



确保通信安全

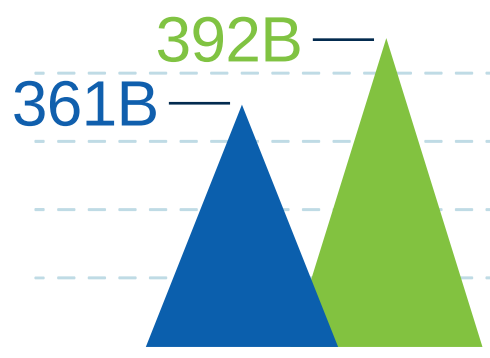
从网络钓鱼防御到自动保护

目录

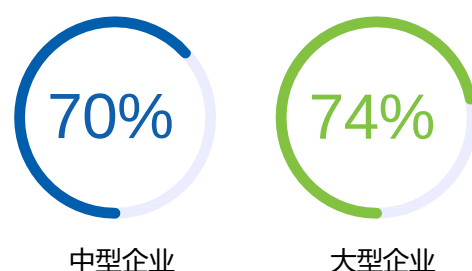
- 3 简介
- 4 了解数字证书和签名
- 7 邮件安全威胁
- 10 S/MIME 简介：确保电子邮件安全
- 12 安全通信自动化
- 14 GlobalSign 和 NoSpamProxy 如何提供帮助
- 16 安全通信的最佳做法
- 16 结论

简介

在当今的数字环境中，电子邮件安全至关重要。根据 [Statistica.com](https://www.statista.com) 的数据，全球每天收发的电子邮件数量约为 3,610 亿封，预计到 2026 年将增至 3,920 亿封。鉴于电子邮件在业务通信中的关键作用，它是网络犯罪分子的首要目标。据 [gov.uk](https://www.gov.uk) 报告，截至 2024 年 4 月，70% 的中型企业和 74% 的大型企业在过去 12 个月中遭遇过网络安全漏洞。这些漏洞中有 84% 是网络钓鱼攻击。本电子书深入探讨了电子邮件安全方面不断变化的挑战，并深入探讨了自动化如何简化和加强保护措施，尤其是考虑到这些令人震惊的统计数据。



每天发送的电子邮件数量，预计到 2026 年还将增加



在过去 12 个月中遭遇过网络安全漏洞

通过探讨 GlobalSign 和 NoSpamProxy 之间的合作关系，我们将展示我们的组合解决方案如何提供一个强大的防御框架来抵御基于电子邮件的威胁。数字证书和加密在这一防御战略中发挥着关键作用，可确保电子邮件通信的真实性、完整性和保密性。自动化可简化数字证书管理、自动执行 S/MIME 等安全协议并降低人为错误风险，从而进一步加强安全措施。在本电子书中，我们将进一步探讨自动化如何简化这些流程，并促进更具弹性的电子邮件防御策略。

了解数字证书和签名

在日益脆弱的数字环境中，了解数字证书和签名至关重要，因为它们是安全电子邮件通信的基础

数字证书

数字证书是验证身份的电子凭证。它们对于建立数字通信中的信任至关重要。这种验证需求延伸到人工智能应用中，通过数字证书确认可信算法和用户的身份，加强自动决策过程的完整性和可靠性。

- **定义和目的**

数字证书可验证个人、设备或服务的身份。数字证书由被称为证书颁发机构（CA）的可信实体颁发。

- **公钥基础设施（PKI）**

PKI 管理数字密钥和证书，是安全通信的支柱。PKI 创建、分发和验证公钥和私钥，确保参与通信的实体是真实可信的。

- **证书类型**

现有各种类型的证书，包括用于确保网站安全的安全套接字层（SSL）和传输层安全（TLS）证书、用于验证用户身份的客户端证书，以及用于确保软件/应用程序安全的代码签名证书。



了解数字证书和签名续

证书颁发机构（CA），如 GlobalSign，是颁发这些证书的可信实体。它们为有效的证书管理提供解决方案，并确保其认证的实体是合法的，因此在证书生命周期中发挥着至关重要的作用。

数字证书是数字安全的关键组成部分，因此企业必须妥善管理数字证书。这种管理包括证书的签发、更新和撤销。作为抵御不断变化的威胁（包括利用人工智能的威胁）的主要防御手段，有效的证书生命周期管理对于维护安全通信至关重要。



