身边电磁辐射有多少

我们的身边有哪些有害辐射？我们使用的电器安全吗？

厨房电器辐射，电磁灶最大，微波炉第二

调查显示：电磁灶工作时的辐射竟然达到了400毫高斯（电磁波安全标准使用术语），是各种电器中辐射最大的，走到电磁灶两米以外，电磁辐射才降到2毫高斯以下。微波炉居第二，工作时的辐射达到130~360毫高斯，在1.5米以外才能降到2毫高斯以下。电磁辐射排名第三的电器是女士们经常使用的电吹风，辐射能达到80毫高斯。此外，空调的电磁辐射为50毫高斯，电动剃须刀19毫高斯，电饭锅15毫高斯，洗衣机12毫高斯，电冰箱10毫高斯。家中最常用的电视机，显像管电视和液晶电视的辐射差别也很大。如25英寸的显像管电视正面辐射达到20毫高斯，半米以外辐射能降到2毫高斯以下，而液晶电视的辐射只有1.3毫高斯。

办公室电器辐射，电脑背面大于正面

除了生活中的电器辐射，工作中也会碰到电磁辐射。

通过仪器测量，17英寸的显像管显示器表面的辐射为6毫高斯，距离10厘米以外，辐射会下降到2毫高斯以下。也就是说，只要人们在使用电脑时坐姿正确，将前臂自然伸直，身体就会在有害辐射以外。但是显像管显示器背面的辐射却远远大于正面，为20毫高斯。电脑主机的情况也一样，正面为1毫高斯，背面为20毫高斯，在30厘米左右才能降到2毫高斯。液晶显示器不存在上述问题，无论正反，它的电磁辐射都在2毫高斯左右。复印机、打印机的电磁辐射在3~6毫高斯。

通讯设备辐射，手机超过小灵通

通过仪器对十几个型号的手机测量发现，手机待机时辐射只有2毫高斯左右，也就是说不接电话是安全的。但是，手机接通的瞬间辐射会迅速增加几十倍。在接别人来电时，手机铃声响起前的一瞬间，手机的电磁辐射能达到50~79毫高斯；而给别人打电话时，手机拨出的瞬间辐射能达到50~100毫高斯，之后的3~4秒，手机的电磁辐射则降到待机时的水平。

用手机发短信的情况也类似，但发短信时的手机辐射要低于打电话的辐射，在接收或发送短信的瞬间，辐射为20毫高斯左右。

小灵通的辐射要远远小于手机，待机时小灵通的辐射仅为1毫高斯左右，接通或拨打的瞬间辐射只有10毫高斯左右；而固定电话的辐射几乎测不出来。

●防辐射小知识

利用可接收AM(调幅)频道的收音机，能了解电器使用的安全距离。收音机打开后靠近电器，会发现收音机传出的噪音突然变大。走出一段距离后，才会恢复原来较小的噪音量。

电脑操作者日常应多吃些胡萝卜、白菜、豆芽、豆腐、红枣、橘子以及牛奶、鸡蛋、动物肝脏、瘦肉等食物，以补充人体内的维生素A和蛋白质。还可多饮茶水，茶叶中的茶多酚等活性物质有利于吸收与抵抗放射性物质。

另外，使用手机时别性急，接电话之前最好在手机响过一两秒后接听电话，打电话时也要等电话拨出几秒后再放到耳边。（山晚）

家电课堂

←整款灯非常可爱，看上去就像是一个小人正在拔墙上的插头，而小人的头正是那圆圆的灯泡！

➡这是太阳能百叶窗灯。百叶窗朝外的一面是太阳能电池和蓄电设备。白天，在你拉上百叶窗阻挡阳光的同时，电力也在产生和储存。到了夜晚，它们就可以用来点亮百叶窗朝屋内一面的灯。

←你是否感觉到它们其实和我们一样拥有生命？它们会不会趁人不注意偷偷换个姿势呢？

捆绑型病毒感染量暴涨 三类对象最受青睐

喜欢使用游戏外挂、看网络小说或者看视频的网友，近期需要多加小心了。金山云安全中心最新病毒感染数据显示，游戏外挂、电子书阅读程序、视频播放器已成为最受黑客团伙欢迎的三大捆绑对象。捆绑型病毒的感染量单周就超过750万台次。

网民“小河马”为看网络红人“暴力熊”的视频，在一个不知名的小型下载站下载了视频播放器，随后发现自己的电脑运行速度明显变慢，并且出现了大量陌生的启动项。

反病毒工程师对大量样本进行分析后发现，几乎所有中招的用户都有一个共同点，就是网民所下载的程序要么非官方下载链接，要么就是一些连数字签名都没有的“三无产品”。

反病毒专家指出，不法黑客团伙将病毒捆绑于游戏外挂、电子书阅读程序、视频播放器中，然后发布于一些不知名的小型下载站点，或是在各个论坛中张贴带毒的下载链接，“搭乘”社会热点吸引用户下载。

