2027 STATE OF EMAIL SECURITY AND SPAM REPORT · OPENING CHAPTER

From Junk Mail to AI: The Evolution of Email Spam

A history of email abuse, the defenders who fought it, and the new battle over digital trust.

EFAsecurity Research · November 2026 · Read online at efasecurity.com/research/history-of-email-spam.html

1978 The first commercial spam

In May 1978, Digital Equipment Corporation marketing representative Gary Thuerk sent an unsolicited advertisement to hundreds of users of ARPANET, the predecessor of today's Internet. It promoted a computer demonstration. Recipients were not particularly pleased. What the sender saw as an efficient way to reach customers, others saw as an unwelcome intrusion.

At first, spam was largely a nuisance: unsolicited offers and unwanted advertisements. But as email became essential to business and personal life, criminals discovered that it could do more than sell products. It could exploit trust. Over the following decades, spam would become a vehicle for fraud, credential theft, malware and impersonation. Every time defenders developed a new countermeasure, attackers adapted. The history of spam is the history of that technological arms race.

1990s When spam became a business

Email was moving beyond research networks into companies and homes. The economics were compelling for senders: a postal advertisement required printing and postage, while an email campaign could reach thousands at almost no marginal cost. Even a tiny response rate could be profitable. The costs fell on recipients and network operators through lost time, bandwidth, storage and administrative effort.

Many early mail servers operated as open relays, forwarding messages for outsiders. Spammers exploited those configurations to distribute messages using other people's infrastructure. Administrators tightened relay settings, introduced content rules and blocked abusive senders. In 1997, the Real-time Blackhole List from the Mail Abuse Prevention System helped operators share information about spam sources. The Spamhaus Project was founded in 1998, contributing to organized anti-spam efforts.

But blocked senders moved elsewhere. Secured relays sent abusers looking for new weak systems. When filters recognized certain phrases, spammers changed the wording. The problem was no longer just what a message said; it was the abuse of an interconnected delivery system at scale.

2000s When spam became cybercrime

By the 2000s, the objective was changing. Unsolicited advertising continued, but criminals increasingly used email to steal passwords, financial details and access to systems. Phishing, already seen in the 1990s, expanded alongside online banking and commerce. Messages impersonated banks, eBay, PayPal and other familiar brands. A warning about a password or transaction led recipients to counterfeit websites designed to capture credentials.

Attackers also used botnets: networks of compromised computers capable of sending huge volumes of mail from constantly changing sources. Blocking individual addresses became less effective.

Defenders responded with layered controls. SpamAssassin, first released in 2001, combined multiple detection signals into a single score. Bayesian and other statistical filters, popularized in 2002, learned patterns from message content. SPF let domain owners designate their authorized sending servers, while DKIM added cryptographic signatures that receivers could verify. Malware scanning, reputation, policy rules and authentication became foundational.

But authentication could not establish intent. A message could originate from an authorized server and still be malicious. A compromised account could send fully authenticated mail. The CAN-SPAM Act of 2003 also set rules for commercial email in the United States, reflecting growing regulatory attention. By the end of the decade, effective email security required much more than a list of suspicious words.

2010s When email became a target for organized fraud

By 2010, organizations depended on email for invoices, contracts, payments and daily decisions. That reliance increased the value of deception. Symantec MessageLabs estimated that spam made up 89.1 percent of the email it monitored in 2010. By 2015, Symantec put the share at about 53 percent. That decline reflected real progress against bulk spam, but it did not mean the danger was disappearing.

Attackers increasingly focused on the value of a single successful message. An accountant could receive what appeared to be a request from the CEO. A vendor could seem to have changed its bank account. A payroll administrator could be asked to update direct-deposit details. These messages sometimes contained neither malicious links nor attachments: only a persuasive instruction.

Business Email Compromise (BEC) became a major financial threat. The FBI's Internet Crime Complaint Center (IC3) reported 7,838 BEC complaints and more than $263 million in losses in 2015. In 2019, it reported 23,775 BEC and email-account-compromise complaints, with losses exceeding $1.7 billion. Reporting categories and coverage change over time, so these figures are best read as reported losses rather than a complete count of all attempts.

DMARC, published as RFC 7489 in 2015, built on SPF and DKIM to let domains publish an authentication policy. Yet attackers could sidestep the spoofing problem by compromising a real mailbox. An authentic message could still be controlled by a criminal. Verifying origin was not the same as verifying intent. The most consequential attacks increasingly exploited relationships, authority and trust.

