资料及时销毁。

（二）远程控制管理

所有终端关闭远程端口，禁用远程控制功能。确有开启需求的，必须有专人负责，监视使用，使用结束后立刻关闭。

（三）互联网权限管理

本着“谁上网，谁负责；谁审批，谁负责”的原则，计算机连接互联网必须有主管领导审批，连接互联网的计算机必须有专人负责，严禁单台计算机同时连接内外网。

（四）电子邮件安全

在收发电子邮件前，务必确认防病毒软件实时监控功能已开启；不打开可疑邮件、垃圾邮件、不明来源邮件等提供的附件或网址。

（五）办公环境安全

应加强对外来人员进出办公区域的管控，严禁外来人员接触办公终端，严禁外来人员电脑设备私自接入公司网络，外来访客必须有工作人员随时陪同。

（六）设备安全

不使用来历不明的移动存储设备，严禁私搭无线网络，操作人员离开办公电脑时，应将电脑置于注销或锁屏状态。下班后应将电脑关机并断电，不得使电脑长期处于无人操作自运行状态。

（七）防病毒安全

办公终端必须安装亚信防病毒软件，并保持病毒库最新。打开系统防火墙，关闭移动存储自启动功能，更新操作系统补丁至最新版本。

（八）业务系统安全

各单位定期组织排查梳理业务管辖范围内的信息系统，对于开放在互联网上的管理后台、开放在互联网上的测试系统、无人维护的僵尸系统、拟下线未下线的系统、疏漏的未纳入防护范围的互联网开放系统，应及时加强防护措施，如非必要，建议关停。

组织对在用信息系统的账号权限进行梳理，严格限定各系统管理员的账号授权，删除僵尸账号及测试账号。

加强对在用信息系统的运维单位进行检查和要求，严格杜绝使用互联网远程控制或VPN连接方式进行系统运维工作，确有必要的，必须有专人负责，监视使用，使用结束后立刻关闭。

（九）社会工程学安全

不在外部网站或社交平台上谈论本次专项工作；不在外部网站使用与工作网站相同的账号密码；不在私人手机、电脑、Pad上记录工作网站账号密码；严格禁止个人手机接入内部网络；不使用个人终端存放、处理工作信息，不使用办公终端处理个人信息。

规避漏洞攻击

漏洞是指信息系统的软件、硬件或通信协议中存在的设计、实现或配置缺陷，从而可使攻击者在未授权的情况下访问或破坏系统，导致信息系统面临安全风险。

防范建议：

1. 关注软件漏洞安全提醒，及时排查隐患。
2. 提示补丁修复，千万别嫌麻烦。操作系统、浏览器和其他应用软件，都要及时打补丁。
3. 关闭无用服务，卸载没用软件。减少暴露途径，提高安全基线。
4. 禁用危险端口，系统安全改善。开启防火墙，设置规则，禁止对危险端口的访问。

防范恶意软件

恶意软件指可以中断用户的计算机、手机、平板电脑或其他设备的正常运行或对其造成危害的软件。

恶意软件主要包括：

1. 病毒：通过感染计算机文件进行传播，以破坏或篡改用户数据，影响信息系统正常运行为主要目的。
2. 蠕虫：能自我复制和广泛传播，以占用系统和网络资源为主要目的。
3. 木马：以盗取用户个人信息，甚至是远程控制用户计算机为主要目的，如盗号木马、网银木马等。
4. 逻辑炸弹：当计算机系统运行的过程中恰好某个条件得到满足，就触发执行并产生异常甚至灾难性后果。
5. 后门：绕过安全性控制而获取对程序或系统访问权的方法。
6. 勒索软件：以锁屏、加密用户文件为条件向用户勒索钱财。用户数据资产包括文档、邮件、数据库、源代码、图片、压缩文件等。

