2022年9月全员安全意识周

网络信息安全意识学习培训

汇报人：李雪梅

中国电信 CHINA TELECOM | 云堤

www.damddos.com

什么是信息安全

信息安全与我的关系

如何实现信息安全

相关法律法规

01 什么是信息安全

什么是信息安全 | 信息安全与我的关系 | 如何实现信息安全 | 相关法律法规

什么是信息安全

什么是信息?

1 有意义的内容

2 对企业具有价值的信息,称为信息资产;

3 对企业正常发展具有影响作用,敏感信息，不论是否属于有用信息。

什么是信息安全

信息安全的3要素

Confidentiality
保密性

保证信息不泄露给未经授权的用户

Integrity
完整性

保证信息从真实的发信者传送到真实的收信者手中，传送过程中没有被非法用户添加、删除、替换等。

Availability
可用性

保证授权用户能对数据进行及时可靠的访问。

02 信息安全与我的关系

什么是信息安全 | 信息安全与我的关系 | 如何实现信息安全 | 相关法律法规

信息安全与我的关系

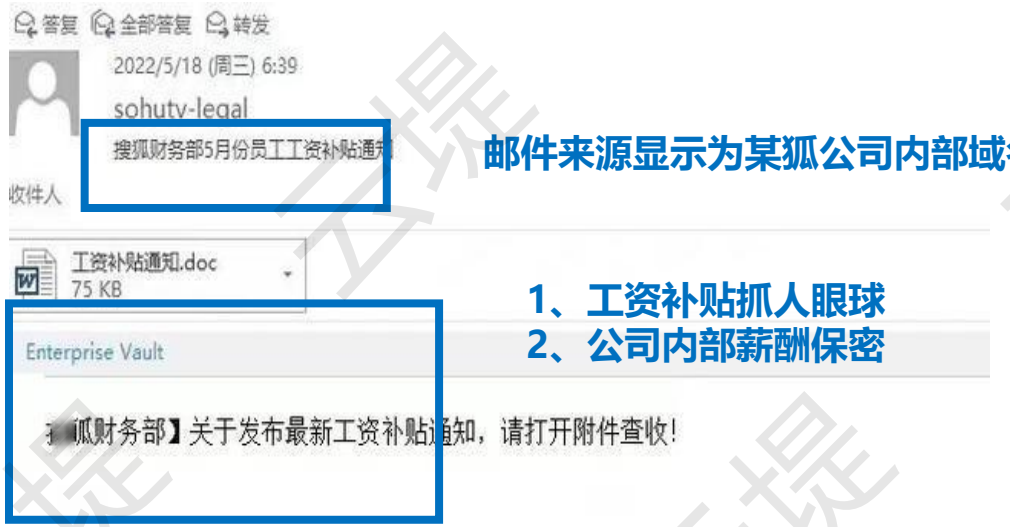
信息安全 → 技术 → 流程 → 人

信息安全

1. 以企业为目标的攻击威胁数字上升;
2. 攻击工具的普及使网路罪行较以往变得更轻易;
3. 基于网站的攻击有增无减
4. 针对个人身份资讯的安全威胁持续增长。
5. 以企业为目标的攻击威胁数字上升;

信息安全与我的关系-案例分享

2022年5月25日 **#某狐全体员工遭遇工资补助诈骗#** 冲上微博热搜第一：近日，一份流传网络的聊天记录显示，某狐全体员工在5月18日早晨收到一封来自“某狐财务部”名为《5月份员工工资补助通知》的邮件。聊天记录称，不少员工受骗，工资卡余额被划走。



邮件来源显示为某狐公司内部域名

1、工资补贴抓人眼球
2、公司内部薪酬保密

搜狐表示，经调查，**此事为某员工使用邮件时被意外钓鱼导致密码泄露，**进而被冒充财务部盗发邮件。事发后，公司IT及安全部门第一时间采取了行动，包括立刻删除了相关邮件，并由ES部门出面汇总遭遇诈骗员工的信息到派出所报案。

信息安全与我的关系

信息安全就在我们身边!

信息安全需要我们每个人的参与!

你该怎么办?

