

阳普国和菜市场插上“智慧”翅膀

市民买菜、商户卖菜开启新模式

“如今,各种智能化运用正慢慢融入生活的方方面面,千家万户的菜篮子也紧跟步伐进入“智慧”新时代。

国庆前夕,中原路 209 号的阳普国和菜市场在经历了两个多月的改造升级后,成功插上了“智慧”的翅膀,成为杨浦首家“智慧菜场”。市民能便捷获取菜价、检测、销售等信息,商户也可通过 AI 智能系统实现高效“算账”。



市民
买菜省心,吃菜放心

走进国和菜市场,映入眼帘的便是一整块可视化多媒体大屏幕。今日菜价、食品检测结果、商品销售数据等一目了然。记者发现,不少市民进入市场的第一件事,就是来到大屏幕前“做功课”,了解一下当天的农副产品种类、价格以及平价蔬菜、平价肉等信息。

一位市民表示,“大屏幕上面的信息很全面,我最关注的有两点,一个是菜价,另一个是菜品农药检测结果。我每天过来看一看,买菜省心,吃了也放心。”

此外,在菜品称重结算后,电子秤会自动打印出一张销售小票。每张小票上都印有二维码,市民扫一扫即可查询商品的来源,更全面地了解菜品信息。

商户
电子秤自己能“算账”

这次智慧化改造过后,市场内所有的商户都换上了新的电子秤。电子秤被植入了 AI 智能系统,具有自动货物识别的功能。大多数的货物一上秤,电子秤的屏幕上就会显示品名、重量、单价、小计等信息。

市场经营户张梦伟说,“电子秤还可以计算总价。比如某位市民来买菜,一次买了十几样,每种菜品价钱打出来以后,我们只要点击一下‘加号’,电子秤就会自己计算总价,免去了人工算账的麻烦。”

据悉,市场还能通过电子秤,记录下每一笔交易信息,并录入市场的管理平台系统。“新的电子秤集合了后台数据搜集的功能,我们可以看到每种单品销量,市场销售额以及单品最高价、最低价、均价分别是多少。对于市场来说,通过大数据搜集,一旦发现菜价高了,



菜场智慧屏

可以进行适当的干预,起到平抑菜价的作用。同时,从这些数据中还可以看出哪些业态比较好,今后也可以适当考虑增加这些业态的招商。”国和菜市场场长戴俊仑说。

市场
消除日常管理“盲区”

此外,国和菜市场的外围、入口等多个位置安装了智能摄像头。这些摄像头运用 AI 智能识别技术,可自动捕捉经营户不戴口罩、不当操作、违规停车、消防通道堆物等行为,并将相应问题画面实时推送到市场管理员的掌上终端设备。如此一来,管理员能快速进行处理,及时消除日常管理盲区,实现市场经营行为可查、可管、可控。

“依托现代互联网技术,实现传统菜市场数字化运营、信息化管理,提升老百姓买菜的幸福感,是智慧市场建设的根本所在。”阳普菜市场公司经营拓展部经理朱骏豪说,“我们以基础条件相对较好的国和菜市场为切入点,先行先试,率先探索传统菜市场智慧化改造的变革之路。今后也会努力让所有的标准化的、传统的菜市场都装上智慧大脑,在经营、管理方面实现飞跃。”

阳普菜市场公司将进一步完善与充实自营线上销售平台“阳普生鲜”,及时把小菜场“搬”到线上,给予周边市民更好的网上买菜体验,进一步打通线上线下买菜模式,提升智慧菜场服务能级,实现“互联网智慧菜场”新模式。

(上海杨浦)

网络安全

这些网络安全“漏洞”,你堵好了吗?

漏洞一
个人敏感信息随意外泄

一张照片就能泄露全部家庭成员信息,容易给不法人员创造行骗、行窃的机会,尤其是老人、小孩的信息,更要注意保护,包括姓名、幼儿园和学校的地址等。

1.晒娃要注意
有些爱晒孩子的家长没有关掉微信中“附近的人”这个设置,骗子通过微信搜索“附近的人”,轻易就能获取孩子的信息。

2.行程要保密
外出时,日程安排、行踪等信息要注意保密,不要给犯罪分子行窃的机会。所以,外出期间能够显示姓名、身份证号的车票、护照、飞机票等不要“晒”。

3.保护好隐私
尽量不要在照片中出现特征明显的东西,例如你的家门钥匙、车牌号码,以及身份证、驾照和护照等证件。

漏洞二
密码过于简单或多账户设同一密码

对于密码我们都不陌生,每当我们登录论坛、邮箱、网站、网上银行或在银行取款时都需要输入密码,密码的安全与否直接关系到我们的工作资料、个人隐私及财产安全。

以下几点要注意:

