易念科技

改变认知 建立文化

E-Phishing

2020

邮件钓鱼演练分析报告

目录

简介

每个企业的安全负责人都面临过同样的难题：纵使不断增加在复杂安全技术上的投资，针对企业的网络犯罪仍在持续上升。诚然，世上没有绝对的安全环境，但绝大多数企业宁愿花重金在安全技术和产品上，也不愿在全员信息安全意识教育上有所投入，黑客往往能够采用最低的成本，从企业最薄弱的人员突破，使得企业的安全防线如同虚设。由此可见，从容易被管理者忽视的企业内部员工安全意识着手，定期进行***安全意识培训和模拟社会工程演练***才是根本上降低企业安全风险的最优方案。

今年 Verizon 的《 2020 年数据泄露调查报告》显示，网络钓鱼仍是社会工程和恶意软件最常用的攻击手段和载体。根据国内全网监测评估，2019 年，全国企业邮箱用户共收到各类钓鱼邮件约 344.3 亿封，相比 2018 年收到各类钓鱼邮件的 204.3 亿封增长了 68.5%。2019 年全国企业邮箱用户收到的钓鱼邮件数量约占企业级用户邮件收发总量的 5.3%，平均每天约有 0.9 亿封钓鱼邮件被发出和接收。

这里引入一个我们钓鱼系统中常用的概念“钓鱼邮件中招率”（*Phishing Susceptibility Rate*，后文简称 PSR）表示员工收到钓鱼邮箱后，做出点击链接，扫描二维码和下载附件等危险操作的倾向。这里我们通过将风险转化为可衡量的术语和数值，方便企业领导者识别与排列人为风险优先级，从而有针对性地对症下药。

了解企业风险

一个企业的整体 PSR 表示有多少员工可能因社会工程或网络钓鱼受骗，从而进一步泄露个人或者公司的一些敏感信息。较高的 PSR 显然表示企业内部存在更大的风险，因为它通常反映了会有更多的员工做出危险操作。较低的 PSR 表明员工网络安全意识较强，并了解如何识别社会工程或网络钓鱼特征，避免做出危险的尝试。**网络钓鱼中招率（PSR）**在本报告中还将提供更多有价值的信息，比如我们将 PSR 在同行业内做了横向对比，方便企业了解自身在同行业中的风险定位。类似的我们用 PSR 在时间线上做了纵向对比，帮助企业能够了解整体行业在安全意识培训和模拟社会工程演练的投入，经过时间推移是否得到了对应的回报。

易念科技

中国首创的人为因素风险教育管理平台，已帮助中国上百家企业通过安全意识培训和模拟社会工程演练筑起了一道道坚实的企业“人脑防火墙“。易念科技的年度钓鱼行业分析报告通过严格的数据分析，帮助企业了解自身风险定位，设置安全意识学习目标。

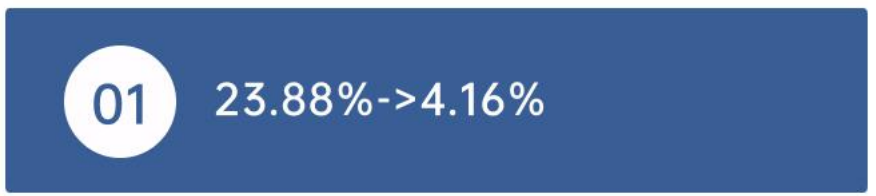
关键发现

我们的研究报告从后文三个阶段的数据发现了几个关键点：

在没有进行过安全意识培训和模拟社会工程演练的前提条件下，不管身处什么行业，每个企业都面临严重的信息泄露风险。统计结果表明所有行业的基准测试钓鱼中招率平均值是令人不安的 23.88%。这意味公司有超过五分之一的员工受到社会工程和网络钓鱼欺诈的威胁。

任何企业都可以用三个月至半年的时间，通过员工安全意识培训和模拟社会工程演练来减少企业信息泄露风险。前提是企业需要谨慎地定制一个培训计划，来帮助员工在短时间内提升自身的安全意识和技能水平。

长期坚持进行安全意识培训和有计划的模拟社会工程演练，可以帮助各行业把人的风险因素降到最低。从我们的数据来看，经过持续有计划的安全意识培训可以使各行业的平均钓鱼邮件中招率从 23.88%降至 4.16%，从另一个角度看，钓鱼邮件平均中招减少率达到了 83.19%。



横向分析各行业安全意识

在钓鱼演练完成后很多公司都会问这样的一个问题："**我们公司的网络钓鱼中招率相比其他同行业企业处于怎么样一个水平？**"为了在本报告中提供更为准确的答案，我们分析了近一年半内通过我们公司 **E-Phishing™** 平台进行的钓鱼测试，其中涵盖了 13 个不同行业，**106** 家企业，近 **120 万**用户，超过 **312 万**封钓鱼邮件，我们通过这些数据进行三个时间节点上的横向 PSR 对比，帮助企业了解自身在同行业中的安全意识水平和风险定位。

本报告中包含了十三个行业[1]，包括制造业；能源业；建筑业；交通运输、仓储和邮政业；信息传输、计算机服务和软件业；批发和零售业；医疗业；证券业；保险业；金融业（其他）；房地产业；科学研究；技术服务和地质勘查业；水利、环境和公共设施管理业。报告中的所有企业都按照上述行业进行了分类，**统计了每次钓鱼演练中员工点击链接，扫描二维码和下载邮件中附件的百分率作为企业网络钓鱼中招率（PSR）**。