03 如何实现信息安全

如何实现信息安全

1. 安全保密意识
2. 机密信息保护
3. 办公环境
4. 社会工程学
5. 恶意代码防范
6. 软件安装使用
7. 移动设备安全
8. 密码安全

如何实现信息安全

SECURITY
BACKGROUND

培养意识

- 知道如何去识别一个潜在的问题
- 利用正确的判断力

掌握和实行良好的安全习惯

- 在日常事务中将养成良好的习惯
- 同时鼓励其他人也这么做

报告任何异常事件

- 如果您发现了某件安全事件,通知适当的联系人

如何实现信息安全-（1）安全保密意识

安全保密意识

1 U盘使用

Ø 不得在涉密计算机与非涉密计算机之间交叉使用U盘等移动存储介质，在使用司私人所有的USB驱动器从家中来回传输工作相关文件之间，请检查您公司的信息安全策略
Ø 不要将未知来源的USB驱动器插入计算机
Ø 不要在USB设备上存储敏感工作信息
Ø 将工作和私人使用的USB存储设备区分开来

2 涉密笔记本

Ø 在一般情况下，不允许携带涉密笔记本电脑及移动存储介质外出。
Ø 确需携带外出的，要严格履行审批手续，采取有效管理措施，确保涉密笔记本电脑及移动存储介质始终处于严密监控之下，同时采取强身份认证，涉密信息加密等保密技术防护措施。

3 快递与邮寄

Ø 认真执行涉密载体使用保密管理规定，不得将涉密载体通过普通邮寄渠道寄运或违规交由他人使用、保管。

如何实现信息安全-（2）机密信息保护

1 通过电子邮件发送机密信息

电子邮件的传递也要经过多处中转，所以通过电子邮件发送的文档可能被许多人读取。在通过电子邮件发送机密文档时，可供选择的解决方案有相当简单的给文档设置密码或稍复杂的文件加密的方式。

2 防范公共场所的窃听

不要讨论公司机密信息，特别是当有陌生人在场之时。如果迫不得已，在讨论公司敏感事项时，一定要注意附近的环境安全。

3 认识商业信息侦探

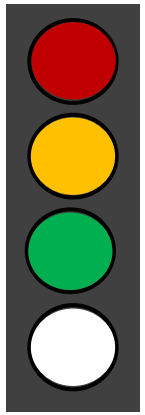
信息侦探、商业间谍

公司员工（包括已离职员工）

客户、供应商

如何实现信息安全-（2）机密信息保护

4 信息分级与保护方案整合



用红灯来关联安全级别最高的“机密”信息数据

用黄灯来关联安全级别稍低的“敏感”数据

用绿灯来关联“内部”数据

用新加一个白色的灯来关联“公开”数据

信息安全“三思而后行”小技巧

一、信息是否涉密?

二、我有权提供吗?

三、对方有权了解吗?

5 自动回复消息泄漏机密信息

- Ø 只将自动答复回复给公司内部人员
- Ø 保持自动答复消息的精炼和概要，避免告知详细的休假或外出的日程计划。
- Ø 不要在自动答复中加入详细联络方式的签名

6 视频拍照及泄露产品研发相关机密信息

- Ø 未获得公司场所区域主管的事前批准不得在相关区域内拍照
- Ø 在公司场所内，未获得被拍摄人员的同意不能对其进行拍摄
- Ø 不得拍摄公司敏感和机密材料，除非获得这些信息资产的所有者或安全部门的同意

如何实现信息安全-（3）办公环境

清洁桌面

- 在离开座位时，要注意把重要信息和文件锁起来，并随身携带个人贵重物品。

离开时锁定计算机

- 养成在离开位置时锁屏或退出登录的好习惯非常重要。使用键盘上的Windows键+L能够快速锁屏。

工卡安全使用不乱扔

- 不要随意放置您的工卡
- 让未授权人员获得进入敏感区域或设施的权限
- 未授权人员的不当甚至犯罪活动都可能会栽赃给您
- 如果工卡遗失，请立即报告。

工作场所环境安全

- 不要让陌生人尾随您进入单位区域
- 保持工作场所清洁，在会议之后收走会议资料和设备
- 及时取走打印出的涉密文件，复印之后记得取走原件
- 发现异常情况或可疑人员立即报告安全响应部门

