

看一看 你家的电器该“退休”了吗

《家用电器安全使用年限细则》出台,过了寿限出现安全事故厂家不担责

国家标准化管理委员会审批出台的《家用电器安全使用年限细则》(以下简称《细则》)近日推出,彩电、冰箱、洗衣机等日常使用家电的使用年限首次有了明确规定,市民使用时可参考选择。

据悉,《细则》规定的家电“退休”年龄,对家电使用年限和再生利用等方面作了详细规定。其中包括厂家要对其生产的家电标明安全使用期限,并规定安全使用期限从消费者购买之日起。在厂商标明的安全期限内,消费者正常使用家电产品时发生安全事故,所有责任都将由厂商承担。

记者近日在家电卖场看到,从彩电、洗衣机到电吹风等家电产品,多数均未明确标明使用年限。促销员对此回答也很含糊,以空调为例,不同品牌促销员回答的使用年限有三四年的差距。

家电维修协会相关人士认为,超龄家电不仅耗电而且危险,通常高龄家电的耗电量要超过原耗电量的40%。《细则》有利于界定在安全年限内出现安全事故时的厂家责任,这也是企业向消费者作出的安全承诺。当然,家电过了“寿限”出现安全事故,厂家将不再承担责任,因此消费者要时刻关注家电的安全使用年限。

维修专业人士介绍,《细则》规



定的家电安全使用年限可供参考,消费者还需结合实际使用情况考虑。比如,有的地方存在酸雨现象,可能影响空调的使用寿命,另外有的家庭电视每天长时间开启,其寿命也相对较短。

据了解,目前,各家电卖场均对“超龄”家电实行回收,市民也可将

“超龄”家电卖给废品回收站。
(万里)

“超龄”家电识别特征

彩电:显像管电视,当出现图像不清晰、画面颤抖等情况,就意味着相关元器件出现老化,同时辐射也会增大,一旦遇到碰撞、骤冷、骤热等情况,都能引起显像管爆炸。

(平板电视出现时间较短,不涉及超龄问题)

冰箱:出现制冷剂泄漏,运转声音过大,甚至运转时发生较严重颤抖,同时耗电量比以前大增等,都是“超龄”化的特征。据悉,一台使用10年后的冰箱,耗电量将变成最初使用时的2倍。

洗衣机:经常出现渗水、漏电等毛病,消费者可考虑换机。

空调:一开机就直喷尘土,吹出的风掺杂着一阵霉味,有的甚至流出黑黑的脏水,这些都在提醒主人:该空调可能已经到使用极限了。

家电安全使用年限参考

彩色电视机 8~10年

电热水器 8年

空调器 8~10年

电熨斗 9年

电子钟 8年

电热毯 8年

电饭煲 10年

电冰箱 12~16年

个人电脑 6年

电风扇 10年

燃气灶 8年

洗衣机 8年

电吹风 4年

微波炉 10年

电动剃须刀 4年

吸尘器 8年

☆病毒播报

国家计算机病毒中心提醒用户:

警惕网页“挂马”攻击

新华社天津2月8日电 国家计算机病毒应急处理中心7日发布公告称,通过对互联网的监测和用户求救的数据显示,网络犯罪分子越来越倾向于通过网页“挂马”方式来传播病毒。

据介绍,“挂马”是指在网页中嵌入恶意代码,当存在安全漏洞的用户访问这些网页时,会自动下载、激活木马程序,然后盗取用户敏感信息或者进行各种攻击、破坏。这种通过网页浏览方式进行攻击的方法具有较强的隐蔽性,用户难以发现,因此,潜在的危害性较大。

国家计算机病毒中心提醒,广大计算机用户必须重视网页浏览器和各种流行应用软件的安全性,及时升级到最新版本,提高对“挂马”攻击方式的防范能力。

另外,U盘也是病毒传播的主要途径。由于U盘等各种类型的移动存储介质被广泛应用,成为数据交换的主要工具。病毒、木马借助“Windows自动播放”的特性,通过Autorun.inf文件自动调用执行移动存储介质中的病毒、木马等程序,感染用户的计算机系统,进而感染其他移动存储介质。U盘病毒具有隐蔽性高的特点,病毒会采用“映像劫持”技术、进程守护等技术实现入侵。病毒通常还会关闭杀毒软件等安全软件的进程,远程下载木马等一系列恶劣的行为,进一步威胁用户系统安全。

因此,建议用户对U盘等移动存储设备的使用加强管理,通过修改系统配置、关闭系统自动运行功能等方法,提高系统安全级别,封堵病毒入侵的入口。

☆教你一招

保障无线网络安全有妙方

很多人家里现在都有台式机 and 笔记本等多台电脑,所以通过自己架设的家庭无线局域网就可以方便地随时上网。但是,在享受便捷的同时,也要注意不要让自己的无线网络被他人随意使用,以免暴露个人隐私或是造成其他不必要的损失。本期,我们就针对两种常见的无线设备的使用,介绍几种保障无线网络安全的小技巧。

