反钓鱼邮件演练实践指南

文 / 郑海山　陈灿彬

钓鱼邮件是指利用伪装的电子邮件，欺骗收件人将账号、口令等信息回复给指定的接收者，或引导收件人连接到特制的网页。这些网页通常会伪装模仿真实网站，如银行或理财的网页，令登录者信以为真，输入信用卡或银行卡号码、账户名称及密码等，进而盗取用户财产或数据信息。同时，钓鱼邮件也会对内部信息网络安全造成隐患。

演练的必要性

钓鱼邮件攻击实际上是社会工程学攻击的一部分，“社工”指的是通过与他人的合法交流，来使其心理受到影响，做出某些动作或者是透露一些机密信息的方式，通常被认为是欺诈他人以收集信息、行骗和入侵计算机系统的行为。

钓鱼邮件出现的根源在于发送者来源的不可信，例如日常生活中收到一封平邮，实际上很难了解该邮件是否一定由其所宣称的人发出。互联网充斥着大量虚假的信息，拥有辨别能力和水平成为互联网时代必备的基本素质。除了邮件外，攻击者也会利用包括电话、短信、IM、社交平台、游戏平台大厅等各种渠道进行诈骗。由于电子邮件收发便捷，成本低廉，导致其更为大众所熟知。

在攻防场景中，如果正面无法突破，攻击者也会尝试社工的方法进行内网渗透，钓鱼邮件往往是攻击者最先尝试的方法。一旦一个用户被成功钓鱼，往往会导致其负责的所有信息泄露或周边同事继续被钓鱼。所以钓鱼邮件危害巨大，轻则只对单个用户产生影响，重则造成组织敏感信息泄露，网络防护体系整体崩溃。

在高校内，近年来的钓鱼邮件攻击目标选择和邮件内容上变得更有针对性[1]。攻击者会根据各单位的官方组织架构网站获取人员信息，并根据通知公告热点编制诸如新冠肺炎、科研申报、论文发表、年度考核、系统升级、健康打卡等内容的钓鱼邮件。高校邮件系统一般也会部署安全网关，但是安全网关针对垃圾邮件或者特征明显的钓鱼邮件效果尚可，而面对精准的钓鱼攻击显得有些力不从心。

《网络安全法》和网络安全等级保护制度均明确要求，应当定期对从业人员进行网络安全教育、技术培训和技能考核，告知相关的安全责任和惩戒措施。《2020邮件钓鱼演练分析报告》[2]对除教育行业外的其他多个行业钓鱼中招率等做了对比。2021年5月18日，北京大学开展“钓鱼邮件”攻防演练，演练取得了良好的警示效果。由此可见，为预防钓鱼邮件攻击，除了邮件服务器进行加固外，经常性培训和演练是一种提高组织内全体人员的网络安全意识的有效方法。利用电子邮件成本低廉的特性，宣传反垃圾邮件和反诈骗相关信息，切实提高使用者的网络安全素养，降低网络安全风险。

演练开展步骤

进行反钓鱼演练之前，应当首先确认邮件服务器自身的安全性。应使用市面上占有率高的安全的邮件服务器软件，邮件服务器软件应当可以正常处理From字段畸形、代发显示、方便地报告钓鱼邮件等功能。邮件服务器应当做好DMARC、DKIM、SPF等加固，使用邮件安全网关对垃圾邮件和钓鱼邮件进行过滤，对用户普及校内邮件地址后缀，防止子域名没有设置SPF被恶意利用。

开展反钓鱼演练也需要考虑演练是否会造成草木皆兵，虽然养成提交敏感信息

钓鱼邮件的分类

1. 附件钓鱼：这类邮件的风险在于邮件中含有附件，附件的类型为可执行文件，一般是病毒执行程序。其他常见的还有Office文件、PDF等，主要是利用宏或者客户端软件CVE漏洞。也有利用加密的压缩文件绕过反病毒监测的。

2. 链接钓鱼：这类邮件风险在于邮件中有网页链接，点开链接是假造的以假乱真的钓鱼网站，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；另一种链接指向网页暗藏木马程序，用户如果浏览器存在未修复的漏洞，那么点开的同时就中招了。

3. 二维码钓鱼：邮件中不直接放过于明显容易识别的单位网站，而是包含有二维码，引导用户扫描二维码进入钓鱼网站。网站会要求用户输入账户信息用于获取用户敏感信息。二维码也会指向附件或者App，要求用户下载App或者相关附件，在App或者附件中植入病毒。

4. 内容钓鱼：这类邮件通常附件不存在病毒，或者无任何外链或者二维码，通过多次邮件来往获取信任后实施进一步欺骗。

时再次确认是一个基本的安全意识，但是由于用户的网络安全意识水平不一，如果不做好培训，贸然开展演练会影响正常工作发送通知邮件的便利性。反钓鱼演练也要防止演练导致敏感信息被提交，所以在演练中对用户提交的密码不记录，也不验证。

