故事一：

集团信息安全月小故事第一期：诈骗反杀技术

大家好，我是小秦，本来是个平凡人。这个月，我身上发生了一系列不平凡的故事。

我中奖了，20万，脑力男人时代，腾讯赞助，一向很豪。我怀着激动的心情先行缴纳了个人所得税。

看到这里你可能已经知道我妥妥的被骗了。

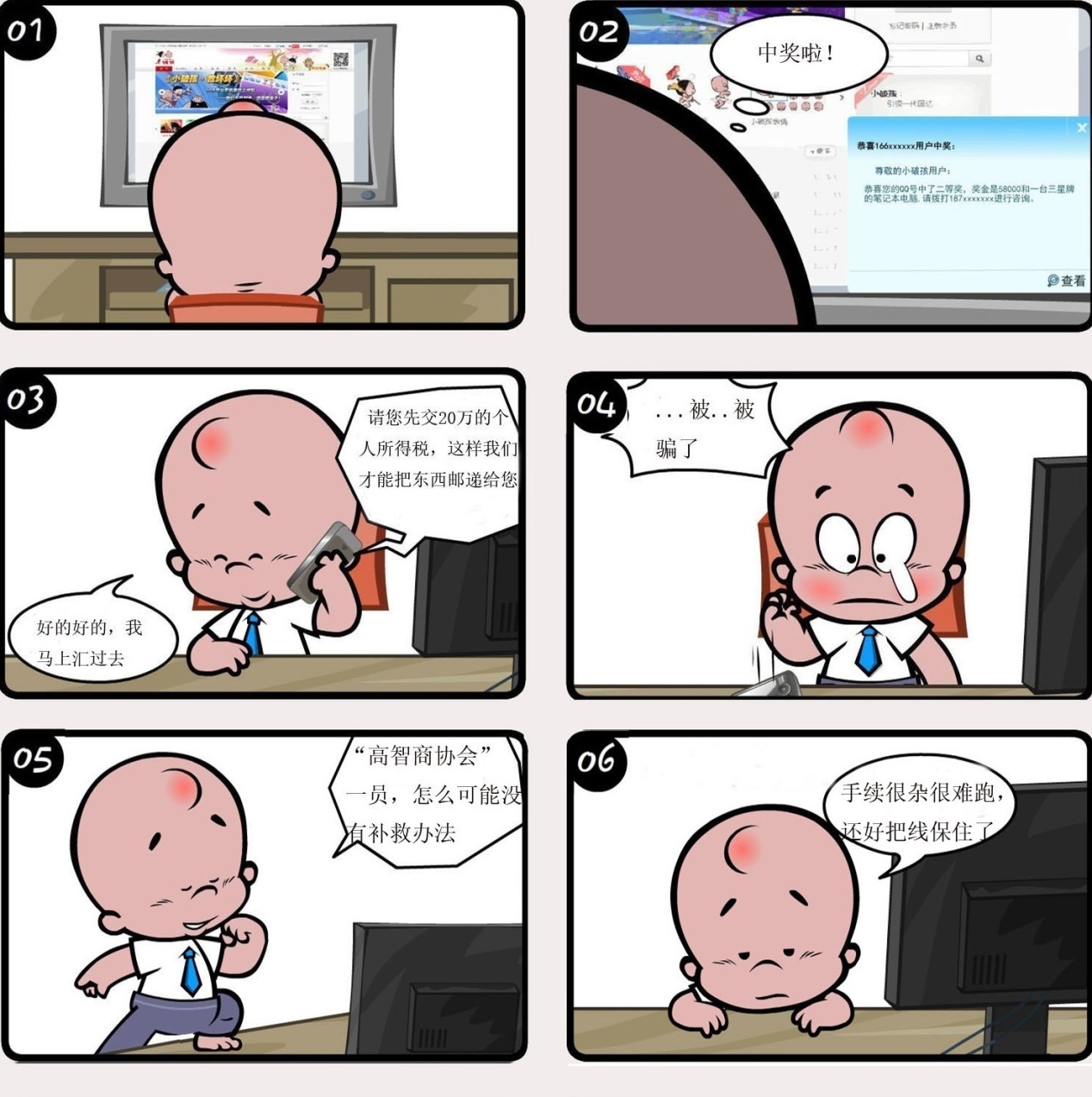
但是，身为“高智商协会”的一员，怎么可能没有补救办法。

虽然银行公安手续很杂很难跑，但是好在把钱保住了。

戳下面的链接，不看后悔辨识方法和补救操作。

http://anquan..com/video.html

需要配套图片



辨识诈骗:

各种网赚兼职、公司回馈活动、中奖信息，要求你交手续费、保证金、押金、定金。称警务人员，告诉你被涉案通缉，要求你把资金转入安全账户。自称各种客服人员，引领你进入各种网站操作等。总结一句话：陌生人先取得你信任，然后要求你把资金通过各种手段交给他，这些都是骗子！！！