我们的统计结果显示，近 120 万企业用户基本都完成了第一次的钓鱼邮件基准测试，我们把这次测试作为横向对比 PSR 的第一个时间节点。其中有 **67%** 的用户会在基准测试后的 3 到 6 个月的时间内做了第二次钓鱼邮件测试，我们把它作为第二次横向对比 PSR 的时间节点，我们把时隔一年左右的钓鱼测试作为最后一次横向对比 PSR 的时间节点。

纵向分析培训影响

为了方便企业了解安全意识培训的效果，我们同样沿用了上面提到的三个重要时间节点进行纵向的 PSR 数据分析：

- 第一阶段：企业尚未对员工进行安全培训，并且第一次做钓鱼邮件演练，我们监测各行业员工在钓鱼基准测试中的表现，并用 PSR 量化呈现数据。
- 第二阶段：经过几个月的安全意识培训后，我们再次对企业员工在钓鱼邮件测试中的表现进行监测，观察比较基准测试和网络安全意识培训后的演练在 PSR 数据上的变化。验证各行业在安全意识培训和模拟社会工程演练的投入是否得到对应的回报
- 第三阶段：经过持续的安全意识培训和模拟网络钓鱼测试，我们选取一年后的时间节点进行钓鱼测试，检验员工安全意识和技能经过一年时间提升对 PSR 产生的巨大影响。

[1] 参考中华人民共和国国家标准 国民经济行业分类 GB/T 4754—2017

- 制造业
- 能源业
- 建筑业
- 交通运输、仓储和邮政业
- 信息传输、计算机服务和软件业
- 批发和零售业
- 医疗业
- 证券业
- 保险业
- 金融业（其他）
- 房地产业
- 科学研究、技术服务和地质勘察业
- 水利、环境和公共设施管理业

谁在安全的“风口浪尖”

近 120 万企业用户的测试结果，为那些不愿在全员安全意识培训和模拟社会工程演练上有所投入的企业敲响了警钟，我们收集的 PSR 数据表明仅有少数行业的员工在识别网络钓鱼邮件方面做得很好。绝大多数情况下企业员工未经过安全意识测试或培训，很容易陷入钓鱼邮件预先设下的陷阱，使企业面临信息泄露的风险。

我们的统计结果表明，总共 13 个行业的钓鱼基准测试 PSR 平均值是 23.88%。不同行业的钓鱼邮件中招率各不相同，总结情况如下：

•在企业分类中**信息传输、计算机服务和软件业**的钓鱼基准测试中招率为 **43.61%**位列中招率第一。这一结果看似不太合理，究其原因，其一主要是计算机服务，软件服务业的员工需要长期坐在电脑屏幕前工作，对邮件信息相对比较敏感，其二，从事 IT 服务业并不代表其员工安全意识高，相反我们的数据佐证了恰恰相悖的结果。

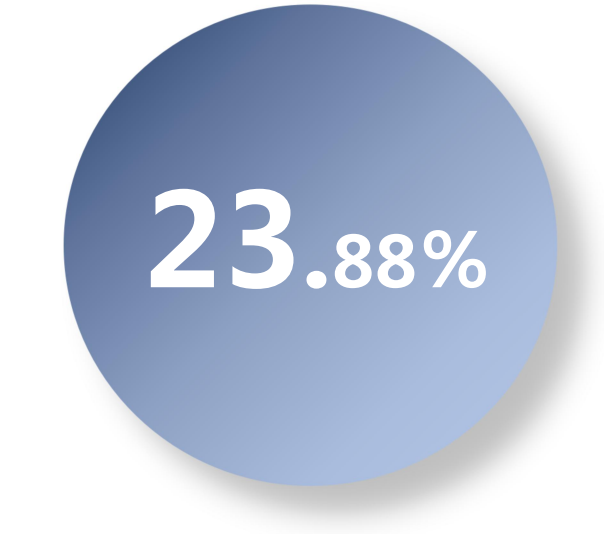
•在企业分类中钓鱼中招率排名第二的是**医疗业**，高达 30.5%。钓鱼邮件基准测试中招率排名第三的是**制造业**为 28.40%。金融业的钓鱼邮件中招率一般在 21%~25%左右，

•在基准测试中 PSR 排名最低的是科学研究、技术服务和地质勘查业，中招率仅为 8.77%。但无论数值如何，PSR 都反应了企业在真实钓鱼攻击中可能的中招率，都值得企业引起足够的重视，因为黑客只需要正确一次就足以突破企业的防线，造成严重损失，而对于企业而言则必须全力抵抗持续不断的攻击，不容有失。

第一阶段：

钓鱼邮件基准测试是在企业员工没有进行过安全意识培训和模拟社会工程演练的前提条件下进行的，PSR 数据客观反应了企业员工最初的安全意识和技能水平，真实表明了企业可能存在的数据泄露风险。统计结果表明所有行业的钓鱼基准测试 PSR 平均值是 **23.88%**。这意味着超过 1/5 员工可能会做出点击钓鱼链接，扫描二维码和下载附件的危险行为。在第一次的钓鱼基准测试中，很少有行业中招率低于 20%，其中信息传输、计算机服务和软件业的中招率最高为 43.61%；医疗和制造业分别为 30.50%和 28.40%，位列第二和第三；金融行业的中招率在 21%至 25%左右，科学研究、技术服务和地质勘查业中招率最低为 8.77%。从数据中我们不难得出以下结论：**企业员工在没有进行过安全意识培训和模拟社会工程演练的情况下，无论企业所处什么行业，无论在安全技术和产品上的投入如何，都容易成为网络钓鱼和社会工程的攻击对象。**

