

Alternate formats: [HTML](#) | [plain text](#)

US Financial Services Industry Group Endorses SPF

April 21, 2007 — *BITS*, a nonprofit industry consortium formed by many of the largest financial institutions in the USA, has [announced](#) their *BITS Email Security Toolkit* white-paper, describing "protocols and recommendations for reducing the risks" in institutions' e-mail correspondence, addressing prominent problems such as *identity forgery* and *phishing* (password fishing). *BITS* held an industry e-mail security summit in November 2006, which developed these recommendations. The *SPF Project* participated in this summit.

The *BITS Email Security Toolkit* points out, and recommends to *BITS* members the deployment of, three major complementary technologies that are considered to provide a significant contribution "to [mitigating] the threat to email security and [restoring] customer confidence in email as a channel of communication with financial institutions":

- *Transport Layer Security (TLS)* (an update to the well-known *SSL*) for message transport confidentiality and server-to-server authentication,
- *Sender Policy Framework (SPF)* and *Sender ID* (a [Microsoft derivative of SPF](#)) for sender address authentication, and
- *DomainKeys Identified Mail (DKIM)* for sender authentication and message integrity.

According to *BITS*, *SPF* is a computationally light-weight means for protecting the credibility and reputation of brands and domains while improving the deliverability of messages and reducing the volume of non-delivery receipts received by spoofed domains. It also acknowledges the ease of deploying *SPF*.

Specifically, the *BITS Email Security Toolkit* calls for e-mail senders and recipients to:

- publish *SPF* records for both e-mail and non-e-mail domains enabling sender authentication within eighteen months,
- enable *SPF* record validation on incoming e-mail immediately,
- publish *SPF* records as (hard) "Fail" (-all) as opposed to "SoftFail" (~all), which should only be used while testing out one's *SPF* record,
- honor records in receiving environments that are published as (hard) "Fail", and reject failing messages.

"We welcome the initiative of *BITS* and we support their clear recommendations for financial institutions to deploy *SPF* in combination with other e-mail security technologies", says *Scott Kitterman*, member of the *SPF Council*, the project's steering committee. "Sender address forgery is among the biggest problems of the e-mail medium and provides significant potential for criminal conduct. However, *SPF* is not just for banks and insurance companies. Anyone with a domain or a mail server, ranging from governments through sports clubs to hobbyist individuals, can benefit from protecting their domain and brand name with an *SPF* policy and checking *SPF* on incoming e-mails."

About the *SPF Project*

The *SPF Project* was founded in 2003 by [Meng Weng Wong](#) and other dedicated internet technologists to act against the increasing levels of e-mail sender address forgery by spammers, imposters, and computer viruses. The project has developed the sender authentication technology called *Sender Policy Framework*, which aims to fix various ambiguities in the standards underlying the e-mail system that have essentially remained unchanged since their inception in 1982. *SPF* allows domain owners to define who may and may not send mail using their domain names.

For more information about *Sender Policy Framework* see:

<http://www.openspf.org>

About the SPF Council

The *SPF Council* is a group of participants elected by the *SPF Project's* community who are commissioned to steer and represent the project based on community consensus. The council drives the project's technology standardization and research efforts, and maintains contact with other e-mail anti-abuse initiatives and industry organizations.

For more information about the *SPF Council* see:

<http://www.openspf.org/Council>

Press Contacts

USA:

Scott Kitterman
SPF Council
e-mail: scott@kitterman.com
phone: +1 301 325-5475

Europe:

Julian Mehnle
SPF Council
e-mail: julian@mehnle.net
phone: +49 179 5145688