2020s When trust became the target

Email had become the communication layer connecting cloud services, payments, contracts and customer records. In 2024, Google and Yahoo tightened authentication requirements for mail sent to their consumer inboxes, including DMARC requirements for bulk senders. These measures raised the bar for some kinds of impersonation, but could not stop misuse of legitimate accounts.

Consider a supplier and customer discussing an invoice. An attacker who compromises one mailbox can read the thread, wait for the right moment and insert new payment instructions. The message may arrive from the real address, pass authentication and look ordinary. Microsoft's security research has described conversation hijacking, malicious inbox rules and other account-abuse techniques. The FBI's 2025 Internet Crime Report put BEC losses at more than $3 billion for the year, illustrating the scale of the harm reported by victims.

Generative AI added another dimension. Attackers could draft polished, personalized messages in multiple languages, quickly vary wording and imitate routine business exchanges. AI did not invent phishing; it reduced the effort involved. Defenders continued relying on authentication, reputation, rules and malware scanning, while increasingly adding behavioral analysis, machine learning, identity signals and shared threat intelligence. No single technique could answer every question about trust.

The numbers behind the shift

Year	Measure	Reported figure
2010	Share of monitored email that was spam (Symantec MessageLabs)	**89.1%**
2015	Share of monitored email that was spam (Symantec)	**about 53%**
2015	BEC losses reported to the FBI (7,838 complaints)	**$263 million+**
2019	BEC and account-compromise losses reported to the FBI (23,775 complaints)	**$1.7 billion+**
2025	BEC losses reported to the FBI	**$3 billion+**

Bulk spam's share fell while losses from a single convincing message rose more than tenfold. Figures are as published by each source and are not adjusted for changes in reporting.

2026 AI versus AI

For nearly five decades, email security has evolved through a contest between attackers and defenders. In 2026, artificial intelligence is used on both sides. Criminals use generative AI to write convincing phishing messages, personalize attacks, imitate business correspondence and produce endless variations. Defenders use machine learning and AI-assisted analysis to detect patterns, weigh context and investigate suspicious behavior.

This is no longer simply spammers writing messages and administrators writing filtering rules. Automated systems increasingly shape both attack and defense. Yet AI has not made authentication, reputation systems, filtering rules or human judgment obsolete. It has added another layer to an already complex security problem.

Attackers still seek to exploit trust. Defenders still seek to tell legitimate communication from deception. What has changed is the speed, scale and sophistication with which both sides can operate.

The first commercial spam email in 1978 was written by a person and sent to hundreds of recipients. Nearly fifty years later, artificial intelligence can help generate, personalize, distribute and analyze malicious messages on a scale unimaginable to email's early pioneers.

> **The technology has changed dramatically. The fundamental struggle has not.**

The next chapter of email security will be decided not simply by which side has better artificial intelligence, but by which side can establish trust more reliably.

Coming in spring 2027: the State of Email Security and Spam Report

This history opens our 2027 annual report, due in March or April 2027. The report will look at what changed in email threats during 2026 and how defenders are adapting, drawing on what OpenEFA and EFA Collective Intelligence observed in production alongside public data from the FBI and other sources.

Last year's edition, The State of Spam and Security in the Modern Communication Era, is available from OpenEFA Research. To hear when the 2027 report is published, sign up for EFAsecurity email alerts.

Sources

- Symantec MessageLabs Intelligence, 2010 Annual Security Report.
- Symantec, Internet Security Threat Report, Volume 21 (April 2016), covering 2015.
- FBI Internet Crime Complaint Center, Internet Crime Reports for 2015, 2019 and 2025, ic3.gov.
- IETF RFC 7489, Domain-based Message Authentication, Reporting, and Conformance (DMARC), March 2015; RFC 7208 (SPF); RFC 6376 (DKIM); rfc-editor.org.
- Google, Email sender guidelines (bulk sender requirements effective February 2024); Yahoo Sender Hub, sender best practices.
- Microsoft Security blog and Microsoft Threat Intelligence reporting on business email compromise, inbox-rule abuse and conversation hijacking.
- CAN-SPAM Act of 2003, 15 U.S.C. 7701 et seq.

About EFAsecurity and OpenEFA. EFAsecurity connects email, servers, websites and network infrastructure through EFA Collective Intelligence, so what one deployment learns protects all of them. OpenEFA is the family's email security service: intent-based filtering with every verdict explained. Learn more at efasecurity.com and openefa.com.

© 2026 Quantum Logic Systems, LLC. This article may be shared in full with attribution.