易念科技

改变认知 建立文化

E-Phishing

2021

企业邮件钓鱼演练分析报告

易念科技|Coremail

目录

介绍

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钓鱼邮件演练***才是根本上降低企业安全风险的最优方案。

Verizon 的《2021 年数据泄露调查报告》（DBIR）指出，2021 年数据泄露的主要原因来自 Web 应用程序攻击、 网络钓鱼和勒索软件。在疫情、远程办公等时势的影响下，涉及网络钓鱼的违规行为相较去年增加了 11%，占比达到了 36%。和去年一样，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 Coremail 与奇安信行业安全研究中心的联合监测评估，2020 年，全国企业邮箱用户共收到各类钓鱼邮件约 460.9 亿封，相比 2019 年收到各类钓鱼邮件的 344.3 亿封增长了 33.9%，2021 年钓鱼邮件规模可达 500亿封。2020 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 6.9%，平均每天约有 1.3 亿封钓鱼邮件被发出和接收。

由此可见钓鱼邮件引起的安全风险日趋严峻，若员工未接受任何钓鱼邮件的培训或演练，员工收到钓鱼邮件 “中招” 的概率将极高。

这里引入一个我们钓鱼系统中常用的概念 “钓鱼中招率”（*Phishing Fraud Rate*，后文简称 PFR）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 PFR 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 PFR 显然表示企业内部存在更大的风险，因为它反应了通常会有更多的员工会做出危险操作。较低的 PFR 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（PFR）在本报告中还将提供更多有价值的信息，比如我们将 PFR 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 PFR 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钓鱼邮件演练的投入经过时间推移是否得到了对应的回报。

易念科技和 Coremail

易念科技在中国首创了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钓鱼邮件演练筑起了一道道坚实的企业 “人脑防火墙 “。本报告结合了易念科技和 Coremail 多年在企业钓鱼邮件演练领域的丰富实践经验及研究成果，希望此份报告能为企业了解自身风险定位，设置安全意识学习目标有所帮助。

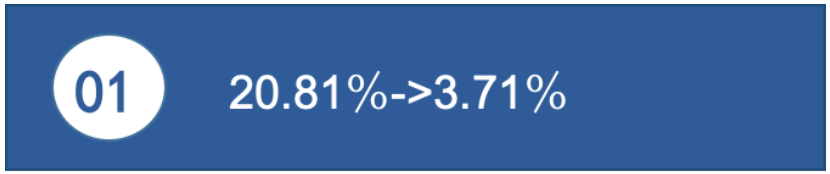
关键结果

我们的研究报告从三个阶段的数据结果可以总结以下几个结论：

在没有进行过安全意识培训和模拟钓鱼邮件演练的前提条件下，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钓鱼基准测试 PFR 平均值是令人不安的 20.81%。这意味公司有将近五分之一的员工受到社会工程和网络钓鱼诈骗的威胁。

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钓鱼邮件演练来加强企业信息泄露风险抗性。前提企业需要谨慎地定制一个优秀的培训计划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钓鱼邮件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 **20.81%**降至 **3.71%**，从另一个角度看，钓鱼邮件中招减少率也高达 **82.17%**。



2021 年钓鱼邮件行业分析报告

横向分析各行业安全意识

在钓鱼邮件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 2021 年通过我们公司平台进行的钓鱼测试，其中涵盖了 **14** 个不同行业，**148** 家企业，**164** 万测试用户，超过 **342** 万封钓鱼邮件，我们通过将这些数据进行三个时间节点上的横向 PFR 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。

本报告中包含了十四个行业[1]，包括制造业；电力、燃气及水生产和供应业；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；银行业；证券业；保险业；其他金融业；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（PFR）。**

我们的统计结果显示，164 万企业用户都完成了钓鱼邮件基准测试，我们把这次测试作为横向对比 PFR 的第一个时间节点。今年有 77%的企业会在基准测试后的 3 到 6 个月的时间内做了第二次钓鱼邮件测试（比去年高 10%），我们把它作为第二次横向对比 PFR 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 PFR 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 PFR 数据分析：

- 第一阶段：企业尚未对员工进行针对性的安全培训，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 PFR 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 PFR 数据上的变化。验证各行业在安全意识培训和模拟钓鱼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演练，我们选取一年后的时间节点进行钓鱼邮件测试，检验员工安全意识和技能经过一年时间提升对 PFR 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；
- 电力、燃气及水生产和供应业；
- 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；
- 银行业；
- 证券业；
- 保险业；
- 其他金融业；
- 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

谁在安全的“风口浪尖”

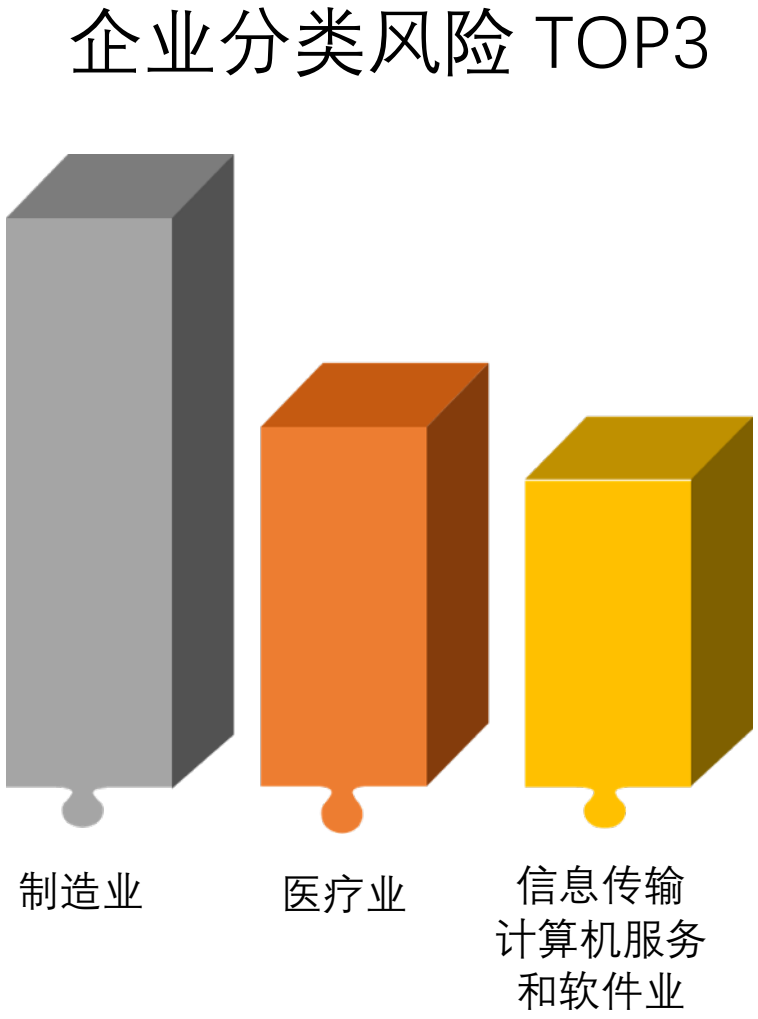
164 万企业用户的测试结果为那些不愿在全员安全意识培训和模拟钓鱼邮件演练上有所投入的企业敲响了警钟，我们收集的 PFR 数据表明仅有少数行业的员工在识别网络钓鱼邮件方面做得很好。绝大多数情况下企业员工未经过安全意识测试或培训，很容易陷入钓鱼邮件预先设下的陷阱，使企业面临信息泄露的风险。