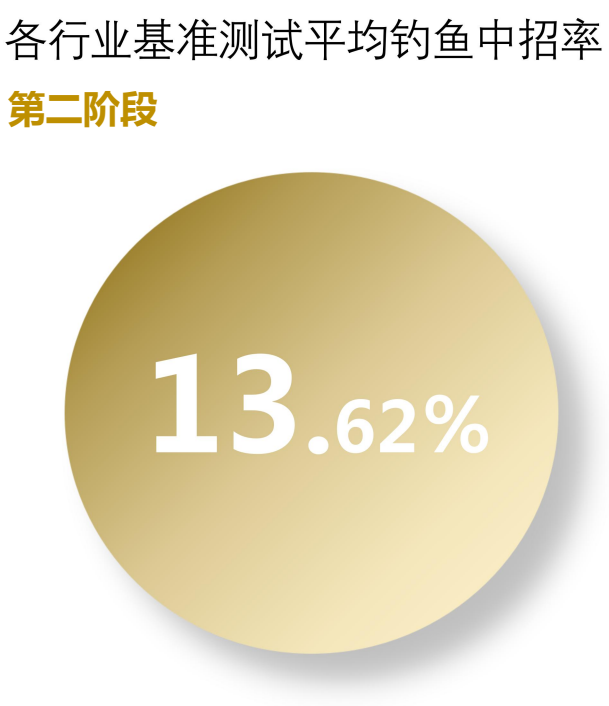
行业	PSR
制造业	28.40%
能源业	25.06%
建筑业	12.31%
交通运输、仓储和邮政业	20.02%
信息传输、计算机服务和软件业	43.61%
批发和零售业	17.67%
医疗业	30.50%
证券业	21.67%
保险业	24.98%
金融业(其他)	22.15%
房地产业	25.47%
科学研究、技术服务和地质勘查业	8.77%
水利、环境和公共设施管理业	12.84%



第二阶段：

我们的数据表明有 67%的企业用户会在基准测试后的 3 到 6 个月内做第二次钓鱼邮件测试，在这段时间内多数企业会通过我们的平台或者企业内部对自己的员工进行安全意识培训，这些企业的钓鱼邮件中招率相比第一次的基准测试降低了一半左右。但如果仔细观察下表我们同样发现少数行业的 PSR 并没有明显下降的趋势，甚至有些行业的 PSR 还略微上涨了一些，究其原因，可能在于部分企业割裂了钓鱼邮件演练和安全意识培训，他们仅仅为了合规要求进行了钓鱼邮件演练，而没有对员工做持续的安全意识培训，导致第二次钓鱼测试的 PSR 出现了不降反升的情况。尽管如此，所有行业第二次钓鱼测试总体的 PSR 平均值还是从 **23.88%**大幅**下降**到 **13.62%**，证明**在企业内部开展有效安全意识培训可以加强企业整体的安全状况，有效降低钓鱼邮件带来的信息泄露风险。**

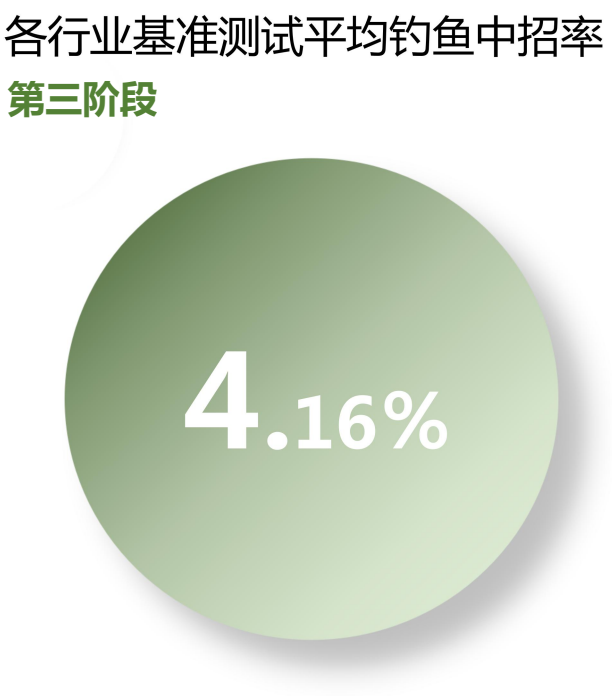
行业	PSR
制造业	11.72%
能源业	2.06%
建筑业	15.70%
交通运输、仓储和邮政业	19.77%
信息传输、计算机服务和软件业	28.63%
批发和零售业	2.76%
医疗业	14.16%
证券业	15.78%
保险业	12.13%
金融业(其他)	9.79%
房地产业	15.31%
科学研究、技术服务和地质勘查业	6.47%
水利、环境和公共设施管理业	10.28%

