

2010 年中国企业员工信息安全意识 调查报告

北京谷安天下科技有限公司



目录

第一章	调查活动介绍.....	5
一.	调查活动背景.....	5
二.	调查方法说明.....	5
三.	报告概述及摘要.....	6
第二章	个人及公司物品保护意识.....	8
一.	胸卡.....	8
二.	物品保管意识.....	9
第三章	物理环境安全意识.....	9
一.	办公地点紧急通道.....	9
二.	出差.....	10
三.	办公区域陌生访客.....	10
四.	关门.....	10
第四章	个人信息、密码的保护意识.....	11
一.	个人信息保护意识.....	11
二.	个人密码保护意识.....	12
第五章	数据安全意识.....	15
一.	数据备份.....	15
二.	敏感数据分类与加密.....	16
三.	工作资料.....	16
四.	移动介质外借.....	17
一、	社会工程意识.....	17
一.	不明邮件.....	17
二.	熟悉发件人发出的自动播放附件和内嵌网页.....	18
一、	终端安全意识.....	19
一.	屏保设置及密码.....	19
二.	系统升级.....	19
三.	杀毒.....	20
四.	防火墙.....	20
二、	上网安全.....	21
一.	网银.....	21
二.	下载.....	22
三.	弹出链接.....	23
四.	恶意插件、病毒的攻击.....	23
三、	对安全意识教育、信息安全的认知.....	24
一.	信息安全培训频度.....	24
二.	对企业信息安全隐患的认知.....	25
三.	有效保护信息安全面临的最大障碍的认知.....	25
四、	问题与建议总结.....	26

图表目录

图表 1 受访者保管工作胸卡情况统计	8
图表 2 受访者抽屉中物品保管情况统计	9
图表 3 受访者对办公地点紧急通道情况统计	9
图表 4 受访者是否主动了解出差安全环境的统计	10
图表 5 受访者对陌生访客认知的情况统计	10
图表 6 受访者在办公区域随手关门情况的统计	11
图表 7 受访者网上发布信息情况统计	11
图表 8 受访者使用即时通讯工具情况统计	12
图表 9 受访者电脑是否设置密码情况统计	12
图表 10 受访者密码设置情况统计	13
图表 11 受访者是否会在手机中保存含有密码的短信情况统计	13
图表 12 电脑日常工作应用软件使用排名统计	14
图表 13 受访者电脑中应用系统设置密码情况的统计	14
图表 14 受访者个人应用的密码使用情况统计	15
图表 15 受访者定期更换密码情况的统计	15
图表 16 受访者电脑数据备份情况统计	16
图表 17 受访者电脑敏感数据保护情况统计	16
图表 18 受访者资料外借情况统计	17
图表 19 受访者移动介质外借情况统计	17
图表 20 受访者处理不明邮件情况调查	18
图表 21 受访者对熟人发出邮件中自动播放附件和内嵌网页处理情况统计	18
图表 22 受访者屏保和密码设置情况统计	19
图表 23 受访者电脑系统升级情况统计	20
图表 24 受访者杀毒软件安装与升级情况统计	20
图表 25 受访者防火墙设置情况统计	21
图表 26 受访者使用网银情况统计	21
图表 27 受访者下载软件情况统计	22
图表 28 受访者下载途径统计	22
图表 29 受访者下载软件操作情况统计	23
图表 30 受访者对网页弹出链接处理情况统计	23
图表 31 受访者受病毒攻击的情况统计	23
图表 32 受病毒攻击受访者具体情况统计	24
图表 33 受访者接受信息安全培训情况统计	24
图表 34 受过信息安全培训受访者详情统计	25

图表 35 受访者信息安全隐患认知情况 25

图表 36 受访者对有效保护信息安全面临的障碍的认知情况 26

第一章 调查活动介绍

一. 调查活动背景

信息作为一种资产，是企业或组织进行正常商务运作和管理不可或缺的资源，也是企业财产和个人隐私等的重要载体。与此同时，信息安全的重要性也越加凸显：从最高层次来讲，信息安全关系到国家的安全；对组织机构来说，信息安全关系到正常运作和持续发展；就个人而言，信息安全是保护个人隐私和财产的必然要求。无论是个人、组织还是国家，保持关键的信息资产的安全性都是非常重要的。

对于企业而言，信息安全保障的第一道防线是人员的信息安全意识。但现实情况是，为企业带来无法挽回的经济损失的，恰恰是由于企业员工信息安全意识薄弱导致的信息安全事件。因此，进行中国企业员工信息安全意识调查，掌握我国企业员工信息安全意识现状，对普及企业员工信息安全知识，提高企业员工信息安全防范意识具有重要意义。

本次调查活动以问卷调查和网络在线调查为基本形式，问卷题目范围涉及当前中国企业员工信息安全意识认知及相关应用情况。希望统计结果能够为中国各企业提供详实可靠的参考数据，并通过对调查结果的推广，增强企业员工对信息安全意识的重视，提高企业员工信息安全意识水平。

基于取得的有效调查数据样本，报告主要对 2010 年中国企业员工信息安全意识状况进行解读，包括企业员工个人及企业物品保护意识、物理环境安全意识、个人信息与密码的保护意识、数据安全意识、社会工程意识、终端安全意识、上网安全意识、信息安全教育情况等。

本次调查活动网络在线调查部分，由华安信达信息安全专业论坛和信息安全专业网络社区安帮网联合主办。

二. 调查方法说明

（一） 调查方法

本次调查采用问卷调查和网络在线调查两种方式。其中本报告中相关数据成果主要来自这两种调查方式的有效问卷。

（二） 在线调查方法说明

1. 调查时间

本次调查时间为：2010 年 12 月 08 日至 12 月 30 日

2. 样本分布

调查的样本目标是中国大陆（除港、澳、台三地）公民，共得到有效数据样本 1636 个

三. 报告概述及摘要

调查问卷题目设计围绕企业员工个人及企业物品保护意识、物理环境安全意识、个人信息与密码的保护意识、数据安全意识、社会工程意识、终端安全意识、上网安全意识、信息安全教育等涉及个人信息安全意识的几大主要主题展开。

通过对有效调查问卷的分析与统计，发现受访者在物理环境安全意识中的了解办公地点的紧急通道、随手关门、个人信息、密码的保护意识中的电脑设置密码，数据安全意识中的 U 盘外借前做安全操作，终端安全意识中的安装杀毒软件和防火墙设置为开启状态，上网安全意识中的下载软件、正确的下载软件途径以及对下载软件的安全操作等方面做的较好；

而受访者在个人及公司物品保护意识中的工作胸卡保管、物品保管；物理环境安全意识中的出差物理环境安全、工作区域的陌生访客；个人信息、密码的保护意识中的个人信息网上发布、个人密码保护；数据安全意识中的数据备份、敏感数据保护、工作资料保护；社会意识中的不明邮件、熟悉发件人发的链接和动画处理方式；终端安全意识中的电脑设置屏保和密码以及系统升级；上网安全中的网银使用、网页弹出的链接处理等方面做的相对较差，受访者在这些方面的安全意识普遍较低。例如绝大多数的受访者会在日常应用、办公应用、电脑等设置密码，但是在设置正确的密码、密码的正确使用、密码的保存与更换方面大多数人存在诸多问题。