开展反钓鱼演练需要选择是自行开展或者采购外包服务。市面上有较多可实施反钓鱼邮件演练的公司[3]。外包服务通常较为专业，钓鱼模板全面，培训物料完善，拥有大量可以用来发送、接收和处理演练过程中的IP池和域名。但是也存在以下问题：

1．外包服务无法覆盖全部工作量。反钓鱼邮件培训网站需要跟校内统一身份认证对接，也需要提供校内组织架构，需要收集邮件地址，需要提供近期校内热点事件，需要提供部分业务系统敏感数据，需要在OA等群发培训通知，这些外包公司无法完成。

2. 数据安全性问题,反钓鱼演练的准备、过程和结果数据应当保密，如果更换外包服务后，需要考虑如何整合历史数据和新外包服务的系统，以便数据具有延续性。

3．外包服务通常以次数或发送邮件封数来计算成本。高校的特点是人员众多，各个角色人数多且更替频繁，每年均有新生和新进教职员工，各个人员有工作邮箱和私人邮箱混用，多层次，常态化反钓鱼演练成本较高。

如高校邮件管理部门有一定的技术能力，并且邮件系统可控，则可考虑自建反钓鱼演练平台和培训站点，达到数据完全掌握可控，钓鱼模板紧跟校内热点和业务系统数据。一旦选定了模式，可通过下列步骤来开展反钓鱼演练。

报主管部门批准

实施反钓鱼邮件演练之前应当报告主管部门批准。如果需要以某部门的名义发送，应当通知该部门，并协助该部门做好用户电话咨询等应对措施，以免对该部门工作造成干扰。也应当告知相关的安全部门，否则会对一些安全设备的告警或者态势感知设备的分析造成污染。

开展培训

反钓鱼演练的目的不在于最终抓住普通用户的网络安全意识问题并进行各种惩罚性措施，而是在于评估机构内所有用户的安全素养水平和提高用户的网络安全意识，所以在钓鱼之前一定要做好培训。

在校内在线学习平台开设防钓鱼邮件课程,课程内容包括“什么是钓鱼邮件”“身边的案例”“如何识别钓鱼邮件”“如何防范钓鱼邮件”“我被钓鱼了怎么办”“反钓鱼邮件小测验”“相关资源和链接”等，通过办公自动化通知、群发邮件、群组通知等广泛多次通知用户阅读培训。

建立钓鱼邮件报告机制。在培训时告知用户可通过将钓鱼邮件发送到特定邮箱、在Web标记钓鱼邮件、打电话咨询等方式完成报告。

开展自测

为了检验培训的成果，也为了在用户被钓鱼后可以自学，需要在在线平台开设测试。使用题库，鼓励用户多次答题。并根据反馈和案例充实题目。

如何识别钓鱼邮件

1．看发件人地址，是否为熟悉的人。如果看到发件地址内有错误字符，或者发件地址较长，或者是代发的，应引起警惕。即使是熟悉的朋友或同事，也要多一份警惕，因为对方可能密码已经泄露。

2. 从发送时间看，是否有异常，比如凌晨等。

3. 从内容上看，使用领导或者官方机构语气，夸大事件影响范围，使用通用问候语或者称呼的，制造紧急气氛的，吸引人的内容的，应引起警惕。

4. 从内容上看，如果邮件附带链接或者二维码，应引起警惕。

5. 从附件上看，如果带可执行文件，或者加密ZIP的，应引起警惕。

6. 不确认是否合法邮件的，应当多向其他同事询问。

7. 如果确认是钓鱼邮件，应当向管理员报告，以免其他同事受害。

如何防范钓鱼邮件

只要安全防护到位，即使遇到钓鱼邮件也不用太担心。如果打开的附件带有病毒，只要系统安装了防病毒工具，并且保持更新到最新，系统会自动隔离该附件避免遭到恶意利用。

1．常规的安全防护措施要做，经常接受一些网络安全素养培训。

2. 密码使用强密码。

3. 应定期更新操作系统、邮件客户端、Office文档查看器、PDF查看器、看图工具等软件的安全补丁，保持最新。

4. 应安装防病毒软件并保持启用和定期更新病毒库。

5. 邮件客户端和Office等会对互联网文件有防护配置，比如Outlook的“信任中心”，或者Word会在“受保护的视图”打开来自互联网的文件，不应当为了方便而关闭防护。

6. 辨认邮件内链接是否可信。有些链接打开后实际上不是显示的链接，或者多次重定向的短链接。所以网页URL应当尽量从收藏夹打开或者手工输入。

7. 在任何网页输入密码、验证码、个人信息等，一定要确认URL地址。如果在微信内打开应当下拉网页查看网页源地址。应尽量不使用无法显示源地址或者显示不全的部分手机浏览器。

