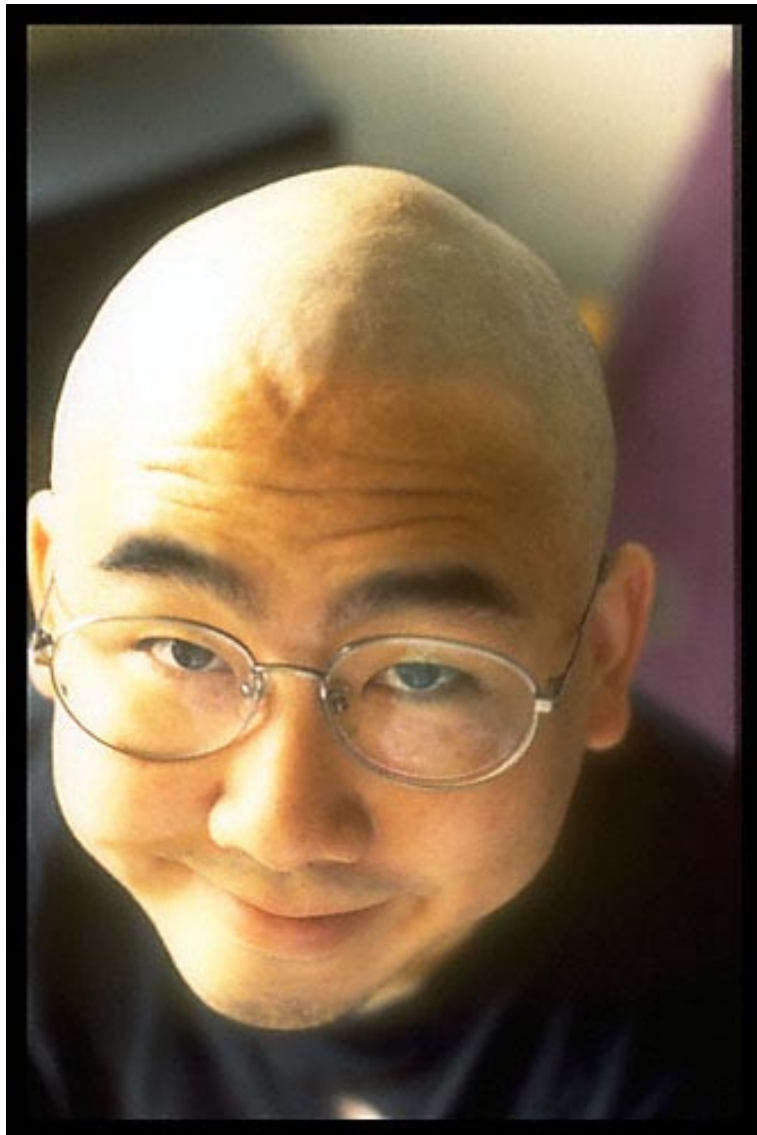


# **2004 Antispam Roundup**

with a focus on Sender Authentication Schemes  
and a sneak peek at a Next-Generation Email Architecture



**Wong Meng Weng <mengwong@pobox.com>**  
**Founder & CTO for Special Projects, Pobox.com**  
**Visiting Fellow, Earthlink**  
**Senior Technical Advisor,**  
**Messaging Anti-Abuse Working Group**

**December 10th 2004**  
**at Infocomm Development Authority**  
**Singapore**

## **Current Symptoms**

- **commercial spam (buy Cialis! Viagra!)**
  - **419 scams (Hi, I am ex-President Tofu's wife, I need your help to move \$50 million)**
  - **phishing (please enter your credit card number and all your personal information)**
  - **worms & viruses**
  - **80% of all email**
  - **big problem**
- 
- **at the ITU, delegate from Syria complained loudly about spam**
  - **many developing countries have less bandwidth than Hotmail**

## **What's the threat model?**

- **Internet email is wonderful because anyone can send mail to you for free**
- **Internet email is terrible because anyone can send mail to you for free**
  
- **email can contain anything**
- **once humans see an eBay logo they ignore everything else**
- **humans like to open attachments and [click on links](#)**
- **this is how humans work, there's no use complaining that people are gullible**

**What's the immediate concern?**

- **lots of money spent on bandwidth, cpu, disk, Brightmail, antispam solutions**
- **lots of money lost in productivity by people deleting spam by hand**
- **lots of intangible costs in missed communications due to poor integrity and reliability**
- **antispam is a \$2bn/year industry and growing**
- **that's great for antispam companies, but society shouldn't have to bear that cost**

**What's the strategic concern?**

- **not that individual victims lose thousands of dollars on scams and identity theft**
- **not that banks lose hundreds of millions of dollars on fraud**
  
- **the real problem is that people might give up on email**
- **society has invested a lot of money in ecommerce, especially banks**
- **banks saved a lot of money on ATMs.**
- **banks hope to save just as much money on Internet banking**
- **banks have spent billions of dollars reinventing themselves for the Internet**
- **phishing undermines consumer confidence**
- **billions of dollars wasted**

## **Current solutions**

- **content filtering, Brightmail, Postini, Cloudmark, Ciphertrust, Mailfrontier, etc. etc. etc.**
- **80 to 90% effective**
- **costs roughly \$1/user/month**
- **they are collecting a nice tax on email**
- **also the operating and capital expense of running lots of CPUs**
- **90% is not good enough**
- **there is no such thing as a small security hole**
- **the antispam vendors push out a new rule**
- **spammers respond within 4 hours**
- **cannot fight an arms race**



## Small Town Philosophy

- email was invented in the 1980s. mostly geeks online
- “let’s get the mail through”. hence open relays, hence spam.
- functionality before security
- leave your doors unlocked
- greet people on the street





## The Internet is now a Big City

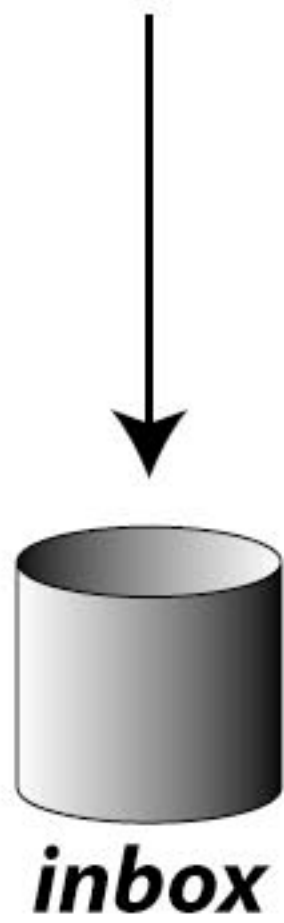
- lock your doors
- don't talk to strangers
- frown at everyone
- if someone wants to talk to you, they need to be introduced.