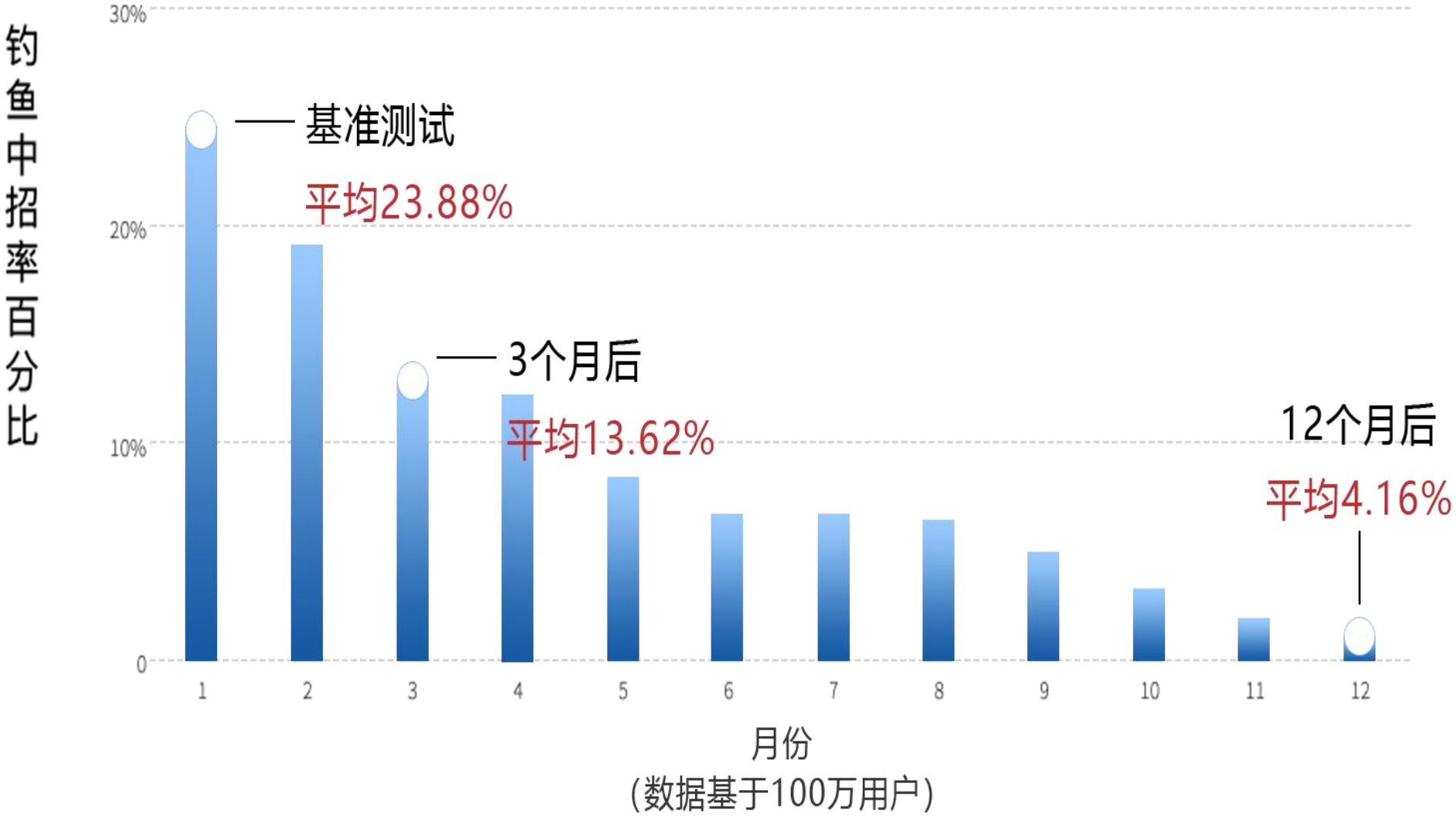


第三阶段：

在此阶段，我们为了排除上述一些企业带来数据上的干扰，突出安全意识培训的效果，故仅衡量了在 12 个月中始终坚持进行安全意识培训和按时模拟社会工程演练的企业。从下表上看，结果是显而易见的，持续有计划的安全意识培训使各行业的平均钓鱼邮件中招率从 23.88%降至 4.16%。各行业的中招率都基本下降到了原来的 1/5 左右。其中原先基准测试中，**钓鱼中招率排名第一的信息传输、计算机服务和软件业从 43.61%降到了 2.43%，金融行业的中招率也从 21%至 25%左右降到了 3%到 5%左右，**这些有目共睹的数据无不例外地说明了在企业内开展安全意识培训的巨大收益。

行业	PSR
制造业	5.42%
能源业	1.97%
建筑业	5.87%
交通运输、仓储和邮政业	6.74%
信息传输、计算机服务和软件业	2.43%
批发和零售业	2.06%
医疗业	5.07%
证券业	3.49%
保险业	2.13%
金融业(其他)	3.79%
房地产业	5.78%
科学研究、技术服务和地质勘查业	2.18%
水利、环境和公共设施管理业	3.23%




钓鱼中招率百分比
30%
20%
10%
0
基准测试
平均23.88%
3个月后
平均13.62%
12个月后
平均4.16%
1
2
3
4
5
6
7
8
9
10
11
12
月份
(数据基于100万用户)

各行业钓鱼邮件中招减少率

经过一年持续的安全意识培训和模拟社会工程演练，所有行业企业员工的安全意识和技能都有明显的提升。 **其中信息传输、计算机服务和软件业的钓鱼邮件中招减少率最高，是 94.43%，而金融行业的中招减少率在 82%到 91%左右。** 所有行业中交通运输、仓储和邮政业中招减少率最低为 66.33%。纵观所有行业从钓鱼基准测试经过一年左右的安全意识培训及定时的模拟网络钓鱼测试，PSR 平均中招减少率高达到 83.19%。这一结果验证了我们开头的观点——**安全意识培训和模拟社会工程演练是根本上降低企业安全风险的最优方案。**

