

# 校园个人终端安全小贴士

图书信息中心 龚一轩

## 一、网络安全实名制

学校校园网仅限于学校师生使用的计算机接入，所有要求接入学校校园网的网络终端设备都要遵守《上海科技大学校园网实名登记制度及网管理办法》的相关规定，进行实名制登记。

## 二、防范病毒或木马的攻击

1、不随意下载、打开未经检测和来历不明文件，接收可能携带有病毒、木马、恶意插件等的文件时，打开之前要使用杀毒软件进行扫描查杀；

2、不随意访问可能存在钓鱼、仿冒信息的不明网站，不访问带有色情、赌博等不良信息的非法网站等；使用网络通信工具（如QQ、微信等）时不随便接收陌生人的文件，若必须接收的，可取消“隐藏已知文件类型扩展名”功能来查看文件类型；

3、不在公共和私人电脑处理、存储和传输涉密信息；不在网络聊天、论坛和电子邮件中轻易泄露姓名、家庭住址、电话号码和银行账户等个人隐私信息；长时间离开计算机时，应关闭计算机或退出用户桌面；

4、科学的使用密码：a、尽量做到不同的系统和资源使用不同的密码；b、各类应用系统首次登录时应立即修改账号密码；c、设置开机密码、屏保密码等多重密码，保证密码的长度和复杂度，避免使用与个人相关数据和一些常用的单词当做密码；d、定期修改密码；e、妥善保管所掌握的各类办公账号和密码，不随意向他人泄露、借用自己的账号密码；f、密码在系统中保存或传输时，采取安全措施以保证账号的安全性，例如对口令进行加密等；

5、避免使用来历不明的U盘等移动存储设备进行文件拷贝和传输，确需使用时，应先进行病毒查杀；根据数据的重要性，定期将文件通过刻录成光盘、或拷贝到专门移动存储设备上，重要文件定时、异地备份；

