Soverin.

10 Years
MAKING E-MAIL SMILE

Top 10 Predictions on Email Security

What does the next decade have in store for email?

Table of Contents

Introduction

As the digital landscape continues to evolve, so do the threats and opportunities surrounding email security. Over the next decade, the convergence of artificial intelligence, evolving regulations, and **heightened security demands will reshape how both organizations and individuals approach the protection of email communications**. With privacy breaches becoming increasingly sophisticated, and users demanding greater control over their data, the need for user-centric, privacy-first email platforms is more urgent than ever.

Soverin, as a leading provider of secure, privacy-focused email solutions, is committed to staying at the forefront of these challenges. For a decade, our mission has always been to **empower users and hosting companies, resellers, SMBs, MSPs, and ISPs—by offering email services that prioritize privacy, security, transparency, and data sovereignty**. Unlike many large providers, we don't mine users' data or sell their information, making us a trusted partner for those seeking privacy without compromise.

In this whitepaper, we share our top **10 key predictions for the future of email security**, offering deep insights into the emerging risks and opportunities that will shape the next decade. By addressing issues such as the growing role of AI, stricter regulatory landscapes, and the need for global sovereignty in data control, Soverin is prepared to meet the challenges ahead—offering solutions that are as secure as they are user-friendly.

We hope this whitepaper will guide both businesses and individuals in understanding the **key trends shaping email security** and provide actionable strategies to fortify their communications in an ever-changing environment.

> “Google is reading your email. The personalized advertising in Gmail shows that Google is reading your email, and that's not something you want from a Big Tech company.
>
> Within the next decade, privacy will become more and more important... **people are paying more attention to data and privacy**.”
>
> **Twan Welboren**
> Commercial Manager,
> Freedom Internet

Soverin.

The Rising Complexity of Cybercrime: Evolving Threats and the Human Factor

The Rising Complexity of Cybercrime: Evolving Threats and the Human Factor

Email continues to be a primary mode of communication for businesses and individuals alike. Because of this, **cybercrime is becoming more sophisticated**, leveraging advanced technologies to exploit human error—one of the biggest vulnerabilities in email security. The increasing reliance on online platforms has made cybercriminals more adept at deploying tactics like ransomware, spear-phishing campaigns, and identity theft, all of which pose significant risks to businesses and individuals.

While **technological defenses must evolve** to meet these escalating threats, the human element cannot be overlooked. Attackers often exploit the weakest link—users themselves—by using highly personalized phishing attacks, exploiting poor email hygiene, or taking advantage of inadequate awareness around security best practices.

At Soverin, we recognize that security cannot be limited to software alone; **user education** plays an equally critical role. By offering secure email services that prioritize user privacy and control, Soverin empowers individuals and organizations to take ownership of their digital mailboxes' security.

Top Prediction 1

The combination of sophisticated cybercrime and human vulnerability will require a holistic approach to email security—one that blends cutting-edge technology with user empowerment and education. The more users understand the threats, the better equipped they will be to avoid falling victim.

Ongoing education within organizations about phishing risks, identity theft, and secure email practices will be essential in mitigating the human factor in cybercrime.

> “In the digital era, email remains the backbone of business communication. **A secure and steady email platform is not merely a necessity — it is a strategic asset.** It forms the bedrock of trust, collaboration, and sustained productivity in any organization. **That's why we've partnered up with Soverin**, so we offer best-in-class email service to our users.”

Gaëtan Allart
Founder & CEO, Nexylan

Soverin.

Evolving Rules and Regulations for Email Security: Identity Proofing and Regulatory Framework

Evolving Rules and Regulations for Email Security: Identity Proofing and Regulatory Framework

As cyber threats evolve, so must the rules and regulations that govern email security. As previously mentioned, email remains a prime target for identity fraud, phishing attacks, and other forms of cybercrime, and as these threats grow more sophisticated, the need for stronger identity verification protocols becomes clear.