如何实现信息安全-（4）社会工程学

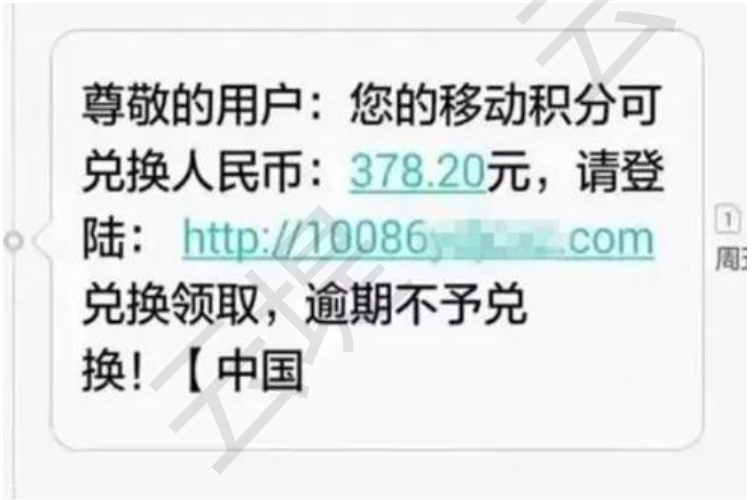
1、邮件钓鱼

- 确认发件人信息、与发件人核对
- 谨慎扫码、点击链接、下载附件
- 钓鱼内容多为薪资调整、疫苗登记、优惠活动等企业通知

2、电话钓鱼

- 未经许可和批准不要提供商业信息
- 在没有确认请求人员身份的情况下不要披露商业信息，披露信息之前请先获得批准
- 当有不熟悉的人向你询问信时，要特别加以注意
- 在任何情况下 公司都不会要求您提供密码

3、短信钓鱼



- 一看短信是否真实
- 二看网站链接和页面是否为官方渠道
- 三看对方索要信息是否为个人重要敏感信息

如何实现信息安全-（5）恶意代码防范

Word中的危险图片

病毒不仅可能潜伏于常见的可执行文件中，也会在办公文件、布景主题甚至屏保壁纸中。避免在工作电脑中下载和安装未授权的软件和插件。

勒索软件防范

避免访问未知的或不良的网站，保持防病毒软件的启用和更新，定期备份重要数据以免丢失

广告点击僵尸病毒

不接收可疑文件，不开启可疑附件，不访问可疑网站，不安装非法软件

如何实现信息安全-（6）软件安装使用

不要下载和安装未授权的软件

这些软件是恶意软件和间谍软件的首选载体。间谍软件悄悄潜伏于你的系统之中，截取、记录和传送你所输入敏感信息

不要下载盗版软件或音频

多部法案强化了对在互联网上传播和分享非法盗版软件以及通过破解来突破软件加密限制行为的惩罚力度

当心娱乐软件，这是散布流氓软件的最佳方式之一

不要安装不知道来源的软件。有趣的或诱人的游戏可能隐藏诸如病毒，蠕虫，木马，后门程序，间谍软件或键盘记录器之类的流氓软件

如何实现信息安全-（7）移动设备安全

移动僵尸网络

移动僵尸网络这个词由“移动”、“僵尸”和“网络”组成，顾名思义，使用移动终端计算设备做“肉鸡”的僵尸网络。网络犯罪分子使用特别的木马病毒来突破移动设备的安全防线，进而远程控制它们。大量的被远程控制的移动终端设备便构成一个移动“僵尸”网络。

如何避免移动设备变成移动僵尸网络

- 只从可靠的信誉度高的应用商店下载软件
- 小心您所收到的消息，他们可能包含恶意附件或链接
- 如果碰到异常的状况比如电池耗用很快、自动重启、运行极慢或网络中断，则可能是中招的前兆
- 确保安装和启用了可信的移动防病毒程序

如何实现信息安全-（7）移动设备安全

公司移动设备安装软件

- 未获得 IT 批准而安装的软件可能影响到其它工作用软件和系统的稳定性
- 非授权的软件，可能会让您触犯知识产权保护相关的法律，也会让公司处于危险之中
- 轻度地使用公司的便携式设备用于私人目的，如使用 Office 和互联网等是可接受的