我们的统计结果表明所有 14 个行业的钓鱼基准测试 PFR 平均值是 20.81%，相较于于去年降低了 3%，有一定的改善，但整体基本仍处于较高风险的水平。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**制造业**的钓鱼基准测试中招率为 27.84%位列中招率第一。2021 年新冠疫情的持续影响给制造行业带来了冲击，催化了不少制造企业信息化、数字化的进一步转型升级，员工相比于过去增加了更多使用 IT 设备工作的时间，这导致了钓鱼邮件和社会工程有了更多可乘之机。

•在企业分类中钓鱼中招率排名第二的是**医疗业**，高达 25.28%，最近几年针对医疗行业的钓鱼邮件攻击、勒索软件事件时有发生，需要该行业同仁加以重视。钓鱼邮件基准测试中招率排名第三的是**信息传输、计算机服务和软件业**，值得注意的是该行业去年排名第一，今年有了较大的提升，中招率下降到 23.48%。

•今年在基准测试中 PFR 排名最低的是建筑业，中招率仅为 6.33%。但无论数值如何，PFR 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，因为黑客只需要成功一次就足以突破企业的防线，造成严重损失。



第一阶段：

钓鱼邮件基准测试是在企业员工没有进行过针对的安全意识培训和模拟钓鱼邮件演练的前提条件下进行的，PFR 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 PFR 平均值是 **20.81%**。这意味着将近 1/5 员工面对钓鱼邮件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，多数行业中招率在 20%左右，其中制造业的中招率最高为 27.84% ;医疗和信息传输、计算机服务和软件业分别为 25.28%和 23.48%，位列第二和第三。所有行业中建筑业中招率最低，为 6.33%。从数据中我们不难得出以下结论：**企业员工在没有进行过针对的安全意识培训和模拟钓鱼邮件演练的情况下，每个企业无论所处什么行业，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	PFR
制造业	27.84%
能源业	13.31%
建筑业	6.33%
交通运输、仓储和邮政业	18.15%
信息传输、计算机服务和软件业	23.48%
批发和零售业	18.31%
医疗业	25.28%
银行业	21.41%
证券业	19.87%
保险业	20.06%
金融业(其他)	21.47%
房地产业	18.04%
科学研究、技术服务和地质勘查业	15.41%
水利、环境和公共设施管理业	7.22%

第二阶段：

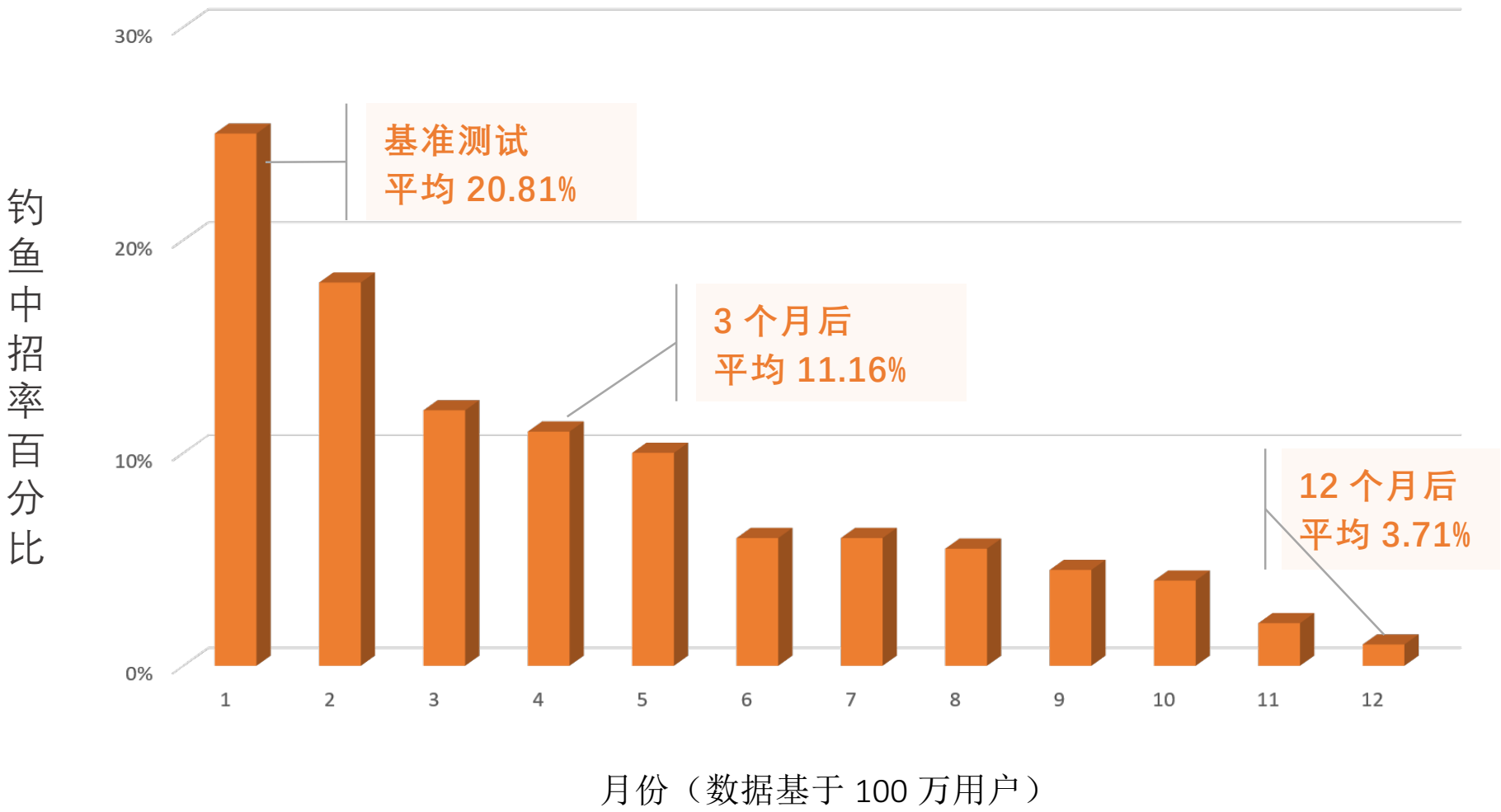
我们的数据表明 2021 年有 77%的企业用户会在基准测试后的 3 到 6 个月内做第二次钓鱼邮件测试，对比去年的 67%有了明显增加。在这段时间内多数企业会通过我们的平台或者企业内部对员工进行安全意识培训，这些企业的钓鱼邮件中招率相比第一次的基准测试降低了将近一半。但如果仔细观察表 2 我们同样发现少数行业的 PFR 并没有明显下降的趋势，甚至有个别行业的 PFR 还略微上涨了一些，究其原因，可能在于钓鱼邮件的仿真度和钓鱼模板对员工的吸引力过高，导致第二次钓鱼测试的 PFR 出现了不降反升的情况。尽管如此，所有行业第二次钓鱼测试总体的 PFR 平均值还是从 **20.81%**大幅**下降**到 **11.16%**，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	PFR
制造业	12.78%
能源业	8.50%
建筑业	7.25%
交通运输、仓储和邮政业	11.21%
信息传输、计算机服务和软件业	10.34%
批发和零售业	13.93%
医疗业	13.15%
银行业	8.85%
证券业	9.76%
保险业	9.07%
金融业(其他)	7.72%
房地产业	17.01%
科学研究、技术服务和地质勘查业	5.52%
水利、环境和公共设施管理业	4.38%