数字签名

数字签名是由数字证书支持的电子签名，可提供身份证明。数字签名被广泛用于文件签名，同时也是电子邮件安全的关键，可确保电子邮件的真实性和完整性。通过使用证书验证发件人的身份，数字签名大大降低了恶意行为者冒充合法用户或篡改电子邮件内容的难度。因此，了解实施数字签名的好处对于旨在加强安全措施的组织来说至关重要。

在电子邮件安全中实施数字签名的好处：



强化安全

数字签名可验证发件人的身份，并确保电子邮件在传输过程中保持不变。这有助于防止篡改并确保信息的完整性。



增强信任

它们通过验证发件人的身份来建立通信双方之间的信任，从而降低网络钓鱼攻击和其他电子邮件威胁的风险。



成本效益

通过降低欺诈和数据泄露的风险，数字签名可以降低与安全事件、法律纠纷和违规行为相关的潜在成本。

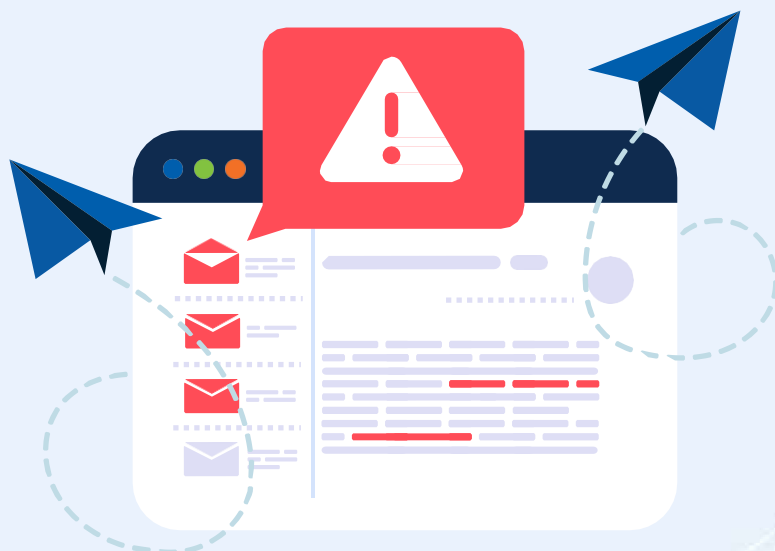


电子邮件安全威胁

要了解如何保证电子邮件通信的安全，首先必须了解企业可能面临的各种威胁：

最常见的电子邮件网络钓鱼攻击类型有：

- 邮件爆炸
收件箱中充斥着大量电子邮件，往往是真正攻击（如未经授权的金融交易）的烟雾弹。
- 商业电子邮件泄密 (BEC)
高级管理人员或财务部门成为目标，目的是提取敏感数据。
- 矛式网络钓鱼
攻击者冒充可信来源，利用熟人关系说服收件人共享机密信息。
- 一般钓鱼电子邮件
犯罪分子通过欺骗手段诱使用户点击恶意链接或下载有害附件。



电子邮件安全威胁续

网络安全中的人工智能

随着网络威胁日益复杂，人工智能在网络安全中的作用也在迅速扩大，既提供了新的防御能力，也带来了新的风险。在本节中，我们将讨论关键术语，并探讨人工智能如何改变电子邮件安全的格局。了解这些概念对于有效防范不断演变的威胁至关重要。

基本术语

AI (人工智能) :