由于受访者普遍信息安全意识的薄弱，平时的办公与生活中较多错误的信息安全操作，导致超过半数（58.8%）的受访者遇到过 1、2 次或者经常遇到恶意插件和病毒的攻击，并有所损失。

调查结果还显示，在受访者信息安全意识普遍薄弱的情况下，而提高信息安全意识的培训和宣贯等工作却做的很少。接受定期的信息安全培训受访者仅占 15.8%。

同时，受访者在信息安全隐患的认知和有效保护信息安全面临的障碍的认知方面，42.8%的受访者认为所有的安全隐患中，个人信息安全意识不足是最大的安全隐患，然后依

次是没有安全制度或制度未落实、投入或人员不足或缺乏信息安全培训、安全产品功能不足和其他。而对于目前有效保护信息安全面临的最大的障碍，受访者认为最大的障碍是普遍缺乏信息安全意识，其他依次是管理水平落后、技术不过关、法律不健全、信息安全人才不够和其他障碍。

20 大显著问题：

1、67.9%的受访者采取的是不锁抽屉、不锁抽屉钥匙放在抽屉里和锁抽屉但钥匙放在桌上或笔筒等地方这些不安全的物品保管行为，仅有 32.1%的受访者采用锁抽屉并随身携带钥匙的物品保管安全行为。

2、拥有胸卡的受访者中，接近半数的人曾经外借过自己的胸卡。

3、在去陌生环境出差的情况下，仅有 38.9%的受访者会去主动了解自己工作或居住场所的紧急通道位置或楼层结构图，61.1%的受访者都选择不会主动了解。

4、调查结果显示，仅有 30.7%的受访者选择了会主动询问到自己办公区来的陌生访客；52.1%的受访者选择在看情况，不忙的时候询问，忙的时候就不问；17.2%的受访者选择从来不问。

5、95.3%的受访者曾经将自己的个人信息发布在网上；公布最多的是姓名、性别、年龄等个人基本信息，其次是网络联系方式、电话号码、证件号码、联系地址、照片和工作信息。

6、针对日常办公的应用，仅有 14.5%的受访者设置的密码都不一样，还有 14.8%的人所有密码完全一样。

7、对于银行卡账户、邮箱、QQ 等涉及个人信息安全的服务的密码设置，43%的受访者选择的是大部分相同或相似，选择少部分相同或相似的占 24.8%，选择都不一样的占 25.4%，选择完全一样的占 6.8%。

8、58.6%的受访者半年以上更换一次密码，或者从不更换密码。

9、所有受访者中，仅有 26.4%的人会定期给电脑做备份，不做备份和不定期做备份的比例共为 73.6%。

10、接近半数的受访者对敏感数据没有进行安全的分类和加密操作。

11、如果遇到与工作无关但关系要好的同事要工作资料，94.4%的受访者会根据情况的不同，最终还是选择给同事。

12、面对内容吸引人的不明邮件，42.5%的受访者会看邮件内容。

13、所有受访者中，当收到熟悉发件人发送的自动播放 flash 动画或邮件内部嵌入的网页时，69%的人会看动画、下载动画、浏览网页或点击网页链接。

14、仅有 38.0%的受访者为自己的电脑设置了屏保和密码。

15、仅有 36.4%的受访者知道如何做且定期做升级。

16、受访者中有 76.8%的人使用网银，而使用网银的受访者中，有 39.7%的受访者在使用网银时不使用 U 盾。

17、76.8%的受访者会经常下载软件，其中有 13.7%的人会到任意的网站上下载好玩的软件，还有 26.9%的人会直接打开或使用的下载软件。

18、47.1%的受访者会点击网页上吸引自己的链接。

19、确定电脑从来没遇到过恶意插件、病毒的攻击的人数比例仅占 19.6%，58.8%的受访者遇到过 1、2 次或者经常遇到并遭受损失。

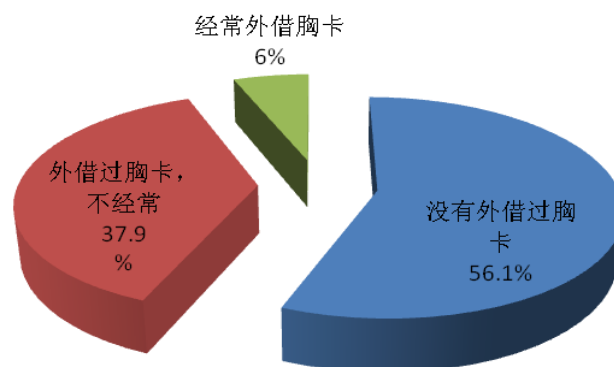
20、仅有 15.8%的受访者会接受定期的信息安全培训，25.2%的受访者是在入职时接受过信息安全培训，而 59.0%的受访者从来没有接受过或接受不定期的信息安全培训。

第二章 个人及公司物品保护意识

一. 胸卡

现在，越来越多的企业由于形象统一、员工身份识别等需要，为员工配备胸卡。但同时，胸卡作为企业员工的一个识别标志之一，也成为很多信息窃取者借助的工具。

调查结果显示，所有受访者当中，77.5%的受访者有胸卡；而拥有胸卡的受访者中，曾经借过胸卡给同事的比重达到了 37.9%，经常外借胸卡的比重占 6%，因此，拥有胸卡的受访者中，接近半数的人曾经外借过自己的胸卡。

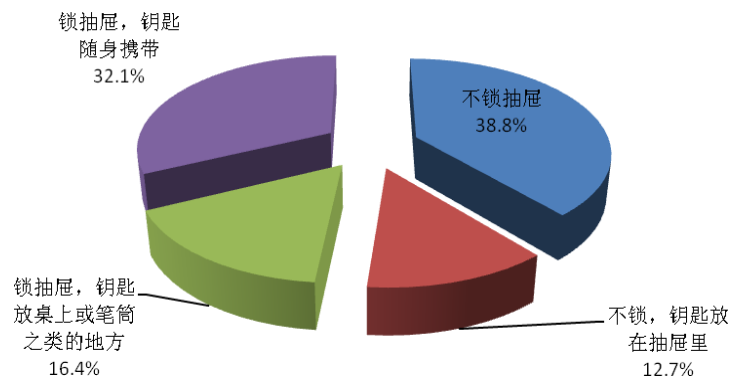


图表 1 受访者保管工作胸卡情况统计

二. 物品保管意识

抽屉是放置资料的一个普遍、常用地点，但是越普遍和常用的资料保管方式，其安全性反而越被疏忽。

调查结果显示，67.9%的受访者采取的是不锁抽屉、不锁抽屉钥匙放在抽屉里和所抽屉但钥匙放在桌上或笔筒等地方这些不安全的抽屉物品保管行为，仅有 32.1%的受访者采用锁抽屉并随身携带钥匙的抽屉物品保管安全行为。