Wi-Fi 无线局域网

从设计上来说,Wi-Fi在安全方面所主要依靠WEP(有线对等保密)技术进行加密。然而这种保护手段已经被证明是不够可靠的。更重要的是,WEP加密本身存在一些问题。所以就需要我们采取下面的一些措施来弥补WEP的不足。

使无线局域网更安全

■加强WEP 虽然WEP加密存在不足,但总比什么都不设——“裸奔”要好得多。所以设置WEP的一个基本原则就是采用尽可能高强度的WEP密钥。

■设置SSID SSID是一个无线网络的标识。尽可能不要使用无线设备默认的SSID。另外,把家里的无线网络设置为封闭的无线网络,并且不响应那些将SSID设置为“任意”的无线设备,也不要开启SSID广播功能,这样就能减少你的无线网络被发现和偷偷使用的可能。

■定期更换密钥 没有必要每周都换一次密钥,但应该考虑至少每个季度更换一次密钥。一个从不更换密钥的无线网络的安全性会大幅度下降。

■绑定无线设备 通过绑定家里的无线设备地址,可以最大程度上保证只有得到授权的电脑才能

访问无线网络。

蓝牙

尽管蓝牙规范在推出伊始就针对安全性做了较好的设计,但由于实际生产以及用户的使用习惯等各种因素的影响,蓝牙的安全性依然存在漏洞。目前已经有一些方法可以突破蓝牙设备的安全防线。理论上来说,设置为不可见的蓝牙设备是不可能被发现的。然而,利用一些黑客工具,却可以发现处于不可见模式的蓝牙设备,并进行入侵。

防范蓝牙攻击

■不使用就关闭 对于蓝牙设备来说,一个最基本的原则是:在不

需要蓝牙连接的时候就将其关闭。

■使用高安全级别 蓝牙设备通常有高中低三种安全级别,最高级别就是设备安全。需要说明的是,启用了高级别的蓝牙设备还可以对传输的数据进行加密,进一步增加破解的难度。

■注意异常连接 由于破解蓝牙PIN码的过程有赖于强制进行重新配对,然后才能建立连接进行入侵,所以对可疑的配对请求要特别留意。另外,在可能的情况下,尽量采取保存配对信息的方式进行连接,而不要采用在每次连接时都进行配对的方式。

(秦歌)

☆选购窍门

如何鉴别 原装电池

买个新手机,如果碰上一块组装电池,或者是一块别人用过的旧电池,那是再堵心不过的了。所以,对于消费者,新手机理应配新原装电池。下面介绍几个鉴别原装电池的方法:

1.原装电池的包装皮颜色比较暗,是亚光漆,组装电池的颜色比较亮。

2.带一块原装电池去比较,先对比原装电池的防伪,这点很重要,电池用过一次就有划痕。

3.在买电池的时候,可以用指甲推一下包装皮的边缘,原装电池不会起皮,组装电池肯定会。

4.一般在国内销售的行货手机,电池上面的标贴都是印刷着简体中文的,而水货电池由于很多都是销往外国,因此标贴上面的都是英文。有的卖家用假电池替代真电池,上面也是中文印刷。但假电池的做工很粗糙,而真电池外观整齐,没有多余的毛刺,外表面有一定的粗糙度且手感舒适,内表面手感光滑,灯光下能看到细密的纵向划痕。而且真电池标贴字迹清晰,有与电池类型相对应的电池标号,标注的生产厂家字体轮廓清晰,防伪标志亮度好,看上去有立体感。(王文)

☆潮流新品

电力存钱罐



这款存钱罐不仅可以用来存放零钱,还可以帮助你养成节约用电的习惯。它采用了传统的小猪造型,猪尾巴为一根电线,猪鼻子则是一个插座。但是它可不仅仅是起到延长线的作用哦。想要用电就要向存钱罐里面投入硬币。每投入一个硬币你就可以用电30分钟。30分钟之后,电源会自动切断。想要再用还要继续“破费”。

数字时代的 瑞士军刀



在整个世界被电子产品包围的时候,瑞士军刀顺应时代潮流,推出了这款带有液晶显示屏,具有测温 and 感应高度功能的数码瑞士军刀。这款新产品增加了温度计 and 测高仪两个功能。液晶显示器可以告诉用户所处位置的高度以及周围温度等信息。对于喜欢野外探险的用户来说,这两个新功能在特殊情况下将会提供更多帮助。

(新华)