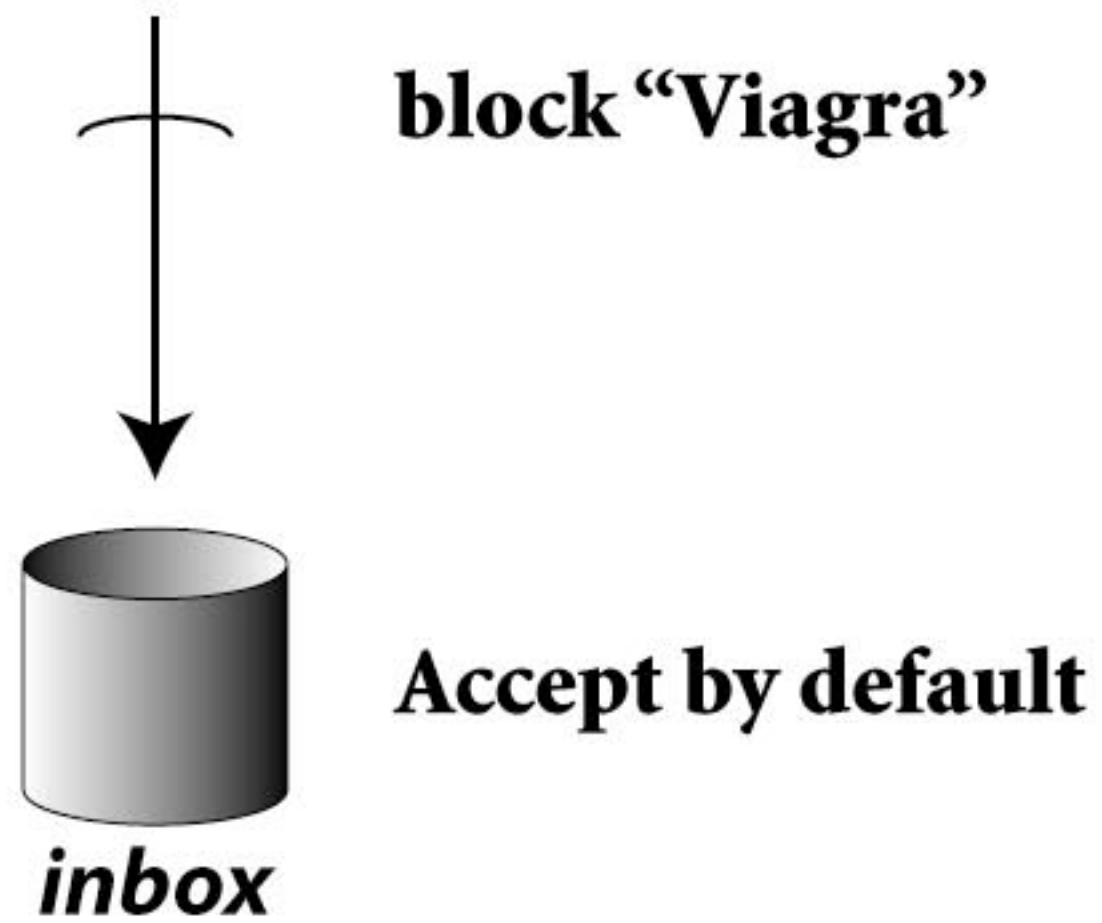


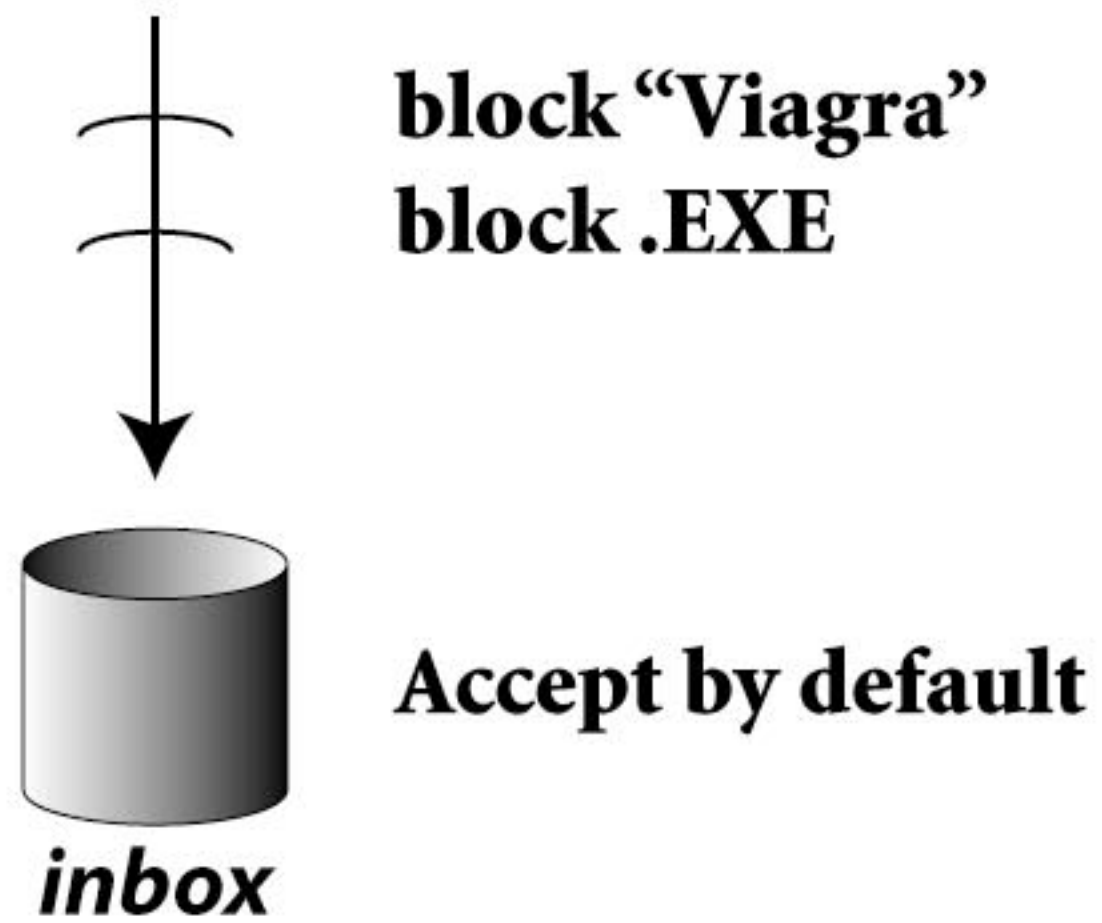


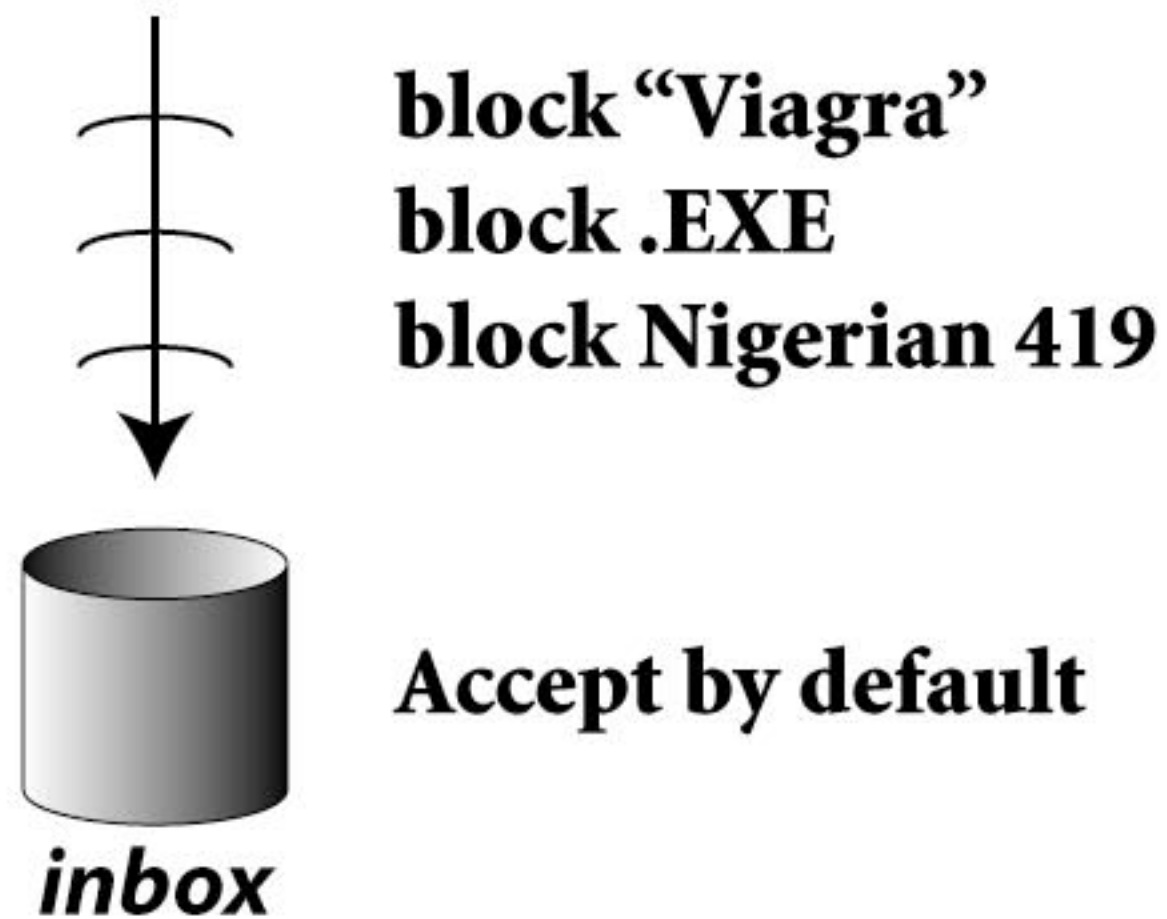
***inbox***



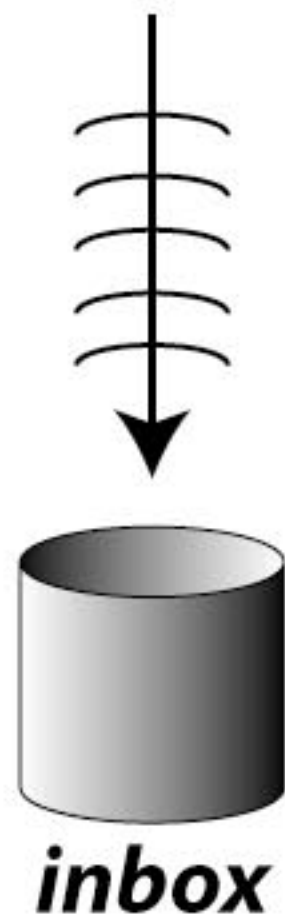
**Accept by default**





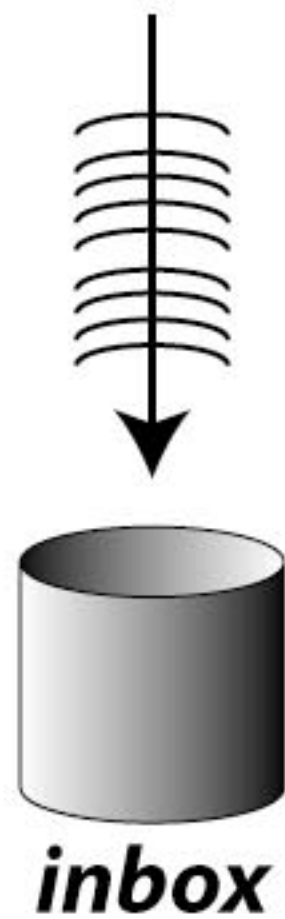