补救措施：

一、一旦汇款后发现自己被骗了，第一时间冻结诈骗账号阻止对方将钱转移，并为警方破案提供时间：

1、电话银行冻结止付：可及时拨打中国银联95516转1，根据语音提示输入该诈骗账号，然后重复输错5次密码，就能使该账号冻结时限24小时。

2、网上银行冻结止付：进入网上银行界面输入该诈骗账号，然后重复输错5次密码，就能使该账号冻结，时限24小时。在次日凌晨重复上述两项操作，则可继续冻结24小时。

二、如果自己的银行卡号/支付宝、密码等信息已经被嫌疑人获取，请第一时间到对应银行冻结自己的银行卡/支付宝，阻止嫌疑人继续转账、提款。

三、有问题立即拨打110报警，及时与汇款的银行柜台联系，要求协助。

防范意识：

一、保护好个人重要信息：身份证、银行卡号、手机号和密码不要轻易告知陌生人。

二、不要把自己的手机钱包载体交给他人使用，保护好个人短信验证码。

三、在密码设置上，手机银行密码尽量不与QQ、微信、微博、邮箱、论坛等密码相同，规避资金风险。

四、不点击不明来源的链接、不扫描不明来源的二维码，不轻信积分、礼品及中奖信息。

故事二：

集团信息安全月小故事第二期：无线wifi安全

我是小秦，不知道为什么，今天我的私人网络很卡。

我登录祖传的路由器看了看，里面居然多了个陌生连接。fxxk，我这是被蹭网了啊。

是因为admin123弱口令吗？我把密码改复杂点吧。

卡。。。啊。卡。。。啊。怎么不管用啊。我去搜索一下什么情况，这是。

原来如此！路由器wps连接方式可以被破解！！

怎么样？黑科技想不想学？

戳下面连接，看看99%人不知道的预防以及破解方法。

http://anquan..com/video.html

配套图片



辨别方法：

一、360wifi创建的无线上网，直接在界面上可以看到有没有别人链接，有的话直接拉黑；

二、常登录路由器管理后台，看看有没有不认识的设备连入了WIFI，如果有，及时将其清除；

三、下载一个wifi万能钥匙，不输入密码直接链接能连接上说明已被破解（测试后改了无线网密码）。

防御意识：

一、路由器管理网页登录账户、密码，不要使用默认的密码，可改为字母加数字的高强度密码；

二、WIFI密码选择WPA2加密认证方式，长度至少要在10位以上，大小写字母、数字、特殊符号的组合；

三、路由器默认的管理IP修改为自己指定的特殊IP，开启MAC地址过滤功能只允许已知设备接入；

四、在设备中安装具有ARP局域网防护功能的安全软件；

五、不要随便告诉不可信人员你的无线密码；

六、移动设备不要“越狱”或ROOT，连接来路不明的无线网络；

七、关闭路由器WPS/QSS功能。

破解方法：

http://www.hack80.com/thread-21980-1-1.html

故事三：

集团信息安全月小故事第三期：密码攻防技术

哈哈哈，我是Helen，曾经黑客中的王者。昨天破解了小秦的路由，今天就把他号盗了。

哼，他以为用xiaoqin0230这种密码我就猜不出来吗？

一个名字加个日期，太简单了！！！我直接就猜出来了，更莫说我社工库里有你们所有人的常用密码。

听说他们正在宣传反制我的方法。哼哼，我能让他们如愿吗？

千万不要点下面的链接，才不是反制我的方法~

http://anquan..com/video.html

配图弱口令，信息泄露，数据库泄露都可以。



辨别方法：

一、弱口令类型如键盘位置口令：如123456、qwer1234、asdf、qaz123等有键盘规律的口令；

二、弱口令类型如懒惰口令：test、root、123456、111111、admin、admin123等；

三、个人属性口令：名字、生日、电话号码、QQ号、微信号，如zhangwei0201、qq123456等；

四、公司属性口令：名字、域名、楼层、行业、系统名，如haoweilai、、yunwei1213等。

防范意识：

一、账号口令的有效长度至少8位；

二、账号口令的设置应满足：至少包含大、小写字母、数字、特殊符号中至少三种及以上类型，如iL0V1@；不允许使用4个及以上重复的字母或数字、普通的名字或昵称或个人信息，如生日日期-19900102、wangwu1990、wangwu0102等；