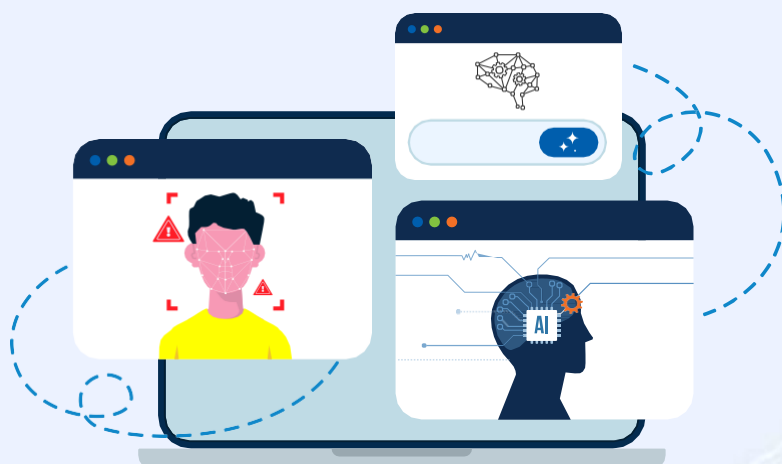
- 指能够执行通常需要人类智能才能完成的任务的计算机系统。
- 包括从数据中学习、推理、解决问题、感知和语言理解。
- 利用算法和数据做出决策和预测。

深度伪造 :

- 利用人工智能创建或处理音频、视频或图像。
- 可生成高度逼真的虚假内容，与真实媒体难以区分。

GPT (生成式预训练变换器) :

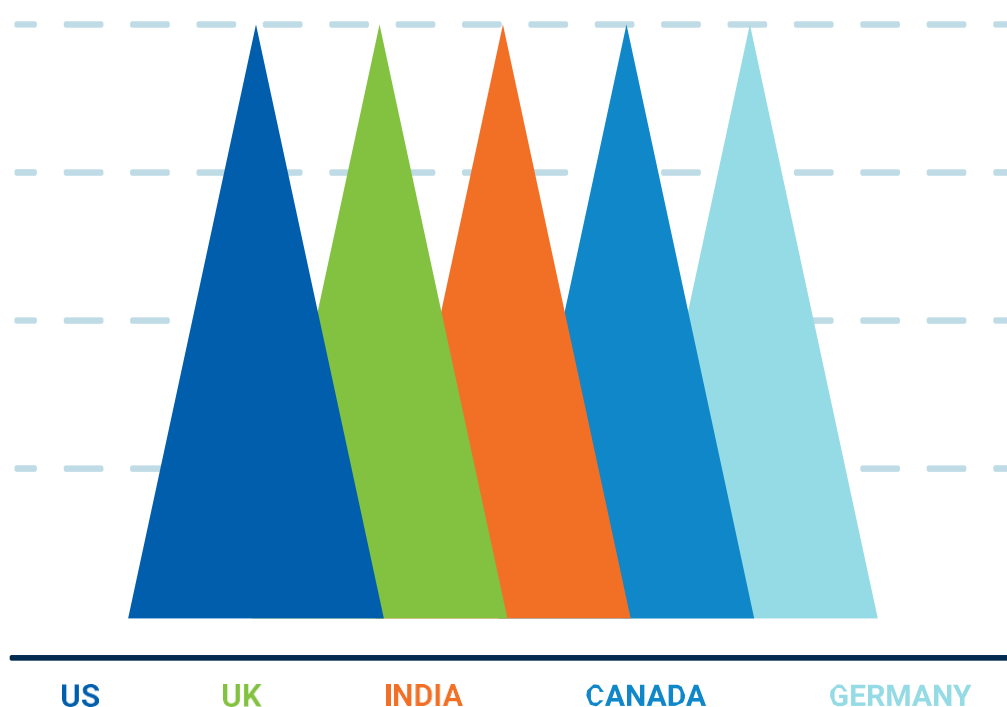
- 由 OpenAI 开发的大型语言模型。
- 利用深度学习，根据输入生成类人文本。
- 在大型数据集上进行训练，以理解并生成连贯的文本。



电子邮件安全威胁续

由于人工智能（Artificial Intelligence）和深度仿冒（Deep Fake）技术的日益普及，网络攻击正迅速变得更加复杂和难以察觉。[Zscaler 的研究表明](#)，攻击者正在利用人工智能加强社交工程策略，导致人工智能驱动的网络钓鱼攻击大幅增加了 60%。美国、英国、印度、加拿大和德国位居网络钓鱼诈骗目标国家的榜首，尤其对金融和保险业造成了巨大影响，攻击次数同比增长了 393%。