第三阶段：

在 2021 年我们发现，能够持续坚持进行钓鱼邮件演练的的企业相比 2020 年多。诚然，合规需求是目前钓鱼演练的核心驱动，但同时我们也从数据上看到了越来越多的企业出于保护自身信息资产，在安全意识教育上有更多的投入。在 12 个月中坚持进行安全意识培训和模拟钓鱼邮件演练的企业，从表 3 上看，效果是显而易见的，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 20.81％降至 3.71％。各行业的中招率都基本下降到了原来的 1/5 左右。其中，基准测试中钓鱼中招率排名第一的**制造业**从 27.84％降到了 2.77％，医疗行业的中招率也从 25.28％降到了 4.38%左右，这些有目共睹的数据都说明了在企业内开展安全意识培训和钓鱼邮件演练带来的显著收益。

行业	PFR
制造业	2.77%
能源业	1.87%
建筑业	1.53%
交通运输、仓储和邮政业	2.05%
信息传输、计算机服务和软件业	4.52%
批发和零售业	3.33%
医疗业	4.38%
银行业	2.45%
证券业	3.30%
保险业	3.73%
金融业(其他)	4.05%
房地产业	4.12%
科学研究、技术服务和地质勘查业	3.22%
水利、环境和公共设施管理业	1.79%


钓鱼中招率百分比
30%
20%
10%
0%
基准测试
平均 20.81%
3 个月后
平均 11.16%
12 个月后
平均 3.71%
1
2
3
4
5
6
7
8
9
10
11
12
月份（数据基于 100 万用户）

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钓鱼邮件演练，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，**制造业取得了最高的钓鱼邮件中招减少率为 90.05%。交通运输、仓储和邮政业**的减少率为 88.71%，**银行业也达到 88.56%**。纵观所有行业，从钓鱼基准测试到经过一年左右的安全意识培训及定时的模拟网络钓鱼邮件测试，PFR 平均改善率高达到 82.17%。这一结果验证了我们的观点——**安全意识培训和模拟钓鱼邮件演练是根本上降低企业安全风险的最优方案。**

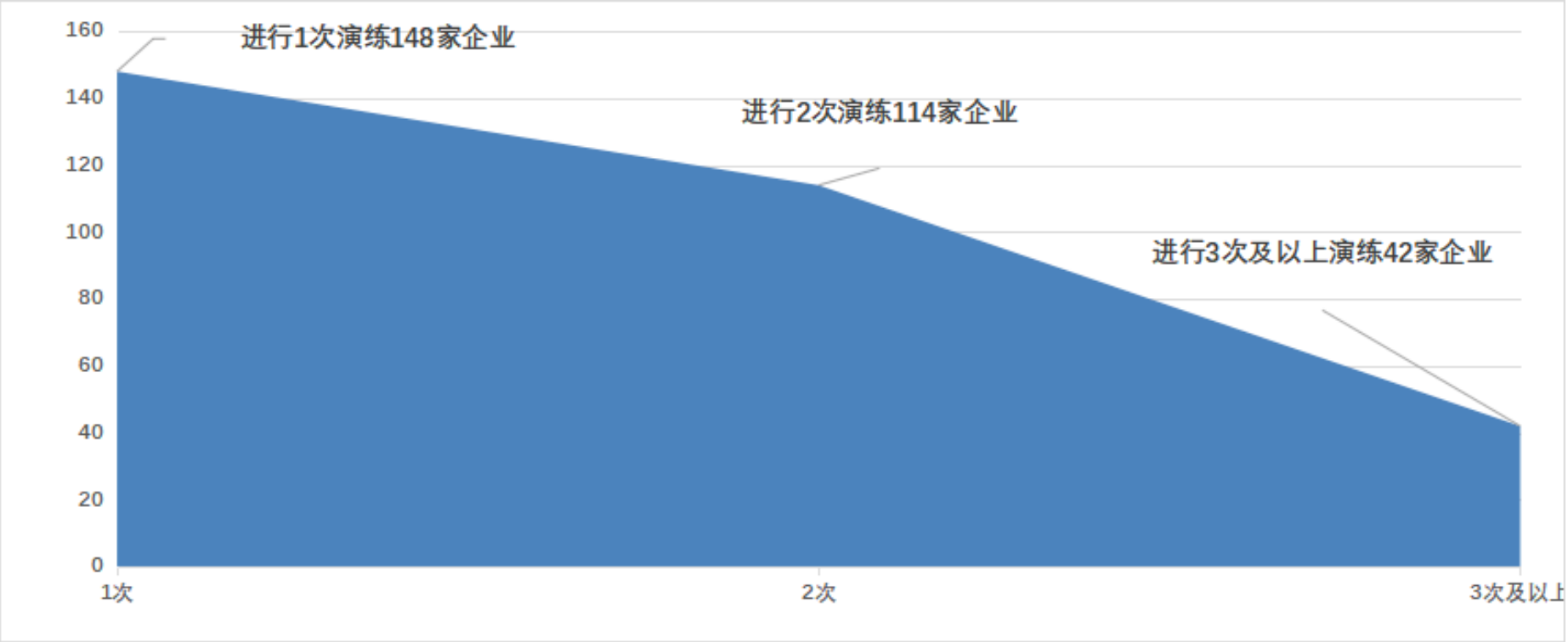
行业	PFR
制造业	90.05%
能源业	85.95%
建筑业	75.83%
交通运输、仓储和邮政业	88.71%
信息传输、计算机服务和软件业	80.75%
批发和零售业	81.81%
医疗业	82.67%
银行业	88.56%
证券业	83.39%
保险业	81.41%
金融业(其他)	81.14%
房地产业	77.16%
科学研究、技术服务和地质勘查业	79.10%
水利、环境和公共设施管理业	75.21%