行业	PSR
制造业	80.92%
能源业	92.14%
建筑业	52.32%
交通运输、仓储和邮政业	66.33%
信息传输、计算机服务和软件业	94.43%
批发和零售业	88.34%
医疗业	83.38%
证券业	83.89%
保险业	91.47%
金融业(其他)	82.89%
房地产业	77.31%
科学研究、技术服务和地质勘查业	75.14%
水利、环境和公共设施管理业	74.84%

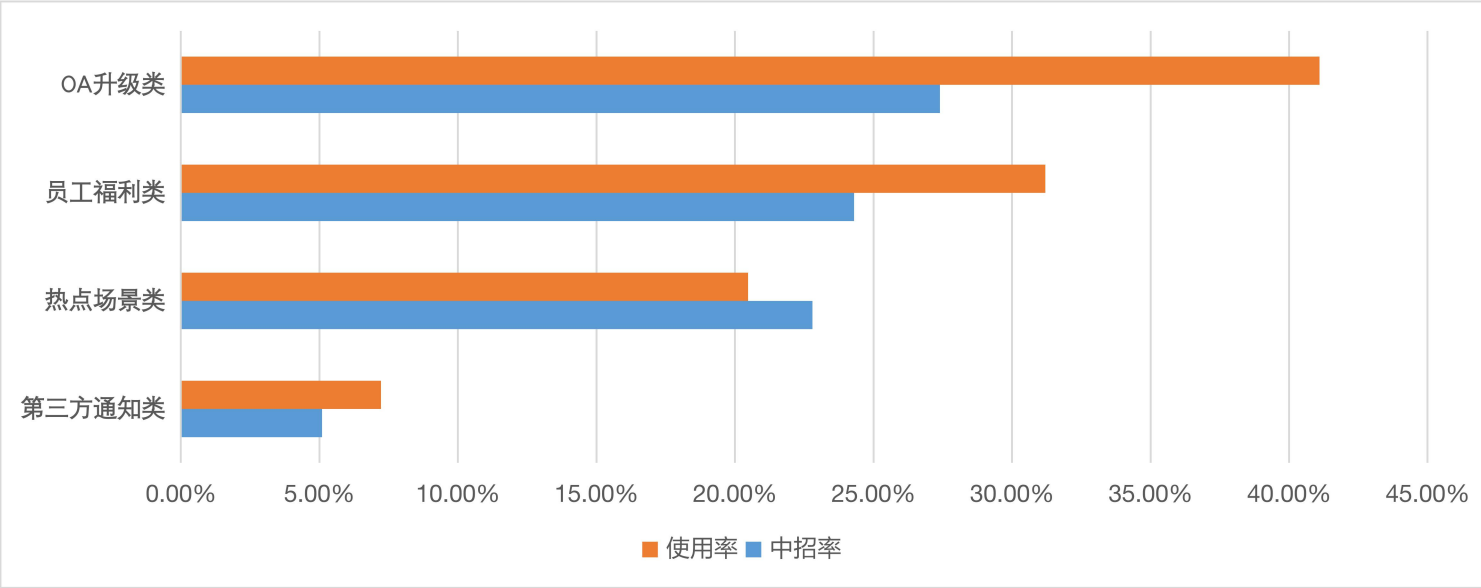
各行业钓鱼邮件中招减少率

83.19%

模板主题中招率和使用率对比

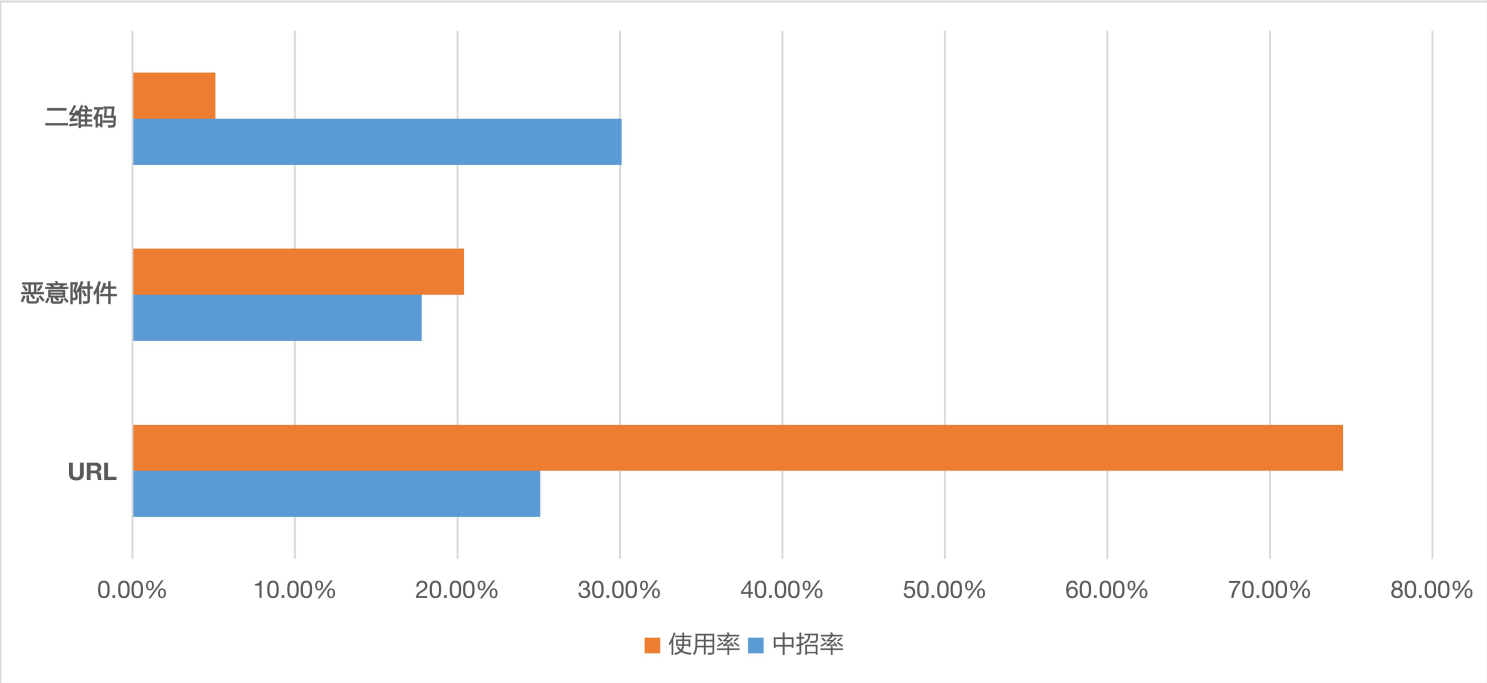
之前我们分析了不同企业在时间线上横向和纵向的 PSR 表现，这个小节我们比较一下不同主题模板的钓鱼邮件中招率和使用率。在易念科技的钓鱼演练中，我们为客户提供了匹配真实世界场景的各类主题模板，我们通常把主题分为 4 大类：**OA 升级类；员工福利类；第三方通知类和热点场景**。我们一年半收集的数据表明，“OA 升级类”和“员工福利类”主题在基准测试中获得了最高的钓鱼邮件中招率分别为 27.4%和 24.3%，使用率也高达 41.1%和 31.2%。除了这两个主题以外，热点场景类的主题模板因为国内疫情的原因，PSR 为 22.8%排名第三，使用率在 20.48%左右。排名最后的是第三方通知类的模板中招率为 5.1%，使用率为 7.22%。