393% 网络钓鱼攻击同比增长



虽然人工智能通过检测欺诈性电子邮件、分析网络钓鱼企图和增强威胁检测能力来增强防御能力，但它也带来了新的风险。攻击者利用人工智能来自动化和优化攻击，以前所未有的逼真度创建令人信服的网络钓鱼电子邮件和操纵数字内容。根据《[IBM X-Force 2024 年威胁情报指数报告](#)》，2023 年非法市场和暗网论坛上有超过 80 万个帖子提到了人工智能和 GPT，这凸显了网络犯罪分子对这些技术的兴趣与日俱增。人工智能的这种双重性质突出表明，迫切需要采取能够适应不断变化的威胁的强大网络安全措施。降低这些风险的一个有效方法是采用 S/MIME（安全/多用途互联网邮件扩展）来确保电子邮件通信的安全。

S/MIME 简介

确保电子邮件安全

[S/MIME](#)或安全/多用途互联网邮件扩展是发送数字签名和加密邮件的关键。它们能确保电子邮件通信的真实性、完整性和保密性，从而提高电子邮件的安全性。

- **数字签名**

S/MIME 使用数字签名来验证发件人并确保信息未被篡改。这就保证了电子邮件真正来自所述发件人。

- **加密技术**

加密技术利用公共和私人密钥将信息转换成代码，以防止未经授权的访问。这可确保只有目标收件人才能读取信息。S/MIME 还对电子邮件内容进行加密，防止未经授权的访问。只有目标收件人才能解密并阅读电子邮件。



S/MIME简介续

设置S/MIME需要几个步骤：



生成密钥

第一步是创建一对公钥和私钥。公开密钥与他人共享，而私人密钥则保持安全。



申请数字证书

从 CA 获取公开信任的 S/MIME 证书。证书将公开密钥与证书持有者的身份联系起来。



配置电子邮件客户端

电子邮件客户端必须配置为使用 S/MIME。这通常包括安装 S/MIME 证书，并设置客户端使用它来签署和加密电子邮件。



实施 S/MIME 的好处：



真实性

验证发件人身份，确保电子邮件来源合法。



完整性

确保电子邮件内容在传输过程中未被更改。



保密性

保护敏感信息，只有预定接收者才能访问。



行政管理

简化安全和管理流程，无需大量用户培训或 IT 资源。

安全通信自动化

自动化是高效管理证书的关键，尤其是在大规模环境中。它可以减少人工操作，提高安全性，并确保合规性。就安全电子邮件而言，自动执行 S/MIME 证书至关重要。通过自动配置和更新 S/MIME 证书，企业可以确保所有电子邮件通信保持加密和验证，而不会出现证书过期或配置错误的风险。尽管自动化的重要性与日俱增，但一些企业对其可能带来的潜在挑战仍持谨慎态度。