移动设备越狱与维修

- 越狱后的手机往往更容易被恶意程序和犯罪份子利用，让整体的安全性降低
- 使用可信的在线备份方案备份重要数据，在出现手机丢失等意外事故时能及时恢复
- 当便携式移动终端设备出现故障时，需寻找可信的服务机构进行维修，防止数据丢失
- 当工作用移动终端出现异常情况时，马上联系信息安全专业团队人员寻求帮助，不要私自维修
- 手机丢失后远程擦除手机上的数据

如何实现信息安全-（8）密码安全

社交网站被黑

社交网站被黑，我及时修改了密码，为什么还是中招了？

- 不要将用于私人事务的密码和用于工作的密码设置为相同。
- 为不同的网站应用设置不同的密码，可以使用的小技巧是在通用密码部分上加入不同网站的信息。
- 当怀疑帐户信息泄露时，立即更改可能受到影响的系统的密码，以及安全提示问题等等。

密码防范小知识

- 即刻更改系统初始化密码
- 分级分类设置密码，不同场所使用不同密码，避免撞库
- 不要使用网站或APP记住密码功能
- 不在办公电脑及桌面上存放明文保存的用户名和密码
- 不要通过任何渠道向任何人透漏你的密码
- 如有人以邮件、电话等渠道向你索取密码，应拒绝并提高警惕

如何实现信息安全-天翼安全

社保变更：链接钓鱼

2022年度社保缴费机制变更通知

linmandi@chinatelecom.cm 2022-06-16 14:50
收件人：我 详情

检测到该发件人未标记过，可标记发件人重要程度，帮你更好进行分类管理
低优 普通 高优

各位同事：

根据2022年社保局《关于申报2022年度社会保险缴费工资的通知》和《住房城乡建设部 财政部 人民银行关于改进住房公积金缴存机制 进一步降低企业成本的通知》，我司员工社保已经根据政策的要求进行了调整，可进入官网查看个人社保情况，请勿直接保存密码，以防信息泄露。

官网查询地址：http://www.rbj.gov.cn/csibiz/home/

如有问题请及时联系！

特此通知！

综合管理部

2022年6月9日

疫苗预约：二维码钓鱼

新冠疫苗免费接种预约通知

liufengyun 2022-06-16 15:57
收件人：我 详情

检测到该发件人未标记过，可标记发件人重要程度，帮你更好进行分类管理
低优 普通 高优

各位同事：

根据集团联防联控机制、集团防控指挥部工作部署，全国各区正在有序推进重点人群新型加强疫苗（简称"蛋白重组疫苗"）接种工作。现结合公司实际情况，特作出如下安排：

请户籍具备社区接种条件的员工从即日起按照所在社区的工作部署和安排，合理安排时间前往接种并做好登记；外地户籍、无自有住房的员工均可前往就近社区参加接种并及时做好报备。

前期已完成新冠疫苗接种的员工请扫码填写接种时间，感谢配合

天翼安全

居家办公：附件钓鱼

关于疫情居家隔离新政策的通知

王梦 2022-07-01 13:35
收件人：我 详情
附件1个（《2022年7月1日确诊者到访区域》.html） 查看附件

各位同事：

鉴于近期我市出现新冠阳性病例，依据最新政策和要求，本市疫情防控领导针对疫情处理办法指导安排如下日至今本人（或共同居住人员）曾到访过或者接触过（附件：确诊者到访区域）地区的人员、到访过中高风险地或无症状感染者同一时间具有相同轨迹的人员，需尽快进行核酸检测并暂先居家隔离（满14天且核酸检测结果正异常可正常办公，其他特殊情况以公司通知为准）。所有同事，请严格遵守当地防疫要求，做好疫情防护工作，流动和不必要的出行。

再次倡导各位同事少聚集，少外出，减少不必要的聚餐聚会，始终绷紧疫情防控这根弦，落实好常态化防控外出时随身携带和科学佩戴口罩，以及勤洗手、常通风、少聚集、用公筷、一米线等卫生健康习惯。

