Sender ID Framework:

Protecting Your Brand, Users & Infrastructure

Craig Spiezle
Director, Online Safety
Trustworthy Computing Group
craigspi@microsoft.com

Microsoft®

Overview

- Why do we need authentication?
- What is Sender ID?
- How does Sender ID work?
- Why we need reputation data?
- Adoption & Results
- Optimization Recommendations
- Tools & Resources

Why we need authentication

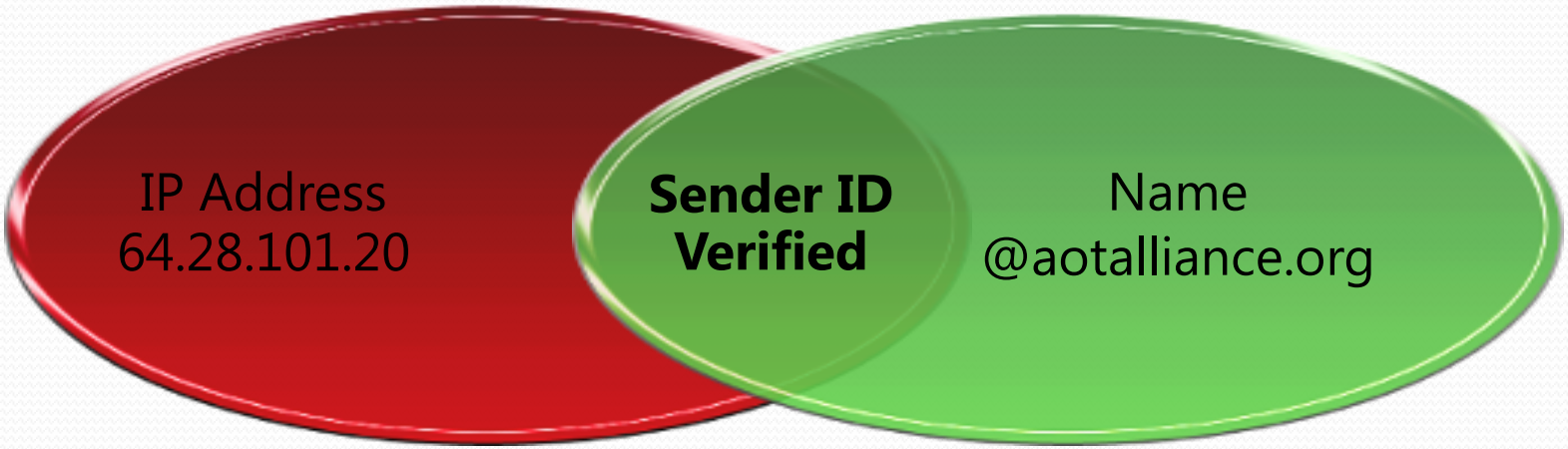
Broad spoofing of top domains

- Worldwide spoofing & phishing
  - ISPs & Carriers
  - Financial Institutions
  - Government & ecommerce sites
  - Prevalent in 95% of phishing exploits