- 1.不要所有账户使用同一密码;
- 2.重要的账户应使用更为安全的密码;

现代人须臾离不开网络,然而,对于网络安全“漏洞”,每天上网的你,了解多少?知道怎样保护自己的个人信息吗?今年的网络安全周刚刚闭幕,“网络安全为人民,网络安全靠人民”,来看网络安全知识科普,从自己做起,堵住安全漏洞,防范风险隐患。



- 3.偶尔登录的论坛可以设置简单的密码;
- 4.日常使用的电子邮箱、网上银行、公司信息系统需设置复杂的密码;
- 5.不要把论坛、邮箱、网上银行、信息系统账户设置成相同密码;

设置密码的几个窍门教大家:
短语拼接:自己熟悉的短语,最好有数字有字母,大小写结合;如“5G时代@”转换为密码“5Gshidai@”。

整句化散词:使用喜爱的诗词拼音首字母加上数字与特殊符号组成密码;如“天生我材必有用”

首字母加数字与特殊字符组成密码“tswcbyy@6”。

数字换文字:可以将汉字转换成对应的阿拉伯数字如“二月春风似剪刀”转换成密码“2ycfsjd@”。

中英文匹配:选择熟悉的一句话,部分用拼音其余用英文单词代替,并加上数字与特殊字符进行组合。如“我爱工作”“wo love work@7”。

漏洞三
使用没有密码的公共 Wi-Fi

为了满足网民手机上网需求,现在不少商家都配备 Wi-Fi 来吸

引消费者。“公共 Wi-Fi”虽然方便,却也有不少安全隐患。黑客们喜欢在“公共 Wi-Fi”里设置埋伏,网民一不小心就会中招,轻则损失钱财,重则个人信息全泄露。

手机如何安全使用“公共 Wi-Fi”?下面几招教你:

- 1.手机设置禁止自动连接 Wi-Fi;
- 2.拒绝来源不明的 Wi-Fi;
- 3.使用安全软件检测 Wi-Fi;
- 4.不使用陌生 Wi-Fi 进行网购;
- 5.警惕同一地区多个相同或相似名字的 Wi-Fi;

漏洞四
放松对“熟人”钓鱼邮件的警惕

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、点击嵌入邮件的恶意链接或者打开邮件附件以植入木马或恶意程序,进而窃取用户敏感数据等的一种网络攻击活动。

防范钓鱼邮件要做到“五要”:杀毒软件要安装;登录口令要保密;邮箱账号要绑定手机;公私邮箱要分离;重要文件要做好防护。

另外,不要轻信发件人地址中显示的“显示名”。因为显示名实际上是可以随便设置的,要注意阅读发件邮箱全称;不要轻易点开陌生邮件中的链接;不要放松对“熟人”邮件的警惕。如果收到了来自信任的朋友或者同事的邮件,你对邮件内容表示怀疑,可直接拨打电话向其核实。

漏洞五
扫描来路不明的网站或 APP 上的二维码

移动支付时代,扫描二维码已经成为我们生活中最稀松平常的事儿。可是,这些二维码看起来方便,但是一不小心,你可能就要付出钱财损失的代价。

以下是常见的几种二维码诈骗伎俩:

- 1.在商场购物时,遇到称“扫二维码”就能免费赠送商品的“推销员”,大家决不能抱着“不要白不要”的想法顺手扫码。有些不法分子利用了这种心理,通过各种方式诱导受害者扫描二维码。受害人在不知情的状态下登录预设网站自动下载木马病毒,导致个人信息、网银密码被窃取。
- 2.有不法分子会通过微信向大家发送一个二维码,谎称扫描二维码帮忙刷一下淘宝店的信誉,还能得到佣金。市民一旦输入了手机号和银行账号,不久后微信钱包里的余额会被转走。
- 3.有人在车窗上看到“违法停车单”,单子底部附有一个二维码,如果车主扫二维码进入,屏幕上就会出现一个 200 元的转账界面。该手段比传统诈骗有较强的迷惑性,群众容易上当受骗,社会危害相当大。

一定要慎重甄别网络虚拟身份,切不可相信来路不明的二维码,填写账号、密码时,一定要验明对方身份真假,谨防受骗。一旦发现钱财被转走,及时报警。

(新华社、上海杨浦)