手机上了锁,为啥还丢钱

专家支招:重新设置SIM卡PIN码,可给手机卡再上一道保险

智能手机一旦丢失,不仅会带来诸多不便,甚至还会造成个人隐私泄露及财产损失。

然而很多人认为,自己已经设置了手机屏锁、支付密码、指纹锁等防御措施,如果手机被盗了,小偷拿走的也只是块毫无用处的“砖头”,无法获取自己的隐私和钱财,但事实真的是这样吗?

被绕开的锁屏密码

最近,有媒体报道称,王女士早晨上班时手机被偷了,她和很多人一样,觉得手机设置了各种密码钱财不至于被盗,所以一直到下班才补卡并购买了新手机,但是当她重新下载了软件后才发现,微信、支付宝里面的钱居然全没了,查看交易记录得知,这些损失仅发生在手机丢失后很短的时间之内。

为什么明明设置了那么多密码,钱还是不翼而飞了呢?

金立手机产品经理刘岩告诉笔者,之所以为手机加设了种种安全保障,却依然不安全的原因主要在于:一般用户设置的开机密码或支付密码较为简单,安全性较弱,因而易被不法分子破译;此外,不法分子还可通过将盗来的手机卡插入另一个手机中接收验证码,窃取或更改用户支付账号信息。

笔者用自己的两部手机对此进行了验证。

登录支付宝需要两个条件——解开手机屏锁、输入登录密码。笔者将A手机的手机卡换到B手机上,就可以成功绕过手机屏锁这一关。由此可见锁屏密码不是绝对安全。手机锁屏成功越过后,打开支付宝客户端,选择忘记密码,支付宝就会发送一条验证码短信到B手机上,输入验证码可以重置支付宝登录密码,重置密码后,就可以登录支付宝了。进入支付宝后,不法分子可以通过手机号到黑市查询机主的身份证、银行卡信息,从而重置支付密码,转走支付宝的钱财;还可以打开支付宝付款二维码,用POS机扫码,直接把钱刷走。

给手机卡上道锁

看到这里,很多人都恍然大悟——原来手机里不安全的因素实在是太多了,而不法分子能接收手机验证码无疑是最恐怖的,那么能不能给手机卡也上道保险呢?

“可设置手机卡密码即PIN码,它可以保护手机卡的使用安全。”中国移动客服人员告诉笔者,用户若在手机上设置了“锁卡”功能,每次开机时,手机屏上就会显示要求用户输入PIN码,正确输入后手机才能正常使用。PIN码初始密码是1234或0000,用户可自行修改为任意4—8位的PIN码。不法分子连续输错几次之后,手机卡就会锁住,无法使用接打电话和收发短信的功能,从而可在很大程度上降低钱财被盗刷的风险。

此外,给手机设置安全的锁屏密码,为重要应用设置应用锁,不安装来历不明的应用,不连接不知来源的WiFi,不随意点击不明链接,谨慎扫码等也很重要。

相关链接▶▶

各种手机的“保安”大招

移动互联网时代,手机安全直接关系到信息安全与防护。对手机用户和生产厂商来说,提高信息安全意识,加大信息安全措施,开发信息安全技术,可谓任重而道远。

为保证手机用户的财产安全和个人隐私,各大手机厂商也是各显其能。如金立手机内置了“私密空间”,可将重要应用放入其中,使不法分子无从知道手机有哪些应用;另外,金立手机独有的安全键盘,也可有效防止密码被第三方输入法记录和泄露。

小米的MIUI8开发出了手机分身功能,支持将隐私、财产类应用放入手机分身,在正常解锁手机后无法看到这些应用,只有当用户主动输入手机分身独立的密码后,才能使用这些应用。小米的MIUI8还支持针对应用设置应用锁,在打开隐私、财产类应用时,需要输入与锁屏、分身空间均不同的密码才能使用此应用。

而华为Mate9采用了硬件级的加密方案,配备了一枚通过央行和银联安全认证的、集成到Kirin960 SoC的金融级安全芯片,并且加入了防伪基站侦测技术,带来金融级安全支付、电信级安全通信、独立隐私空间全方位的安全保护。同时还首次内置银行U盾,实现了支付安全

一旦手机丢失我们应该这么办

有时候虽然我们做好了万全之策,但是也难免百密一疏让小偷钻了空子。一旦手机丢失,我们该怎么做才能让财产损失降到最低呢?