特此通知

1个附件（4.5K）

《2022年7月1日确诊者到访区域...
4.5K

福利饮用券：活动钓鱼

饮用券

集团工会 2022-06-28 16:31
收件人：我 详情

您好：

为了答谢全体员工兢兢业业的工作付出，公司决定于6月29日至6月30日 期间向全体员工分发STARBUCKS的免费畅饮券！点击下面按钮进入活动页面，确认员工信息即可领取价值100元至150元的免费畅饮券3张，先到先得！！！

活动截止日期：2022年6月30日！

点击右侧链接：参加活动

内含更多权益和礼遇

冒充HR：信息钓鱼

阿里巴巴人才招聘

Nico_le 2022-06-29 10:16
收件人：我、modm 详情

Alibaba Group 阿里巴巴集团

Dear莫德铭：

通过我公司在人才库对您个人简历的筛选您已通过我公司的招聘初审，阿里云诚邀您填写相关信息，等待后续面试电话。谢谢！

https://www.wenjuan.com/s/mYBFvaB/?sr=Android&sy=2

阿里巴巴是一家在不断挑战自己、追求卓越的公司。集团有完善的员工职业发展体系，公司为员工建立了不同的职业发展，期望您和我们共赴轰鸣向前的"五新"（新零售、新制造、新金融、新技术、新能源）时代！您将"和一群非凡人，一起去完成一件非凡事"！快乐的阿里人，期待您的到来！

此致！

特别提醒：

1、本邮件为录用意向邮件，在您填写相关信息以后，人力资源将主动联系您，请您保持电话通畅。

2、本意向书以您真实的个人信息和健康检查符合公司要求为生效前提。如您在面试过程中有任何弄虚作假或有意隐瞒等情形，或根据健康检查有公司认为不适合相关工作岗位的情形，公司有权随时单方解除本意向书。

邮箱盗用：真实地址钓鱼

攻防演练方案

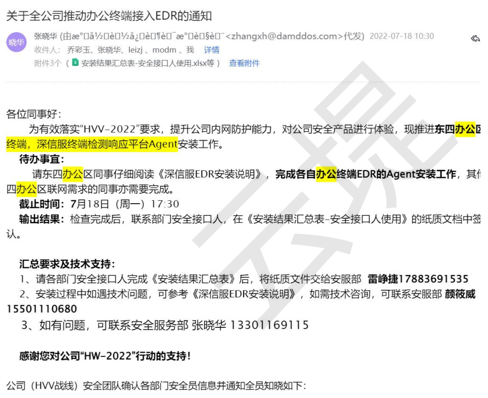
颜筱威 2022-07-08 09:07
收件人：staff 抄送：李爾、张晓华、乔彩玉 详情
附件1个（演练方案-0707.zip） 查看附件

7月8日全天攻防演练方案，请查收
附件密码：gongfang0707

1个附件（85.7K）

演练方案-0707.zip
85.7K

伪造真实邮箱



关于全公司推动办公终端接入EDR的通知

张晓华 (由æ°å½è½å¿è¶è¯æ°è§è¨<zhangxh@damddos.com>代发) 2022-07-18 10:30
收件人：乔彩玉、张晓华、leizj、modm、我 详情
附件3个（安装结果汇总表-安全接口人使用.xlsx等） 查看附件