各行业钓鱼邮件中招减少率

82.17%

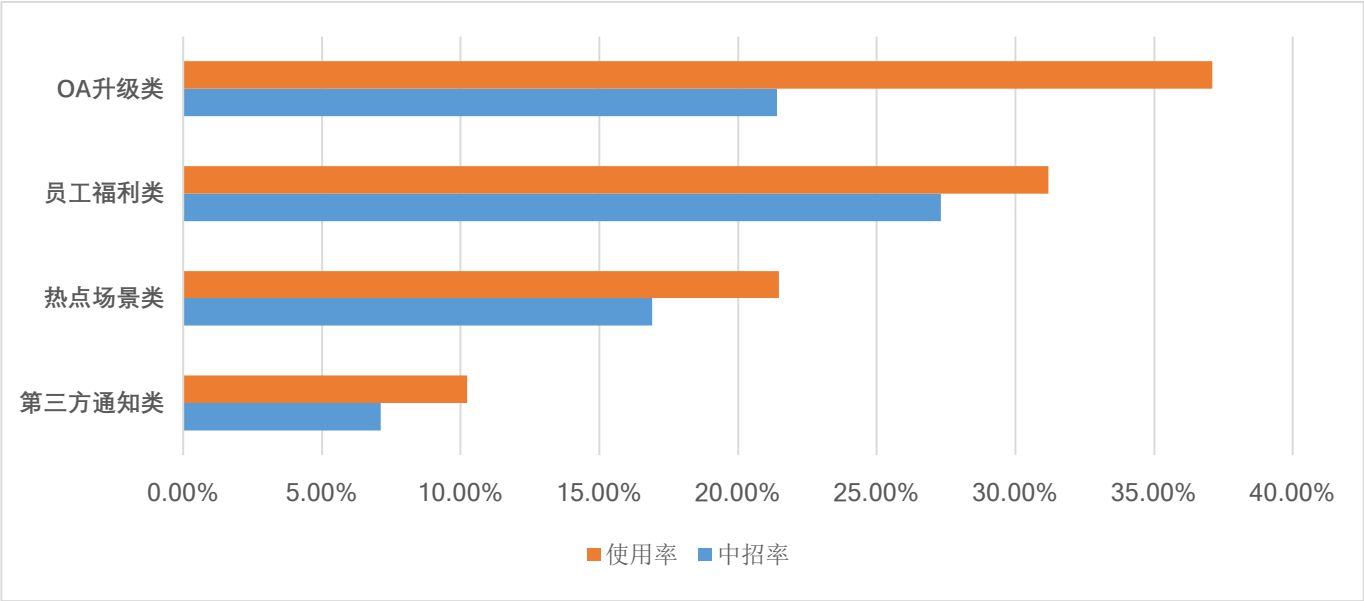
2021 年企业钓鱼演练次数

2021 年我们统计了各行业企业一年内钓鱼演练的次数。 其中，有 **148** 家企业的员工在今年进行了基准测试。有 **114** 家企业会在基准测试后的 3 到 6 个月内做第二次钓鱼演练测试，约占 77%，相比去年提升 **10%**左右。一年内有过三次或者三次以上钓鱼演练的企业有 **42** 家。从结果上看，随着近几年国家**对网络安全宣贯的不断加强和相关活动的增多，企业在安全意识的重视程度和投入比之前都有所增加。**



模板主题中招率和使用率对比

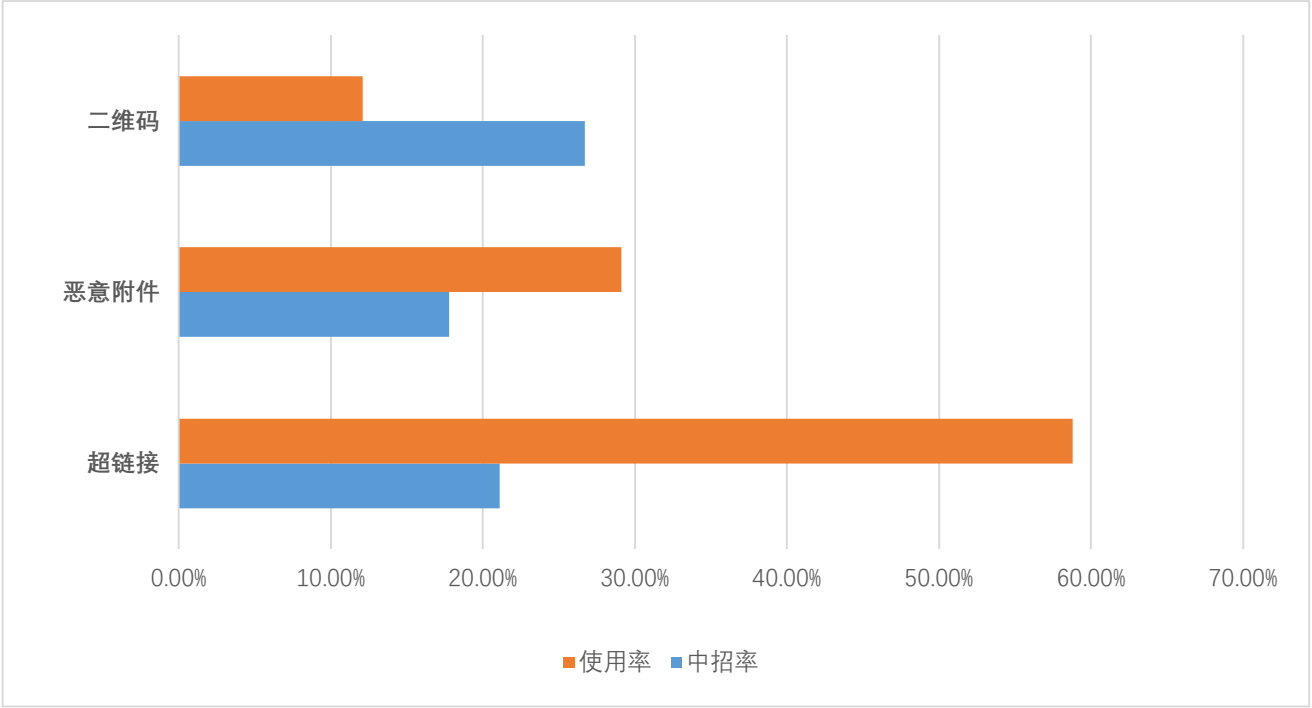
在易念科技的钓鱼演练中，我们为客户提供了匹配真实场景的各类主题模板，我们通常把主题分为 4 大类：**OA 升级类；员工福利类；第三方通知类和热点场景类**。通过比较不同主题模板的钓鱼邮件使用率和中招率，数据表明，“员工福利类”和“OA 升级类”主题在基准测试中获得了较高的钓鱼邮件中招率分别为 27.70%和 21.10%，“OA 升级类”和“员工福利类”使用率也分别高达 37.10%和 31.20%。除了这两个主题以外，热点场景类的主题模板因为国内疫情的原因，PFR 为 16.90%排名第三，使用率在 21.48%左右。排名最后的是第三方通知类的模板中招率为 7.12%，使用率为 10.21%。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**，点击查看的概率很高。相反，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，今年**以疫苗预约接种和疫苗接种情况调查为主题的模板**比较常见，但同样的模板放到免费接种结束后效果就不是很理想，这表明这类模板有极强的时效性，需要不断根据现实场景更改内容来保证演练效果。