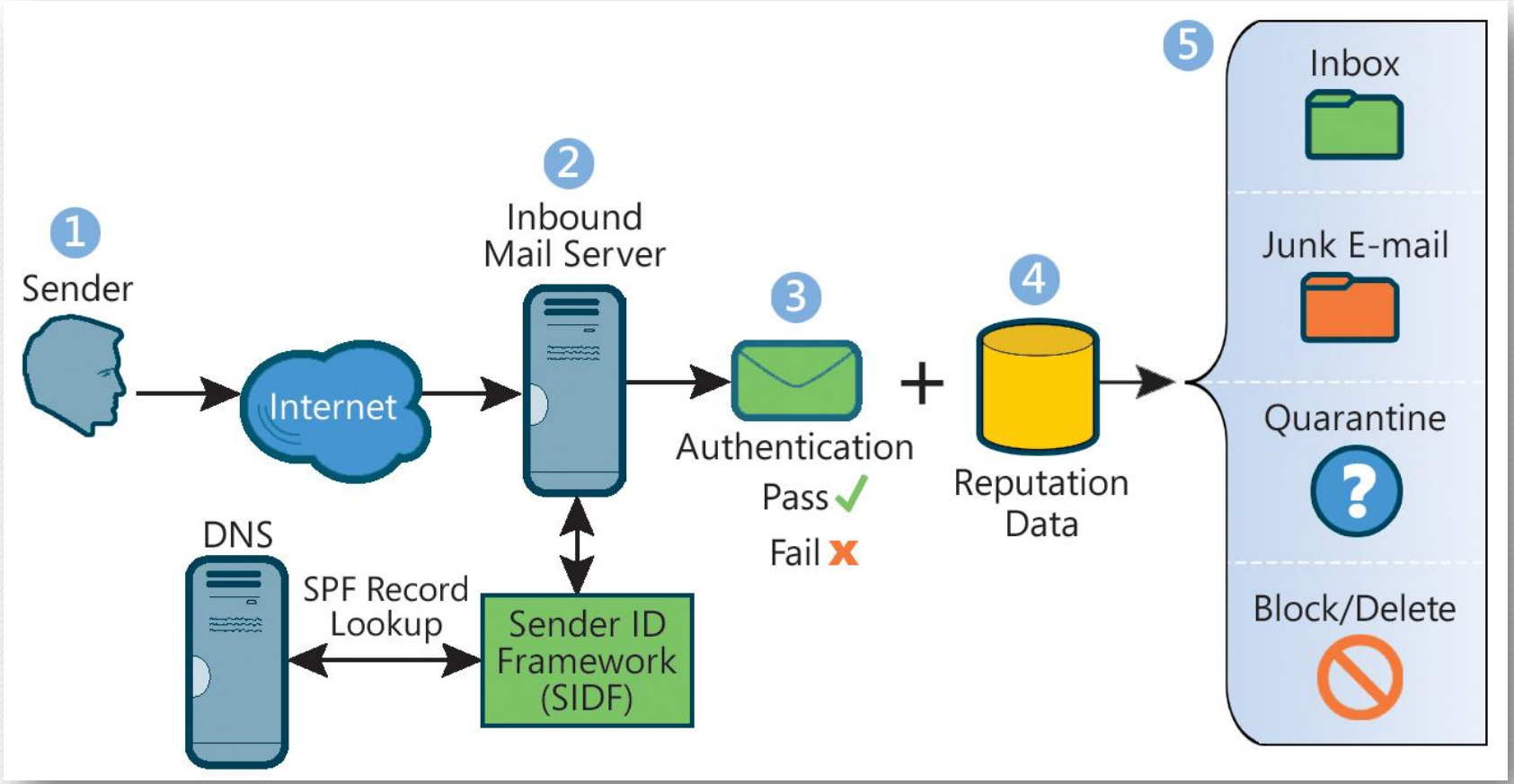
Domain	Spoof Rate
yahoo.com	81.0%
gmx.net	61.3%
bankofamerica.com	47.3%
verizon.com	45.7%
irs.gov	41.2%
telefonica.net	40.4%
paypal.com	37.6%
hotmail.com	33.3%
comcast.net	33.0%
prodigy.net	29.2%
ebay.com	27.9%
aol.com	26.1%
amazon.com	10.4%

What is Sender ID?

- A royalty and license free standard developed jointly by IETF, Microsoft and industry, addressing the difficulty of verifying a sender's identity.
- Provides a “driver's license” for the sending domain, a basis for reputation
- Validates the origin of e-mail by verifying the IP address of the sender against the purported owner of the sending domain.
- Senders and domain owners need to authenticate outbound email and receiving networks & ISPs need to verify
- No outbound server, client changes and no user interaction



How Sender ID Works



SIDF Validation Alternatives

Purported Responsible Address (PRA)	MAIL FROM
▪ Derived from RFC2822 message headers ▪ Resent-Sender, Resent-From, Sender, From ▪ Identity typically seen by users	▪ RFC2821 “bounce” address ▪ Also known as SPF classic
▪ Helps detect phishing ▪ Easier adoption for forwarders	▪ Helps reduce “joe jobs” ▪ Checking can begin before message data is received
▪ Both can utilize the same SPF record format	