各位同事好：

为有效落实"HVV-2022"要求，提升公司内网防护能力，对公司安全产品进行体验，现推进**东四办公区**终端，深信服终端检测响应平台Agent安装工作。

待办事宜：

请东四办公区同事仔细阅读《深信服EDR安装说明》，**完成各自办公终端EDR的Agent安装工作**，其他四办公区联网需求的同事亦需要完成。

截止时间： 7月18日（周一）17:30

输出结果： 检查完成后，联系部门安全接口人，在《安装结果汇总表-安全接口人使用》的纸质文档中签认。

汇总要求及技术支持：

1、请各部门安全接口人完成《安装结果汇总表》后，将纸质文件交给安服部 **雷峥捷17883691535**

2、安装过程中如遇技术问题，可参考《深信服EDR安装说明》，如需技术咨询，可联系安服部 **颜筱威15501110680**

3、如有问题，可联系安全服务部 张晓华 13301169115

感谢您对公司"HW-2022"行动的支持！

公司（HVV战线）安全团队确认各部门安全员信息并通知全员知晓如下：

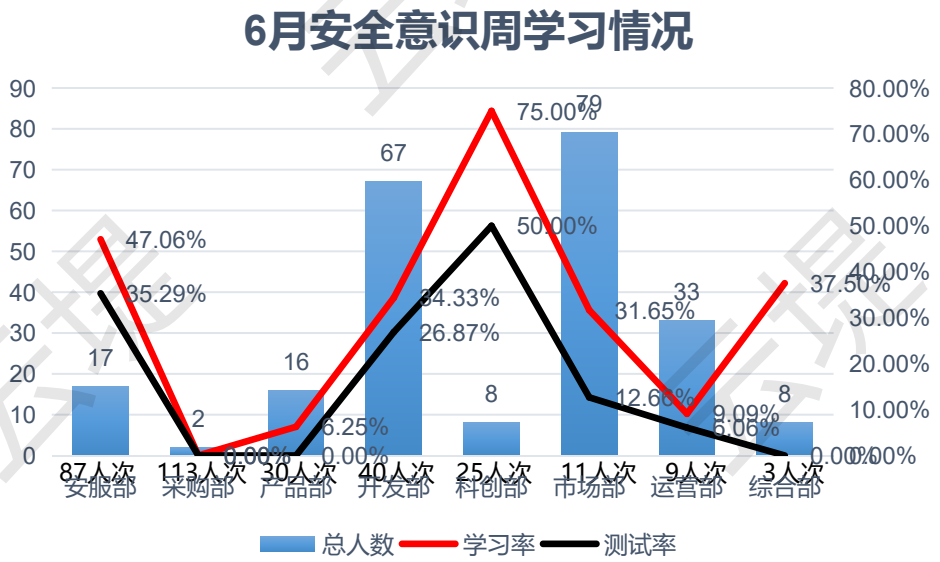
微信钓鱼：伪装HR

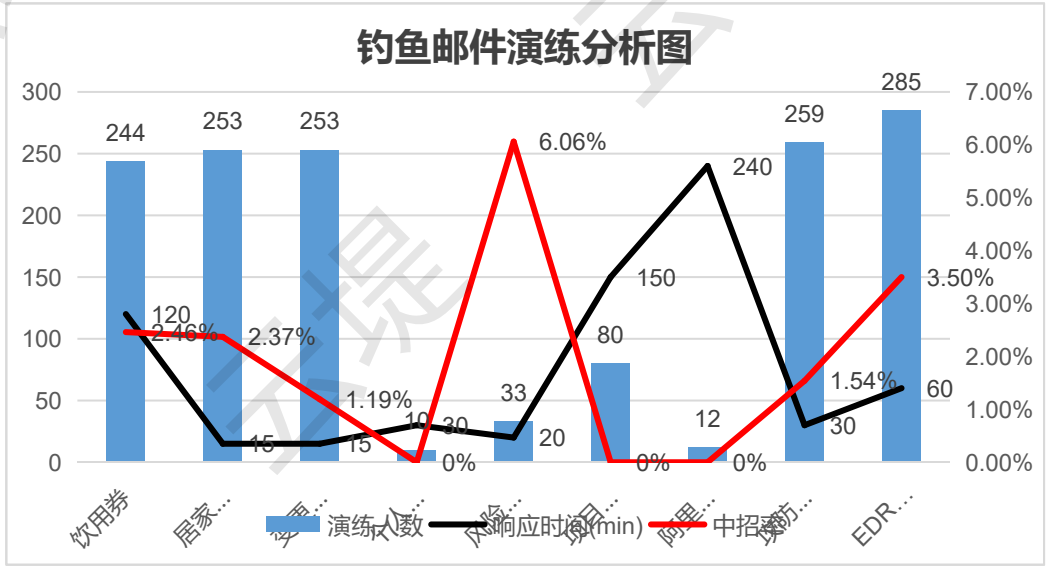
如何实现信息安全-天翼安全

- **钓鱼邮件•第一次钓鱼**
  - **总体**：6月8日-6月9日面向全员（230人）开展钓鱼演练，涉及集团、云堤邮箱318个，累计49人中招，中招率15.41%，其中6人输入了个人信息（高危），高危率1.89%
  - **演练场景**：疫情防控、社保变更
- **详细情况**
  - **详情**：通过数据分析，49.37%的人员未查看邮件，15.41%的人员进行了危险操作，1.89%的人员“沦陷”（高危）
  - **TOP3**：科创、综合、运营中招率分别为44.44%、27.27%、25%

