

关于防范钓鱼攻击的加固及应急方案

尊敬的客户：

近期，我们关注到部分企业遭遇名为“银狐”的木马病毒攻击，控制员工个人电脑，窃取信息并实施非法操作（如拉群发布诈骗信息），已对多家企业造成影响。经紧急溯源与研判，确认系“银狐”木马病毒引发的钓鱼攻击事件。

该攻击手段具有高度隐蔽性和传播性：攻击者通常先通过投递恶意文件获取内网个别终端的控制权，随后利用受害终端已登录的 OA 系统及即时通讯（EM）工具，滥用群发、日程邀请、邮件投递及流程发起等功能，批量扩散钓鱼信息。此类信息多以“社保补贴”、“薪资调整”、“个人退税”等财务利益为诱饵，极具迷惑性，旨在诱导员工点击恶意链接并骗取银行卡号、验证码等敏感信息，最终实施资金盗窃。

鉴于当前网络安全形势严峻，为切实保障 OA 系统平稳运行，阻断病毒横向传播路径，最大限度减少公司及员工的财产损失，我司特制定并建议实施以下安全加固与管控措施：

一、终端安全：个人办公环境防护建议

- 1. 终端安全防护：**强烈建议为所有员工电脑安装终端防护软件，如 EDR、杀毒软件等，开启实时防护功能，定期全盘扫描。

2. **员工安全意识培训：**强烈建议开展专项安全培训，提醒全部员工勿相信，勿点击来源不明的邮件、链接或附件，尤其是包含“社保补贴”、“薪资调整”、“个人退税”等财务利益为诱饵的信息，勿轻易打开微信等工具上陌生人发送的任何文件、勿轻易透露填写银行卡号、身份证号、手机号、验证码、密码等个人敏感信息。

3. **软件合规性：**严禁下载、安装来自非官方渠道的破解软件或“绿色版”工具，此类软件常捆绑远控木马。

二、系统安全：OA 办公平台专项加固措施

经过技术分析，“银狐”木马病毒并非通过 OA 系统本身的安全漏洞进行传播，其攻击主要针对员工个人电脑终端，我们强烈建议同步执行“终端安全”措施。

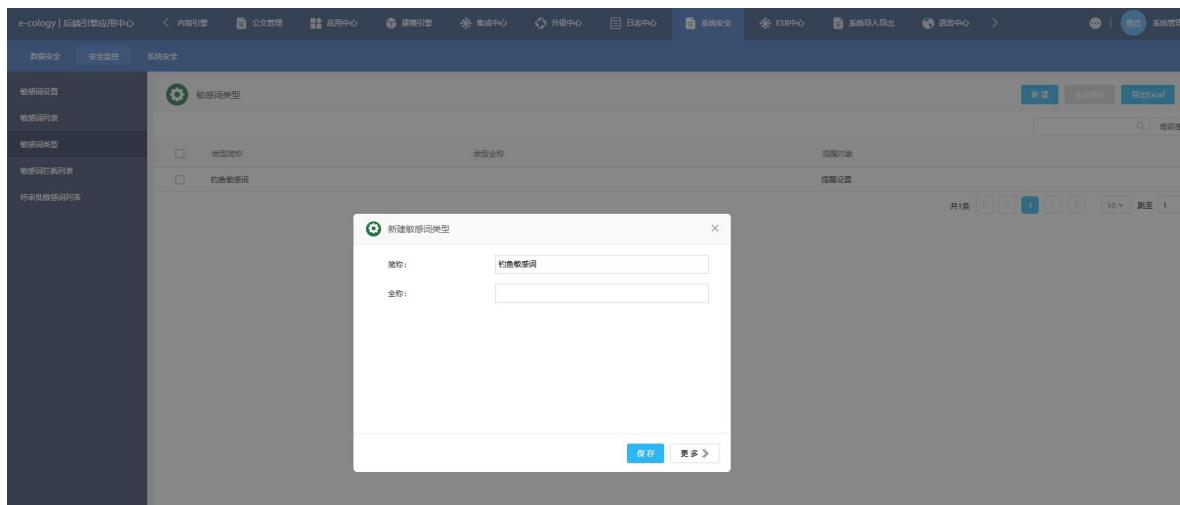
1. 针对敏感词实施增加拦截操作，把补贴、工薪、社保、津贴等词汇纳入敏感词列表，以实现自动过滤。