用自动化克服挑战：我们为何提供自动化解决方案

GlobalSign 和 NoSpamProxy 等值得信赖的公司提供的自动解决方案旨在将潜在挑战转化为机遇：

行政问题

挑战：频繁更新根证书很麻烦。

解决方案：我们的自动化工作流程可轻松管理更新，减少管理任务，确保及时更新。成本和开销。

成本和间接费用

挑战：自动化看似成本高昂，对于小型企业来说尤其如此。

解决方案：我们的解决方案可最大限度地减少人工操作，从而降低运营成本，使各种规模的企业都能负担得起并高效地实现自动化。

技术限制和兼容性问题

挑战：技术限制和兼容性问题可能令人望而生畏。

解决方案：自动化改进了系统集成，简化了流程，减少了技术障碍，确保了顺利兼容。

缺乏知识

挑战：如果没有合适的专业知识，实施自动化可能会很复杂。

解决方案：我们提供专家支持和知识，实现流程自动化，使企业无需额外资源即可无缝实施和维护自动化系统。

安全问题

挑战：确保对自动化系统的管理和控制可能具有挑战性。

解决方案：我们的自动化系统可最大限度地减少人为错误，并提供强大的监控和警报机制，确保适当的证书管理，从而提高安全性。

安全通信自动化续

自动化解决方案的优势：

此外，通过利用自动化认证工作流程，企业还能获得更多好处：



提高效率

通过减少人工操作，自动化系统可实现更快、更准确的证书部署、更新和撤销流程。这种效率可节省大量时间，提高业务灵活性。



加强安全

自动化系统可最大限度地降低与证书管理相关的人为错误风险。它们能确保及时签发、更新和吊销证书，并辅以强大的监控和警报机制，主动检测和减少潜在的漏洞。



可扩展性和一致性

各组织可通过自动化解决方案轻松管理大规模 PKI 部署。这一功能确保了证书配置的一致性，消除了可能危及安全的不一致性。



监管合规

自动化系统简化了行业法规和标准的合规性。它们有助于对证书进行一致的监控、审核和管理，降低违规处罚的可能性。



GlobalSign 和 NoSpamProxy 如何提供帮助

对公司而言，掌握不断变化的有效期和管理证书生命周期既费时又费钱，因此极具挑战性。通过与 GlobalSign 和 NoSpamProxy 合作，企业可以实施一个安全、自动化和可扩展的电子邮件安全解决方案，保护其通信免受不断变化的网络威胁，同时节省时间和资源。

GlobalSign 和 NoSpamProxy 提供全面的解决方案，可无缝集成以提供端到端电子邮件安全。我们的组合方法可确保对网络钓鱼、垃圾邮件和其他基于电子邮件的威胁提供强大的保护，同时实现证书管理自动化，以提高效率和合规性。

此外，我们[长达十年的合作伙伴关系](#)为我们提供了额外的信任和稳定性。

- **NoSpamProxy**

专注于电子邮件安全，针对垃圾邮件、网络钓鱼和其他电子邮件威胁提供全面保护。通过利用先进的算法和机器学习，NoSpamProxy 可确保只有合法的电子邮件才能到达您的收件箱，从而大大降低了源于电子邮件通信的网络攻击风险。

- **GlobalSign**

作为数字证书和身份服务的领先提供商，我们提供的解决方案可通过加密和数字签名实现安全的电子邮件通信。这可以确保邮件的完整性和保密性，保护敏感信息免遭未经授权的访问。



整合 NoSpamProxy 和 GlobalSign 的组合解决方案



安全通信的最佳做法

为了进一步加强公司的通信安全，您应该考虑以下最佳做法：

- **教育员工**
定期举办培训课程，让员工了解安全通信实践、识别网络钓鱼企图和负责任地处理敏感信息的重要性。
- **常规证书续期**
确保定期更新证书，如 S/MIME 证书，以保持其有效性和通信安全的有效性。
- **保持软件和工具的更新**
定期更新软件和工具，防范漏洞。
- **实施加密**
对所有敏感通信进行加密，以保护传输过程中的数据，防止未经授权的访问，并保持机密性。
- **自动监控和警报系统**
实施自动化系统，持续监控通信渠道。这些系统可以实时检测潜在漏洞、未经授权的访问尝试或异常情况。自动警报可确保迅速响应并遵守未经授权访问和保密的安全政策。

通过采用这些最佳实践，贵组织可以大大加强对网络威胁的防御，并确保敏感信息的安全传输。

结论

总之，随着数字环境在机器学习的推动下不断发展，安全通信的重要性怎么强调都不为过。各种类型和频率的网络钓鱼攻击表明，亟需针对这些威胁建立强大的防御机制。对最佳实践的基本了解以及高级 S/MIME 证书和自动化的实施，是正面应对这些问题并确保电子邮件通信的真实性、完整性和保密性的关键。

立即采取积极措施，确保贵组织的通信安全，抵御不断变化的网络威胁。与 GlobalSign 和 NoSpamProxy 合作，部署自动化电子邮件安全解决方案，不仅能保护您的业务，还能提高运营效率并确保合规性。



立即联系我们，讨论您的电子邮件安全需求 - 访问

<https://www.globalsign.cn>

关于 GMO GlobalSign

作为世界上根基最牢固的证书颁发机构之一，GlobalSign 是可信身份和安全解决方案的领先提供商，可帮助全球组织、大型企业、云服务提供商和物联网创新者进行安全的在线通信、管理数以百万计的经过验证的数字身份并自动进行身份验证和加密。该公司的大规模 PKI 和身份解决方案为物联网中的数十亿服务、设备、人和物提供支持。GMO GlobalSign 是日本 GMO Cloud KK 和 GMO Internet Group 的子公司，在美洲、欧洲和亚洲设有办事处。欲了解更多信息，请访问 <https://www.globalsign.cn>。