三、不要使用最近使用过的口令；

四、管理员初次发送账户给用户时，用户应及时更改默认口令；

五、账号口令输入错误超过5次的，系统应该自动锁定该账号；

六、避免将口令记在书面上（可以被安全保管的除外），并严禁贴在电脑屏幕或其它容易泄露的地方；

七、当有迹象显示账号口令可能已遭破解时，用户应立即更改口令；

八、应对用户的口令牌进行保护，财务部门使用的网银U-KEY；行政部使用的住房公积金的USB加密狗等，当不使用时要妥善保管好避免泄露。

故事四：

集团信息安全月小故事第四期：网络安全法

我是小秦，我把号找回来了。哎，再也不用弱密码了。

我看了新闻，昨天盗我号的黑客想跑的时候被抓了，已经进去了。

坏人，不光盗我号，还偷偷在网上大量贩卖个人信息资料！！

国家网络安全法6月1日起正式实施了。想跑？哪跑！

想知道还有哪些行为可能触犯网络安全法吗？

快来学习和做题吧。

http://anquan..com/legal.html

故事五：

集团信息安全月小故事第五期：邮件诈骗

我是小秦，现在被在批评教育。

旁边同事在被大加表扬。

事情是这样的，今天我收到一封邮件：



这种时候当然是快快响应，积极表现了。我马上招呼旁边的同事来一起看最新指示。

万万没想到，我打开这个附件，我的祖传电脑就卡死机了，风扇疯狂转动。

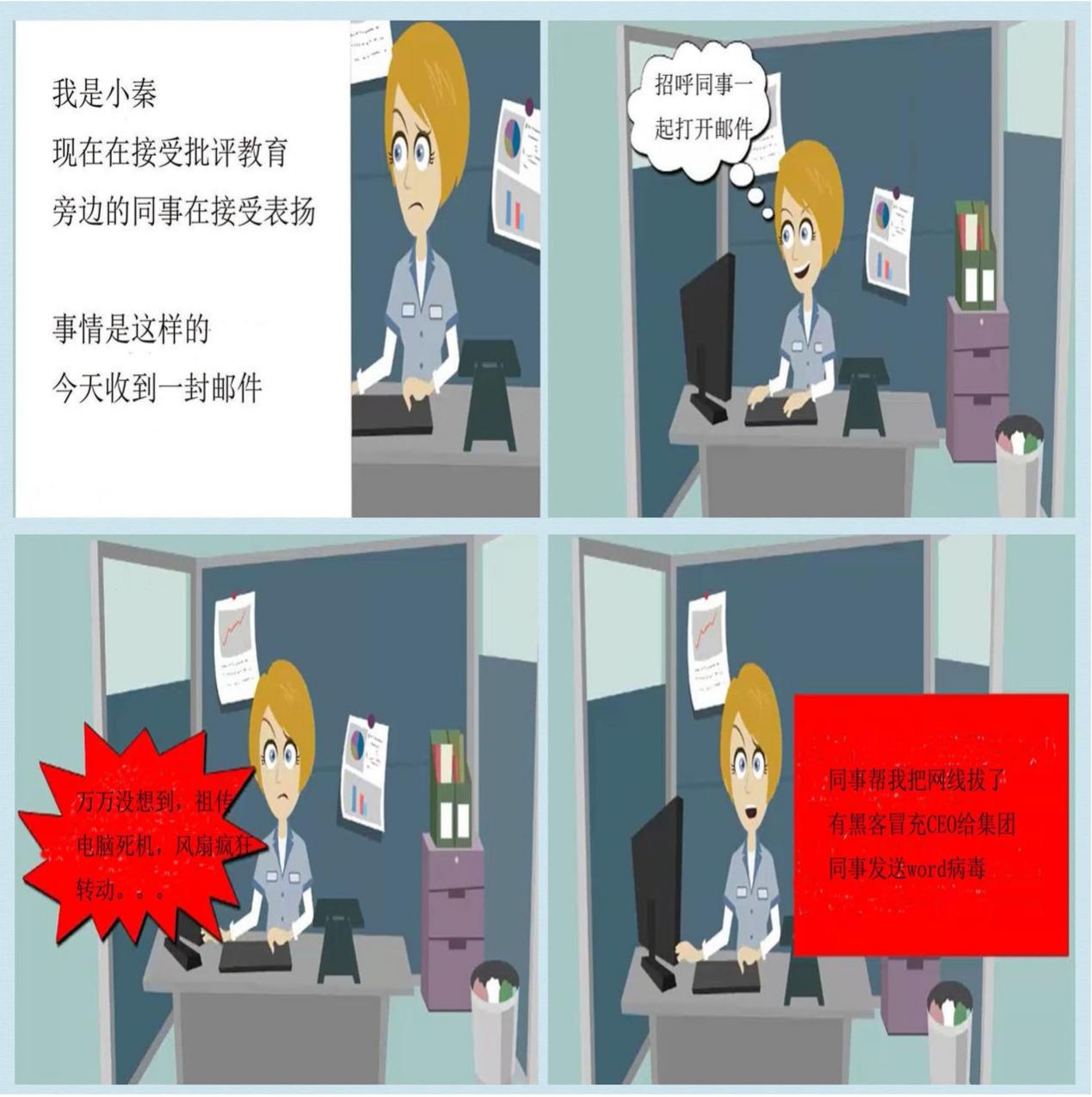
旁边同事马上把我网线拔了。。。。

这时同事收到集团通知，有黑客冒充CEO给集团同事发送word病毒。

里面还详细说了这次邮件的破绽以及其他辨识方法。

快快点击链接，进来看看邮件破绽和其他辨识方法。我去写检讨了……

http://anquan..com/video.html



页面内容

邮件破绽

一、发件邮箱地址不对。

二、全员邮件收件人都不是自己名字。

辨识方法

一、发件人的电子邮件地址或电话号码与所声称的公司不匹配。集团相关邮箱后缀

二、您的电子邮件地址或电话号码与您告知相关公司的信息不同。私人邮箱收到工作邮件内容。

三、链接看似合法，但会带您前往 URL 与相关公司网站网址不匹配的网站。

四、信息看上去与您从相关公司收到的其他信息明显不同。

五、信息要求提供个人资料，比如信用卡号或者帐户密码。

六、信息来历不明，并且包含附件。

故事六

集团信息安全月小故事第六期：数据备份技巧

大家好，我是答题系统的运维。

活动开始不久，答题系统进行了一次紧急升级。

升级之后，很多早就积极答题的小伙伴反馈自己的成绩无效了。

在此，请大家放心。大家的成绩都是有备份的。不会丢的。

有疑问的可以联系我们的安全人员。我们把记录给你看。

数据备份是工作中一个很重要的习惯。

想知道关于数据备份还有哪些技巧吗？

点击链接来我们的安全小课堂看看吧。

http://anquan..com/video.html

配图：数据备份相关



内容：

基本数据备份策略:

一、自动备份一定要有版本控制。

二、最放心的备份方式：两地三份

个人数据备份方法：

一、本地电脑一份，移动硬盘里保存一份，两者要定时更新，物理隔离。比如一份家里，一份办公室里，定期同步。

二、设定计算机在空闲的时候自动进行备份。使用时间戳，保证版本控制策略。

三、根据自己的实际情况做备份计划。选择数据备份的关键节点，备份地点以及重要数据，兼顾备份效率以及数据安全性。

四、线上备份-为保护数据不会因为自然灾害、火灾或者盗窃而丢失，您可以使用在线的备份方式。线上方式仅限于个人数据。

五、经常整理磁盘碎片-整理磁盘碎片有助于延长磁盘的使用寿命，并确保数据的安全性。

服务器数据备份方法:

根据集团的数据分级与等级保护文档规定，三档数据的备份方式建议如下：

核心数据：建议物理异地存储，保存三份，按照时间戳每天或每若干小时做全量本地及异地的物理隔离数据备份，同时建立主从服务器做热备份。操作方式即服务器要有计划任务做异地全量备份，要建立主备服务器，数据库支持集群方式的要用集群方式搭建。

重要数据：建议做到二份备份，按照时间戳每天或每若干小时做全量物理隔离数据备份。操作方式即服务器要有计划任务做异地全量备份。

普通数据：业务根据实际需求评估是否需要备份。

数据备份命名建议：

一、命名尽量要描述性强，多用关键词，少用缩写词。

二、命名要一致，定好适合自己的命名方式，永远不要变。

三、名字里要包含时间，格式要一致。

四、不要用一些特别的符号，会出乱码。建议符号只出现\_下划线。

五、版本号：有的人愿意加版本号，比如V1，V1.1之类的。这个习惯在文件修改过程中有帮助。定稿之后还是按照上面的方式命名最好。

故事七：

集团信息安全月小故事第七期：信息安全规定

大家好，我是小秦同事，拔他网线的那位。哎，说起来我只是做了一点微小的工作。

不值得表扬：）：）：）

作为一个开发人员，数据备份当然是最基本的习惯啦。我们都用代码仓库的。

今天领导说要找我谈话，不知道啥事情，我还是接着写代码吧。

：（：（：（

我被批评了。

我忘记切换代码仓库，把代码传到github上去了，违反了集团信息安全规定。幸亏安全团队及时发现了。

关于信息安全规定，还有哪些重点事项需要注意呢？

请看http://anquan..com/video.html

需要配图：代码泄露相关



需要内容：

Hacker寻觅:

一、检索资源：

1、搜索引擎工具：如Google、百度、搜狗、bing等；

2、代码托管平台：如GitHub、gitlab、coding.net、码云等；

3、文件托管平台：各类网盘，文库，各类社区论坛的文件平台。

二、检索方法：

搜索关键词：业务线名称、域名、产品名字、品牌名字、系统名字、password等；

搜索的语法：如在Github上搜索 'www.baidu.com password' 可以检索是否有源码中泄露密码的。

防御方法：

一、应用系统源代码应使用版本控制系统进行集中管理，对版本控制系统的用户访问授权应遵循最小授权原则，应依据安全配置指南对版本控制服务器及系统进行安全配置。即个人账户只能访问自己以及小组代码库，并且只有普通权限。

二、源代码应保留在公司所配发的开发服务器或办公电脑中，不得将源代码拷贝至个人电脑中，源代码非必要不得带离公司。即公司系统代码不得上传至github，gitlab，coding.net，码云等公共仓库。

三、开发过程中所形成的相关文档，如需求分析、产品设计、系统设计、测试文档都属于公司机密文档，应对文档进行密级标识并实施必要的保护。即不得在公共网络如论坛，社区等地发布这些文档。

故事八

集团信息安全月小故事第八期：运维安全

大家好，我是运维。

我也想做一点微小的工作。

我搞了一个自动发版的系统，以后发版就不用手动去搞了。

虽然我自信绝对不会跟昨天开发那样有疏忽导致安全问题，但是为了集团信息安全规定，还是跟安全团队报备一下吧。

万万没想到，这么个简单系统还是被他们找出问题来了。

自动发版的时候把.git文件夹也给传到服务器上了，导致了代码泄露。

想知道运维过程中还要注意哪些方面吗？

点击链接，我来给你讲解一下吧。

[http://anquan..com/video.html](http://anquan.100tal.com/video.html)