- 针对 E9 系统可以按照如下方式设置：
 - (1) 后端-系统安全-安全监控-敏感词设置-页面内容智能预检，打开此开关(**如果没有此开关，表示该版本不支持敏感词功能，需要先升级系统至最新 KB 版本后开启**)
 - (2) 同时，默认处理方式请选择【删除并记录日志】或者是【脱敏显示并记录日志】。
(删除并记录日志：会将敏感词彻底删除，不会存入数据库)

脱敏显示并记录日志：显示时会将敏感词显示为**，但数据库仍然存储该敏感词数据）

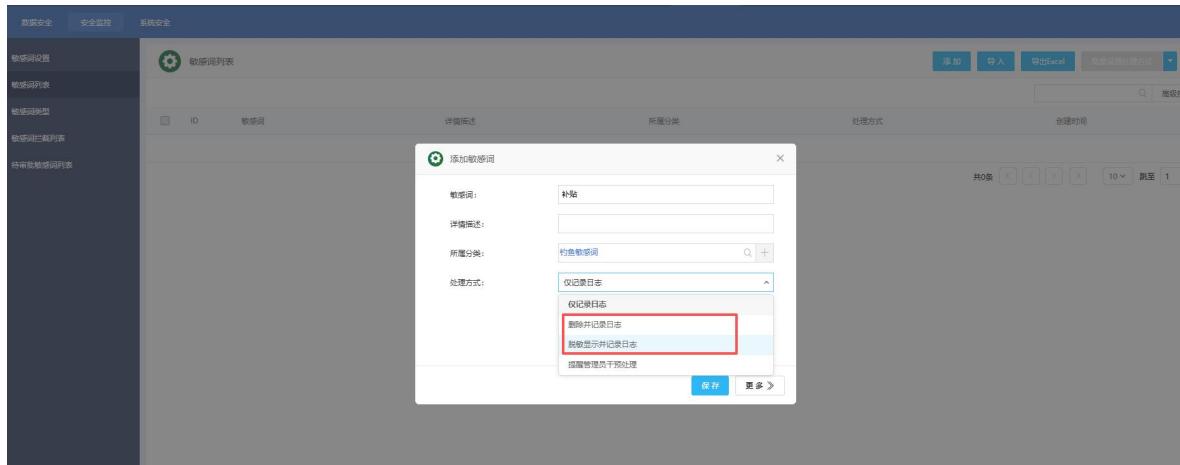


(3) 敏感词类型里先新建一个敏感词类型，设置为【钓鱼敏感词】



(4) 敏感词列表设置中维护好需要处理的敏感词汇，并选择【删除并记录日志】或者【脱敏显示并记录日志】方式。

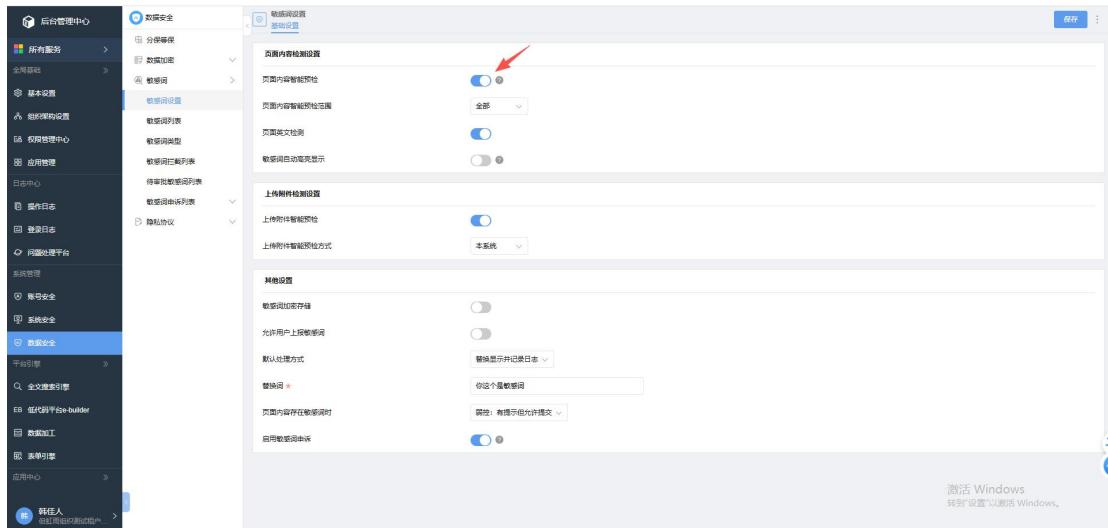
建议至少以下高频词汇录入：**补贴、工薪、社保、津贴、退税**



- 针对 E10 系统，可以按照如下方式设置：

(1) 启用方式：【后台管理中心】→【数据安全】→【敏感词】→【敏感词设置】→

【启用总开关】，如下图所示：



(2) 敏感词配置方式：在敏感词列表设置处，维护好待处理的敏感词汇，并将其设置

为“启用”状态即可，

敏感词	详细描述	所属分类	应用范围	处理方式	创建时间	状态
抢劫	违法	本组织	删除并记录日志	2025-09-04 11:17:35	启用	
赌博	违法	本组织	删除并记录日志	2025-09-04 11:17:35	启用	
偷东西	违法	本组织	删除并记录日志	2025-09-04 11:17:35	启用	
酒店嫖娼	违法	本组织	删除并记录日志	2025-09-04 11:17:35	启用	
抢劫	违法	本组织	删除并记录日志	2025-09-04 11:17:35	启用	