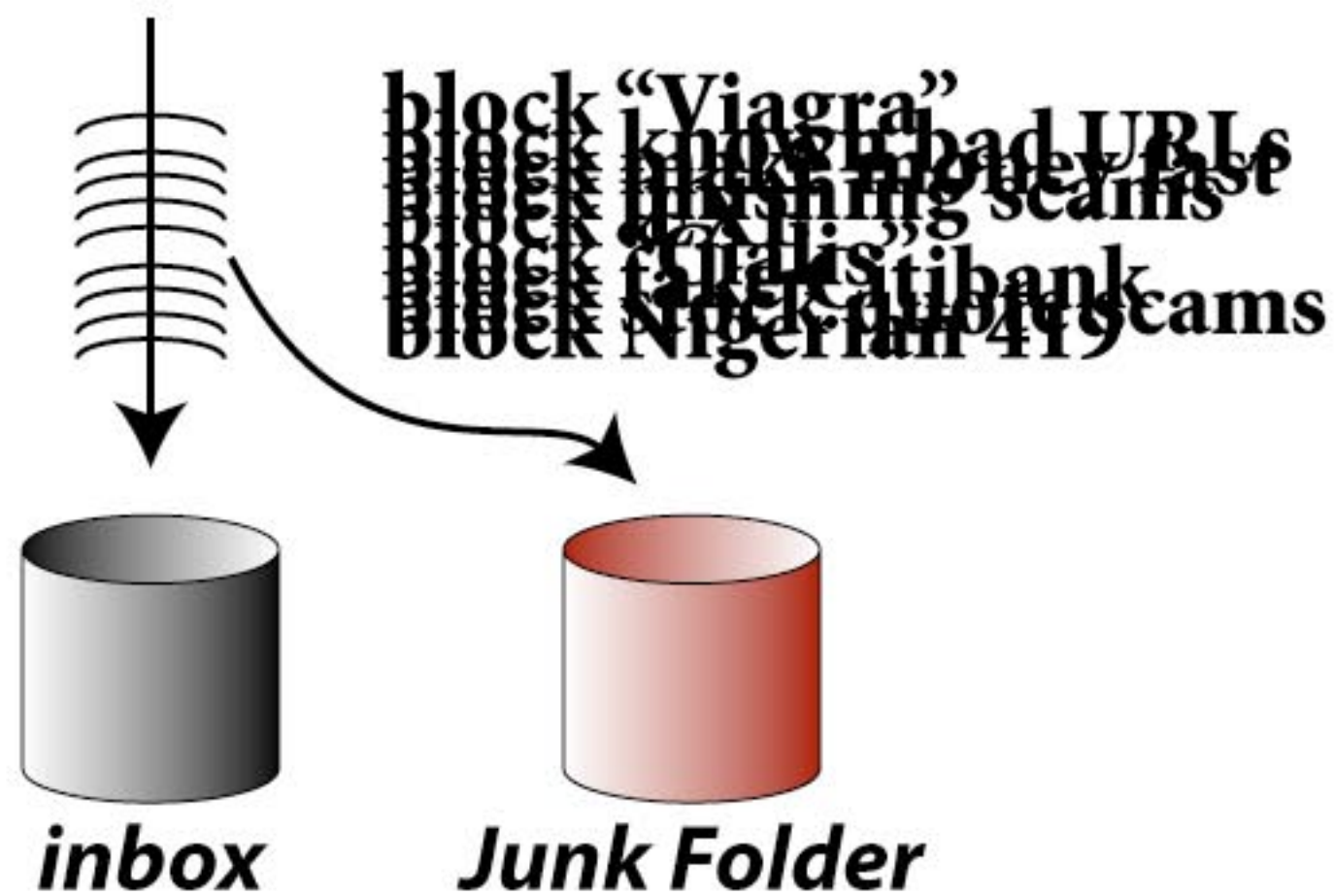
**block "Viagra"**  
**block make money fast**  
**block .EXE**  
**block fake Citibank**  
**block Nigerian 419**

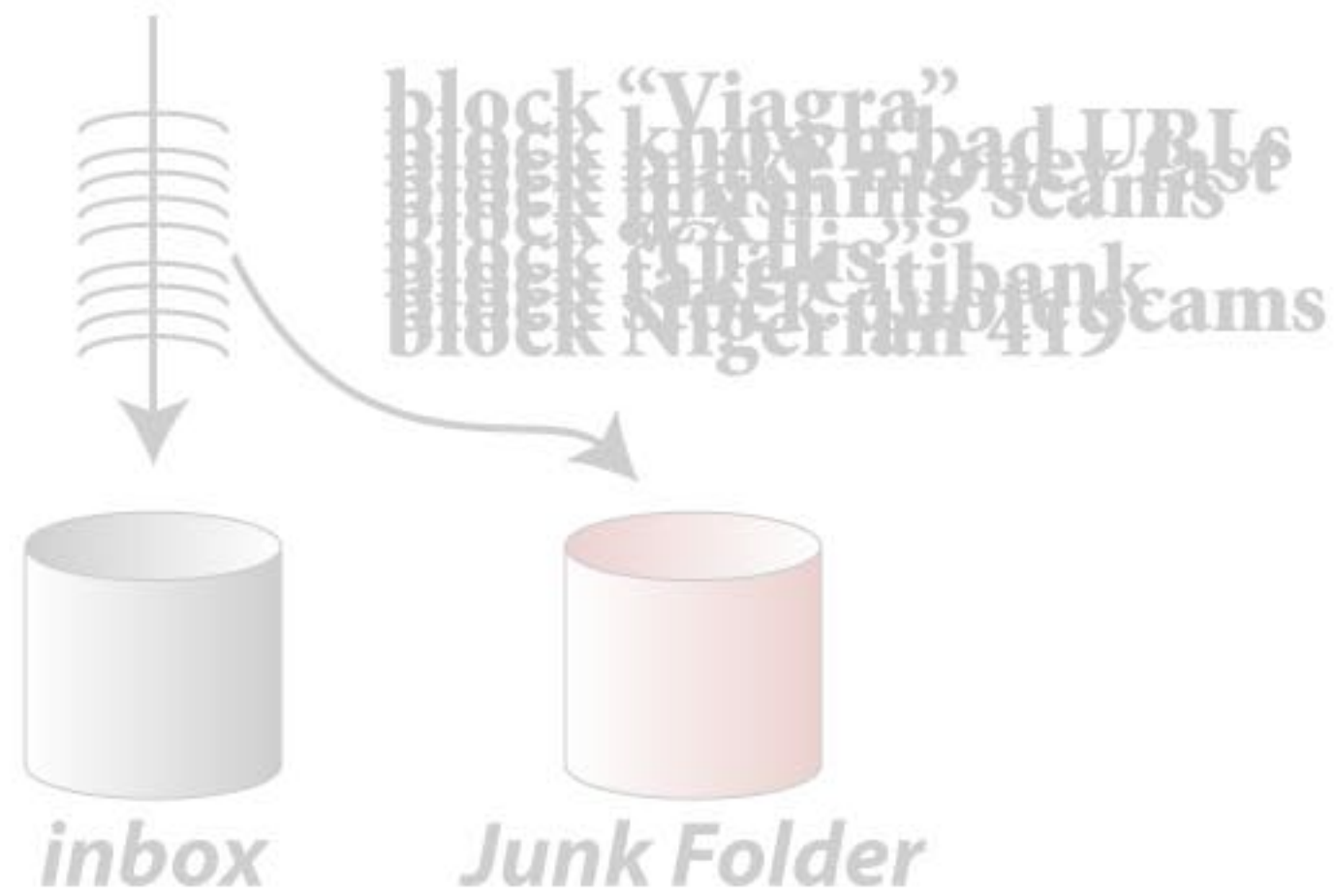
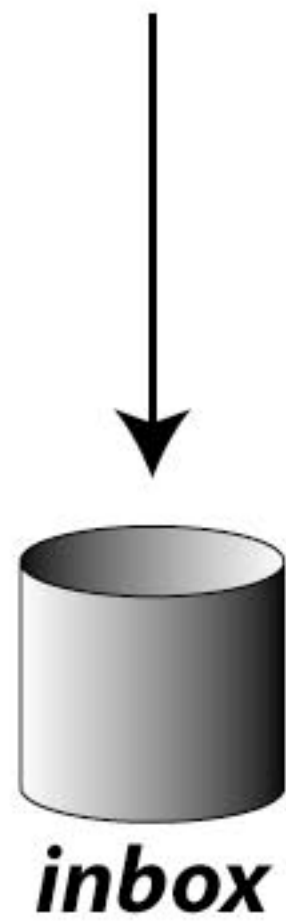
**Accept by default**