配图：



内容：运维安全配置。

一、应用要使用低权限运行，即启动应用要用不可登录的非root用户。

二、应用要采用访问控制。即自带访问控制的组件必须设置访问控制，特别是redis，mongo等重点组件。

三、应用组件的监听地址尽量选择内网地址或本机地址。

四、Tomcat 要删除manage 跟example文件夹。

五、部署的时候尽量选择使用各应用组件的最新版本部署配置。

六、机器尽量配置使用防火墙，只对必要的机器开放必要的端口。

七、定期更新应用组件，可以选择发版时更新。

八、注意备份文件存放位置，不能放在web目录下。

九、注意web目录下隐藏目录及文件（.git/.svn）。

十、注意设置配置文件不能被直接访问下载。

十一、定期检查机器用户账户，测试账户及时删除。

故事9

集团信息安全月小故事第九期：手机使用安全

我是小秦，话说我昨天换了一部新手机。

当天我就给他越狱了，哈哈，so easy。

然后晚上去看了演唱会，浪里个浪。

那时候为了发微博，玩阴阳师下了个插件，连了那的免费wifi。

结果今天发现手机中毒了，TMD，损失惨重啊。

这黑客他把我的式神全喂了狗粮啊，MMP啊。我辛辛苦苦氪金氪肝刷的SSR啊。

不幸中的万幸，幸亏还没装支付宝，微信啊。

朋友们，千万不要越狱啊。安全隐患很大啊。我身上血的教训呀。

快来看看还有哪些手机使用的注意事项吧

[http://anquan..com/video.html](http://anquan.100tal.com/video.html)

故事9配图：手机安全



内容：手机使用安全。

手机安全使用：

一、一定要安装手机安全软件；

二、保持手机设置开机密码的习惯，为万一情况争取处理时间；

三、不随便安装应用软件。有需要安装陌生应用时，注意看软件的需求权限。若是陌生软件要求一些短信，电话，通讯录权限时要格外当心；

四、更换手机号时要注意，要一起更换各种账号验证手机号。特别是微信，商城，银行卡，证券等财产相关账号；

五、定期备份手机数据。比如通讯录、照片等，防止意外丢失；

六、手机丢了，要及时处理银行，支付宝，微信，证券等经济相关的账号，冻结或更改或挂失；

七、旧手机弃用时，要将安装的软件清除数据并卸载删除，并取出额外的内存卡，或者直接恢复手机出厂设置。

日常安全意识：

一、不轻易在网页中填写真实个人信息，多见于各种测试游戏页面；

二、不轻易扫描陌生人给的二维码，比如地铁里自称创业者推广APP；

三、生活场景的各类验证码都是私密信息，千万不要给别人，尤其是财产相关的验证码；

四、不要乱晒个人信息及家人信息，特别是飞机票、火车票等，这类票据的二维码或条形码包含您详细的个人信息。

故事10

集团信息安全月小故事第十期：个人电脑使用安全

我是小秦，在修电脑，第二次了。

流年不利啊，昨天手机中毒，今天电脑中毒。还是大名鼎鼎的wanncry病毒。我辛辛苦苦下的动画片啊，都被加密了：（：（：（

为了不卡，偷懒没打补丁，尝到后果了啊。

哎，我得把这些电脑使用注意事项再看一遍

[http://anquan..com/video.html](http://anquan.100tal.com/video.html)