绑架	违法	本组织	删除并记录日志	2025-09-04 11:17:35	启用	
吸毒	违法	本组织	删除并记录日志	2025-09-04 11:17:35	启用	
杀人	违法	本组织	删除并记录日志	2025-09-04 11:17:35	启用	
人贩子	违法	本组织	删除并记录日志	2025-09-04 11:17:35	启用	
犯毒	违法	本组织	删除并记录日志	2025-09-04 11:17:35	启用	

2. 建群设置人数限制与审批功能

(1) 针对 E9 (EM7) 建群大小设置方式，按照如下操作：

登录 Emobile7 管理后台，点击菜单【emobile 管理】→【消息设置】→【消息服务】

页签。将页面滚动至底部，存在【群人数上限】设置项。该设置项既可以设置全局默认的

群人数上限，也能够依据人员进行区分设置，如下图所示：

消息服务

消息分享 消息菜单 自定义表情 敏感词过滤 发送消息

是否开启消息服务:

* 消息服务地址: 请输入完整的消息服务地址,例如: http://x.x.x:9090,确保在当前移动平台的服务器上通过这个地址能够访问到消息服务

* 消息服务管理员密码:

消息服务接口账号: ****

消息服务接口秘钥: ****

* 移动客户端连接地址:

* 移动客户端连接端口: 5000

移动客户端连接是否加密: 如果开启加密需要确保已经配置相应的证书

移动客户端连接映射配置

* PC客户端连接地址:

* PC客户端连接端口:

开启群聊功能:

选择允许发起群聊的部门 / 成员 / 标签

全体成员

每人每天创建群数量上限: 12 最小为-1。-1表示不限制, 0表示禁止创建, 大于0表示每人每天能创建的群上限

群成员人数默认上限: 500 最小为3人, 最大不超过1000人 [全局设置](#)

[群成员人数上限详细配置](#) [给特殊人权单独设置](#)