从结果上看前两类的主题邮件中招率和使用率排名前二显得理所应当，基准测试中如果员工在办公室收到以公司名义发送的 OA 升级或者员工福利相关的电子邮件，点击查看是再正常不过的情况。相反的因为国内以第三方名义发送的营销广告和钓鱼邮件泛滥，员工看到以第三方名义发送的邮件甚至连打开邮件的想法都没有，导致第三方通知类模板的中招率并不理想。再看热点场景类的模板，比如**新冠疫情类的主题邮件在 3 月份的中招率高达 40%左右**，但同样的邮件在 6 月只有 10%左右的中招率，这表明这类模板有极强的实时性，需要不断根据现实场景更改内容来保证演练的效果。



模板类型中招率和使用率对比

我们的钓鱼系统通常把模板分为 3 大类：**URL 钓鱼**，**恶意附件钓鱼**和**二维码钓鱼**。在基准测试中的中招率和使用率对比如下图，其中 URL 钓鱼的使用率最高为 74.5%，中招率为 25.1%；二维码钓鱼的中招率最高为 30.1%，但使用率最低为 5.1%，恶意附件钓鱼的中招率比较低为 17.80%，使用率为 20.40%。这里我们分析二维码钓鱼中招率比较高的原因有二：其一是国内二维码普及和接受率远超世界其他地区；其二是二维码钓鱼可以有效的规避鼠标悬停对邮件中链接的检查，增加识别钓鱼邮件的困难度；虽然此类钓鱼邮件的中招率尚可，但通常企业对于这种钓鱼类型的接受程度却不是很高，他们潜意识中更倾向于使用传统的 URL 的钓鱼方式去做演练测试导致使用率偏低。