配图：电脑安全



内容d:电脑安全使用

个人PC安全使用：

一、及时更新操作系统和打补丁，永恒之蓝病毒泛滥就是不打补丁导致的；

二、安装并开机启动安全管理软件，定期进行病毒扫描，清理系统垃圾；

三、勿随意下载、接受运行可执行程序，因为这很可能就是一个病毒；

四、设置系统显示所有文件列表、文件的后缀名，辨别文件类型，不被图标迷惑；

五、不随便删除系统文件，不轻信网上各种系统加速的攻略；

六、不开远程桌面服务，也不使用远程软件如VNC，teamview等；

七、设置操作系统登录密码，设置强口令并定期更换；

八、离开电脑时用win+l键锁屏，现在练几下就能记住；

九、使用移动介质传输资料时，务必开启安全软件并扫描病毒后再打开使用；

十、无法确认对方身份时不接受远程协助操作自己电脑。

故事11

集团信息安全月小故事第十一期：安全开发

大家好，我是前面的开发。

已经晚上12点了，而我还在加班

话说今天测试服务器流量有些异常，我以为被黑了，就让安全团队帮忙查了查。

结果到最后查到我自己身上来了。什么问题呢？

查出来是一个未知IP在疯狂调用我的接口，1GB共600W的随机生成的测试数据被查询走了200多万条。

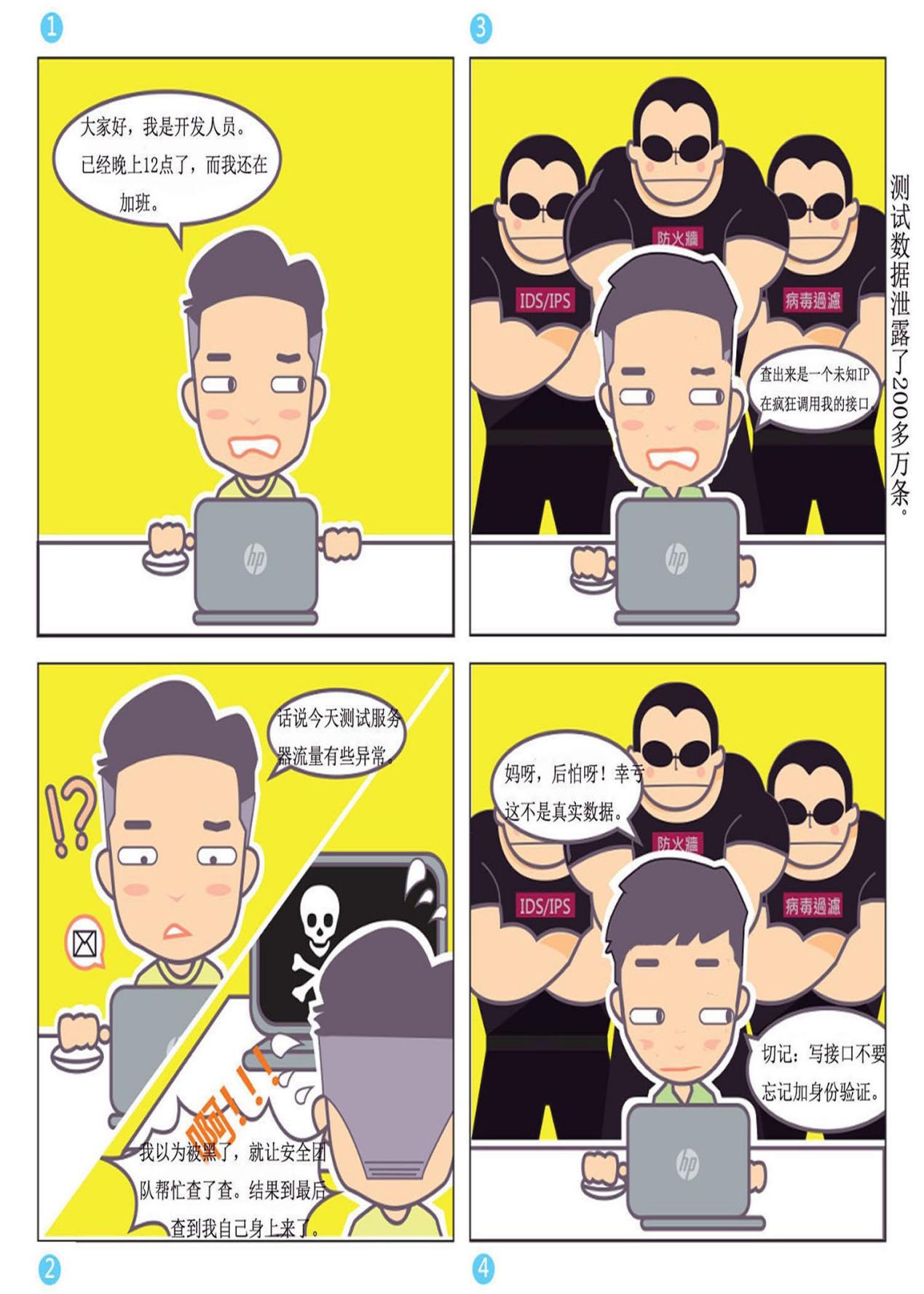
妈呀，后怕呀，这要是真实数据，照网络安全法规定，够我进去4000回了。

原因啊？我TM写接口忘了加身份验证了，导致任何人都能调用。

伙伴们，赶紧来看看吧。开发过程中这么多安全坑，我是一个也不想踩了的。

快戳[http://anquan..com/video.html](http://anquan.100tal.com/video.html)

配图：数据泄露



内容：开发注意安全事项/

一、SQL注入

漏洞表现：注入拖库。

防御方法：使用预编译的查询方式。

二、XSS漏洞

漏洞表现：盗取登陆凭证。

防御方法：对输入进行验证，对输出进行正确转义。

三、身份认证及会话管理漏洞

漏洞表现：越权及身份复用。

防御方法：身份认证体系完善，全局应用。

四、不安全的加密和存储

漏洞表现：简单加密存储。

防御方法：MD5或SHA1加盐。

五、不安全的对象直接引用

漏洞表现：任意文件下载，命令执行。

漏洞防御：校验文件引用。

六、CSRF漏洞

漏洞表现：点击链接之后执行非自愿操作。

漏洞防御：功能使用双因素校验，校验token以及cookie。

七、未验证的转发及重定向 漏洞表现：SSRF漏洞，内网探测。

漏洞防御：验证请求地址。

八、文件上传

漏洞表现：上传恶意文件，网络木马。

漏洞防御：校验上传文件。

九、XXE注入

漏洞表现：XML注入。

漏洞防御：验证输入过滤特殊字符。

开发指南：详情请看http://ops..com 安全开发指南，Java和PHP都有哦。

故事12：

文档打印安全

我是小秦

我摊上大事了

昨天加班做的竞标文档，今天来竞标，本来信心满满，结果竞争对手的标书跟我们一样，还比我们优惠？！！！

见鬼了啊！

等等，难道是这样？？！

我是昨天加班打印的文档，点了打印就走了。今天取文档的时候发现有被动过的痕迹。我以为是同事路过蹭的就没在意，难不成是有人偷拍了照片？

赶紧回去查录像！

果然是这样，凌晨一穿着清洁工衣服的人把文档一页一页的都拍了照！

对我的处罚是免不了的了

但是你还有机会

只要你认真来看看[http://anquan..com/video.html](http://anquan.100tal.com/video.html)