近9场钓鱼演练分析，在三种钓鱼类型中员工对伪造企业邮箱钓鱼的演练防范意识很高，中招率几近于零；对伪装成第三方HR的钓鱼演练员工反应较不敏感；对于员工企业邮箱被盗用的钓鱼邮件演练由于邮箱地址真实，邮件内容逼真，员工对该类型邮件反应速度较慢且中招人数较多，提升空间很高。

自6月第一场安全意识培训后，各部门越来越重视安全意识，在之后的两场培训中，学习率及考试率都有显著的提升；经过观察员工在日常生活中基本能养成离开工位及时锁屏，工位不留纸质敏感信息，打印机打印文件及时带走等好习惯；钓鱼邮件的中招率从一开始的15.41%下降至1.71%，员工对钓鱼邮件的识别能力提升非常明显。





如何实现信息安全-天翼安全

外因是条件，内因是根本

提升信息安全意识，

增强安全防御能力！

思考：如果企业邮箱收到了疑似钓鱼邮件，你该如何处理？

如何实现信息安全-天翼安全

- **社工攻击响应机制：设立安全员**

1、发现疑似攻击行为后，上报部门安全员

2、部门安全员初步判定是疑似攻击行为，否，结束流程；是，向全体员工发出预警告知邮件，上报公司安全员，统计本部门受影响人员数量。

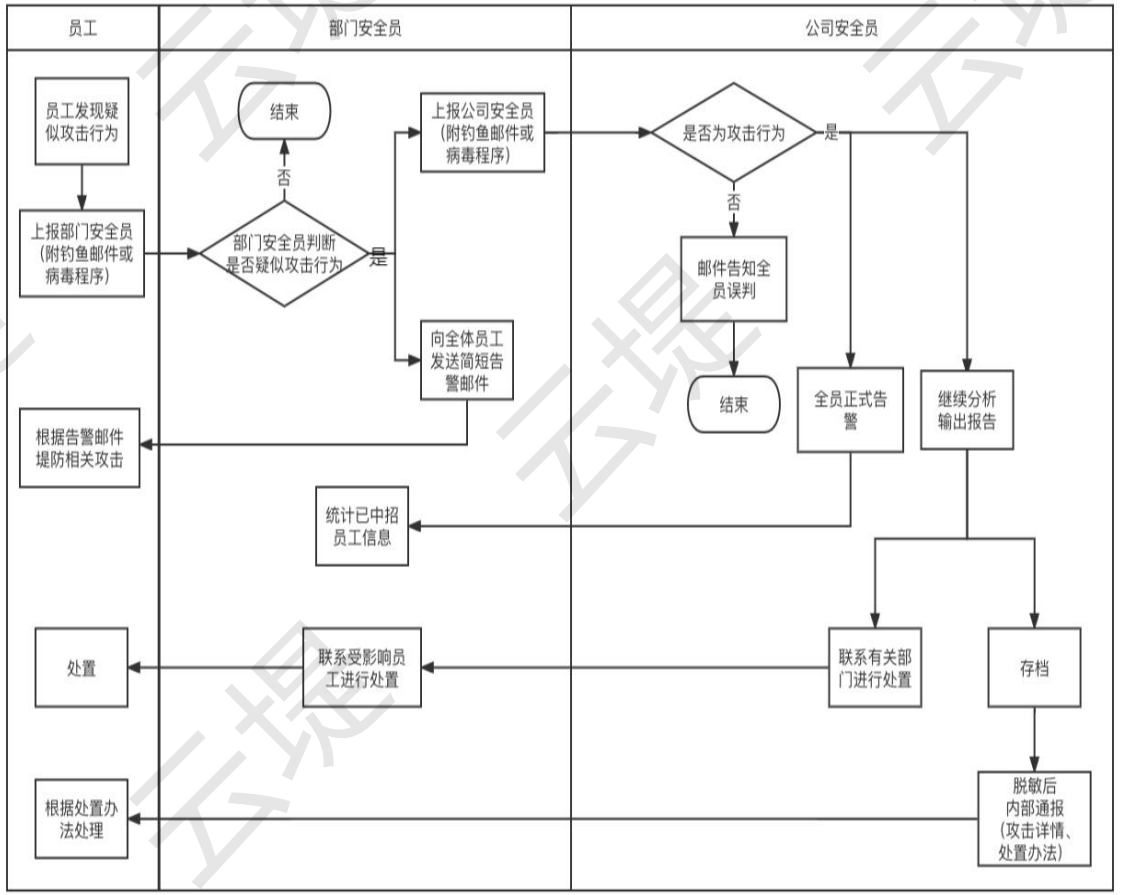
3、公司安全员对疑似邮件进行分析，判定为非社工攻击，则通知解除警报

4、公司安全员对攻击样本进行提取，做技术分析，根据分析结果对攻击行为进行严重程度和影响范围定性。

5、判定疑似邮件为社工攻击，向全体员工发正式告警邮件，并通知各部门安全员统计受影响人员和系统，启动应急处置流程。

6、处置结束后，对全体员工进行攻击处置结果说明，攻击行为相关文档存档。

- **社工攻击响应机制:监测和防御手段**



04 相关法律法规

相关法律法规

在多方面因素的驱使下，网络安全已经受到国家战略层面的高度重视。近年来，国家陆续颁布了有关网络安全建设的系列政策措施，2021年相关条例的出台尤为频繁，推出了《数据安全法》《个人信息保护法》等多项法律法规。网络安全政策的陆续出台，既有利于提高全民对于网络安全的重视，提高国家网络安全防护能力，在产业层面，也能够为网络安全产业的发展注入强有力的政策支持与发展活力。

2017-2021年实施法律法规

