

(照片部分由主办方添加)

钓鱼演练: 基于攻防模式的人为因素风险教育

宋琼 易念科技 产品研发总监

网络钓鱼发展趋势:调查报告





- 2021年网络犯罪造成的破坏将让全球每年损失6万亿美元
- 超过90%的黑客攻击和数据泄露源于网络钓鱼诈骗
- 联邦调查局报告称,商业电子邮件欺诈(BEC)在过去5年中已报告损失了超过**125亿美元**(截至其最后一次到2018年5月),已报告的网络犯罪数量仅占美国每年实际犯罪总数的10%至12%。
- 勒索软件成为增长最快的网络犯罪类型,全球勒索软件损坏成本达到200亿美元,每11
 秒就有一家企业成为勒索软件攻击的受害者
- 90%以上的中小企业缺乏安全意识与技能
- 由于企业声誉或竞争因素,50%以上的高净值企业可能成为网络攻击的目标。

安全意识教育观点: 人为因素风险





网络安全问题产生的原因有三种:

技术漏洞、流程漏洞、人的漏洞, 人是网络安全防线中最脆弱的一环!



IBM公司统计, 95%的网络攻击是以安全意识淡薄的员工做为突破口

—IBM Cyber Security Intelligence Index

企业安全防御手段: 以人为本



Gartner

《安全意识计算机培训的魔力象限》2019年7月18日出版

- · 人比技术, 政策或流程更能影响安全结果。
- 以最终用户为中心的安全教育和培训是一个快速增长的市场。
- 交互式培训是综合安全教育和行为管理计划的核心组成部分
- CISO和HR理认识到员工行为对企业风险管理功效的影响越来越大
- 到2022年, 60%的大型/企业组织将拥有全面的安全意识培训计划;
- ・ 主要趋势是SaaS服务、邮件钓鱼、游戏化运营



钓鱼演练——降低人为因素风险





 ...
 ...
 ...
 ...
 ...
 ...
 ...
 ...
 ...
 ...
 ...
 ...
 ...
 ...
 ...
 ...
 ...
 ...
 ...
 ...
 ...
 ...
 ...
 ...
 ...
 ...
 ...
 ...
 ...
 ...
 ...
 ...
 ...
 ...
 ...
 ...
 ...
 ...
 ...
 ...
 ...
 ...
 ...
 ...
 ...
 ...
 ...
 ...
 ...
 ...
 ...
 ...
 ...
 ...
 ...
 ...
 ...
 ...
 ...
 ...
 ...
 ...
 ...
 ...
 ...
 ...
 ...
 ...
 ...
 ...
 ...
 ...
 ...
 ...
 ...
 ...
 ...
 ...
 ...
 ...
 ...
 ...
 ...
 ...
 ...
 ...
 ...
 ...
 ...
 ...
 ...
 ...
 ...
 ...
 ...
 ...
 ...
 ...
 ...
 ...
 ...
 ...
 ...
 ...
 ...
 ...
 .

像营销人员一样计划、像攻击者一样测试



最佳实践1: 使用真实世界的攻击方法

模拟钓鱼演练必须仿真真实的攻击和方法。否则,企业的"培训"只会给组织一种虚假的安全感。

身份仿冒 网站克隆 情绪诱因

惯用攻击手法——身份仿冒



关于HW期间账号安全性验证通知 😭 🗗

发件人: 管理员

时 间: 2020年12月23日(星期三) 晚上8:22

收件人:

附件: 1个(優弱密码检测工具使用方法.html)

关于HW期间账号安全性验证通知 🛊 🗗

发件人: 管理员 <admin@appIe.com>

时 间: 2020年12月23日(星期三) 晚上8:29

收件人:

附件: 1个(優弱密码检测工具使用方法.html)

关于HW期间账号安全性验证通知 😭 🗗

发件人: **管理员** <admin@apple.com>

时 间: 2020年12月23日(星期三) 晚上8:23

收件人:

附件: 1个(優弱密码检测工具使用方法.html)

