

EMAIL SENDER VERIFICATION



(650) 837-0000

info@StrategyGroup.net

"the practical solution to spam"

Instead of trying to filter-out spam, filter-in real email

A single email is not a problem, but a collection of emails is. As email is personalized communication, it is impossible to solve the spam problem after email is already sent. Centralized solutions are not viable, if the beneficial values of current Internet email are to be preserved. We have a patent pending technology that takes into account these perspectives to significantly reduce or potentially eliminate spam. The name of the new anti-spam technology is "Email Sender Verification System" - ESVTM for short.

The key concepts are:

- Tag non-spam emails before they are sent.
- Empower email users with automated tools to set and manage the **use policies** and **usage patterns** for their email addresses and identities.

The solution to spam problem consists of embedding a tamperproof tag in emails before they are sent. This solution will be 100% effective if both the sender and the recipient use it. The tamperproof tag provides an automated and efficient way for differentiating spam and non-spam emails on the receiver-side.

The solution is an overlay over existing Internet email infrastructure. It is totally transparent to SMTP-compliant systems, whether or not the systems implement the ESV technology. The solution is also backward compatible.

Email is personalized communication. So no generalized solution for distinguishing spam is possible. The only real solution is to let individual email users determine the use policies and usage patterns of their email addresses and identities, and empower them to manage their email usage.

The ESV technology makes this possible. By empowering the email users directly with automated tools, the ESV technology equalizes the current technology imbalance between senders of spam and spam recipients. Adoption by legitimate email users is sufficient to turn the tide against spam using the ESV technology.

The ESV system consists of (1) ESV user software, (2) ESV server software.

This is how the system works:

1. Email users download the ESV user software, and choose a ESV service provider (or setup their own ESV server).
2. Email users define their email use policies and usage patterns.
3. Before an email is sent, the system verifies that the email transmission complies with the usage patterns specified by the email address owner. Otherwise, the system will alert the email user and the system administrator — without sending the email. **ESV is the only solution that prevents or decreases spam transmission.**
4. If the email transmission is valid, the ESV system will create a tamperproof tag that is included in the email.
5. The email is then sent using standard Internet protocols.
6. On systems that implement the ESV technology, upon receiving an email the system verifies that the ESV tag is present and valid. If the ESV tag is valid, then the email is non-spam. If the ESV tag is not valid (likely spam) or present, then it can be processed using non-ESV methods. There is no difference in the way an email is processed on the recipient system if ESV is not implemented. As the adoption increases, it is expected that legitimate non-ESV email will decline rapidly.
7. Once the solution reaches sufficient adoption levels, it is possible to make the Email Sender Verification a feature of email products and services, and not required as an add-on.

We are seeking resources and collaboration to commercialize the ESV technology, and bring it into market — including

- ESV standard development
- Development partnerships
- Distribution partnerships
- Technology commercialization

To learn more, please send an email to george@StrategyGroup.net.