配图：文档打印安全



内容：机密文档保护

一、打印机密文档时要在打印完成时及时取走；

二、打印过程中如果出现打印机损坏的情况，要先清除打印队列再保修；

三、使用复印机复印机密文件时要记得取走原文件；

四、机密文档要妥善保管，如档案资料归档后及时放入带锁的柜子中，妥善保管钥匙，避免资料外泄；

五、废弃的机密文档要完全粉碎之后才可以丢弃；

六、打印机在打印文件时会给文件添加隐藏信息，其可用于取证和溯源。

故事13：

集团信息安全月小故事第十三期：信息安全规定二

我是小秦。

我被炒了。

大佬跟我要这次活动所有的稿子。

我想都没想就把所有东西打了个包传网盘分享给他了。

他想都没想就告诉我收拾东西回家吧，我被炒了。

我一脸懵逼的问老大什么情况。

老大跟我说大佬很反感把工作文件传网盘。

这些事情在安全规定都有啊！

所以大佬很生气，后果很严重。

所以工作必看，不看可能被辞退！！！

http://anquan..com/video.html

配图：



信息安全部分规定

一、邮件使用：带附件的邮件在打开前，必须进行安全扫描并与发送方确认发送内容；

二、即时通讯软件使用：接收的文件在打开前，须进行安全扫描并与发送方确认内容；

三、外部信息平台使用：禁止在外部平台泄露公司资料、开会记录、内部敏感信息等，外部平台指网盘，论坛，社交平台，文库等；

四、下载软件使用：从网上下载或从移动介质拷贝的文件在打开之前须进行安全扫描。

故事14

集团信息安全月小故事第十四期：商业机密

我是小秦

昨天做个梦，我被炒了，太可怕了。

可能跟今天要去的地方有关系。

今天是法院宣判的日子，看看上次偷窃我的标书的人判几年。

据说这人是专门假扮清洁工，到处偷窃文档，然后找买家卖的。也接受订单，到指定的地方盗窃。

判决结果出来了。

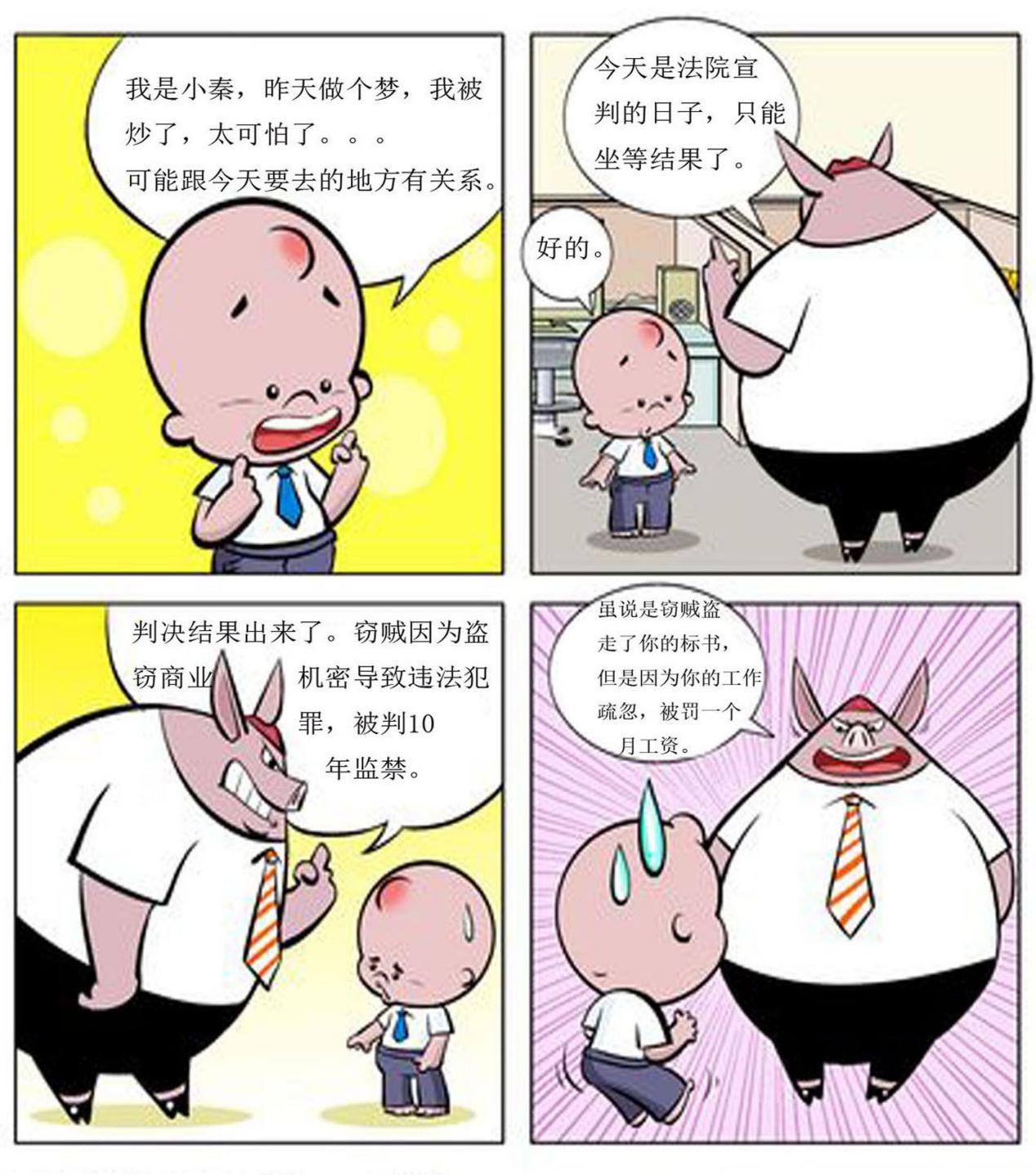
窃贼因为盗窃商业机涉嫌违法犯罪，被判10年监禁。

我因为工作疏忽，被罚一个月工资。

所以，快来看看集团的商业机密规定吧

[http://anquan..com/video.html](http://anquan.100tal.com/video.html)

配图



**知识产权和保密原则**

**一、员工在履行员工义务的过程中或在公司工作过程中，主要通过使用公司资产或资源开发的所有发明、创造性作品、计算机软件和技术或商业秘密均视为公司财产；**

**二、员工必须就公司或其客户或委托的任何信息保密，授权披露或法律强制披露的信息除外。保密信息包括一经披露，对竞争对手有利的、或对公司或其客户不利的所有非公开信息；**

**三、公司主张严格的保密原则。在员工与公司的雇佣关系期间，员工须遵守任何和所有有关保密原则的书面或口头规定和政策，须履行适用于员工的与保密原则相关的职责和义务。；**

**四、除履行与员工在公司职位相关的义务外，未经公司的事先许可，员工不得披露、宣布或公布公司的商业秘密或任何保密的商业信息。员工还不得在公司之外的工作中使用该类机密资料。