One emerging standard, **Brand Indicators for Message Identification (BIMI), is gaining traction** as a way for businesses to help users verify that the emails they receive are legitimate. BIMI enables brands to display their logo in supported email clients once their identity is authenticated. While this is a step toward a more trustworthy email ecosystem, **BIMI is just the beginning**. As phishing and identity spoofing continue to proliferate, **we anticipate the development of even more advanced email authentication protocols**. These will not only help businesses stand out by showcasing their legitimacy but will also become essential in protecting users from increasingly sophisticated identity fraud and spoofing attempts.

In the future, these **sender verification standards will evolve** to keep pace with emerging threats. **Innovations in identity proofing will play a critical role in email security**, offering users more clarity about the legitimacy of the emails they receive and enabling organizations to protect their brands from impersonation. Companies that fail to adopt these protocols will not only expose their customers to risk but may also face regulatory consequences.

Beyond identity proofing, **regulatory frameworks for email and data protection are tightening** across the globe. As privacy concerns rise and data breaches become more frequent, governments are increasingly scrutinizing how organizations handle email security. Stricter laws are being implemented, not only dictating how emails should be sent, stored, and encrypted but also imposing **more stringent penalties for breaches** and non-compliance.

Organizations are being held to higher standards regarding how they protect the personal information of their customers, and email providers will need to ensure they meet these evolving requirements. The **penalties for non-compliance will continue to grow**, making adherence to regulatory frameworks not just a best practice but a legal necessity.

As a **leading user-centric, privacy-first, and secure email provider, Soverin is already equipped to help businesses** navigate these changes. By offering privacy-first solutions that adhere to the highest standards of data protection, Soverin ensures that users and organizations are prepared for both current and future regulatory demands. Our commitment to transparent, secure email services enables businesses to stay ahead of the curve while offering users the privacy and protection they deserve.

Evolving Rules and Regulations for Email Security: Identity Proofing and Regulatory Framework (cont.)

Top Prediction 2

In the next decade, email identity proofing will become an essential pillar of email security, evolving beyond BIMI to include more robust sender verification standards that protect users from identity fraud and phishing attacks. Email providers that prioritize identity verification will help create a more trustworthy email ecosystem.

Top Prediction 3

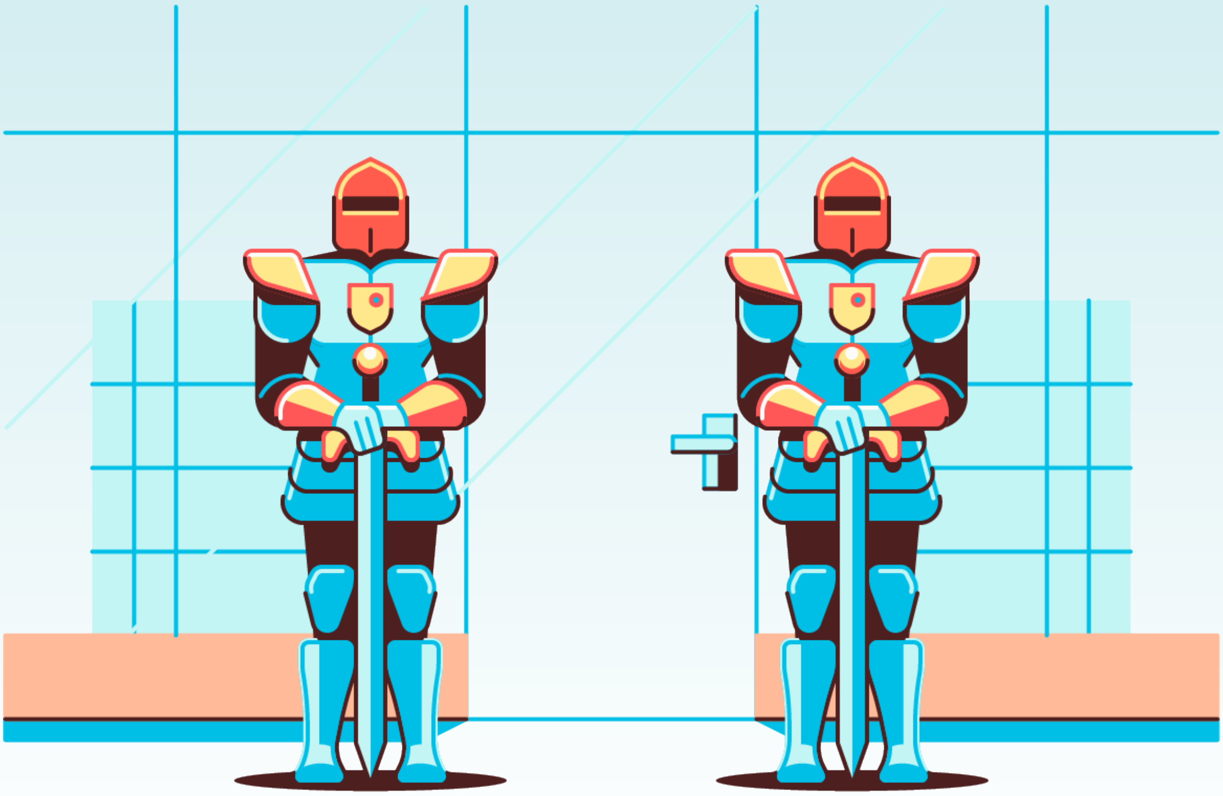
Global regulatory frameworks will continue to tighten, placing greater demands on how organizations manage, store, and secure email communications. The penalties for non-compliance will increase, making it critical for businesses to adopt privacy-first email solutions like those offered by Soverin to ensure regulatory adherence and data protection.