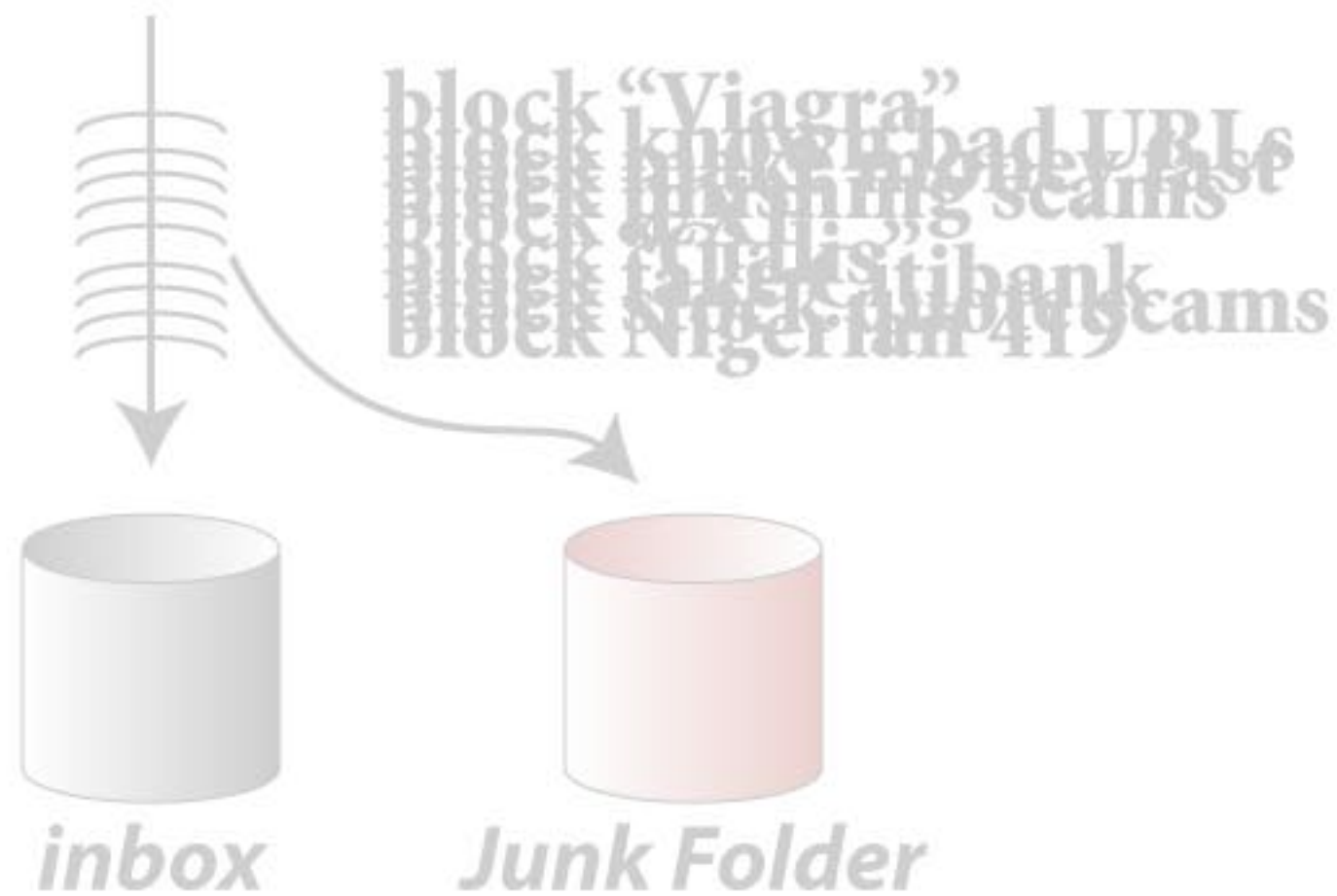
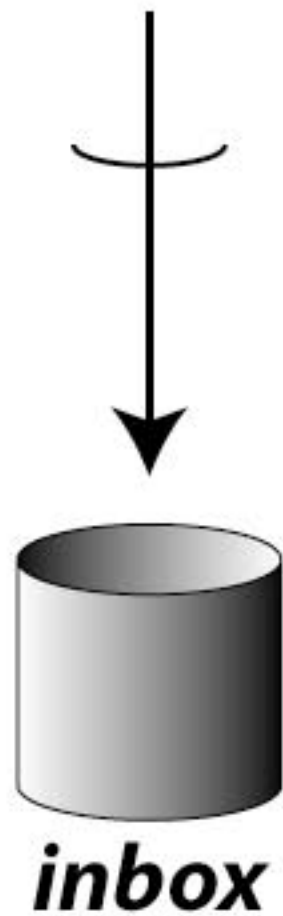
block "Viagra"  
block known bad URLs  
block phishing scams  
block "Gali" scams  
block Citibank  
block Nigerian 419 scams