开启必达: 开启短信 1

选择允许发起必达的部门 / 成员 / 标签

全体成员

[保存功能设置](#)

当前版本:20250928

(2) 针对 E10 (EM10) 建群大小设置方式, 按照如下操作

登录 E10 管理后台, 点击菜单【工作消息】→【功能设置】→【群聊设置】页签, 该页签下方设有【群聊最大人数上限】设置项。在此设置项中, 既能够设定全局默认的群人

数上限，也可依据人员进行区分设置，如下图所示



3. 启用系统超时功能，建议设定在 30 分钟内无操作的情况下，系统自动退出。此举旨在防范计算机遭受病毒侵袭后，因系统持续在线而引发的安全风险。

(1) 针对 E8 / E9 系统，可以按照如下方式设置：

以 sysadmin 身份登录 OA 系统，访问 <http://oa 地址/security/monitor/Monitor.jsp>，点击【安全开启详情】。于该页面查找【系统超时功能】，并点击【开启】。若显示为“开启”，则表明系统超时功能已启用。默认情况下，若 30 分钟内无操作，再次进行操作时，系统将要求重新登录。（**若为集群环境，需在每个节点分别登录并开启此功能**），具体情况如下图所示

安全开启详情			
12	是否开启了WEBSERVICE限制IP访问功能	检查WEB-INF/weaver_security_config.xml中的enable-service-check是否为true	添加到指定的类的方法体下，修改WEB-INF/weaver_security_customer_rules_1.xml文件，添加以下代码 <ip>80</ip><ip>123.40.12.2</ip><ip>192.168.</ip></webservice-ip-list> 其中 <ip>就是在此处填写webservice的IP地址，可以是一个网段，也可以是一个完整的IP地址，可以配置多个<ip>节点；
13	是否开启了对HTTP分母应用限功能	检查WEB-INF/weaver_security_config.xml中的http-sep是否为true	添加部署在WEB-INF/weaver_security_config.xml中的<http-sep>为true
14	是否启用了系统超时功能	检查WEB-INF/weaver_security_config.xml中的is-check-session-timeout是否为true	添加部署在WEB-INF/weaver_security_config.xml中的<is-check-session-timeout>为true <is-check-session-timeout>true</is-check-session-timeout> 超时时间配置方法： 添加部署在WEB-INF/weaver_security_config.xml中的<session-timeout>为超时时间（单位分钟），默认为30分钟 <session-timeout>30</session-timeout>
15	是否启用了log文件、数据库连接访问权限控制的功能	默认开启，不可关闭。可以添加相应的资源到控制列表中。	添加部署在WEB-INF/weaver_security_customer_rules_1.xml文件，添加以下代码 <allow-urls><url>/user/</url><url>/admin/</url></allow-urls><forbidden-urls></forbidden-urls>

(2) 针对 E10 系统，可以按照如下方式设置

在【后台管理中心】→【账号安全】→【安全设置】→【登录设置】，配置各终端失效时长，如下图所示



4. 若具备相应条件，建议启用零信任防护系统，以避免直接在互联网上暴露。

若存在零信任防护系统，建议将办公自动化（OA）系统纳入该防护系统进行管控，以

避免其直接暴露于互联网，从而扩大潜在攻击面。

三、应急响应：发现感染后的快速处置指引

1. 即刻将系统内的相关钓鱼信息予以删除。

- 立即撤回已发送的诈骗信息并解散群聊
- 删除钓鱼流程、日程、邮件等内容，以尽快减少消息传播范围。

2. 解散群聊及撤回消息的方式

(1) E9 (emobile7) 系统：

- ① 用 sysadmin 账号登录 emobile7 后台；
- ② 点击【emobile 管理】→【数据运维】菜单，在这里可以解散相关群聊和删除相关消息，如果看不到这个菜单，请按照如下方式打开这个功能：
 - 1) 远程到 emobile 服务器
 - 2) 编辑 emp\work\config\application-custom.properties 文件
 - 3) 在文件的末尾添加一行 emobile.enable_monitor=1
 - 4) 然后重启 EM 服务
- 5) 重启之后 sysadmin 登录 EM 后台 在 emobile 管理 菜单下会多出一个菜