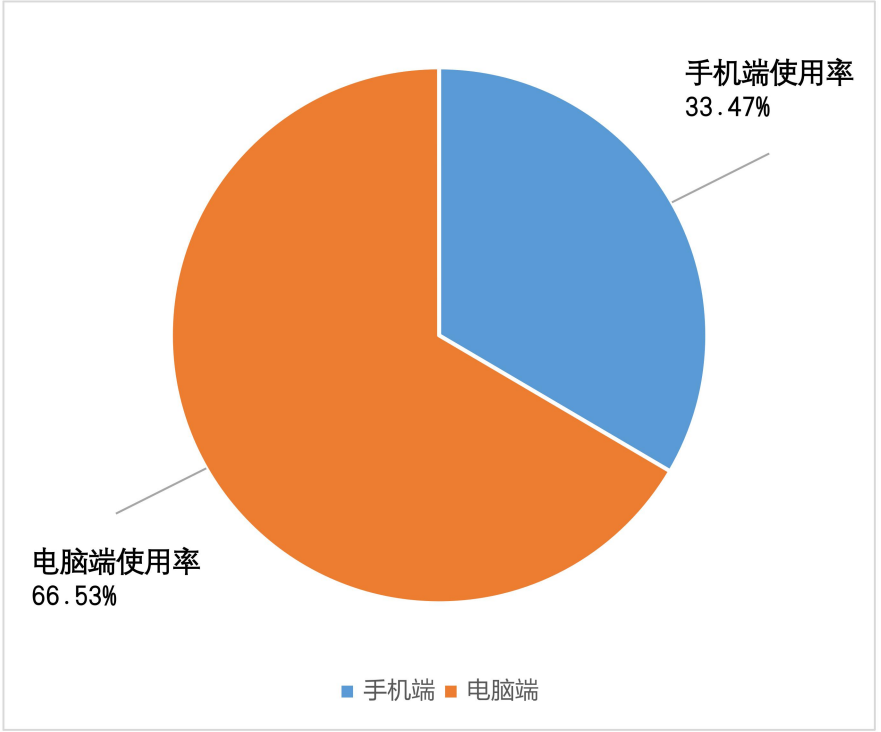


用户客户端对比

我们这里主要对比基准测试中手机平台和电脑平台使用率。

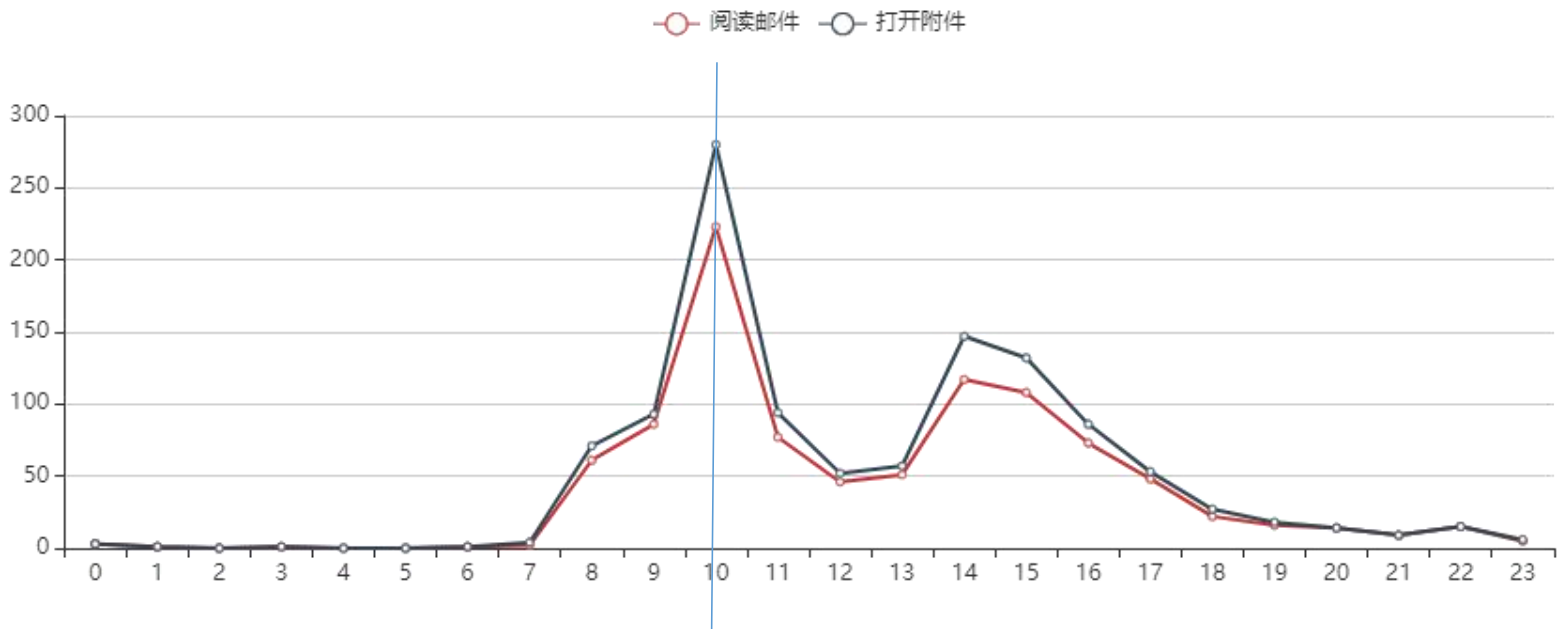
随着移动端硬件配置的不断增强，以及 4G、5G 网络的升级优化和通讯资费普遍降低，移动互联进入了井喷期，白领们已经习惯于通过移动端来处理工作。国内现有数据显示，已有 68%的用户会每天通过手机查邮件。但从我们收集的测试数据来看阅读钓鱼邮件的平台比率，手机端平均占比 33.47%，电脑端平均占比 66.53%，说明除了少数行业，在办公室工作的员工，还是倾向于用电脑作为邮件阅读的主要平台。

行业	手机端	电脑端
制造业	31.09%	68.91%
能源业	29.59%	70.41%
建筑业	24.02%	75.98%
交通运输、仓储和邮政业	36.93%	63.07%
信息传输、计算机服务和软件业	16.59%	83.41%
批发和零售业	21.57%	78.43%
医疗业	32.49%	67.51%
证券业	25.97%	74.03%
保险业	9.33%	90.67%
金融业(其他)	39.90%	60.10%
房地产业	44.59%	55.41%
科学研究、技术服务和地质勘查业	29.77%	70.23%
水利、环境和公共设施管理业	93.28%	6.72%



钓鱼演练时间选择

一天中在什么时间段做钓鱼测试中招率会比较高？我们收集的数据指出，在工作日，除了发送完钓鱼邮件后的 1 到 2 小时内必然会有一个最高的中招峰值，通常员工登录邮箱主要有 9 点和 14 点为波峰的两个高峰期。所以，选择在 9 点–10 点、14 点–15 点做钓鱼演练可能会得到比较令人满意的数据结果。