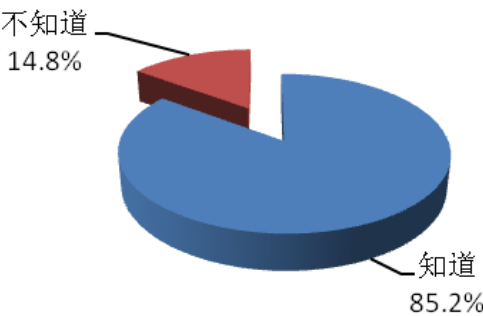


图表 2 受访者抽屉中物品保管情况统计

第三章 物理环境安全意识

一. 办公地点紧急通道

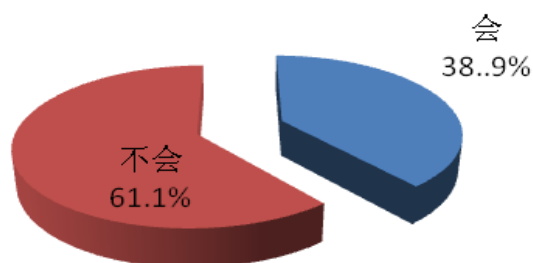
调查结果显示，85.2%的受访者知道自己所在的办公场所紧急通道的位置，仅有 14.8%的受访者选择了不知道。该项目显示了大多数受访者对自己熟悉环境的紧急通道情况还是比较了解的。



图表 33 受访者对办公地点紧急通道情况统计

二. 出差

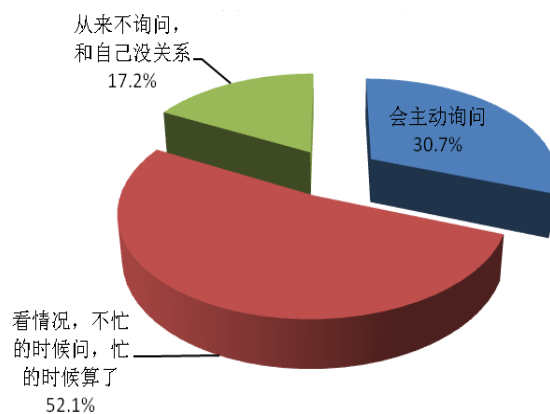
在去陌生环境出差的情况下，仅有 38.9%的受访者会去主动了解自己工作或居住场所的紧急通道位置或楼层结构图，61.1%的受访者都选择不会主动了解。



图表 4 4 受访者是否主动了解出差安全环境的统计

三. 办公区域陌生访客

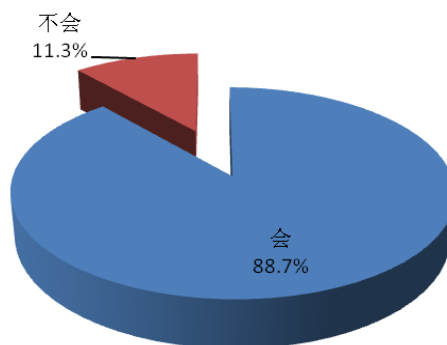
调查结果显示，仅有 30.7%的受访者选择了会主动询问到自己办公区来的陌生访客；52.1%的受访者选择在看情况，不忙的时候询问，忙的时候就不问；17.2%的受访者选择从来不问。



图表 5 受访者对陌生访客认知的情况统计

四. 关门

办公区域内，不明人员尾随，随手拿走信息资料的情况都是利用办公人员不关门这一漏洞。针对该情况，调查结果显示，平时在办公区域内不随手关门受访者的比例为 11.3%。



图表 6 受访者在办公区域随手关门情况的统计

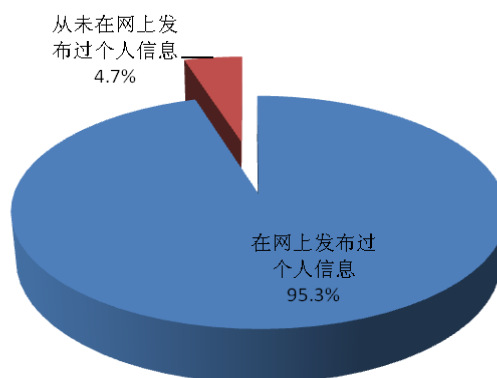
第四章 个人信息、密码的保护意识

一. 个人信息保护意识

（一）个人信息发布

随着网络应用的快速发展，很多网站会要求网民进行注册，要求网民提交个人相关信息和资料，例如姓名、性别、年龄等个人基本信息，或者证件号码、电话号码、地址、联系方式等其他个人信息。那么，当前网民对网上填写个人真实信息的安全认知情况如何？

调查显示，95.3%的受访者曾经将自己的个人信息发布在网上，仅有 4.7%的受访者从未在网上公布过个人信息。

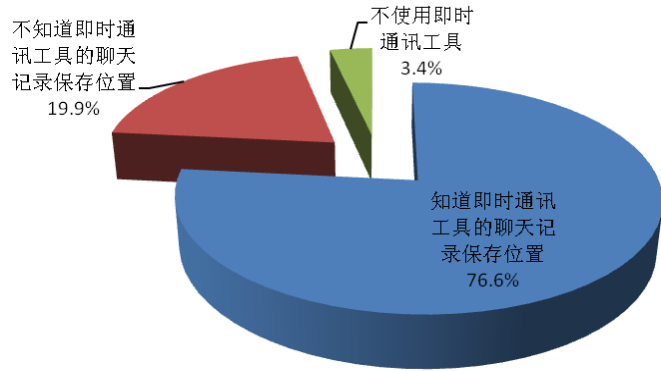


图表 7 受访者网上发布信息情况统计

（二）即时通讯工具聊天记录信息保存意识

现在，越来越多的网民会使用 QQ、MSN 等即时通讯工具办公或者联络家人、朋友。但是，即时通讯工具在给我们带来工作、生活便利的同时，也带来很多的信息泄露风险。

调查显示，受访者中平时上网不使用即时通讯工具仅占 3.4%，96.6%的受访者平时上网使用即时通讯工具，而 76.6%的人知道聊天记录保存位置。



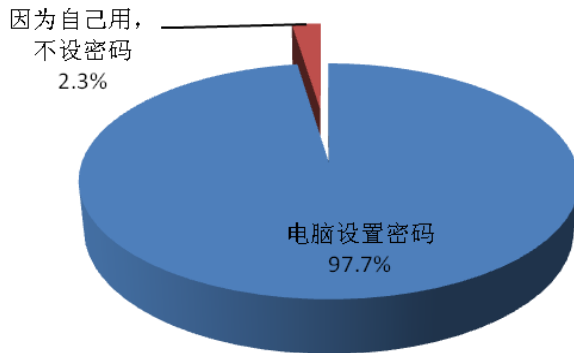
图表 8 受访者使用即时通讯工具情况统计

二. 个人密码保护意识

（一）密码设置

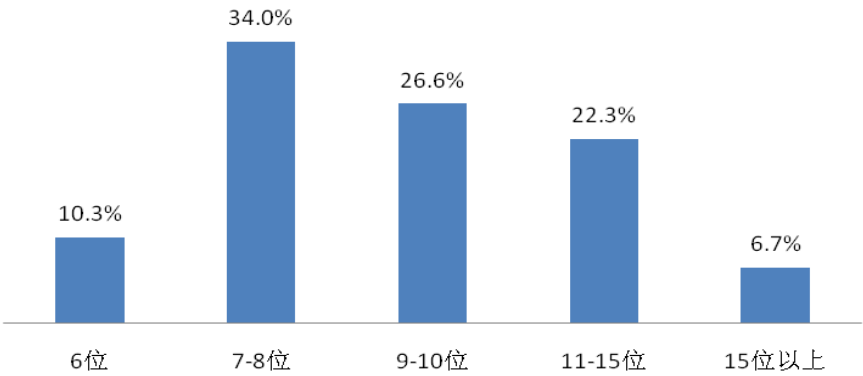
用户名+密码是最简单最常用的身份认证方式，密码与个人私密信息息息相关，而针对密码的攻击简单易行，所以正确使用设置、使用密码显得尤为重要。