；**

**五、即使在工作环境之外，员工必须保持警觉，不得泄露与公司或其商业、客户或员工相关的重要信息；**

**六、员工就公司的保密信息进行保密的职责须持续到员工与公司的雇佣关系终止后，直至公司公开披露该信息或在非员工的过错的情况下，这些信息因其他原因为公众所知；**

**七、在终止雇佣关系时或在公司要求的其他时候，员工必须将包含保密信息的所有资料交还给公司，不得留有备份。**

**职业准则详见：http://www..com/company/careernorm/。**

故事15

集团信息安全月小故事第十五期：智能设备安全问题

昨天庭审回来之后，我想起个事。

那天我们会来查录像的时候，是老师直接进到一个页面操作的。

那IP地址，我还记得！！

马上到家了，在家看看能不能打开。

哇，这个地址可以直接访问啊。还没有密码。这问题很大啊。

现在智能设备的安全问题也越来越多了。

现在生活当中用到的智能设备也越来越多，你的iwatch，手环，智能家居，摄像头等都属于智能设备。

这些智能设备的使用需要注意哪些事项才能避免信息泄露呢？

快来[http://anquan..com/video.html](http://anquan.100tal.com/video.html)



智能设备安全风险表现及危害

一、IOT设备隐私泄露或滥用风险：

此类风险的危害案例有婴儿监护器，监控摄像头 的信息泄露。

二、IOT设备弱口令或者默认口令：

现在就有针对这一风险开发（IOT）物联网病毒，用于DDOS攻击互联网基础设备，造成网络服务的拥堵或宕机，还有进一步引发的信息泄露危害。

三、IOT设备与互联网或局域网的通讯没有加密：

其中最恶劣的案例是使用pos机恶意盗刷银行卡，再有就是智能车锁的破解。两者都是因为通信未加密，被截取之后可以构造恶意数据进行攻击。

四、IOT设备的web 界面存在安全漏洞： 传统安全漏洞的权限绕过、拒绝服务、跨站、命令执行、缓冲区溢出、 SQL注入、设计缺陷等问题。

防范措施：

一、启用设备的安全设置。例如口令设置，黑白名单设置；

二、注意设备使用说明，正确使用安全功能；

三、设备要经常更新升级。厂商修复漏洞会通过更新修复；

四、注意监控摄像头的安装位置，保护隐私；

五、注意设备使用场景，尽量不连接外网；

六、注意路由器安全使用，保护好智能设备第一道锁；

七、匿名使用智能设备，保护隐私。

故事16

本次集团信息安全月活动，旨在提高集团所有老师的信息安全意识，当然是希望集团所有老师都能参与进来。

小故事也是这个背景下的产物，为了吸引老师访问我们的页面，为了老师推广起来不至于无聊，为了一些乐趣与梗，做了一点微小的工作。

小故事的场景也是与我们贴的海报（安全意识页面的图片）、发的宣传手册互相联系的。从几个不同的视角概括现代信息安全事件的危害以及我们每个人可以做的防护措施。

这世界上没有神仙

一个陌生人不可能对我的生平了如指掌

直到我听过见过甚至亲身经历过

直到一个清华教授刚卖完房就被骗走了1760万房款

直到徐玉玉的悲剧

我才明白，在这个时代，没有秘密

所以，我学会了自我保护，学会了火眼金睛，学会了残血反杀，学会了讲故事

在XXX的XXXXX分享，你来，我讲给你听，保证精彩。