7、安装和使用正版软件和操作系统；

8、安装并定期升级、更新杀毒软件，定期进行病毒查杀；定期更新系统补丁，紧急补丁及时更新；

9、使用安全软件定期清理恶意插件和垃圾文件；

10、避免终端设备上的文件夹一直处于“共享”状态，如确需共享时，必须设置密码，或设定用户权限，以限制用户访问，使用完毕后应立即取消共享状态；

11、不使用互联网（电话、传真、未安装加密设备的电脑网络）传递敏感信息资料特别是学校科研成果信息；

12、接入校园网后，不擅自使用调制解调器（Modem）、ADSL、无线上网卡等设备将个人终端设备与外部网络连接，不私自安装非规定的网络协议；

13、远程接入校园网的，应使用学校提供的VPN网关安全措施；

14、禁止运行与工作无关占用大量带宽的应用程序，如网络视频/音频点播、大量文件的下载等。

15、不在个人终端设备中，私自设立WWW、FTP、BBS、NEWS、文件或打印共享等互联网服务。

## 三、防范QQ、微信、微博等社交平台账号被盗

1、账户和密码尽量不要相同，定期修改密码，增加密码的复杂度，不要直接用生日、电话号码、证件号码等有关个人信息的数字作为密码；

2、密码尽量由大小写字母、数字和其他字符混合组成，适当增加密码的长度并经常更换；

3、不同用途的网络应用，应该设置不同的用户名和密码；

4、在网吧使用电脑重启机器，警惕输入账号密码时被人偷看；为防账号被侦听，可先输入部分账号名、部分密码，然后再输入剩下的账号名、密码；

5、涉及网络交易时，要注意通过电话与交易对象本人确认。

## 四、安全使用电子邮件

1、不要随意点击不明邮件中的链接、图片和文件；

2、使用邮箱地址作为网站注册的用户名时，应设置与原邮箱登录密码不相同的网站密码；尽量不使用学校提供的电子邮箱帐号等在互联网上进行注册；

3、当收到与个人信息和金钱相关（如中奖、集资等）的邮件时要提高警惕。

4、不制造及转寄垃圾邮件，以及发放含有粗俗、暴力、色情成份的邮件；

5、使用学校电子邮件传递敏感数据时，对数据进行加密等。

## 五、防范钓鱼网站

1、可以通过查询网站备案信息等方式核实网站资质的真伪；

2、安装安全防护软件；

3、要警惕中奖、修改网银密码的通知邮件、短信，不要轻易点击未经核实的陌生链接；

4、不要在网吧、宾馆等公共电脑上登录个人账户或进行金融业务等。

## 六、防范社交网站信息泄露

1、利用社交网站的安全与隐私设置保护敏感信息；

2、不要轻易点击未经核实的链接；

3、在社交网站谨慎发布个人信息；

4、根据自己对网站的需求进行注册。

## 七、如何防范网络虚假、有害信息

1、及时举报类似谣言信息；

2、不造谣，不信谣，不传谣；

3、要注意辨别信息的来源和可靠度，要通过经第三方可信网站认证的网站获取信息；

4、要注意打着“发财致富”“普及科学”，传授“新技术”等幌子的信息等。

# 集慧

设备与资产处编  
2019年1月8日  
facility@shanghaitech.edu.cn

主编：姚劲松  
责任编辑：李瑞青  
编辑：刘丹 金文虎  
厉莉 陈文琦

2018年第五期 总第20期

## 2018年政府采购、入库、试剂耗材采购情况

一、截至2018年12月底，学校全年合计完成政府采购5.9亿元，具体情况如下：

1、设备采购4.27亿元，其中集中采购5955万元，分散招标3.34亿元，询价3321万元。另外，进口论证4.4亿元；签定490份进口合同并报免税。

2、家具采购1781万元，其中集中采购246万元，分散招标1535万元。

3、耗材集中采购95万元。

4、工程采购3865万元，均为分散招标采购。

5、服务采购6736万元，其中集中采购4978万元，分散招标1758万元。

6、活细胞结构与功能成像等线站工程项目采购3021万元，均为分散招标采购。

二、新增入库设备和配件共计7275台件（包括6846台设备资产，423件配件，6台件在建设备），比上年（5808台件）增加25%，新增设备总值4.60亿元，比上年（3.5亿元）增加32%。

三、新增入库64套软件无形资产，总金额313万元，校内备案登记许可软件5套，总金额109万元。

四、E-supply平台试剂耗材等采购，截至2018年底共有193个课题组/平台的880个账号在E-supply系统采购试剂耗材等，各类订单56475条，同比增加36%，总金额6922万元，同比增加16%。

（统计数据由金文虎、刘丹、厉莉、陈文琦提供）

## 实验室安全论坛之“个人防护”讲座

12月11日，来自3M公司上海研发中心的两位专业人员为上科大的师生带来一场活泼生动的“个人防护”讲座。讲座从个人防护的必要性讲起，列举了国外高校和企业的一些做法，进而对实验室比较常见的危害因素和个人防护措施进行了逐一阐述，主要包括眼面防护、呼吸防护、听力防护、手部防护等。针对个人防护用品的选择、使用和维护等大家关心较多的问题，3M的两位老师也分别进行了细致的讲解，并带来诸多产品用于展示和实践。

讲座现场设置了“安防E学院”在线学习的环节，完成答

题后大家获得了安全眼镜、口罩、耳塞等小礼品。对于没能来现场聆听讲座的小伙伴们也可以扫以下二维码进入“安防E学院”，完成测试后可取得电子证书。后台会统计大家的学习情况，每月还有奖品抽取。另外，我处将培训有关的视频、学习资料等已存放在“实验室安全”的校内FTP上，欢迎大家自行获取和学习：<ftp://10.15.44.153/>。

讲座获得了到场师生的一致好评。我处今后将继续为大家带来实验室安全方面的讲座，欢迎广大师生参加。

（张梅玲报道）