单【数据运维】

(2) E10 (emobile10) 系统:

③ 用管理员账号进入 E10 后台

④ 点击菜单【工作消息】→【消息管理】在这里可以删除、撤回敏感消息

⑤ 点击菜单【工作消息】→【群里管理】在这里可以解散对应的群聊

3. 即刻禁用发送诈骗信息的账号，防止其再次发送此类信息

(1) 针对 E8 / E9 系统，按照以下方式禁用异常账号

入口路径：查找【人事模块】，进而【在通讯录中搜索问题账号】，随后【打开个人卡片】，再进入【系统信息】，完成账号锁定操作。账号锁定后，系统将强制该账号下线，且禁止其再次登录。

E8 / E9 同理

The screenshot shows the 'Personal Card' page of the E8/E9 system. At the top, there is a navigation bar with tabs like '基本信息', '工作运维', '禁用组', '个人信息', '工作信息', '系统信息' (which is currently selected), '工益福利', '资产信息', '待办事宜', '考勤情况', '培训记录', '英语考核', '角色设置', '百度(error)', '测试', and 'yjiceshi'. Below the navigation bar, there is a search bar and a 'Save' button. The main content area is titled '系统信息' (System Information). It contains several input fields and dropdown menus. One of the dropdown menus has a red arrow pointing to it, indicating where to click to access the locking function. The fields include: '登录名': 'yq6'; '账号锁定': a dropdown menu with a green lock icon; '锁屏权限方式': a dropdown menu; '生效范围': a dropdown menu with '全部' selected; '人员类别': a dropdown menu with '非常' selected; '密码': a password field; '确认密码': a password field; '安全级别': a dropdown menu with '10' selected; '二次验证密码': a dropdown menu with '未设置'; and '软证书': a dropdown menu with a QR code icon.

(2) 针对 E10 系统，按照以下方式禁用异常账号

① 解除账号方式：

操作方式为：找到【通讯录】→【搜索问题账号】→【打开个人卡片】→【账号信息】

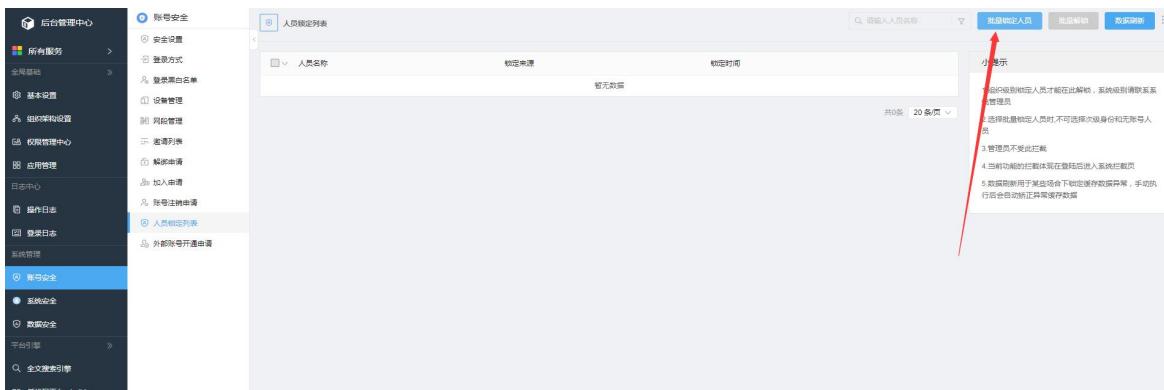
→【解除账号】



② 锁定账号方式：

操作方式为：【后台管理中心】→【账号安全】→【锁定列表】。锁定问题账号后，

该问题账号将自动下线，且不允许再次登录。



泛微网络科技股份有限公司

2025 年 12 月