防范建议：

1. 要安装防火墙和防病毒软件，并及时更新病毒特征库。
2. 要从官方市场下载正版软件，及时给操作系统和其他软件打补丁。
3. 要为计算机系统账号设置密码，及时删除或禁用过期账号。
4. 要在打开任何移动存储器前用杀毒软件进行检查。
5. 要定期备份电脑、手机的系统和数据，留意异常告警，及时修复恢复。
6. 不要打开来历不明的网页、邮箱链接或短信中的短链接。
7. 不要执行未经杀毒扫描的下载软件。
8. 不要打开QQ等聊天工具上收到的不明文件。
9. 不要轻信浏览网页时弹出的“支付风险、垃圾、漏洞”等提示。

线上工作学习风险防范

防范建议：

1. 评估供应方的安全能力，选用合适的用户平台。
2. 谨慎保管登录凭证，设置较为复杂的密码。
3. 设备应配备防火墙、防病毒软件，提高工作设备的安全性。
4. 企业聊天、电子邮件或应用程序需进行加密保护。
5. 如有条件，可以请可信任的第三方对办公系统的安全性进行测试和评估，保障移动设备及移动设备中应用程序的安全性。
6. 提高自身的网络安全意识，使用工作专用设备，将个人数据与工作数据进行严格区分。
7. 移动设备应及时进行系统更新，修补系统漏洞以降低安全风险。

鉴别钓鱼邮件

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，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等的一种网络攻击活动。

种类包括：

广撒网式钓鱼：群发垃圾邮件钓鱼。

鱼叉式网络钓鱼：是指黑客研究目标用户，了解用户的喜好和日常运作，通过特殊定制的邮件来窃取敏感数据和安装恶意软件。

钓鲸邮件：专门针对企业高管发送的精准钓鱼邮件，又称为“CEO欺诈”。

防范建议：

1. 看发件地址，非预期不理。留心利用拼写错误假冒发件人地址或私人邮箱，号称官方邮件等。
2. 看邮件标题，警惕诈骗字眼。典型的钓鱼邮件标题常包含但不限于“账单、邮件投递失败、包裹投递、执法、扫描文档”等，重大灾害、疾病等热点事件常被用于借机传播。
3. 看正文内容，辨明语法错误。忽略泛泛问候的邮件，警惕指名道姓的邮件；诈骗相关的热门正文关键字包括“发票、支付、重要更新”等；包含官方LOGO图片不等于就是真邮件。
4. 看正文目的，保持镇定从容。当心索要登录密码、转账汇款等请求，通过内部电话等其他可信渠道进行核实。对通过“紧急、失效、重要”等词语制造紧急气氛的邮件谨慎辨别，不要忙中犯错。
5. 看链接网址，注意鼠标悬停。鼠标悬停在邮件所含链接的上方，观看邮件阅读程序下方显示的地址与声称的地址是否一致。
6. 看内嵌附件，当心木马易容。恶意电子邮件会采取通过超长文件名隐藏附件真实类型，用迷惑性附件名称诱使用户下载带毒邮件。在下载邮件附件之前，应仔细检查附件文件名和格式，不要因好奇而下载可疑附件。打开前用杀毒软件进行扫描。