2017年6月1日《中华人民共和国网络安全法》

2019年7月26日《加强工业互联网安全工作的指导意见》

2021年1月1日《中华人民共和国密码法》

2021年1月13日《关于开展工业互联网企业网络安全分类分级管理试点工作的通知》

2021年3月12日《常见类型移动互联网应用程序必要个人信息范围规定》

2021年4月26日《移动互联网应用程序个人信息保护管理暂行规定（征求意见稿）》

2021年9月1日《中华人民共和国数据安全法》

2021年11月1日《中华人民共和国个人信息保护法》

网络安全法重点法律法规

第二十一条 国家实行网络安全等级保护制度。网络运营者应当按照网络安全等级保护制度的要求，履行下列安全保护义务，保障网络免受干扰、破坏或者未经授权的访问，防止网络数据泄露或者被窃取、篡改：

（一）制定内部安全管理制度和操作规程，确定网络安全负责人，落实网络安全保护责任；

（二）采取防范计算机病毒和网络攻击、网络侵入等危害网络安全行为的技术措施；

（三）采取监测、记录网络运行状态、网络安全事件的技术措施，并按照规定留存相关的网络日志不少于六个月；

（四）采取数据分类、重要数据备份和加密等措施；

（五）法律、行政法规规定的其他义务。

第二十五条 网络运营者应当制定网络安全事件应急预案，及时处置系统漏洞、计算机病毒、网络攻击、网络侵入等安全风险；在发生危害网络安全的事件时，立即启动应急预案，采取相应的补救措施，并按照规定向有关主管部门报告。

第五十九条 网络运营者不履行本法第二十一条、第二十五条规定的网络安全保护义务的，由有关主管部门责令改正，给予警告；拒不改正或者导致危害网络安全等后果的，处一万元以上十万元以下罚款，对直接负责的主管人员处五千元以上五万元以下罚款。

中国电信 CHINA TELECOM | 云堤

天翼安全科技有限公司
China Telecom Cybersecurity Technology Co.,Ltd
北京市东城区朝阳门北大街19号 100010
No.19, ChaoYangMen North Street, Dongcheng District, Beijing, China, 100010
www.damddos.com