所有受访者中，平时为使用的电脑终端设置密码的受访者占 97.7%，有 2.3%的受访者不设密码。



图表 9 受访者电脑是否设置密码情况统计

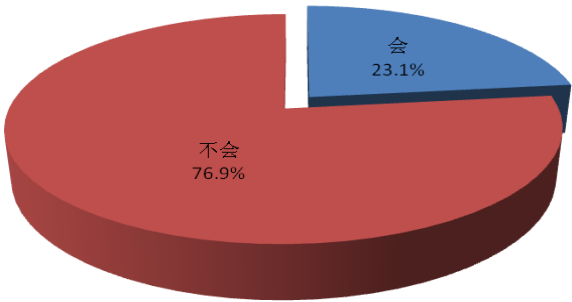
平时使用电脑终端设置密码的受访者中，密码位数设置在 7-8 位的所占比重最大，为 34%，以下依次为密码 9-10 位占 26.6%，11-15 位占 22.3%，6 位占 10.3%和 15 位以上占 6.7%。



图表 10 受访者密码设置情况统计

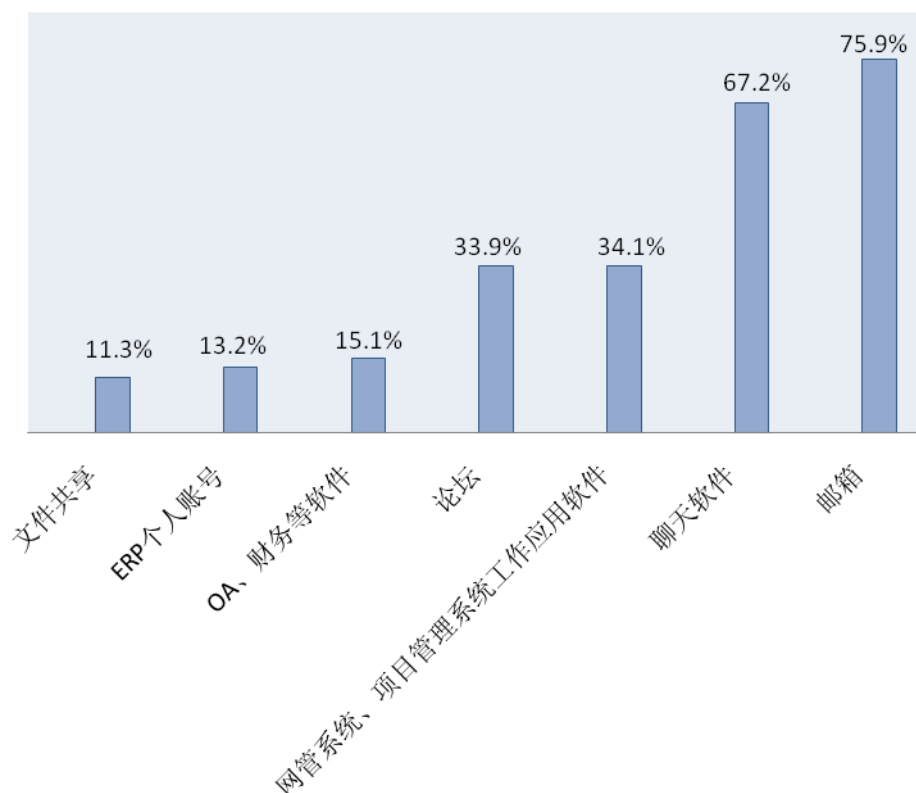
(二) 个人密码使用情况

密码除了设置时要遵守一些安全规则以外，密码的保存也有一些不安全的做法需要避免，例如将密码记在纸上、手机中等等。调查结果显示，还有 23.1%的人会在手机中保存含有密码的短信。



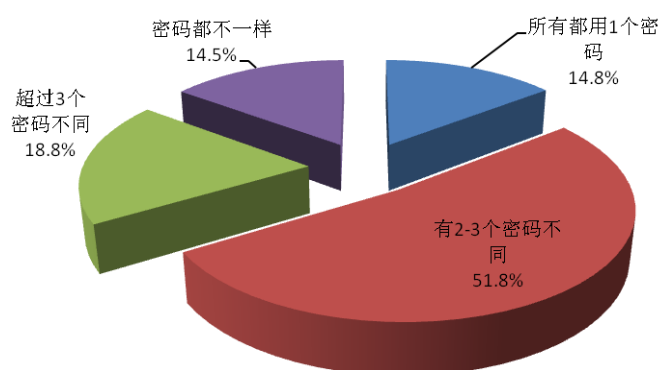
图表 5 受访者是否会在手机中保存含有密码的短信情况统计

目前，人们用电脑进行日常工作常用到的应用软件有：聊天软件、邮箱、论坛、网管系统、项目管理系统等工作应用软件、OA\财务等软件、ERP 账号等，调查结果显示，在个人电脑终端上安装最多的用于办公的软件是邮箱，占到 75.9%的比例；其次是聊天软件，占到 67.2%的比例，然后依次是网管系统、项目管理系统等工作应用软件（34.1%）、论坛（33.9%）、OA、财务等软件（15.1%）、ERP 个人账号（13.2%）和文件共享（11.3%）。



图表 6 电脑日常工作应用软件使用排名统计

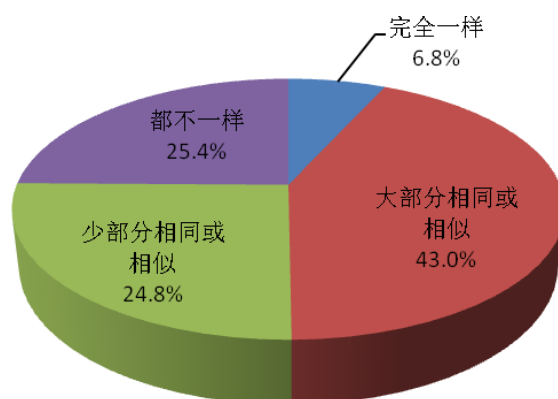
针对以上所调查的 7 种常用于日常办公的应用，仅有 14.5% 的受访者密码都不一样。51.8% 的人选择了有 2-3 个密码不同，18.8% 的人有超过 3 个密码不同，还有 14.8% 的人所有密码完全一样。同时，针对不同职位的工作人员和不同地区、不同年龄阶段的受访者做出统计，都是占选择 2-3 个密码不同的比例最大。