钓鱼邮件演练入门

易念科技已经帮助中国上百家分布在金融，能源，房产，建筑，制造等行业的企业通过安全意识培训和模拟社会工程演练筑起了一道道坚实的企业“人脑防火墙”。从我们的数据上不难看出，企业可以通过测试和培训从根本上减少漏洞并最终改变企业内部员工的行为。但很多企业都有这样的疑问 ***“我们对构筑企业“人脑防火墙”很有兴趣”，但我们应该从何做起呢？***

易念科技提供的解决方案包含如下 4 个步骤：

① 钓鱼基准测试

钓鱼邮件基准测试是在企业员工没有进行过安全意识培训和模拟社会工程演练的前提条件下进行的，其 PSR 数据客观反应了企业员工最初的安全意识和技能水平，真实表明了企业可能存在的数据泄露风险，也是衡量未来安全意识教育是否成功的必要参照，其重要性不言而喻。**企业在规划第一次基准测测试时需要全局考虑，结合自身业务场景定制方案**，客观地评估企业的安全风险，为后面的培训工作打好基础。

② 开展新颖的培训

传统意识教育方式内容枯燥、难以吸引员工注意力。企业可以通过**交互式培训**来教育员工识别与防范钓鱼邮件，也可以通过**竞赛答题、视频教学、互动体验**等多种方式开展安全意识教育工作。针对钓鱼邮件的特征，结合本单位关注主要风险，构建教育素材内容。吸引提高员工对安全意识教育的积极性。

③ 坚持钓鱼邮件演练

坚持**每三个月做至少一次模拟钓鱼演练**，避免长时间后员工放低警惕性。演练同时可以加强和检验企业员工的安全意识教育培训成果。钓鱼测试和培训的最终目的是改变企业内部员工的行为，从量变到质变需要一个长期的时间积累和巩固。

④ 评估结果，让演练本身与员工有关

及时评估员工经过培训后的钓鱼演练结果，让演练本身与员工有关。人们通常只关心对他们有意义的事情，**确保企业的模拟攻击与员工日常活动相关，关注员工的行为改变**。安全培训不是仅仅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，还要集中精力调整他们的安全反应，这样员工才能成为企业有效的最后一道防线。

企业实施中常见的误区

误区一：过分注重员工的情绪及感受

模拟钓鱼演练必须站在攻击者的角度用真实的攻击和方法去评估员工的安全意识和技能水平。否则，企业的“培训”只会给组织一种虚假的安全感。同理，现实中的黑客不存在对企业员工的怜悯和同情。诚然，在演练中权衡员工的情绪是极其重要的，不然钓鱼演练的效果只会适得其反。但是又不能过分注重员工的情绪及感受而影响到演练的仿真效果，企业负责人需要找到其中的平衡点。

误区二：培训和演练完全是企业信息安全专业人员的事。

演练应该团结能够团结的一切力量。让其他团队的人员和主管，包括人力资源、IT 甚至市场营销一起参与其中。创造一种积极地、全公司范围的安全文化。

误区三：信息安全意识教育培训一次就够了

在我们所服务过的客户中，有很多企业和组织的领导者或者人力资源部门认为，提高全员信息安全意识就只是为了国家的一些合规要求，而且搞一次就够了，实际上信息安全意识教育远不止搞一次培训这么简单。正是基于这种思想，即便搞了培训效果也不好，这样就陷入了一个恶性循环的怪圈之中。而在我们服务过的客户中，每年进行 2~6 次钓鱼测试演练的居多，也呈现出了比较好的教育效果。

误区四：高层领导是例外

绝大多数我们服务过的企业和组织在钓鱼演练实施的过程中，会除去企业的管理者，这种情况无可厚非。但是我们从少数没有在演练中除去管理人员的企业那得到的数据显示管理角色在钓鱼演练中的中招率并不低，外加上管理者通常手上拥有企业极其重要的信息资源，其风险等级可见一斑。我们还可以类比之前提过的 IT 从业人员的例子，同样的身处高位并不代表其安全意识就高。

误区五：员工可能无法分辨钓鱼邮件和正常邮件

有些企业害怕频繁的钓鱼邮件测试会影响员工对正常邮件的判断力，从而影响到正常的工作，这里又要重新提及安全意识培训的重要性，永远不要让钓鱼演练和培训割裂，企业完全可以在安全意识课程中加入钓鱼邮件现状以及如何识别钓鱼邮件，强化对钓鱼邮件的认知。

易念科技是中国网络安全意识教育的领导企业

旗下：HumanRisk™是中国首创的人为因素风险教育管理平台

易念科技是中国网络安全意识教育的领导企业，提供在线教育、钓鱼演练、案例体验、风险度量等安全意识教育内容、平台与运营服务，改变员工风险认知，建立企业安全文化。公司秉承意识决定安全的核心理念，致力于打造网络安全人脑防火墙。

HumanRisk™–人为因素风险教育管理平台，由 CSAO™Store 知识库、 HackDemo™案例体验工具、M–learning™主题教育与测评、 E–Phishing™钓鱼仿真演练、EasyMind™人员风险态势感知等五大模块构成，基于中国用户场景，应用行为心理学的核心思想 ，赋能企业建立人员安全教育的测评、教育、验证、运营、度量全过程管理，提升企业风险管理水平。