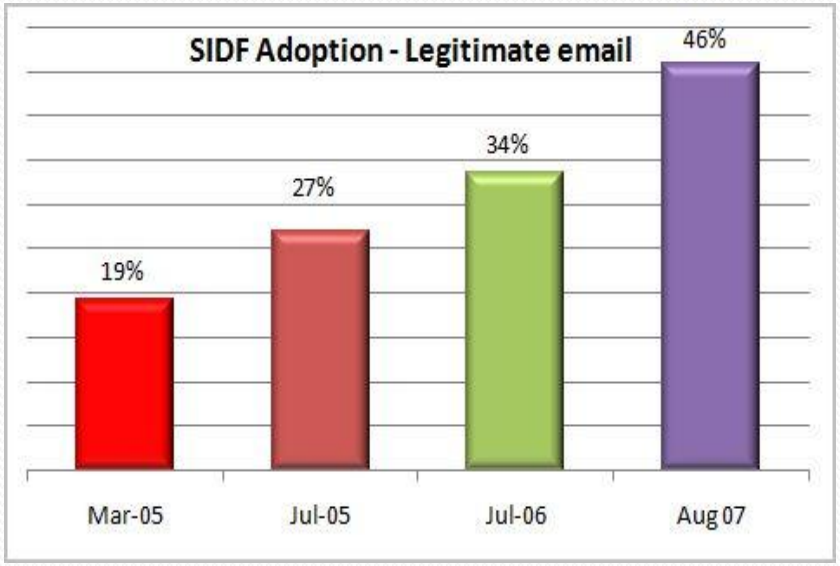
Why Authenticate Email & SIDF?

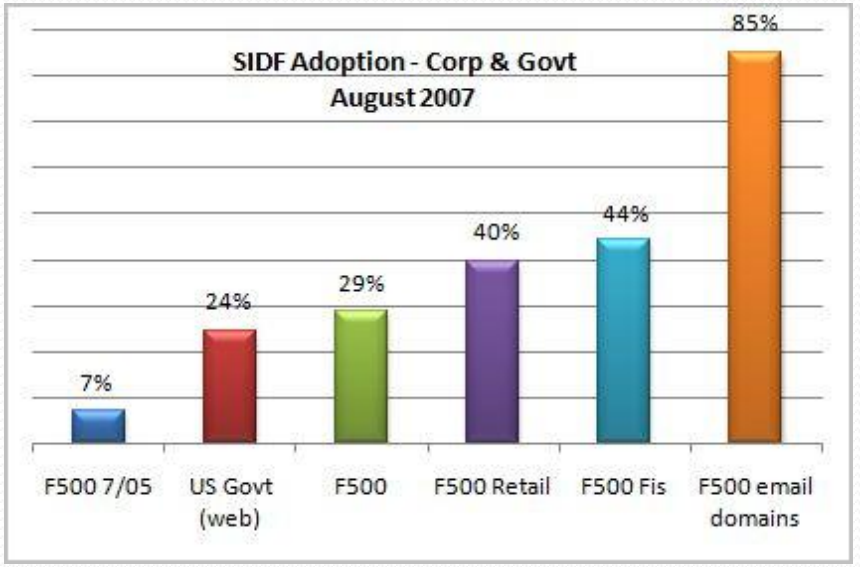
- Senders and brand owners
  - Protect their brands & domain
  - Improved email deliverability
- Receiving networks (corporate ISPs)
  - A tool for more accurate filtering resulting in improved deliverability of legitimate e-mail
  - Identify who is responsible for a message
- For everyone
  - Increased protection from spam & phishing
  - Improved online trust & confidence

- Results
  - 85% fewer false positives for senders with good reputations
  - 8% additional spam detection
  - Blocks 95% of phishing exploits
  - Supported by over 12 million domains

Growing Worldwide Adoption

- Over 46% of legitimate e-mail
- Growing support by Fortune 500 and key vertical markets
- Over 12 million SIDF compliant domains (2)





Sources: Microsoft research 8/31
(2) MarkMonitor Report 7/27

Deploying Sender ID

- Start with planning
  - Form a project team
  - Obtain executive sponsorship
  - Involve all stakeholders
- Assembling the data
  - Need a comprehensive inventory of who is sending mail on your behalf
  - Marketing, DNS, email, ecommerce, international, …
  - Service providers, hosters, registrars, …
- Publish to DNS
  - DNS infrastructure must support TXT records
  - May need different SPF records for PRA and MAIL FROM checks if different domains are used
- Don’t forget maintenance!
  - When new mail servers / services added
  - When IP addresses change
  - Allow for DNS propagation time

Sender ID SPF Record Wizard

www.microsoft.com/senderid/wizard

Quick Links | Home | Worldwide

Microsoft

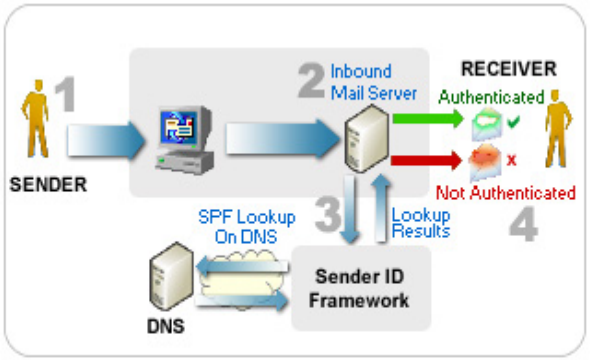
Search Microsoft.com for: Go

Safety

Wizard Home | About Sender ID

Sender ID Framework SPF Record Wizard

This four-step wizard will guide you through the process of creating a new SPF record for your DNS domain. You should add this DNS record to your domain's DNS configuration. Note that you may need to manually edit the SPF record created by this wizard if you want to use some of the more advance features of the SPF format. For complete details please refer to the SPF record specification at http://www.microsoft.com/senderid.