模板类型中招率和使用率对比

易念科技的钓鱼系统通常把钓鱼形式分为 3 大类：**超链接钓鱼、恶意附件钓鱼和二维码钓鱼**。在基准测试中中招率和使用率对比如下图，其中超链接钓鱼的使用率最高为 58.80%，中招率为 21.10%；二维码钓鱼的中招率最高为 26.70%，使用率最低为 12.10%。恶意附件钓鱼的中招率相对较低为 17.80%，使用率为 29.10%。

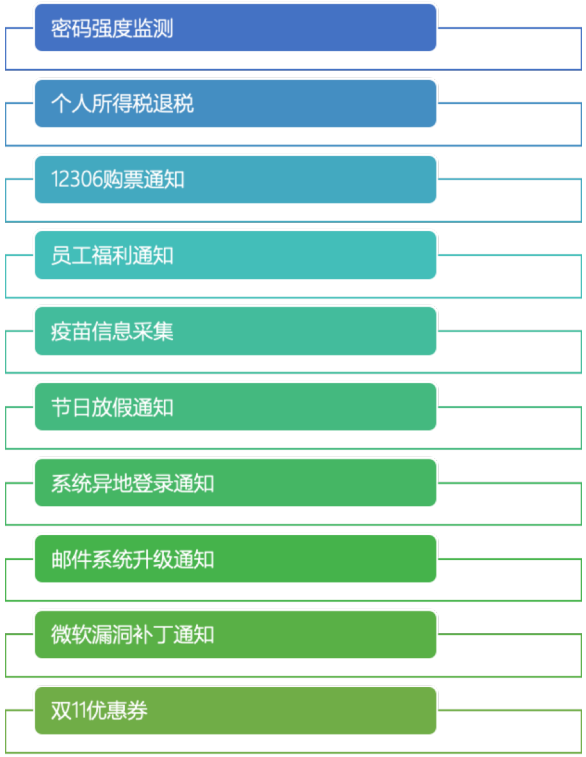
二维码钓鱼中招率比较高的主要原因：其一是国内二维码普及和接受率远超世界其他地区；其二是二维码钓鱼可以有效的规避鼠标悬停对邮件中链接的检查，增加识别钓鱼邮件的困难度。虽然此类钓鱼邮件的中招率很高，但通常企业对于这种钓鱼形式的接受程度却不是很高，他们潜意识中更倾向于使用传统点击超链接的钓鱼方式去做演练测试。



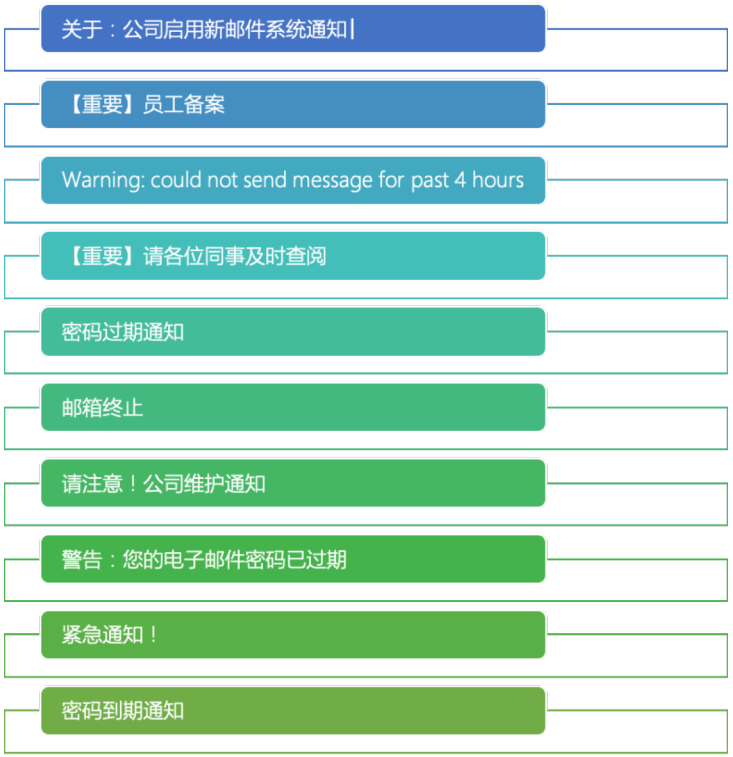
TOP 10 大钓鱼邮件主题

在 2021 年，我们通过钓鱼演练测试平台监测了数以百万计的钓鱼邮件主题数据，同时我们还通过 Coremail 的 CAC 反垃圾日志，监测从 2021 年 1 月 1 日至 12 月 31 日识别出的钓鱼邮件，统计出了 10 大钓鱼常用演练模板主题和 10 大真实钓鱼邮件主题，结果如下;

10 大钓鱼常用演练模板主题（排名不分先后）



10 大真实钓鱼邮件主题（Coremail 排名不分先后）



以下来自于 10 大真实钓鱼邮件主题的部分截图

[重 要]员工备案!

oa_server

发给 wu[redacted]om.cn

发件人: oa_server<run[redacted]na.com>

收件人: wu[redacted].com.cn<wu[redacted].com.cn>

时间: 2021年11月14日 (周日) 03:28

大小: 5 KB

E-mail邮箱系统计划于即日起开始进行迁移升级

请如实填写下列信息，回复此邮件!

姓名:

职位:

邮箱账号:

登陆密码:

历史密码:

注：请在收到邮件后立即进行回复，逾时将被回收账号!