图表 13 受访者电脑中应用系统设置密码情况的统计

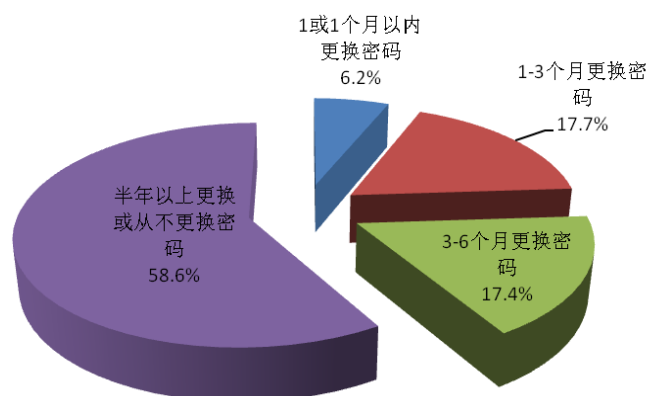
银行卡账户、邮箱、QQ 等涉及个人信息安全的服务都会涉及到使用密码的问题，密码保护安全的做法是不同的场所和应用使用不同的密码。调查结果显示，受访者平时个人常用服务的密码设置，43% 的受访者选择的是大部分相同或相似，少部分相同或相似的占 24.8%，

都不一样的占 25.4%，完全一样的占 6.8%。



图表 14 受访者个人应用的密码使用情况统计

定期更换密码是保护密码的有效途径，更换密码时间至少为 3 个月一次。调查结果显示，58.6%的受访者半年以上更换一次密码，或者从不更换密码。17.4%的受访者 3-6 个月更换一次密码；17.7%受访者 1-3 个月更换一次密码；仅有 6.2%的受访者选择 1 或 1 个月以内更换密码。



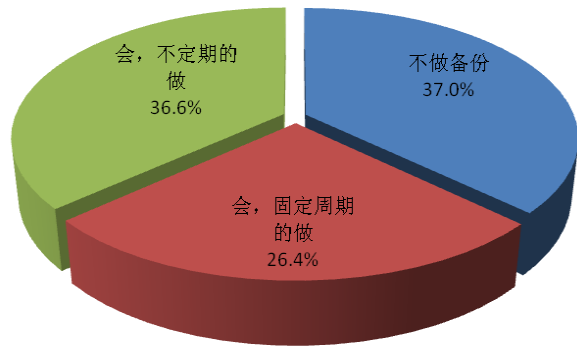
图表 15 受访者定期更换密码情况的统计

第五章 数据安全意识

一. 数据备份

电脑中的数据承载巨大的价值，如果丢失或被窃取、篡改，将承受巨大的时间、金钱和精神上的损失。因为电脑数据定期备份至关重要。

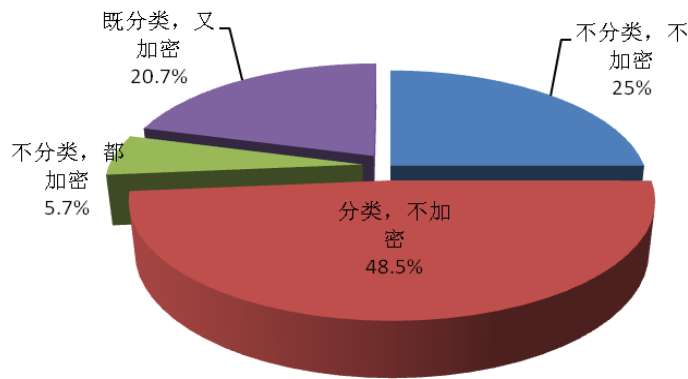
所有受访者中，仅有 26.4%的人 would 定期给电脑做备份，不做备份的比例达到了 37.0%，不定期做备份的比例为 36.6%。



图表 16 受访者电脑数据备份情况统计

二. 敏感数据分类与加密

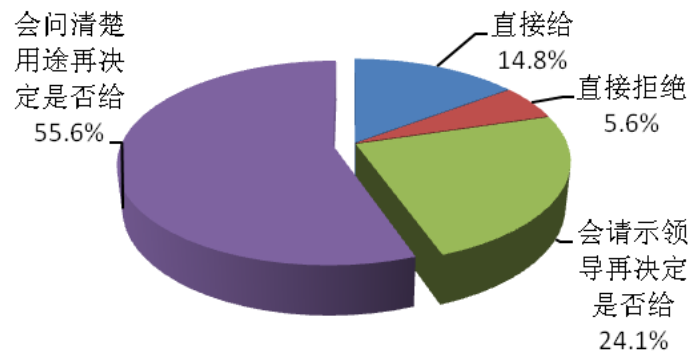
电脑中敏感数据需进行分类与加密进行保护。调查结果显示，接近半数的人选择对敏感数据分类不加密，占到48.5%的比例；有25%的人选择对敏感数据不分类不加密；仅有20.7%的对敏感数据既分类又加密；5.7%的人选择对敏感数据不分类，但是都会加密。



图表 17 受访者电脑敏感数据保护情况统计

三. 工作资料

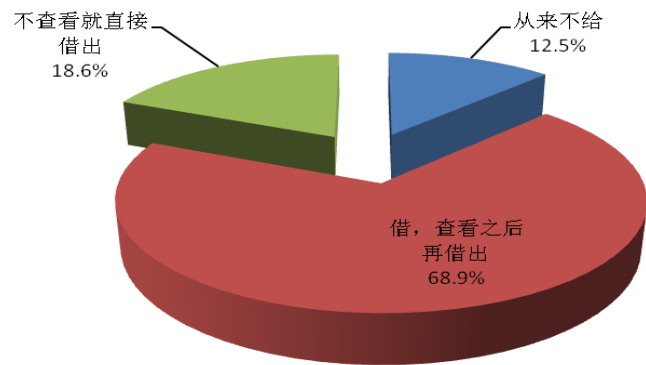
调查结果显示，如果遇到关系好的同事要资料，94.4%的受访者会根据情况的不同，最终还是选择给同事；其中14.8%的受访者是直接给，55.6%的受访者会自己问清楚用途再决定是否给；24.1%的受访者会请示领导后再决定是否给；5.6%的受访者会直接拒绝。



图表 18 受访者资料外借情况统计

四. 移动介质外借

移动介质使用方便，但同时，移动介质是病毒传播的常用途径，也是不法分子盗取数据的便捷工具。调查结果显示，平时使用 U 盘的受访者中，12.5%的受访者从来不外借 U 盘，而 18.6%的人会不查看就直接借出；68.9%的受访者会在查看之后再借出 U 盘。



图表 19 受访者移动介质外借情况统计

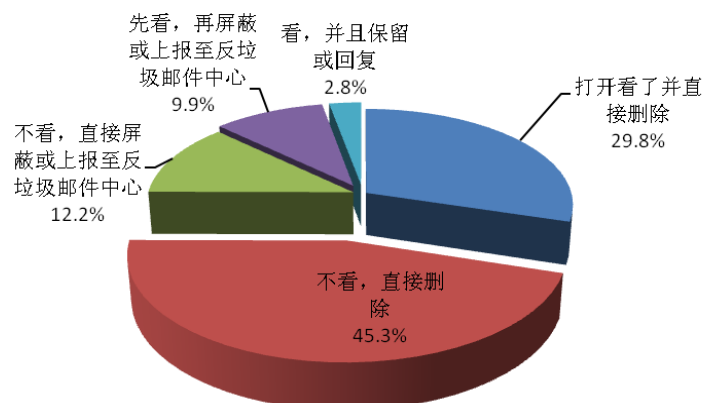
一、 社会工程意识

一. 不明邮件

现在，网民们经常能够收到来自不熟悉的发件人，但主题内容很吸引人，令人感兴趣的邮件，比如明星新闻，商品打折，高中考大学等。

面对这样的邮件，45.3%的受访者会不看，直接删除；12.2%的受访者会不看内容，直接屏蔽或上报至反垃圾邮件中心；其中 42.5%的受访者会看邮件内容，不过看后会有不同