> “As technology evolves, so will the landscape of data privacy. Email providers will need to adapt to emerging threats and regulations. **The future of email lies in ensuring that it remains a secure and private channel for communication.**”

Diana Krieger
CEO, Soverin

Soverin.

Sovereignty and Privacy-First Resilience in Email Platforms



The Rising Complexity of Cybercrime: Evolving Threats and the Human Factor

As global tensions escalate, **email security is becoming increasingly intertwined with issues of national sovereignty and geopolitical strategy**. Europe's dependence on non-EU technology providers, amid a backdrop of technological rivalry between China and the US, raises significant concerns about data security and control. This environment has driven a heightened focus on resilience and the **development of regional, privacy-friendly alternatives** that offer robust data sovereignty.

In response to both privacy concerns and geopolitical dynamics, we anticipate a significant shift toward local data storage and decentralized email platforms. These **platforms, built with privacy at their core, will emerge as the preferred alternatives to Big Tech**, especially within Europe. Soverin, as a leading user-centric, privacy-first email provider, is uniquely positioned to address these challenges by **offering secure and transparent email solutions that prioritize the protection of user data without sacrificing usability**.

Top Prediction 4

The growing demand for data sovereignty and privacy-first alternatives will not only reshape the email landscape but also serve as a catalyst for **developing solutions that promote autonomy, trust, and resilience**.

As privacy becomes a central focus in global digital strategies, **companies like Soverin are set to play a pivotal role in safeguarding both personal and organizational communications** in the years to come.

> “Data privacy is no longer a luxury; it's a fundamental right. **Email providers, no matter where they are located, have a responsibility to protect their users' data** and ensure that it is handled with the utmost care.
>
> The future of email is one where privacy is paramount and where email providers take it seriously.”

Ivo Fokke
COO, Soverin

Soverin.

The Battle Against Reusable Passwords and Data Leaks

The Battle Against Reusable Passwords and Data Leaks

As email continues to be the cornerstone of business and personal communication, one of the most critical vulnerabilities remains the widespread reuse of passwords across multiple platforms. Despite growing awareness of the dangers, **many users still rely on weak or duplicated passwords**, creating a significant risk for businesses and individuals alike. The frequency and scale of data breaches are increasing, and with each breach, millions of credentials are exposed to cybercriminals, leaving sensitive information vulnerable to attack.

The problem of password reuse persists largely because managing unique passwords for every account can be cumbersome for users. However, as the risks of data leaks intensify, **organizations will have no choice but to enforce stricter security protocols, such as unique passwords coupled with multi-factor authentication (MFA)**. MFA has proven to be a crucial layer of defense, but it is not a silver bullet.