警惕网络电信诈骗

网络电信诈骗通常指通过网络、电话、短信等途径，利用虚构事实或者隐瞒真相等手法，骗取他人财物的手段。

种类包括：

信任类诈骗：通过冒充亲友、领导、客服、医保社保、通信运营企业、助学机构等，通过伪造各类图片公文等方式抓眼球，欺骗性很强。

同情类诈骗：伪造车祸、突发疾病等突发事件，假装心急如焚，诱骗受害人转账；虚构寻人、扶困帖予以“爱心传递”方式发布在朋友圈，实施电话吸费或电信诈骗。

威胁类诈骗：假冒公检法办案、黑社会敲诈，虚构包裹涉毒、受害人涉案、医保卡涉嫌违禁药品等场景。

贪婪类诈骗：微信传销、AA红包、天天分红、中奖、购车补贴、刷单刷钻等，利用微信等现代工具在亲友间传播，谎称低投入、高回报，诱惑力比较强。

情感类诈骗：伪装成高富帅、白富美、颜值担当主播等，添加好友骗取感情和信任后，以资金紧张、家人有难、冲业绩等理由骗钱。

防范建议：

1. 凡是打着类似资产解冻旗号进行敛财的、让你交钱的，不管钱多钱少，都是诈骗。
2. 凡是自称党中央、国务院领导干部，通过电话、微信、电子邮件、QQ等方式进行所谓的“委托”“授权”“任命”的，均是诈骗。
3. 凡是声称缴纳数十元、上百元会费就能获利数万元、数十万元甚至数百万元的各类APP、项目，均是诈骗。
4. 要选择信誉良好的网站购物，将官方网站加入收藏夹备用，以免因为输入错误网址而误入钓鱼网站。
5. 不要在网上购买非正当产品，如手机监听器、毕业证书、考题答案等。
6. 不要轻信以各种名义要求你先付款的信息，不要轻易把自己的银行卡借给他人。
7. 不要轻信任何号码发来的涉及银行转账及个人财产的短信，不向任何陌生账号转账。

注意个人信息保护

个人信息包括但不限于姓名、出生日期、身份证号码、个人生物识别信息、住址、电话号码等。个人敏感信息一旦遭到泄露、非法提供或滥用，可能危害人身和财产安全，极易导致个人名誉、身心健康受到损害或遭遇歧视性待遇等。

易造成个人信息泄露的行为：

1. 随手乱丢快递单，泄露姓名、电话号码、工作地点或住址。
2. 星座、性格测试，泄漏姓名、出生年月。
3. 分享送流量，不法分子能确认手机号是否有效。
4. 抢红包输入个人信息，泄露姓名、手机号。
5. 在社交媒体上分享旅行信息，家中没人可能引来窃贼。
6. 晒图，照片原数据中包含GPS位置信息。
7. 允许陌生人查看社交网络个人档案、陌生人查看朋友圈图片，泄露生日、爱好、电话号码等信息。
8. 机构数据泄露，账户信息泄露。
9. 远程办公系统的企业通信录、健康情况汇总、活动轨迹填报等功能，可能收集、存储用户的个人信息，如姓名、电话、位置信息、身份证件号码、生物特征识别数据等，存在被滥采、滥用和泄露的风险。

防范建议：

1. 要利用社交网站的安全与隐私设置保护敏感信息。
2. 要在安全级别较高的物理或逻辑区域内处理个人敏感信息。
3. 要加密保存个人敏感信息，个人敏感信息需带出时要防止被盗、丢失。
4. 要仔细阅读用户许可，只授权将个人信息转移给合法的接收。
5. 要注意保存或及时销毁存有个人信息的纸质资料、快递单，废弃的光盘、U盘、电脑、手机等。
6. 不要在微博、朋友圈等社交媒体随意晒出个人敏感信息。

识别钓鱼WI-FI

攻击者利用人们节省流量费的心理，架设假冒的免费WiFi热点，或者发送断连信号给受害人计算机，强制使其下线，然后将其吸引到同名恶意热点上，对受害人进行窃取数据、注入恶意软件、下载有害内容等侵害。

防范建议：

1. 仔细辨认真伪：向公共场合Wi-Fi提供方确认热点名称和密码；无须密码就可以访问的Wi-Fi风险较高，尽量不要使用。
2. 避免敏感业务：不要使用公共Wi-Fi进行购物、网上银行转账等操作，避免登录账户和输入个人敏感信息。如果要求安全性高，有条件的话可以使用VPN服务。
3. 关闭Wi-Fi自动连接：黑客会建立同名的假冒热点，利用距离近信号强等优势成为直接入点的“邪恶双胞胎”。一旦手机自动连接上去，就会造成信息的泄露。
4. 加固家用Wi-Fi：为Wi-Fi路由器设置强口令以及开启WPA2是最有效的Wi-Fi安全设置。
5. 运行完全扫描：安装安全软件，进行Wi-Fi环境等安全扫描，降低安全威胁。

（鞍钢集团管理与信息化部供稿）