How does Sender ID Framework work?

1. Sender sends an e-mail to Receiver.
2. Receiver's inbound e-mail server receives e-mail and calls its Sender ID Framework.
3. The Sender ID Framework looks up the SPF record of the domain that Sender is using for sending the mail.
4. The receiving Mail Transfer Agent (MTA) determines if the outbound Mail Server IP address matches IP addresses that are authorized to send mail for the user.

Step 1 of 4: Identify Your Domain

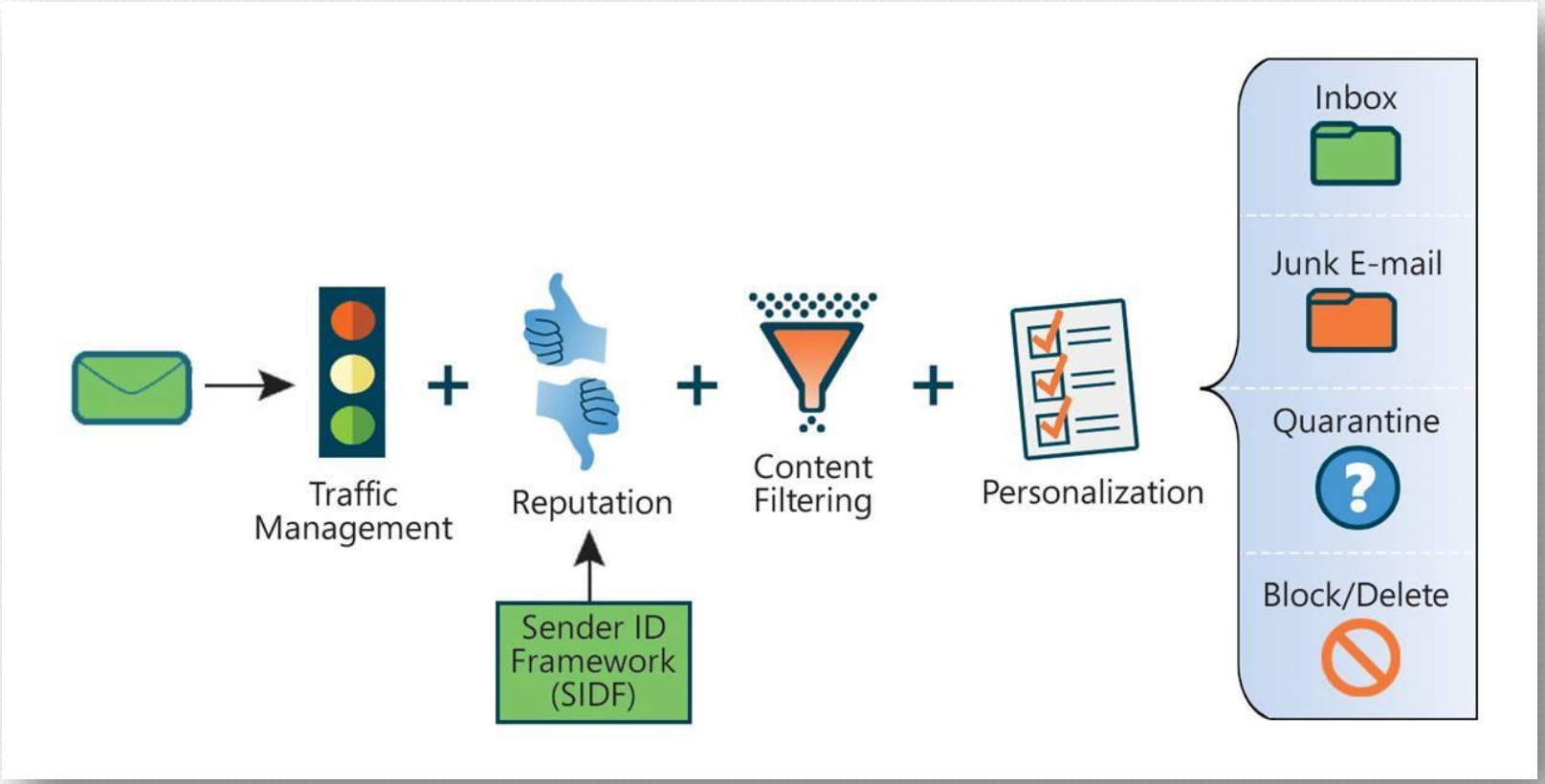
Please enter the domain name for which you want to create a new SPF record
(*for example: example.com*):