At Soverin, we understand the importance of addressing this vulnerability head-on. As we look ahead, we see that **passwordless security solutions are poised to become the new standard**. With our commitment to user-centric security, **we are positioned to lead the shift away from reusable passwords by incorporating advanced authentication mechanisms** that not only enhance security but also prioritize user convenience. These approaches provide a higher level of security while also improving the user experience, as they eliminate the need to remember or store multiple complex passwords.

Top Prediction 5

Within the next decade, **reusable passwords will become obsolete**, replaced by passwordless security systems such as biometric authentication and cryptographic keys.

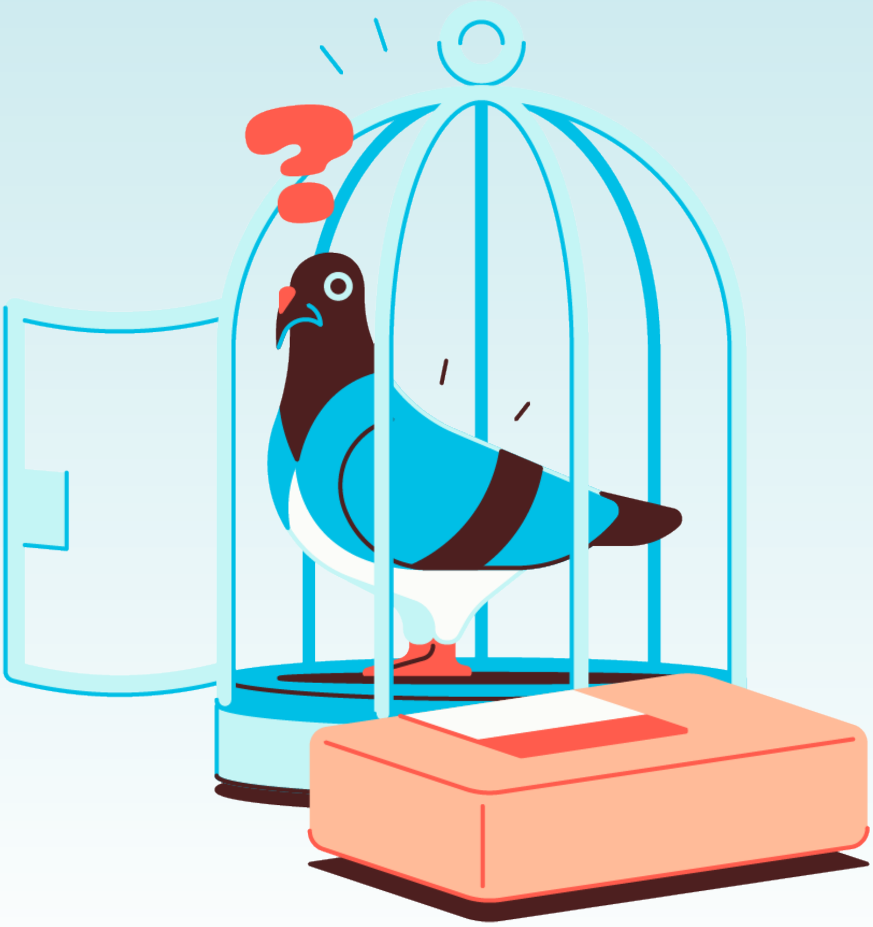
Organizations will adopt these innovations to combat the growing threat of data breaches, and, **email providers like Soverin will lead the way in making passwordless, user-friendly security the norm**, ensuring both privacy and convenience for their users.

> “Email is one of the primary channels for business communication. **Investing in a robust, secure email infrastructure is about more than protecting data; it's about safeguarding your reputation and ensuring operational continuity.**
>
> We wouldn't be able to offer that to our users if we didn't have Soverin offering that safeguard.”

Anco Scholte Ter Horst
CEO, Freedom Internet

Soverin.