**Accept by default**

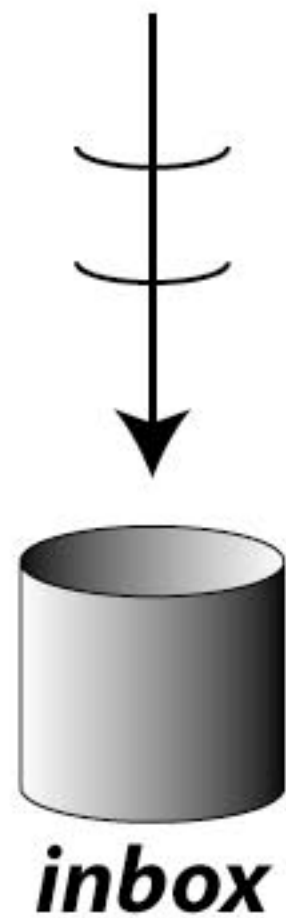




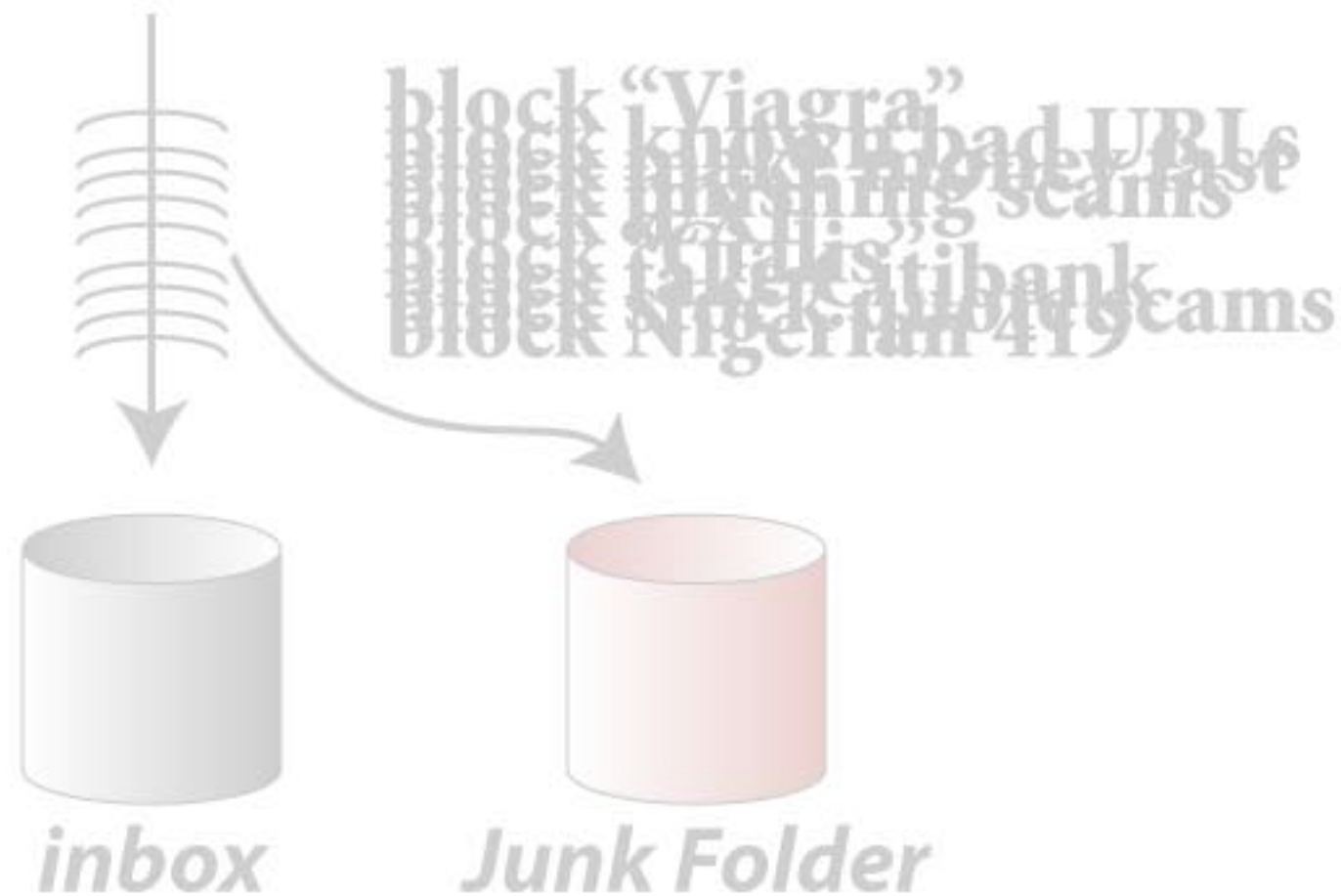
**accept from whitelisted senders**



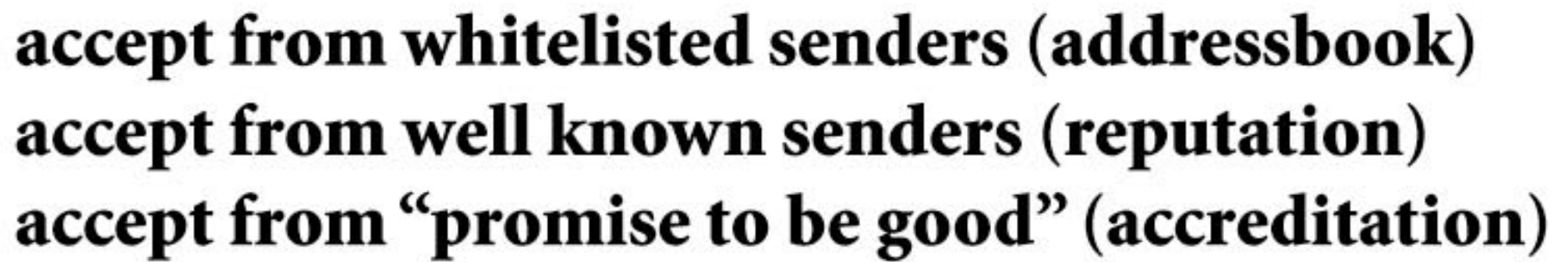




**accept from whitelisted senders (addressbook)**  
**accept from well known senders (reputation)**





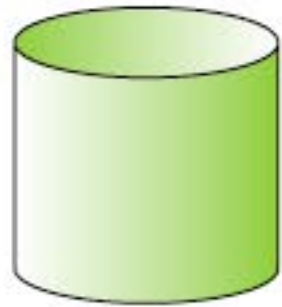


## Reject by default!





**accept from whitelisted senders (addressbook)**  
**accept from well known senders (reputation)**  
**accept from “promise to be good” (accreditation)**



***Spamproof***

**Reject by default!**



block “Viagra”  
block known bad URLs  
block phishing scams  
block “Galleys”  
block Citibank  
block Nigerian 419 scams