加班補貼工資

財務部

发给 gao[redacted]l.com

发件人: 財務部<fuke-wang@163.com>

收件人: gao[redacted].com<gao[redacted].com>

时间: 2021年6月9日 (周三) 09:23

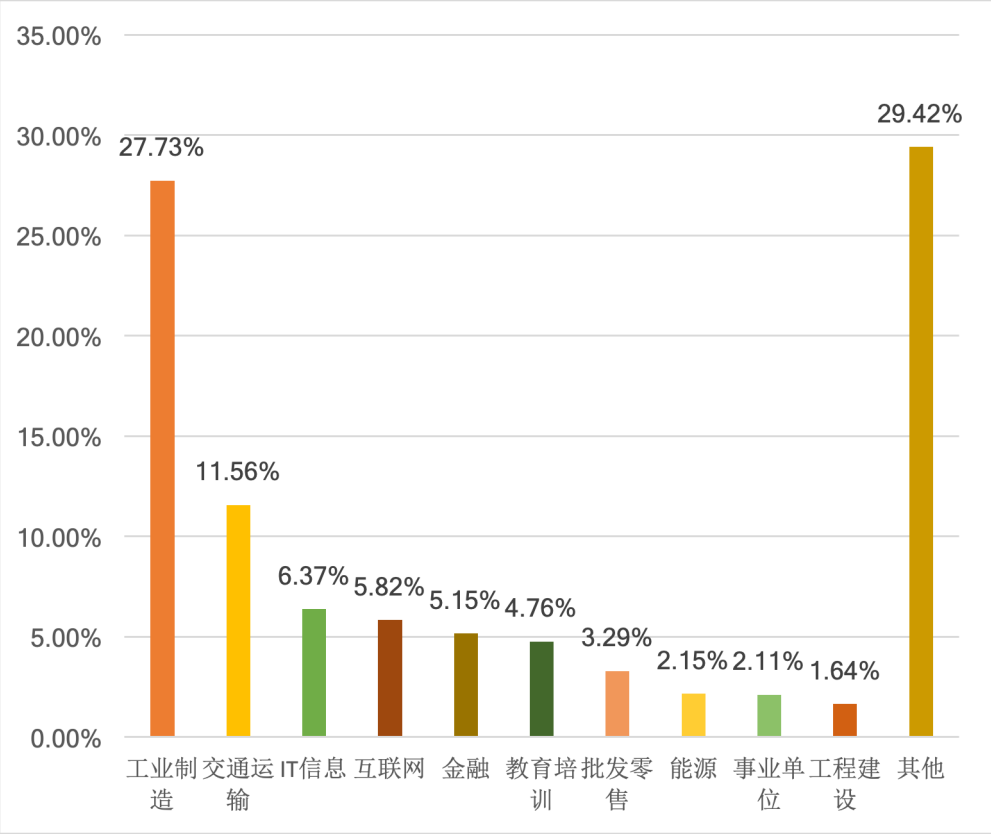
大小: 40 KB

掃一掃實名領取:

排名前十的行业收到的钓鱼邮件数量(Coremail)

根据 Coremail 与奇安信行业安全研究中心的联合监测评估，2020 年，全国企业邮箱用户共收到各类钓鱼邮件约 460.9 亿封，相比 2019 年收到各类钓鱼邮件的 344.3 亿封增长了 33.9%。其数据指出国内钓鱼邮件受害者所在行业比较集中，排名前十的行业收到的钓鱼邮件数量，占钓鱼邮件总数的 70.6%。其中，工业制造行业排名第一，约占钓鱼邮件总数的 27.7%；交通运输排名第二，约占 11.6%；排名第三的行业为 IT 信息技术，占 6.4%。具体 TOP10 行业排名如下所示。

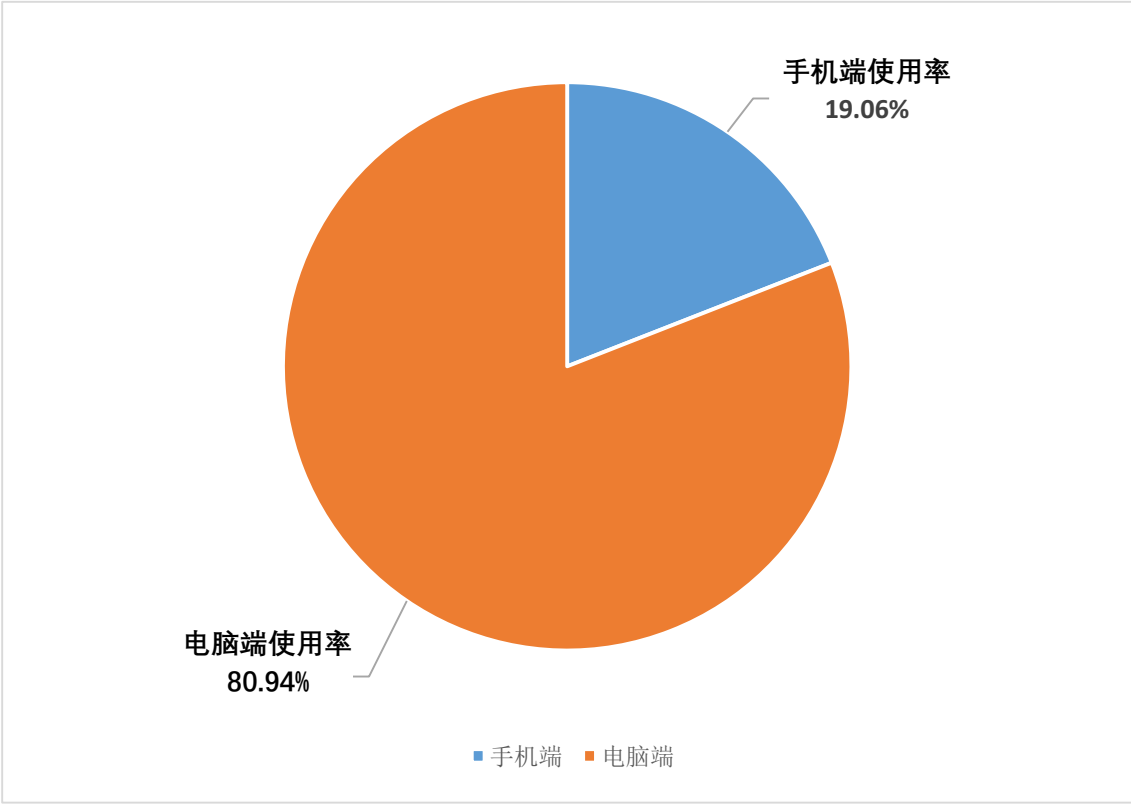
行业	百分比
工业制造	27.73%
交通运输	11.56%
IT 信息	6.37%
互联网	5.82%
金融	5.15%
教育培训	4.76%
批发零售	3.29%
能源	2.15%
事业单位	2.11%
工程建设	1.64%
其他	29.42%