的选择，29.8%的人会打开看后直接删除；9.9%的人会先看，再屏蔽或上报至反垃圾邮件中心；仅有 2.8%的受访者会看并且保留或回复邮件。

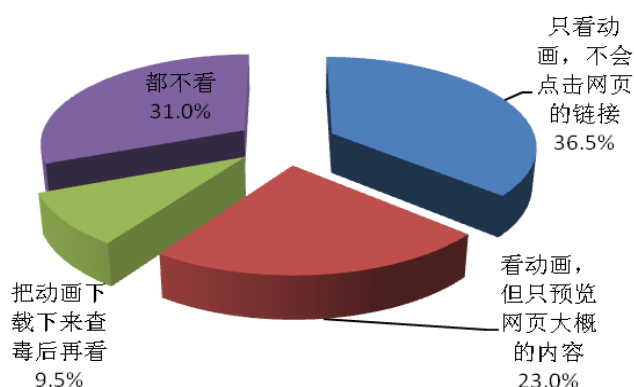


图表 20 受访者处理不明邮件情况调查

二. 熟悉发件人发出的自动播放附件和内嵌网页

附件很容易感染病毒，所以打开附件前应先进行病毒扫描。而熟悉的发件人很容易让收件人放松警惕，忘记对收到的附件进行扫描。

调查结果显示，所有受访者中，当收到熟悉发件人发送的自动播放 flash 动画或邮件内部嵌入的网页时，9.5%的人会把动画下载下来查毒后再查看；23%的人 would 看动画，但只预览网页的大概内容；还有 36.5%的人 would 看动画，但不会点击网页的链接；31%的人选择都不会看。

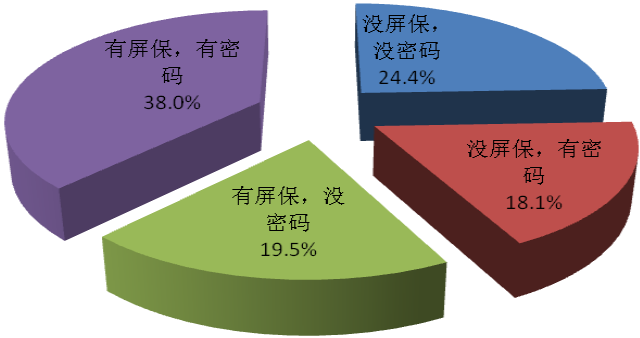


图表 21 受访者对熟人发出邮件中自动播放附件和内嵌网页处理情况统计

一. 终端安全意识

一. 屏保设置及密码

为电脑终端设置屏幕保护和密码是保护电脑终端信息安全一项重要措施。调查结果显示，仅有 38.0%的受访者为自己的电脑终端同时设了屏保和密码；还有 24.4%的受访者电脑终端既没屏保也没密码；19.5%的受访者电脑终端有屏保、没密码；18.1%的受访者电脑终端有密码、没屏保。



图表 22 受访者屏保和密码设置情况统计

二. 系统升级

很多病毒、蠕虫和黑客攻击，都是利用系统漏洞这一点攻击和破坏计算机系统。所以为了保护我们的计算机安全，最根本的问题就是不能让不法分子有机可乘，确保我们的系统及时安装了最新的补丁并做更新，是计算机安全防护的一项重要保障。

有 12.9%的受访者不知道如何做升级且不做升级；22.1%的受访者自己不知道如何做升级，找人做升级；28.5%的受访者知道如何做升级，但想起来才做升级；36.5%的受访者知道如何做且定期做升级。

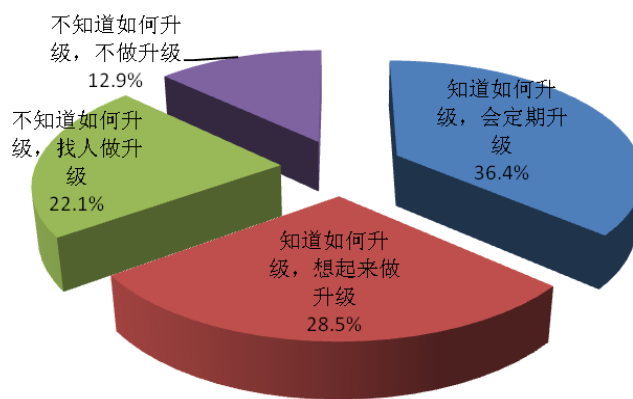


图 7 受访者电脑系统升级情况统计

三. 杀毒

电脑忽然黑屏、操作失灵、莫名奇妙反映迟钝、重要数据不翼而飞.....这些都是电脑可能已经被病毒攻击的表现，因此防毒杀毒工作显得尤为重要。

调查结果显示，所有受访者中，没安装杀毒软件的占 5.2%；94.8%的受访者安装了杀毒软件，定期升级病毒库的占 73.4%，还有 12.9%的受访者想起来才升级病毒库，8.5%的受访者不升级病毒库。也就是说，有 26.6%的受访者没有遵守安全的杀毒规范。

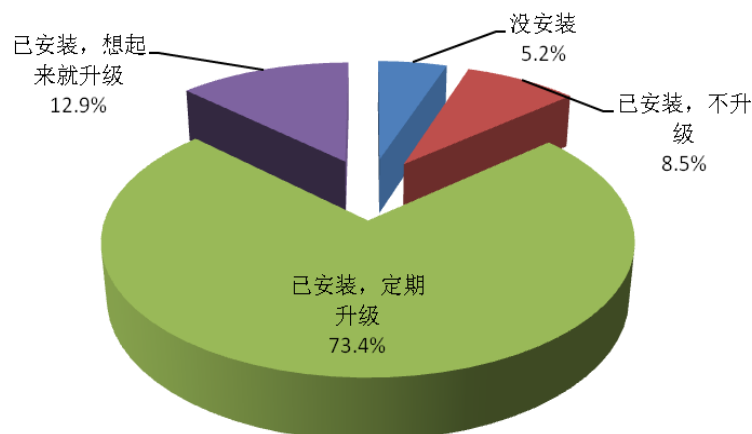
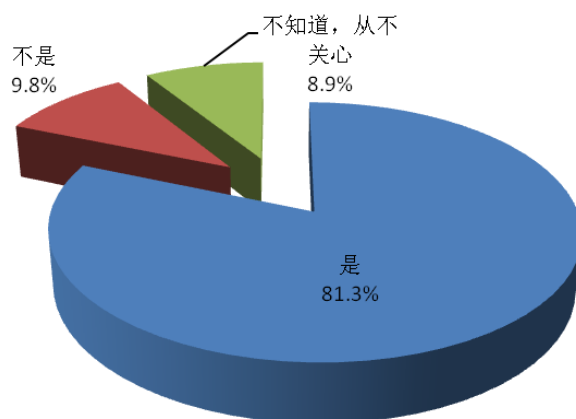