黑客团伙甚至还专门搭建一些不良网站，来吸引用户下载含毒的程序。当用户下载运行后，木马文件就在后台运行，不知不觉中，网友的电脑已被塞进了各种各样的木马程序。（新华）

十大失宠技术

据国外媒体报道，英国IT网站V3日前评出了“十大失宠技术”，台式机、操作系统、CD和MP3播放器等纷纷上榜。

这“十大失宠技术”是：台式机、光盘(CD)、软盘、掌上GPS、外设线缆、FireWire (IEEE 1394)、磁带存储、便携式播放器、固定电话、操作系统。（人民）

IT学院

国家计算机病毒中心发现“U盘杀手”新变种

国家计算机病毒应急处理中心监测发现，近期出现了“U盘杀手”新变种(Worm_Autorun.LSK)，提醒用户小心预防。

该变种是一个被感染的可执行文件(扩展名:exe)，运行后会在受入侵感染操作系统的系统目录下释放恶意驱动程序，并且会将自身图标伪装成Windows默认文件夹的样式，以此来蒙骗计算机用户。该变种会将其自身复制到系统分区以外的所有分区根目录下，将分区下已存在的文件夹隐藏，并且以这些文件夹的名称来自我命名，以此来诱骗计算机用户点击运行变种文件。

另外，该变种还会强行篡改受感染操作系统的注册表相关键值项，最终导致系统中“显示系统隐藏文件”功能失效，同时可执行文件的扩展名被隐藏，以此来保护病毒文件不被发现并清除。该变种还会通过安装消息钩子的方式监视计算机用户操作系统的运行状态，对计算机用户的鼠标、键盘操作以及当前系统中的窗口执行一些恶意破坏行为。

专家建议：1.已经感染该变种的计算机用户应立即升级系统中的防病毒软件，进行全面杀毒。2.未感染的用户需打开系统中防病毒软件的“系统监控”功能，从注册表、系统进程、内存、网络等多方面对各种操作进行主动防御。（新华）

业界资讯

电话欠费诈骗升级

临近年底，远程诈骗案件再次高发，且电话欠费诈骗手法又出“升级”版，骗子省略通知电话欠费环节，直接冒充公安机关、法院及银行工作人员，强硬而直接地告知事主“个人信息被冒用、被卷入洗黑钱案件中，需立即转账申请保护”，不少事主因此上当。

在以往的电话欠费诈骗案件中，犯罪嫌疑人往往冒充电话局的工作人员打电话给事主，称事主家中的电话欠费了，然后又有冒充公安局的电话打了进来。而如今的电话欠费诈骗“升级版”则省略了冒充电话局这一环节，直接冒充公安、检察院或银行的工作人员，称事主家中的电话涉及洗钱犯罪，然后可以帮事主家中的储款转移到一个安全账户中，以实施诈骗。

警方表示，嫌疑人在冒充银行工作人员的诈骗中，嫌疑人的电话背景音中有银行保安与取款人对话的声音，使事主相信来电对方确实是银行工作人员。警方称，骗子冒充电信、公安局、检察院、法院、银行等单位工作人员，多选择工作日的9时至17时作案，针对独自在家的中老年人下手。

类似的电话欠费升级版诈骗案件近期发案频繁。犯罪分子的诈骗方式一直都在不断更新。如果一种旧的方式没有效果后，犯罪分子会立即变更乃至升级新的诈骗方式。北京市公安局刑侦总队反诈骗专家表示，公安、检察机关办案不会给市民家中打电话，市民接到类似电话应及时报案。（北晨）

网络黑客一年吞噬76亿 网民谨慎下载外挂程序

如今，网络上的“盗窃”现象日益严重，网银钱财不翼而飞，网游高价游戏装备被盗……记者从“2009江苏站长年会暨江苏(南京)互联网高峰论坛”上了解到，中国互联网用户每年因为网络安全问题损失的钱财高达76亿元！

网络安全专家李钠介绍，网络黑洞赚取利益主要采用木马病毒窃取账号，其中杀伤力最大的就是“网络挂马”。有浏览者中了木马以后，他的机器上就被植入各种病毒或木马，如果他的电脑上有网银账号或游戏账号，就可能被种木马的人偷走。从制造木马病毒、传播木马到盗窃账户信息、第三方平台销赃、洗钱，一条分工明确的网上黑色产业链已基本形成。

专家提醒网民，应该保持时时升级杀毒软件的习惯，上网时应开启网页防挂马软件，开机时进行杀毒软件实时监控，对不熟悉的网站尽量不访问，不下载软件，网络浏览时应谨慎下载外挂程序和专用播放器。（扬晚）