小米手机首席安全官陈洋表示,手机应开通查找手机功能,丢失时,可第一时间通过查找手机将其锁定,并致电运营商挂失,移动用户可拨打10086的人工服务,提供服务密码使手机停机,如果遗忘则需提供姓名、身份证号及一项验证信息,验证信息包括最近3个月每月的消费金额、现有套餐的名称、主套餐的价格、号码开始使用的时间、最近一次的充值时间和额度、最近3个月新办理的业务等等。

除了致电运营商外,还可借亲友的手机登录自己的支付宝账户,然后故意输错密码,这样支付宝系统就会被冻结,从而可获得3个小时的冻结时间。利用这些时间你可以拨打电话95188挂失支付宝,解除手机号码和支付宝的绑定;也可在手机上点击支付宝APP选择“设置—安全中心—挂失账号”直接挂失;还可以在电脑上登录支付宝,点击“安全中心”,选择“应急服务”,然后选择“快速挂失”,输入支付密码即可使支付宝免于被盗刷。

在确保支付宝账户安全后,我们还应着手保护微信,虽然微信中财产可能相对较少,但若关联了银行卡或聊天记录、朋友圈中存有个人信息,隐患也是非常大的,冻结微信的操作步骤是:用亲友的手机登录微信,进入“设置”,点击“账号与安全”,选择“微信安全中心”,点击“冻结账号”即可,另外也可登录腾讯安全中心或登录网站110.qq.com冻结账号。

此外,手机银行也要进行挂失和冻结,打开工行APP,登录后进入主菜单,在常用功能页面内,点“我的账户”,选择“账户挂失”即可。另外,输错3次手机银行密码,即可当日冻结,次日可再登录,连续输错10次,则被正式冻结,且不会自动解冻。

在做完上述紧急处理之后,还要修改微博、QQ等社交软件密码,最后应将手机丢失的消息传达给亲友,以免他们上当受骗。

i宝机器人陪孩子玩游戏

近日,南京阿凡达机器人科技有限公司研发的i宝机器人实现量产,将面向全球发售。机器人专家认为,它将对日本软银公司生产的“Pepper”机器人构成强有力的挑战,打开人形智能机器人的消费市场。

i宝机器人可以用自然语言进行中文对话;通过人脸识别,追踪跟随对象;10个手指每个都可以灵活运动,能够玩“石头、剪刀、布”等高难度的游戏;被人挠了痒痒也会哈哈大笑,喜怒哀乐都显示在脸上……

阿凡达公司联合创始人、首席技术官熊玮表示,i宝机器人瞄准家庭这个大市场,为3—8岁的儿童提供教育、娱乐、交友、家长监护等功能,与孩子进行多层次互动。

■大开眼界

能正向“爬”楼梯的轮椅

日前,一款由东北大学大三学生设计制作的新一代欠驱动自适应式爬楼梯轮椅在东北大学亮相,这款新型轮椅在保障稳定性的同时,还能让轮椅上的残障人士正向“迈步”走楼梯。

目前市场上的轮椅在爬楼梯过程中,不能正向上下,多是需要倒退上楼,有的还需要他人辅助,使用起来诸多不便,该项目组在国内外率先采用了后支架结构的变形技术来使轮椅满足正向上下楼梯的要求,项目负责人黄伟康同学介绍,利用后支架结构的变形技术,其优势在于无需任何特殊装置或者操作,就能够自己适应不同的路况和台阶,而且平稳性和安全性都有技术保障。

“基因剪刀”可防治视网膜病变

具备治疗血管新生相关眼疾的潜力

俗称“基因剪刀”的基因编辑技术显示了医疗应用的潜力。美国研究人员在动物实验中应用“基因剪刀”成功阻止视网膜血管新生,达到防治视网膜病变的目的。

视网膜血管新生,是指视网膜表面长出新的、异常的血管。随着病程变化,这些新生血管会渗漏、破裂甚至导致视网膜脱落,诱发视力受损乃至失明。增生性糖尿病视网膜病变、湿性老年性黄斑变性、早产儿视网膜病变等,都可能引发视网膜血管新生。

目前主要靠血管内皮生长因子抑制剂类药物来抑制新生血管生长、减轻血管渗漏。但这类治疗手段需持续用药,还有相当数量的患者对血管内皮生长因子抑制剂不响应。

美国马萨诸塞眼耳科医院研究人员在新一期英国《自然·通讯》杂志网络版上报告说,此前研究已知,血管内皮生长因子受体—2在血管新生过程中扮演了重要角色,因此他们此次尝试以腺相关病毒为载体,对编码这种受体的基因进行编辑,阻断眼内病理性的血管新生。

结果显示,在实验鼠身上,只需一次腺相关病毒的注射就能完成基因编辑,阻断了视网膜血管新生。

基因编辑技术可以像人们编辑文字那样修改DNA链编码,此次实验中应用的是目前全球最流行的CRISPR – Cas9技术。研究小组说,下一步有望利用这种基因编辑技术开发出新疗法,临床治疗以病理性眼内血管新生为特征的眼部疾病。

他们接下来将重点研究这种疗法的安全性和有效性,“我们目前的动物实验研究结果显示,CRISPR – Cas9技术是一种精准、有效的工具,具备治疗血管新生相关眼疾的潜力。” **(本版综合)**