Artificial Intelligence: AI as a Threat or Opportunity



Artificial Intelligence: AI as a Threat or Opportunity

As artificial intelligence (AI) continues to evolve, its impact on email security is becoming increasingly apparent. **AI offers both immense promise and significant peril.** On one hand, AI can enhance the efficiency and effectiveness of email security systems, automating threat detection and streamlining filtering processes. On the other hand, it can be leveraged by cybercriminals to carry out more sophisticated and hard-to-detect attacks.

A Double-Edged Sword in Email Security

The dual nature of AI's role in email security is already being recognized. For example, The Guardian recently blocked OpenAI's ChatGPT from scraping its content, raising concerns over how **AI-powered systems can misuse data on a massive scale**. This underscores the risks associated with AI-driven data mining and the potential for AI to be weaponized in ways that compromise privacy and security.

At the same time, AI holds the potential to revolutionize email defenses, using machine learning and pattern recognition to thwart cyberattacks in real time. In an age where AI can be both a weapon and a shield, **Soverin is focused on staying ahead of these trends, utilizing AI to protect email communications while upholding its strict privacy standards**.

Top Prediction 6

AI will become a double-edged sword in email security both a tool for cybercriminals to craft more sophisticated attacks and **an essential technology for defending against those same threats**.

AI-Powered Personalized Spam

Spam emails have traditionally been generic, cast widely in hopes of ensnaring a small percentage of recipients. However, the future of spam is much more insidious. **As AI becomes more sophisticated and accessible**, **cybercriminals will soon be able to generate highly personalized spam messages at scale**.

While this type of targeted spam is still relatively expensive today, it is only a matter of time before it becomes economically viable, making traditional spam filters less effective.

Artificial Intelligence: AI as a Threat or Opportunity (cont.)

AI will allow attackers to gather personal information and craft messages that appear tailored specifically to the recipient, blurring the line between legitimate emails and spam. Soverin's proactive stance on privacy and security will play a crucial role in mitigating this threat. By integrating AI into its spam-filtering technology, Soverin can stay ahead of personalized spam attacks, protecting users from messages that exploit their personal information.

Top Prediction 7

Personalized spam will rise as AI becomes more economically viable, forcing email providers to develop more advanced filtering technologies to keep pace.

AI-Driven Phishing Campaigns

The rise of AI-driven phishing campaigns represents another significant threat. **Highly targeted phishing campaigns, particularly those aimed at high-level individuals such as executives, are already leveraging AI to craft messages that appear nearly indistinguishable from legitimate communications**. As AI continues to evolve, these campaigns will become even more sophisticated and widespread.

The ability of AI to gather and analyze personal data enables attackers to create phishing emails that mimic the tone, language, and content of authentic messages. This creates a new level of risk for individuals and organizations, as traditional defenses may struggle to keep pace with these evolving threats. **At Soverin, the privacy-first approach ensures that personal data is protected from misuse**, while advanced AI-driven tools are integrated into the platform to detect and block these highly sophisticated phishing attempts.

Top Prediction 8

AI-driven phishing campaigns will grow increasingly sophisticated, utilizing personal data to craft nearly indistinguishable phishing emails, **targeting high-level individuals and organizations.**

Artificial Intelligence: AI as a Threat or Opportunity (cont.)

AI in Email Security Defenses

While AI is undoubtedly being used to enhance cybercriminals' tactics, it also holds tremendous potential for defending against these very threats. **The future of email security will rely on AI-powered systems capable of identifying and neutralizing threats in real time**. These systems will use machine learning and pattern recognition to detect suspicious behaviors, continuously learning and adapting to new attack methods.

At Soverin, AI-driven defenses are becoming a cornerstone of its email security strategy. By incorporating advanced AI technologies into its platform, Soverin ensures that its users are protected against the latest threats. These defenses will evolve alongside emerging attack vectors, ensuring that Soverin users are always one step ahead.

Top Prediction 9

AI-powered defenses will become a standard in email platforms, with systems detecting and neutralizing threats in real time through machine learning and pattern recognition.