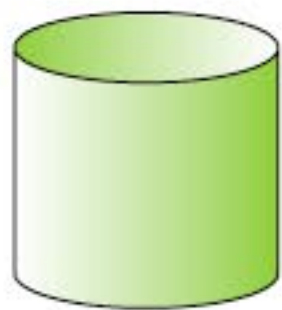


*inbox*



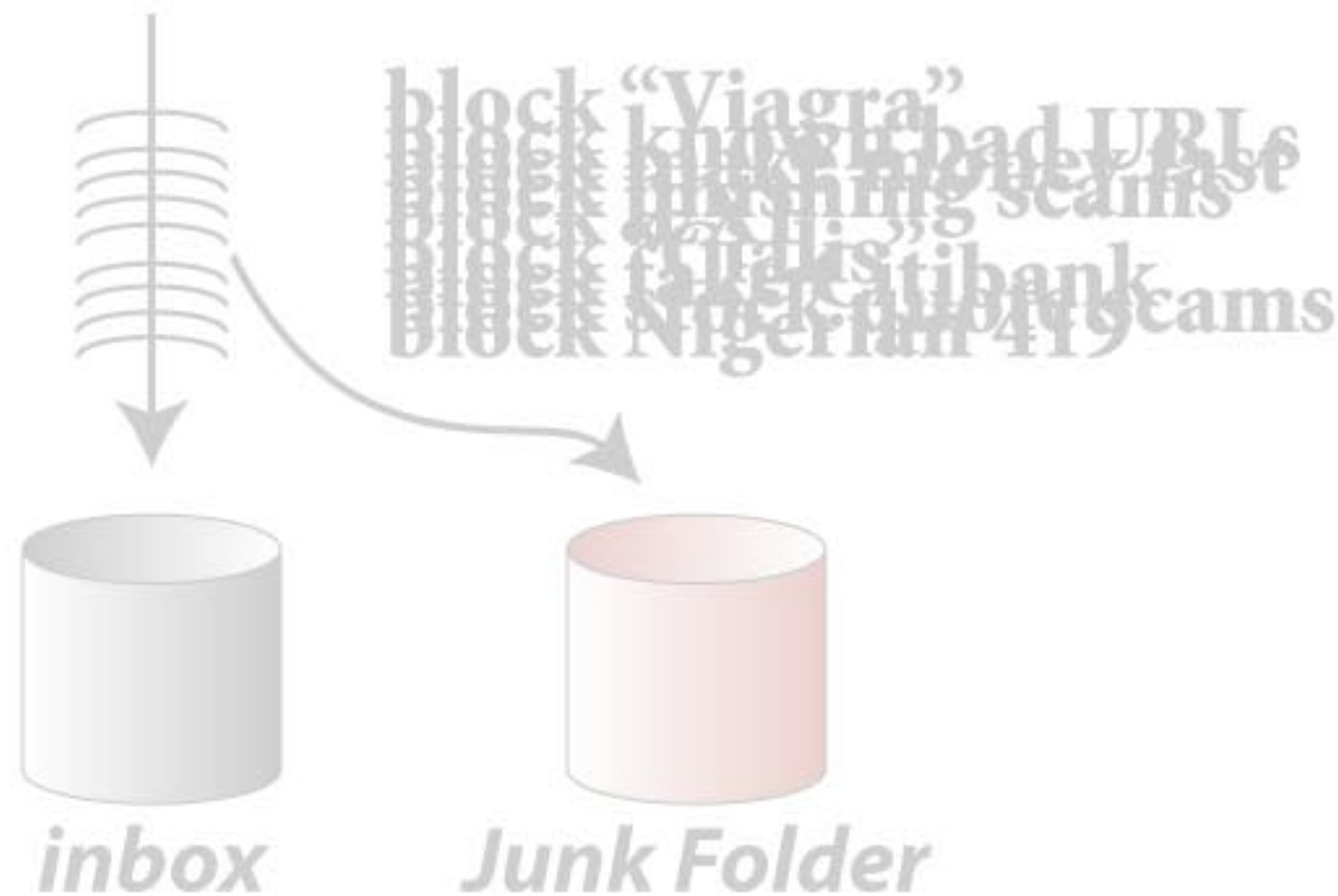
*Junk Folder*

**accept from whitelisted senders (addressbook)**  
**accept from well known senders (reputation)**  
**accept from “promise to be good” (accreditation)**