用户客户端对比

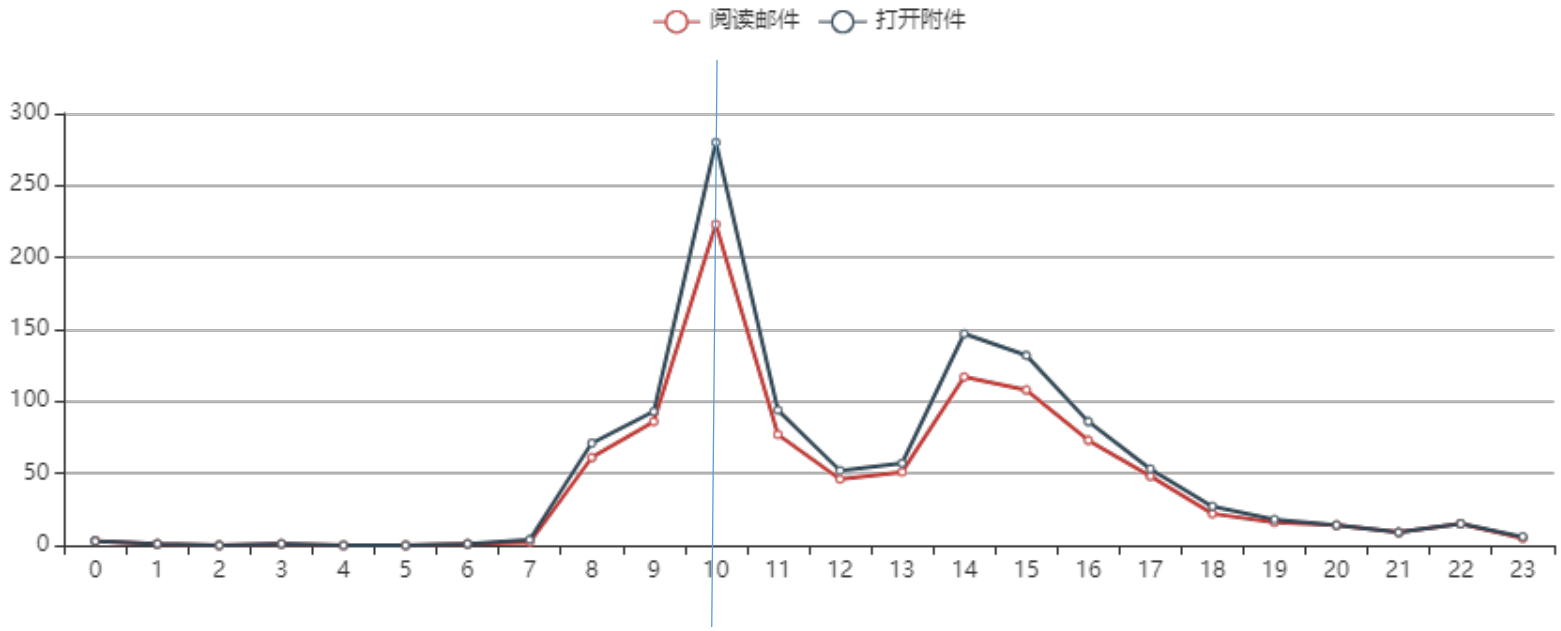
这里主要对比钓鱼邮件演练中手机平台和电脑平台使用率。随着移动端硬件配置的不断增强，以及 4G、5G 网络的升级优化和流量资费普遍降低，移动互联进入了井喷期，白领们开始习惯于通过移动端来处理工作。国内有数据显示，已有 68%的用户会每天通过手机查看邮件。但从我们收集的测试数据来看，手机端平均占比仅有 19.06%，电脑端平均占比 80.94%，说明除了少数行业，在办公室工作的员工绝大多数还是倾向于用电脑作为邮件阅读的主要平台。从细分行业来看，水利、环境和公共设施管理业使用手机端查看邮件占比最高达 49.77%，能源业则是使用电脑查看邮件最高的行业，占比高达 95.43%。

行业	手机端	电脑端
制造业	16.94%	83.06%
能源业	4.57%	95.43%
建筑业	20.59%	79.41%
交通运输、仓储和邮政业	19.06%	80.94%
信息传输、计算机服务和软件业	16.71%	83.29%
批发和零售业	5.23%	94.77%
医疗业	18.41%	81.59%
银行业	11.42%	88.58%
证券业	20.19%	79.81%
保险业	9.32%	90.68%
金融业(其他)	34.73%	65.27%
房地产业	24.08%	75.92%
科学研究、技术服务和地质勘查业	6.59%	93.41%
水利、环境和公共设施管理业	49.77%	50.23%



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 10 点和 14 点为波峰的两个高峰期，逻辑上推测为上班不久和午休结束。所以，选择上班之后的 1-2 个小时，比如公司 8 点上班，测试时间可以定在 9 点-10 点，或者午休结束后的 1-2 小时，比如 13 点吃完午饭午休结束，测试时间可以定在 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、交通、建筑、制造等行业的企业，通过安全意识培训和模拟钓鱼邮件演练筑起了一道道坚实的企业“人脑防火墙“。从数据上不难看出，企业可以通过测试和培训从根本上减少人为的漏洞，并最终改变企业员工的行为。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钓鱼邮件演练的前提条件下进行的，其 PFR 数据客观反映了企业员工最初的安全意识和防范水平，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。吸引和提高员工对安全意识教育的积极性。