图 24 受访者杀毒软件安装与升级情况统计

四. 防火墙

电脑虽然有了杀毒工具，但是病毒的传染速度确实惊人的，电脑终端用户要做好防护工作，将病毒挡在“门”外，就要时刻开启防火墙。81.3%的受访者电脑防火墙是开启状态，9.8%的受访者电脑终端防火墙不是开启状态，还有 8.9%的受访者不知道也不关心自己电脑防火墙是否是开启状态。



图表 25 受访者防火墙设置情况统计

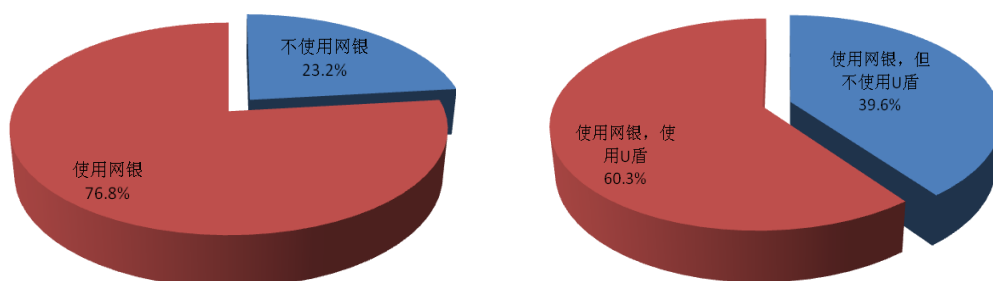
二. 上网安全

一. 网银

2010 年，我国的电子商务得到了飞跃式发展，淘宝每天的交易额都在数十亿元，团购网站已经有 1100 多家，京东、新蛋、当当等商城也发展迅猛。团购网站的火爆促使了网络支付市场的繁荣，但在这一片繁荣之下，网络支付巨大的成交额引起病毒作者的浓厚兴趣，网游木马”转向”网银木马”， 2010 年全年新增网银木马近 400 个。以木马、病毒和网络钓鱼为主的黑色产业也在侵蚀电子商务的根基。

调查结果显示，所有受访者中使用和不使用网银的比例分别为 76.8%和 23.2%。

而使用网银的受访者中，60.3%的受访者会使用 U 盾，还有 39.7%的受访者在使用网银时是不使用 U 盾的。

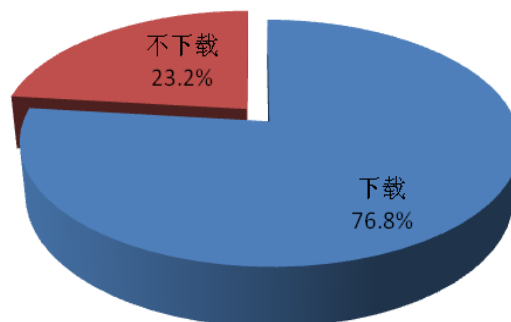


图表 26 受访者使用网银情况统计

二. 下载

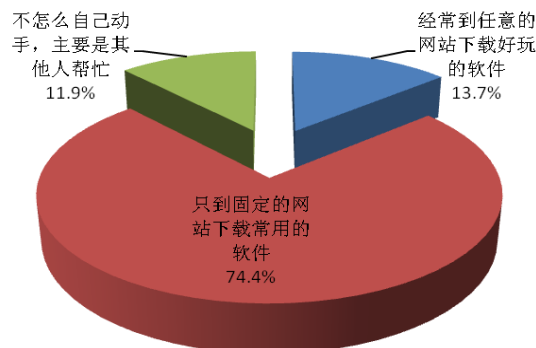
为了工作和生活的便利，网民平时都会需要下载一些软件，但是不当的下载软件途径和操作，都有可能带来信息安全威胁。

调查结果显示，76.8%的受访者平时都会下载软件，不下载软件的比例只有 23.2%。



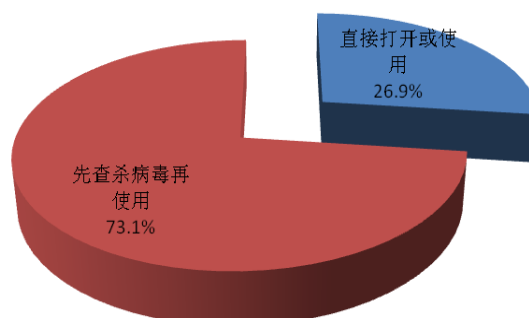
图表 27 受访者下载软件情况统计

下载软件的受访者们有不同的下载途径，其中 74.4%的受访者会在固定的网站上下载常用软件，而 13.7%的人会到任意的网站下载好玩的软件，11.9%的人不是自己动手，主要找他们帮忙。



图表 28 受访者下载途径统计

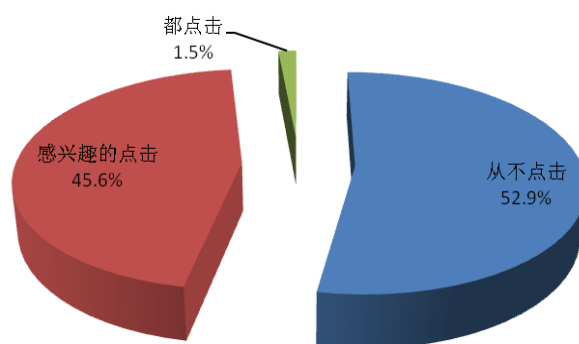
下载软件的受访者中，73.1%的受访者会先查杀下载软件的病毒再使用，而直接打开或使用下载软件的比例是 26.9%。



图表 29 受访者下载软件操作情况统计

三. 弹出链接

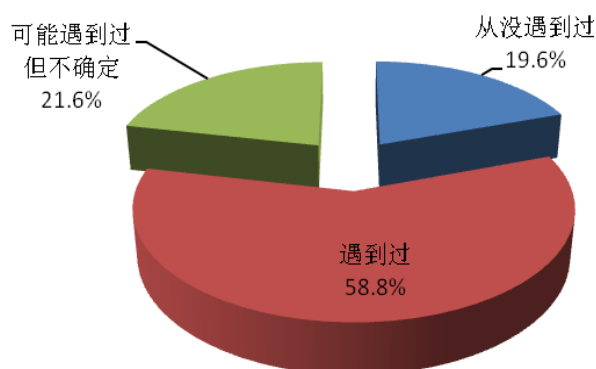
网页弹出链接有可能会带来信息安全威胁，例如病毒、恶意代码、钓鱼网站等。调查结果显示，当即时聊天工具或论坛、网页弹出链接时，52.9%的受访者从不点击这些链接，而45.6%的受访者会对自己感兴趣的链接进行点击，1.5%的人会都点击。



图表 30 受访者对网页弹出链接处理情况统计

四. 恶意插件、病毒的攻击

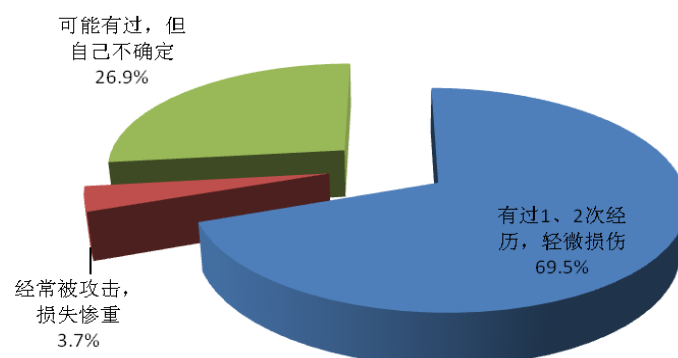
目前，病毒数目呈突飞猛进的速度增加，用户对恶意插件和病毒的攻击防不上防。根据对受访者是否遇到过恶意插件、病毒攻击的情况调查结果显示，58.8%的受访者电脑遇到过恶意插件、病毒的攻击，还有21.6%的受访者不确定自己的电脑是否受到过攻击，从来没遇到过的人数比例仅占19.6%。