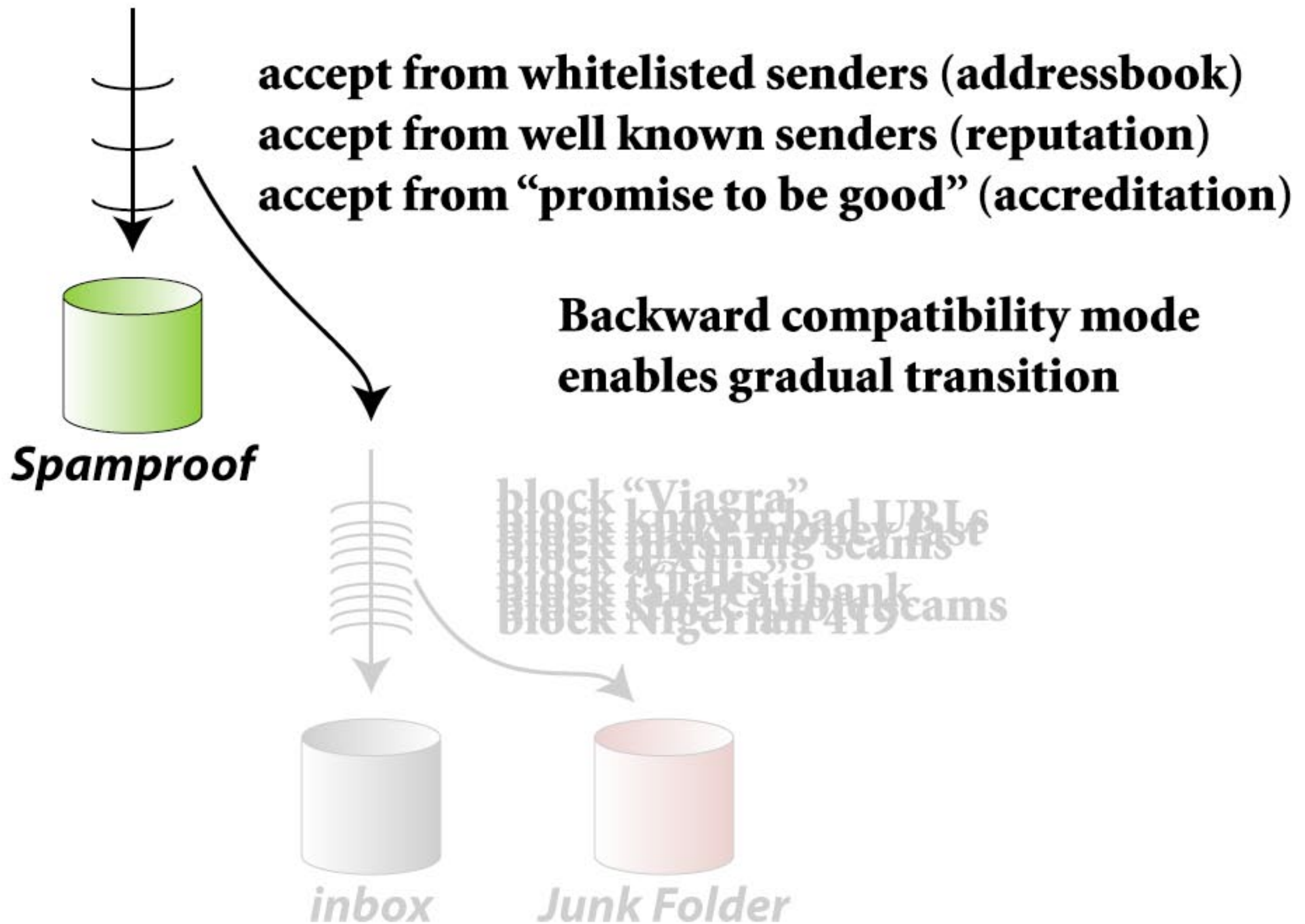


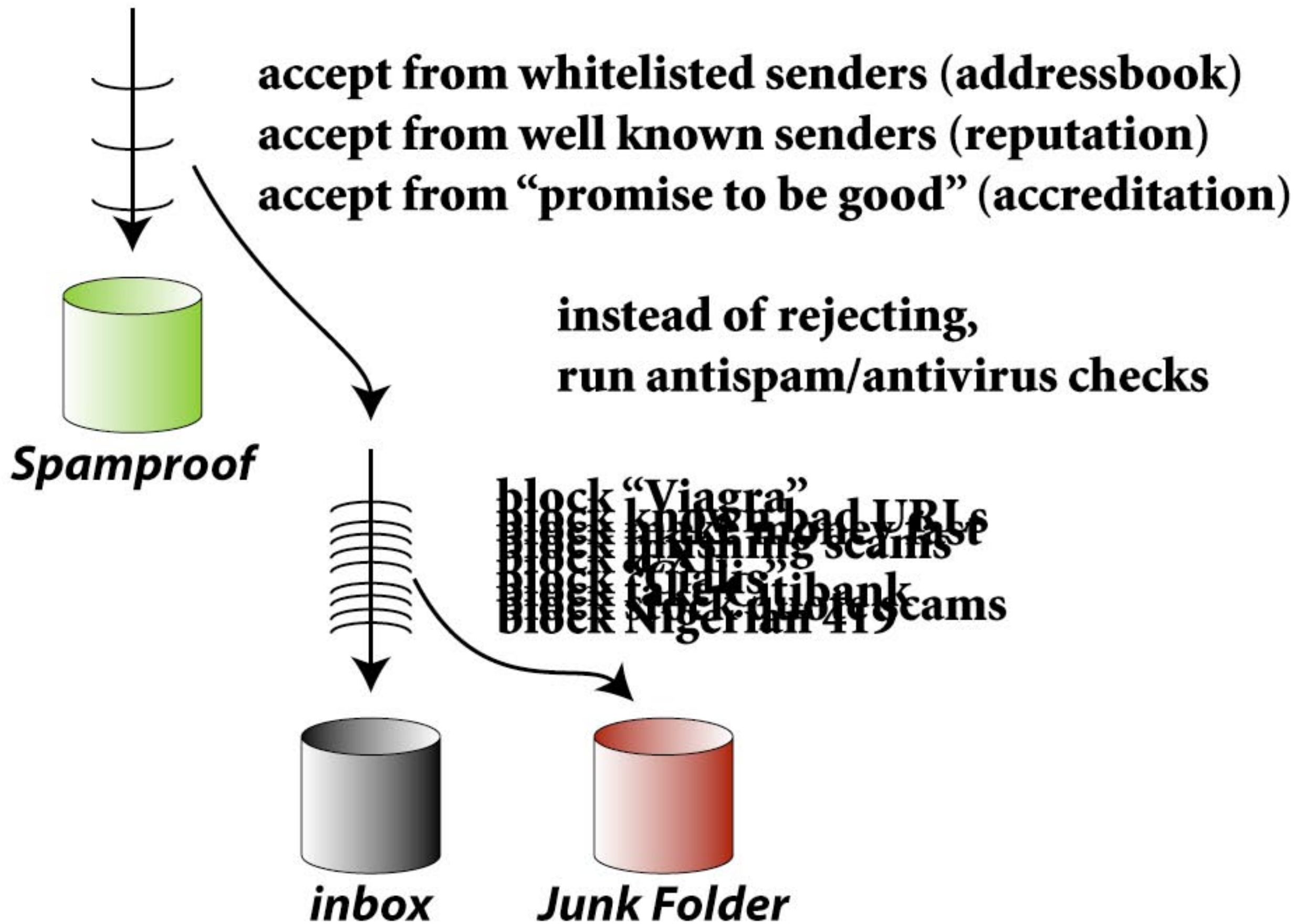
***Spamproof***

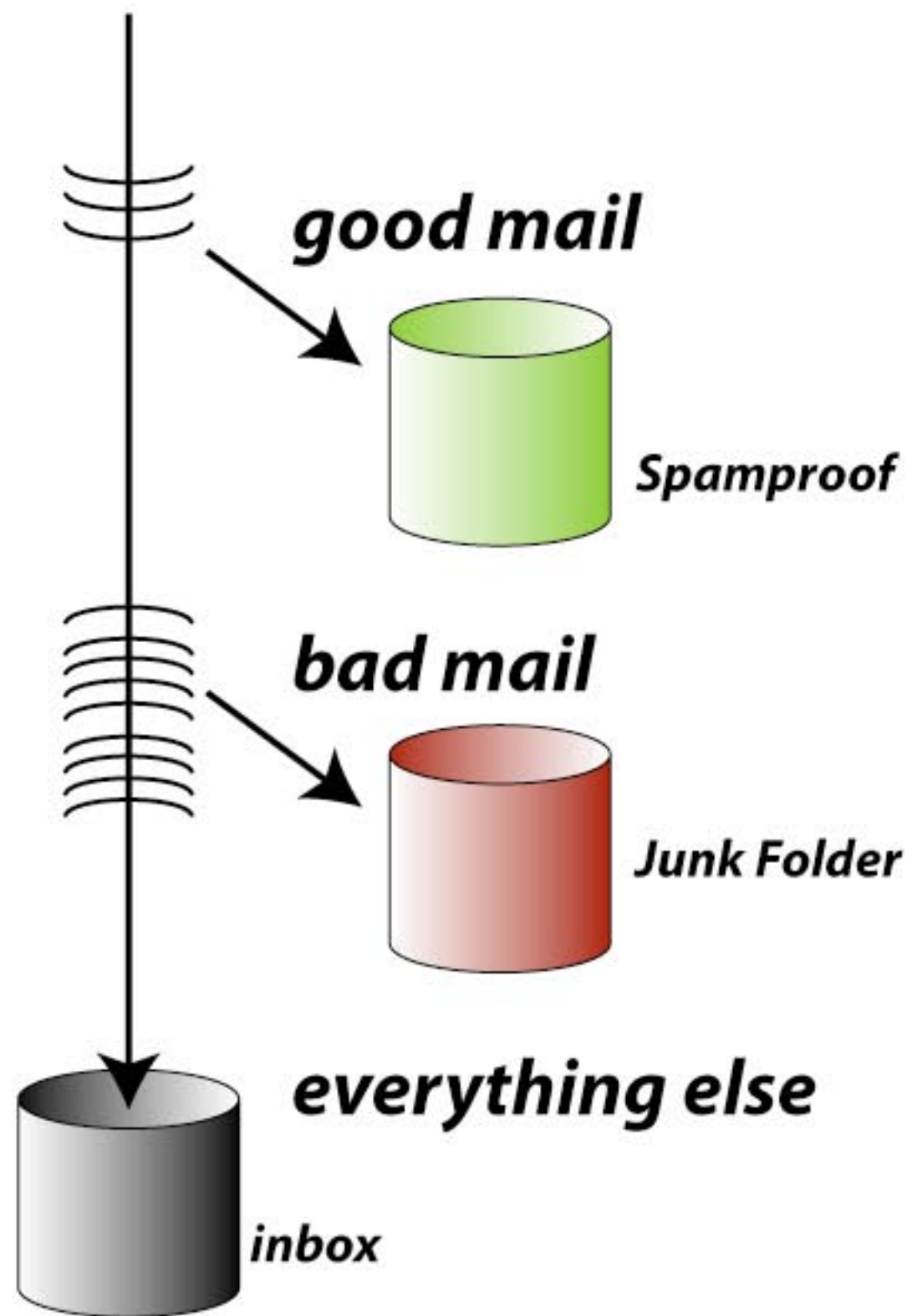
**Backward compatibility mode  
enables gradual transition**