③ 坚持钓鱼邮件演练

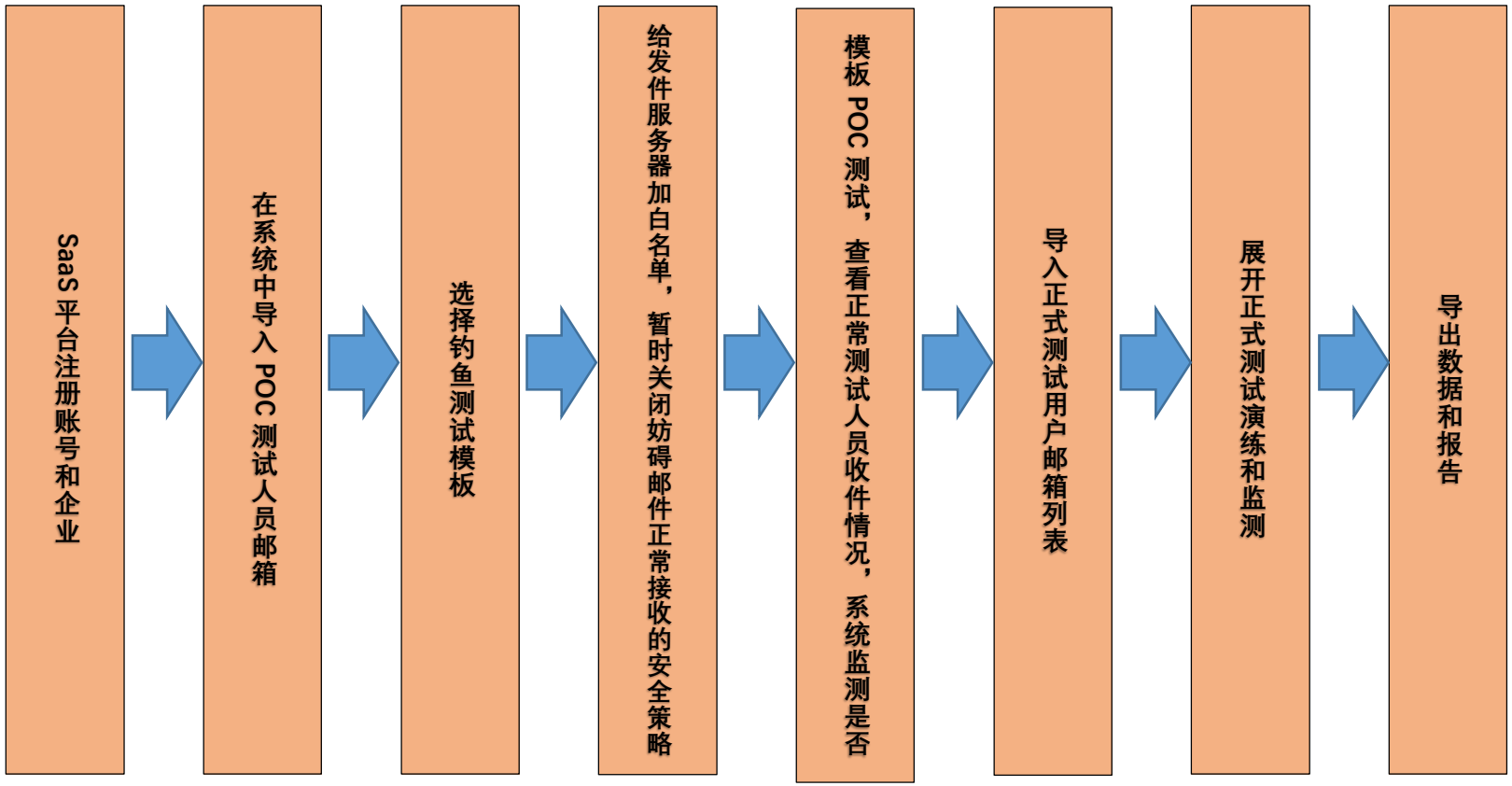
坚持**每三个月做至少一次模拟钓鱼演练**，避免长时间后员工放低警惕性。演练同时可以加强和检验企业员工的安全意识教育培训成果。钓鱼测试和培训的最终目的是改变企业内部员工的行为，从量变到质变需要一个长期的时间积累和巩固。

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。

钓鱼演练基本流程图

鉴于很多新用户并不了解钓鱼演练的基本流程，故此简单介绍演练的基本流程，如下：



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，企业相关负责人需要找到其中的平衡点。

误区二：培训和演练完全是信息安全部门的事。

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。毕竟安全并不是信息安全部门一个部门的责任。

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只是为了满足合规要求，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或演练这么简单。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。

误区四：高层领导是例外

我们服务过的企业和组织在钓鱼演练实施的过程中，很多会除去企业的管理者，这种情况无可厚非。但是我们从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，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。

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。

误区六：钓鱼演练中招率不降反升

钓鱼邮件演练的中招率除了与持续的学习提高钓鱼邮件识别度，不断的演练提升警惕性有紧密关联之外，与钓鱼邮件的仿真度、主题吸引力、场景契合度、心理学揣摩等也有很大的关联，不能因为某次测试出现中招率不降反升，就放弃了钓鱼演练这一有效抓手，长期、多次开展演练更能验证实效。

易念科技是中国网络安全意识教育的领导企业

旗下：Human Risk™ 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。

附录一. 钓鱼技术几种类型

为了防止网络钓鱼，企业用户应该了解黑客是如何窃取信息的，这里我们提供了钓鱼技术相关的常见几种类型。

仿冒邮件

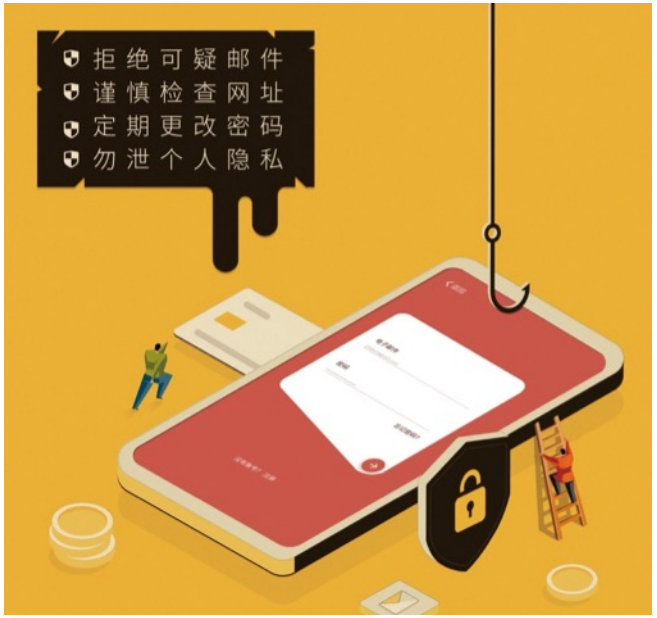
我们知道一般电子邮件都是通过发件服务器来发送的，当骗子能够搭建自己的发件服务器时，仿冒邮件就产生了。骗子通过自己构建的发件服务器，可以实现隐藏真实发件人信息，并伪装成任意发件人。因此，骗子可以轻松的伪装成知名企业的邮箱对外发件。当遇到这种“高仿”邮件，收件人不经确认很容易走入骗子布下的陷阱。

附件钓鱼邮件

顾名思义，这类钓鱼邮件的风险点在附件，很多人看到邮件中有附件时，就习惯性的点开查看。附件钓鱼邮件以 exe/scr 后缀的附件的风险程度最高，一般是病毒执行程序。其他常见的还有 Html 网页附件、Doc 附件、Excel 附件、PDF 附件、Rar 和 Zip 压缩包附件等。

链接钓鱼邮件

这类钓鱼邮件也很常见，骗子在邮件内直接嵌入了钓鱼链接，点开链接是骗子做得以假乱真的钓鱼网站，这类网站通常会要求用户输入账户信息之类以获取用户敏感信息；另一种链接指向的网页暗藏木马程序，用户点开的同时就中招了。



鱼叉式钓鱼邮件

这是一种只针对特定目标进行攻击的网络钓鱼攻击，由于鱼叉式网络钓鱼锁定的对象并非一般个人，而是特定公司、组织的成员，故受窃的资料已非一般网络钓鱼所窃取的个人资料，而是其他高度敏感的资料，比如会议纪要、财务报表、设计文件等。

BEC 钓鱼邮件

BEC 诈骗（Business Email Compromise），又叫商务邮件诈骗，攻击者通过将邮件发件人伪装成收件人的领导、同事、商业伙伴，以此骗取商业信息、钱财，或者获取其他重要资料。

二维码钓鱼邮件

当用户处于内网，无法向外网发送信息时，骗子就会引诱收件人扫描邮件中的二维码进行攻击，利用个人手机获得信息和反馈。