图表 31 受访者受病毒攻击的情况统计

而遇到过恶意插件、病毒攻击的受访者中，确定有过1、2次经历，轻微损伤的人数最多，占到69.5%，确定经常被攻击的人数比例为3.7%，还有26.9%的受访者认为自己的电脑

可能被恶意插件、病毒攻击过但不确定。

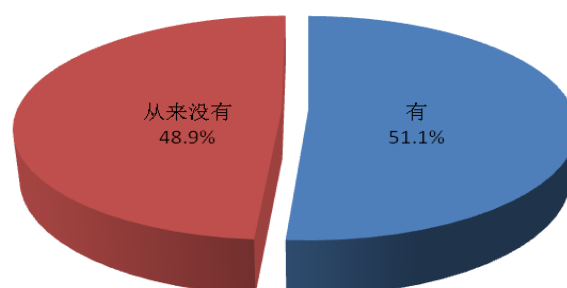


图表 32 受病毒攻击受访者具体情况统计

三. 对安全意识教育、信息安全的认知

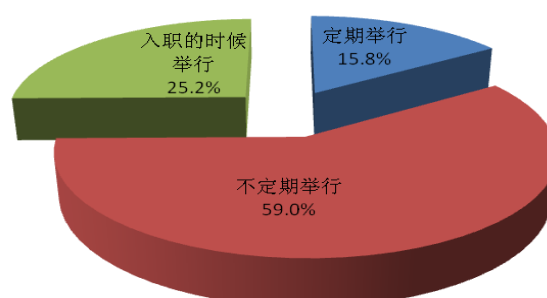
一. 信息安全培训频度

在众多的信息安全管理措施中，信息安全意识培训是一个有效、快捷、省钱的方法。调查结果显示，48.9%的受访者从来没有接受过信息安全培训，51.1%的受访者曾经接受过信息安全培训。



图表 33 受访者接受信息安全培训情况统计

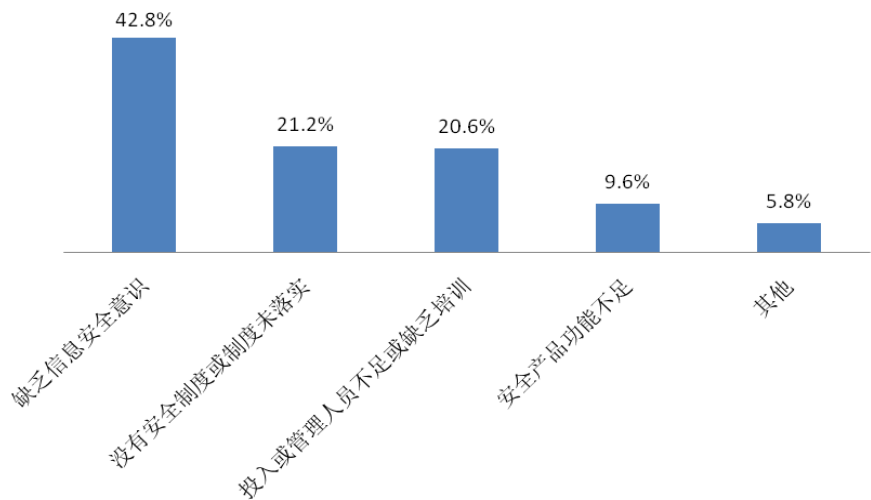
而接受过信息安全培训的受访者中，只有 15.8%的受访者会接受到定期的信息安全培训，25.2%的受访者是在入职时接受过信息安全培训，而 59.0%的受访者接受的是不定期举行的信息安全培训。



图表 34 受过信息安全培训受访者详情统计

二. 对企业信息安全隐患的认知

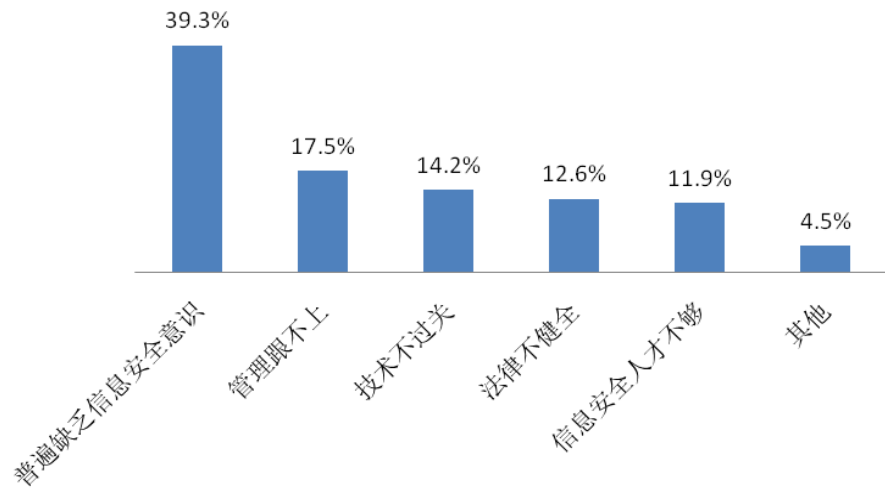
受访者认为所有的安全隐患中，个人信息安全意识不足是最大的安全隐患，占到 42.8% 的比例，然后依次是没有安全制度或制度未落实、投入或人员不足或缺乏信息安全培训、安全产品功能不足和其他。



图表 35 受访者信息安全隐患认知情况

三. 有效保护信息安全面临的最大障碍的认知

对于目前有效保护信息安全面临的最大的障碍，调查结果显示，受访者认为最大的障碍是普遍缺乏信息安全意识，其他依次是管理水平落后、技术不过关、法律不健全、信息安全人才不够和其他障碍。



图表 36 受访者对有效保护信息安全面临的最大障碍的认知情况

四. 问题与建议总结

通过对本次调查有效问卷的分析，显示中国企业员工普遍缺乏信息安全意识。要实现企业信息安全，必须围绕着“人”这个安全主体，关心人的行为安全，保障人的利益，真正做到“以人为本”才是关键。而实现“以人为本”的信息安全管理，第一步就必须提高员工的信息安全意识水平。企业员工信息安全意识的培养是一个漫长而艰难的过程，必须结合企业的文化和具体情况和要求，辅以生动、形象、简洁的方式进行，传统的教科书的方式是不能达到设想的培训目标的。可以采用信息安全海报、动画视频、屏幕保护、安全手册、培训课程等多种方式来不断强化员工安全意识，建立健全适用的信息安全管理规章制度和操作流程并严格落实来不断规范员工行为。只有从根本上解决信息安全管理中人的问题，打造好企业坚实的人力防火墙，才能最终保证企业的信息安全。