● 显示名称

管理员<admin@abc.com>

● 近似域名

管理员<admin@apple.com>

● 域名仿冒

管理员<admin@apple.com>

惯用攻击手法——网站克隆



● 官方网站

● 钓鱼网站



惯用攻击手法——情绪诱导



≪ 返回 □复 □复全部 ● 新除 ● 初度制除 ● 経費 ● 経費	4 4 5 ST ST X
企业员工摄影活动通知! ☆ 『	诱惑性内容
发件人: 人事 部 时 间: 2019年11月6日(4 期三) 下午5:49	
收件人:	
亲爱的各位员工:	
为了丰富大家的业余生活,特此邀请您参加生活摄影创意赛。你可以晒自拍,晒旅游照,或者生活中的小镜头。参加比赛将有机会赢得大奖!	
符等奖2名,奖品是著"病典双人游;	
一等奖7名,奖品是iPhone7s一部;	引导至钓鱼网站
二等奖12名,奖品是尼康单反相机一部;	
三等奖15名,奖品是Blueair空气净化器一台;	
另有最佳创意实,最佳同位实等等原基不断:只要报名参与即可获得星巴克200元抵用券!	
进入网页报名只需要在活动页面输入你的姓名和公司邮箱。照片上传请附上描述。礼品发送按邮箱通知各位!请务必填写正确!	
点击这里,参加报名	
工会	伪造邮件署名/签名



最佳实践2:不要单独做这件事

与参加培训的其他团队和主管,创造一种积极地、全公司范围的安全文化。

高层支持 全员参与



最佳实践3:培训内容要与员工有关

人只关心对他们有意义的事情,确保企业的模拟攻击测试与员工日常活动相关。



典型钓鱼攻击场景



.

● 员工福利

● HW主题

● 疫情主题









最佳实践4: 关注员工行为改变

培训不仅仅是告诉员工希望他们知道什么,而是要给他们必要的关键信息,培养员工对钓鱼邮件的识别与反应能力,这样员工才能成为企业有效的最后一道防线。

应急演练 度量指标 持续教育

基于钓鱼模拟的应急演练

Cyber Security Innovation Summit

• 模拟多种钓鱼邮件发送 方式,测试企业邮件网 关对钓鱼邮件的识别能 力。

穿透测试

模拟攻击

• 选择测试目标,模拟多样化的钓鱼场景,发现企业面对邮件攻击的脆弱点,及员工识别和防范意识中存在的问题。

•阅读、点击、提交敏感信息、打开附件、扫码、 上报等;时间戳;使用 的设备/浏览器;

行为监测

应急处置

员工及时上报、及时修 改账户密码/冻结、防范 通知、事件分析总结等 等。

度量指标

未点击/未报告

未点击/报告



第一个月: 钓鱼测试	数量	统计数据	
发送邮件数	1000	100%	
点击数	750	75%	
报告数	50	5%	
点击/未报告	705	70.5%	
点击/报告	45	4.5%	

15

5

1.5%

0.5%

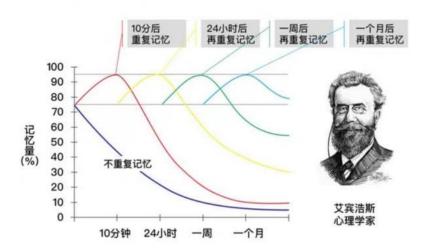


第二个月:钓鱼测试	数量	统计数据	变化
发送邮件数	1000	-	-
点击数	600	60%	-15%
报告数	350	35%	30%
点击/未报告	350	35%	-35.5%
点击/报告	250	25%	20.5%
未点击/未报告	13	1.3%	-0.2%
未点击/报告	100	10%	9.5%

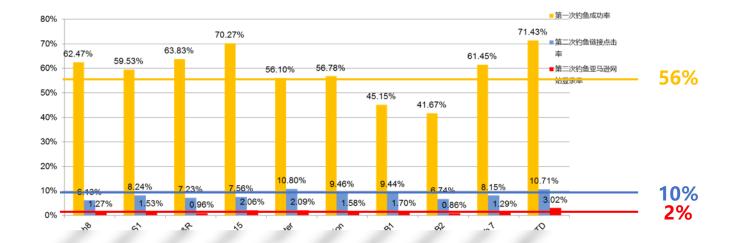
持续教育: 重复



用重复对抗遗忘



● 实践验证 (某企业HW训练)



钓鱼演练报告分享

《2020年邮件钓鱼演练分析报告》





数据来源:

106家企业

近120万用户钓鱼邮件数据

涵盖行业:

银行业; 制造业;

证券业; 建筑业;

保险业; 批发和零售业;

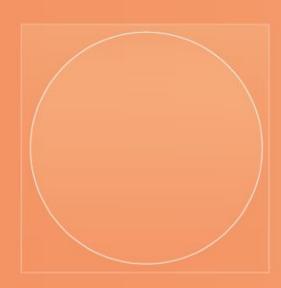
交通运输、仓储和邮政业;

信息传输、计算机服务和软件业;

电力、燃气及水生产和供应业;等等

扫码获取报告







THANKS