8. 下载后的压缩文件要仔细辨认文件后缀名，不应当随意执行任何可执行文件。

演练

演练可以分批多层次举行。初期在小单位内部测试，测试没有问题后再拓展到高价值用户，比如校内所有网站管理员，再拓展到全校师生。在演练发出后，应当跟踪演练平台、发送邮件服务器、接收邮件服务器的日志，防止因为配置不当邮件被拦截。

演练的邮件模板可以根据发送者、发送内容、接收者等多个形式组合。比如：

1. 模拟常规钓鱼邮件，发送者邮件为非校内邮件的地址，邮件较长无规则，非常易于识别的钓鱼邮件。

2. 错别字多，存在常识错误的钓鱼邮件。

3. 邮件内外链域名较长无规则。

4. 发送者邮件跟校内邮件非常接近，只差一个字母等近似或者不可见字符、全角 @、肉眼容易混淆的 Unicode 字符。比如 xmu.eud.cn、xmuu.edu.cn 等类似的域名。

5. 发送者邮件地址为校内师生，模拟校内师生邮箱被黑而恶意发送钓鱼。

6. 外链域名与校内地址类似，比如 id.xmu.edu.cn.l.example.com 等。

7. 外链域名为校内，模拟校内网站被攻击后作为钓鱼。

8. 带上个性化信息，比如在科研信息系统内未结题项目信息，加大迷惑性。

9. 发送多语言的邮件内容，比如英文论文录用通知。

10. 针对特定角色用户。

11. 针对多次被钓鱼用户。

如果用户误点击链接并提交用户名信息后，应引导到一个特定页面，在这个页面告知用户只是个演练，以及如何识别这封钓鱼邮件的特征，并继续引导用户到培训网站。

总结和常态化执行

在一次演练结束后，应当分析数据，形成总结报告，积累经验，并将演练结果脱敏后群发给用户告知，加强培训效果。

多次发送钓鱼邮件后，根据数据跟踪分析得到易中招人员名单，分析共性，针对易中招人员再进行特定培训。

在一次演练结束后，应当分析数据，形成总结报告，积累经验，并将演练结果脱敏后群发给用户告知，加强培训效果。

自建反钓鱼演练平台实施方法

反钓鱼演练平台的搭建可以选择免费的 Gophish 或者 SniperPhish 等开源软件。应使用自动化部署，部署后，应当对系统做好安全加固，提高平台的稳定性。

以 Gophish 为例，应定期更新安全补丁，使用 MySQL 数据库，方便后期做数据分析统计。可通过 supervisor 或放入 systemd 维持 Gophish 进程。不建议直接暴露 Gophish 的 80/443 端口，可使用 Nginx 代理对外提供 HTTP/HTTPS 服务。

Gophish 支持灵活配置不同的钓鱼策略，需搭配邮箱服务器实现发送钓鱼邮件，可使用开源的 Postfix 作为发件服务器。在目标邮件服务器上对发件服务器关闭部分规则校验或者设置白名单，绕过垃圾邮件过滤和发送频率、来源验证等限制。

钓鱼页面可通过采用 Gophish 的 LadingPage 导入，目前只支持一个页面。如果需要在多个页面之间实现跳转和抓取数据，可以在一个页面内嵌入两个步骤的页面，或者独立搭建一台服务器，在站点内嵌入多个 {{.RId}} 来实现跟踪页面打开和数据提交。如果要将钓鱼页面实现得更为逼真，可以搭建 Nginx 反向代理服务器，将站点反向代理到真实服务器，替换跳转页面登录地址，可以达到更好的隐蔽性。

Gophish 还在持续开发演进中，功能上存在以下不足：

1. Gophish 钓鱼活动看板可以看到一次钓鱼启动后所有的时间点，包括某个用户何时发送，何时打开，何时点击外链，何时提交和报告。但是无法将多次钓鱼演练的数据进行合并显示，比如显示 Top 中招的用户，为了更好地进行数据分析，可以通过直连数据库，进一步进行数据分析。

2. Gophish 暂无法发送更高级的钓鱼邮件，比如带个性化信息的钓鱼邮件，邮件模板可替换变量较少，无法发送带跟踪链接的 Word 附件，无法对发送的二维码进行自定义等等。CEN（责编：郑艺龙）

（作者单位为厦门大学信息与网络中心）

参考文献

[1] 郑先伟 . 钓鱼邮件攻击更具针对性！高校需防范 [J]. 中国教育网络 ,2020(12):25.

[2] 易念科技 ,FreeBuf. 易念科技联合 FreeBuf 发布了《2020 邮件钓鱼演练分析报告》[EB/OL]. [2020-12-30]. https://www.freebuf.com/articles/paper/259376.html.

[3]Mr.Lee. 如何规划企业钓鱼邮件演练？ [EB/OL]. [2020-07-25]. https://mp.weixin.qq.com/s/h_yb5_AMSVYjN23rZPYtPg.