Start >

SPF Record Recommendations

- Do NOT use….
  - Pointer (PTR) – DNS overhead and not fully supported
  - "?all" Syntax – Indicates a test record, initially used by spammers. Can result in a negative score
  - "+all" any IP can send mail on your behalf.
- Recommended "–all"
  - Maximum confidence for receiving networks
  - Maximum protection from phishing and brand attacks

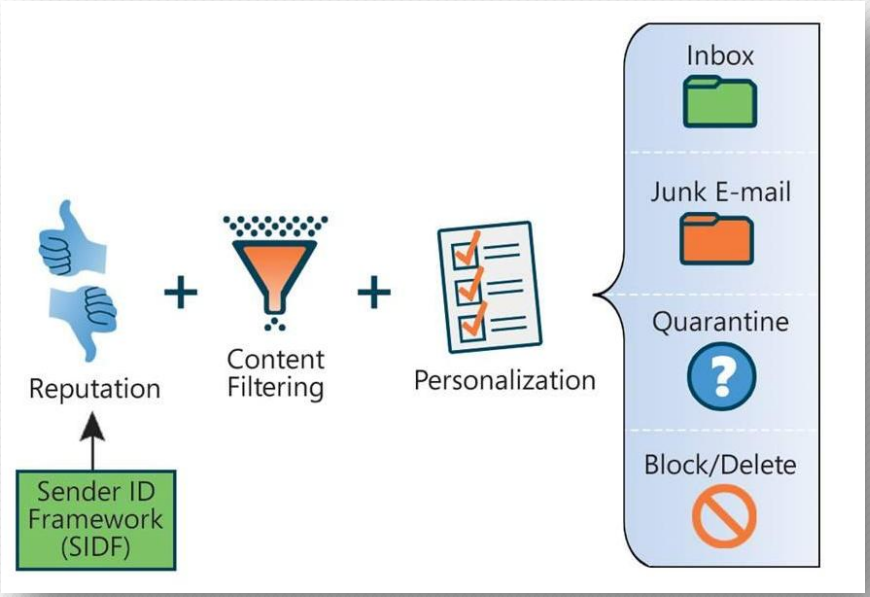
Filtering & Scoring



- All four elements are useful, necessary and imperfect
- Momentum on reputation today to overcome content filtering limitations and spammer tactics

Reputation

- "Pass" ≠ "good mail"
  - Authentication ≈ driver's license
  - Reputation ≈ driving record
- Applied to sender's domain name or IP address
  - Sender authentication a critical pre-requisite
- Contributing factors
  - Recipient feedback
  - Traffic patterns
  - Domain, IP, NS longevity
  - Location
  - Unsubscribe behavior
- Augments content filtering scores



Sender ID + Reputation Example

Current Content Filtering & Scoring

Spam Features		Non-Spam Features	
Feature	**Weight**	**Feature**	**Weight**
Free	- 0.0413	Document	+ 0.0084
Free (Subject)	- 0.2397	Record	+ 0.0402
Hot	- 0.0453	Confidential	+ 0.0925
Sexy	- 0.0756	Job	+ 0.1323
Diploma	- 0.1776	Pen	+ 0.0234
Viagggra	- 0.3222	Apple	+ 0.1196

Sender ID with Reputation

Spam Reputation	Good / Non-Spam Reputation
- 1.7203	+ 3.1642

Example - Email about investments, interest rates, and other financial data

- Content score = -.9103, → mail delivered to junk folder.
- Mail is from legitimate bank, passes SIDF, reputation score = +3.1642
- Net score = 2.2539, → mail delivered to Inbox

- *Note: Weights change frequently. Values shown are for illustration only.*

Resources

- Implement Sender ID – Inbound & outbound
  - Publish your SPF record www.microsoft.com/senderid/wizard
  - Submit your domain to the Windows Live Hotmail cache www.microsoft.com/postmaster (online submission form)
  - Support senderid@microsoft.com
- More Information
  - www.microsoft.com/safety
  - www.microsoft.com/senderid

Thank You

Microsoft