> “The convergence of artificial intelligence and email will bring both opportunities and challenges.
>
> As AI-powered tools become more prevalent, **it will be crucial to ensure that data privacy remains at the forefront of email innovation**.”
>
> **Andre Meij**
> CTO, Soverin

Soverin.

Striking the Balance: Privacy vs. Convenience in Email Security

Striking the Balance: Privacy vs. Convenience in Email Security

Privacy and security have emerged as non-negotiable priorities for businesses and individuals alike. **With privacy regulations tightening across regions—especially in Europe under GDPR and similar frameworks—organizations are being forced to rethink their approaches to data protection.** However, with these new regulations come challenges in balancing the user experience with the need for robust security.

Historically, privacy-friendly solutions have often been viewed as inconvenient or cumbersome. **Features like multi-factor authentication, encrypted communication, and data minimization practices are critical to protecting users** but can also lead to more friction in everyday usage. Striking the right balance between security and usability is a growing challenge, particularly as users demand both seamless, intuitive interfaces and uncompromising protection of their personal data.

Soverin understands that today's users are no longer willing to compromise. They expect their data to be secure but also demand easy, efficient email solutions that do not slow down their workflows. By providing transparent, privacy-first email services that prioritize user control, **Soverin proves that strong security measures do not have to come at the cost of convenience**. As privacy regulations continue to evolve, businesses will increasingly need to follow this model, making sure that their solutions meet regulatory standards without creating a barrier to efficiency.

Top Prediction 10

In the next decade, **the most successful email platforms will be those that seamlessly integrate privacy and security without compromising on usability.**

Businesses will need to offer frictionless experiences while ensuring compliance with privacy regulations, and **users will expect email services that offer both seamless functionality and uncompromising protection of their data**.

> “**The average person doesn't really care about their data privacy and security.** It's really surprising!
>
> Because whether you are an individual or a business, email is very important. That's why we have partnered with Soverin. In my opinion, they are experts in privacy-first, secure email solutions.”

Julius Heyning
CCO, Gekko

Conclusion

Navigating the Future of Email Security

As the next decade unfolds, the landscape of email security will be defined by rapid advancements in technology, more stringent regulations, and a heightened demand for user privacy. Email, as a cornerstone of communication for both individuals and organizations, will be at the forefront of these shifts, facing ever-evolving threats from increasingly sophisticated cybercriminals while also grappling with new opportunities for more robust protection.

Governments worldwide will continue to strengthen data protection regulations, making it critical for organizations to prioritize compliance. The focus will also shift towards local data sovereignty as businesses seek alternatives to Big Tech, and users demand privacy-first solutions that offer greater control over their data. At the heart of these developments is the growing role of artificial intelligence, which will serve as both a tool for innovation and a potential vector for attack.

In the decade ahead, email providers will be judged by their ability to strike the delicate balance between security and usability, between privacy and convenience. Soverin's approach—centered on transparency, data sovereignty, and user-centric security—positions us to lead this shift, ensuring that businesses and individuals alike can communicate with confidence, knowing their data is protected.

Soverin's Commitment

The path ahead may be complex, but secure email platforms like Soverin will continue to evolve, offering solutions that not only meet the highest security standards but also deliver the seamless, privacy-first experiences that modern users demand.

We invite you to join us in shaping the future of email security—one that is secure, compliant, and above all, respects the sovereignty and privacy of every user.

> “With data breaches growing more sophisticated, **investing in a secure and premium email platform like Soverin's is akin to safeguarding your business with insurance**.
>
> It shields your most critical assets—your data and your reputation—ensuring long-term resilience and trust.”

Alexander van Steen
Manager DevOps, Savvii

Soverin.

Let’s Connect.

Every hero needs a loyal sidekick. As you embark on your journey to generate revenue while providing the best customer experience, we can be yours. Partner up with us to offer your customers a secure, scalable, steady, privacy-first email solution that won’t break the bank.

Contact info: 🌐 soverin.com ✉ hello@soverin.com 📍 Vijzelstraat 68-78, 1017 HL Amsterdam, NL