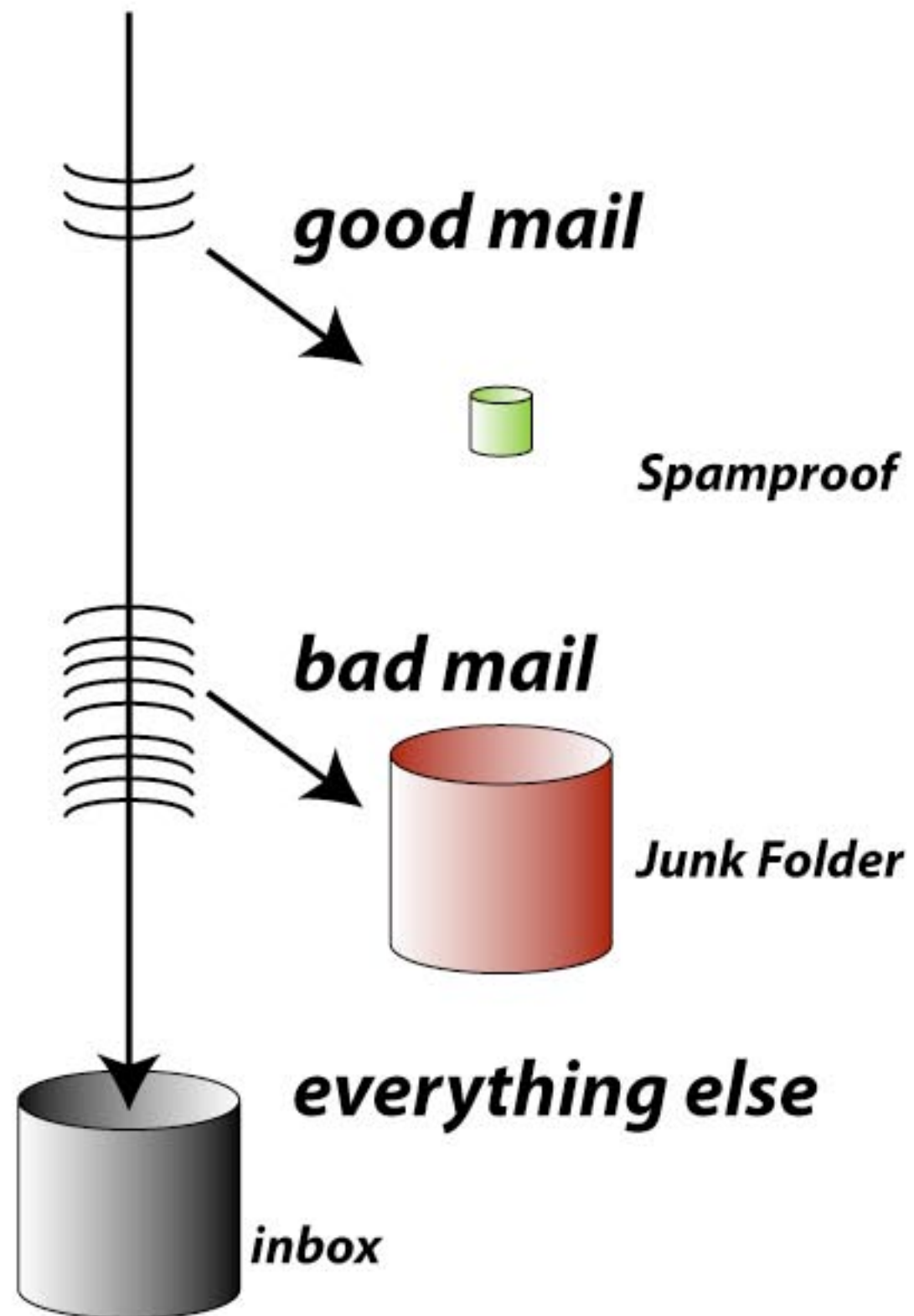




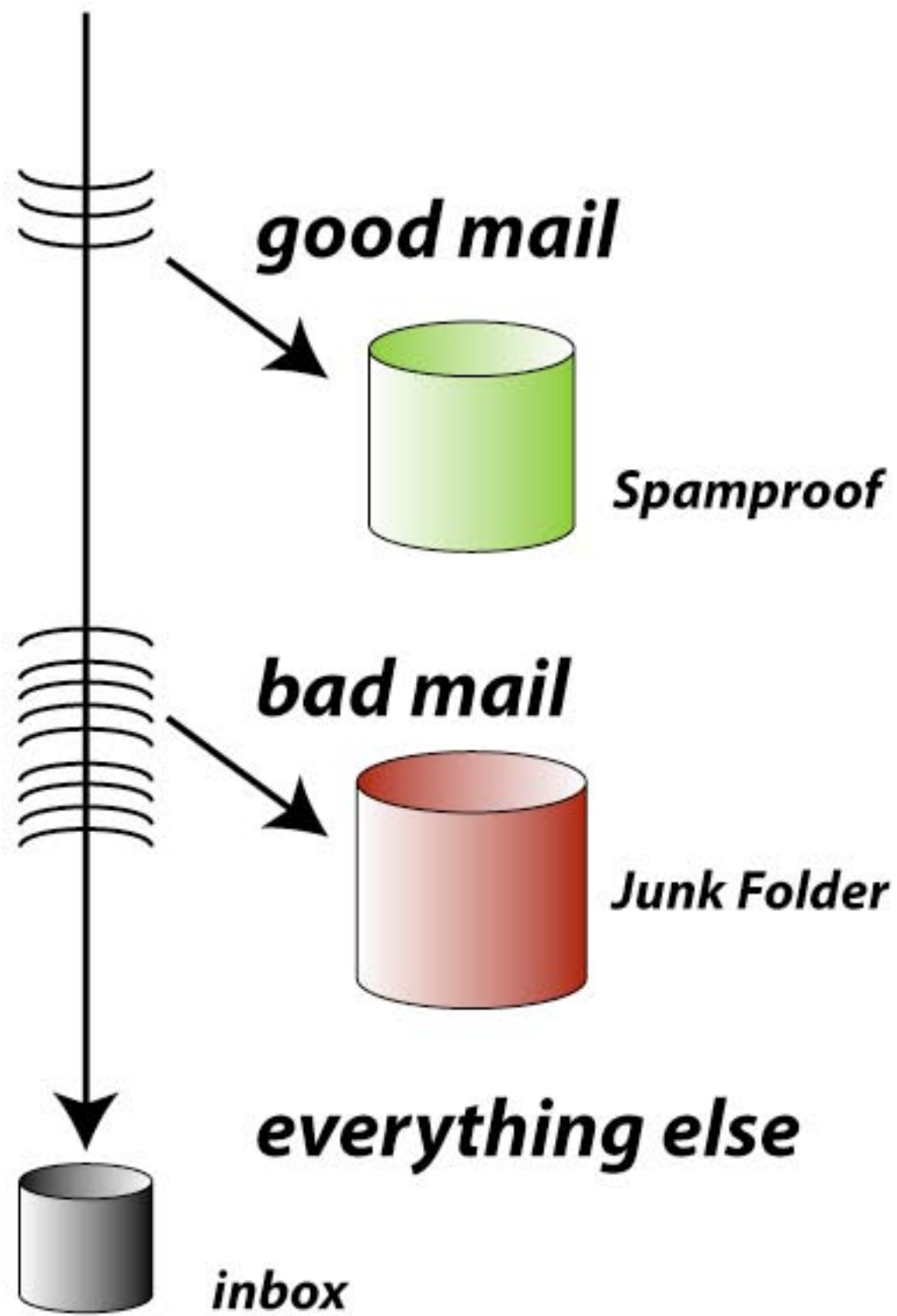




***present day, 2004***

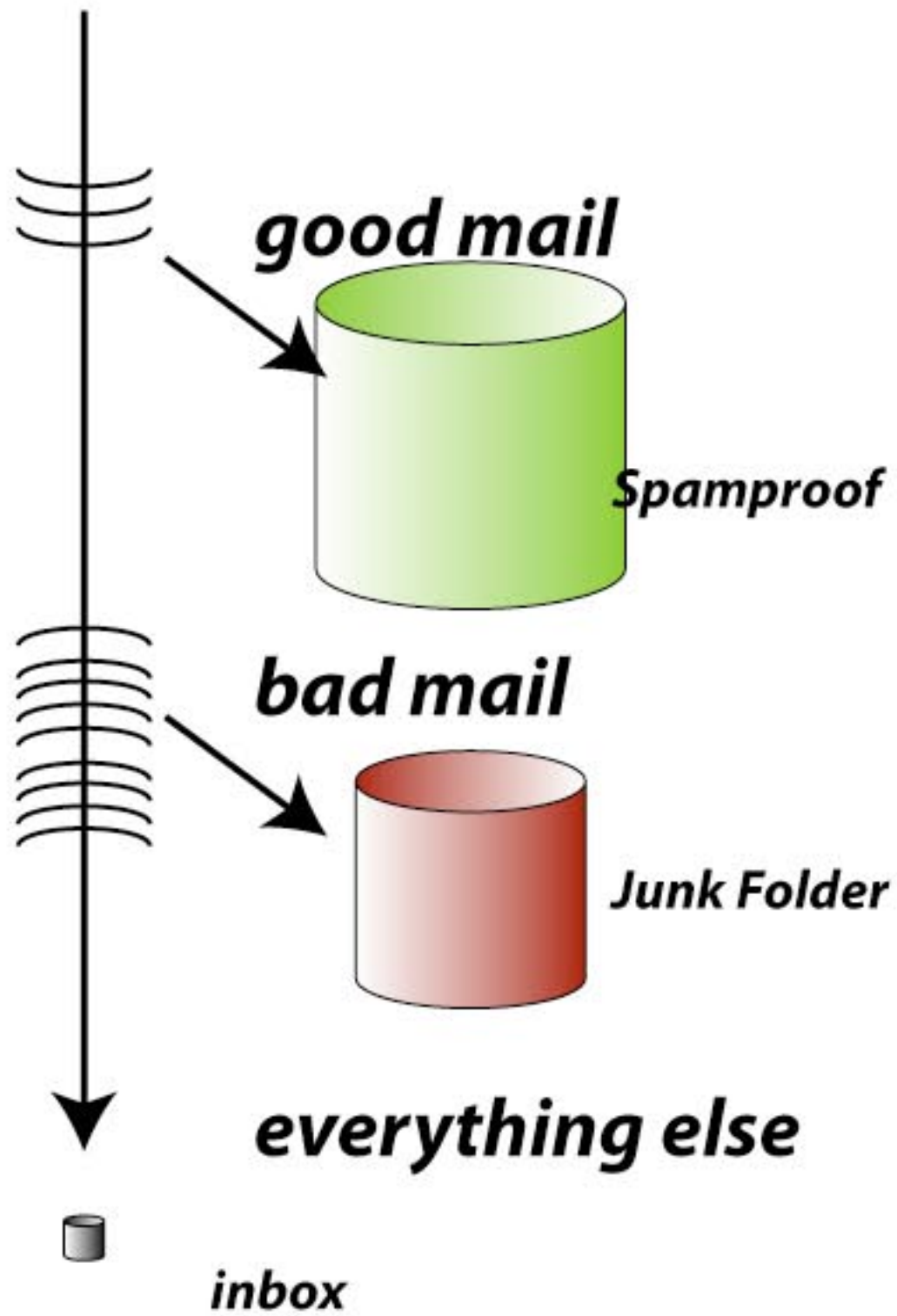


***near future, 2005***

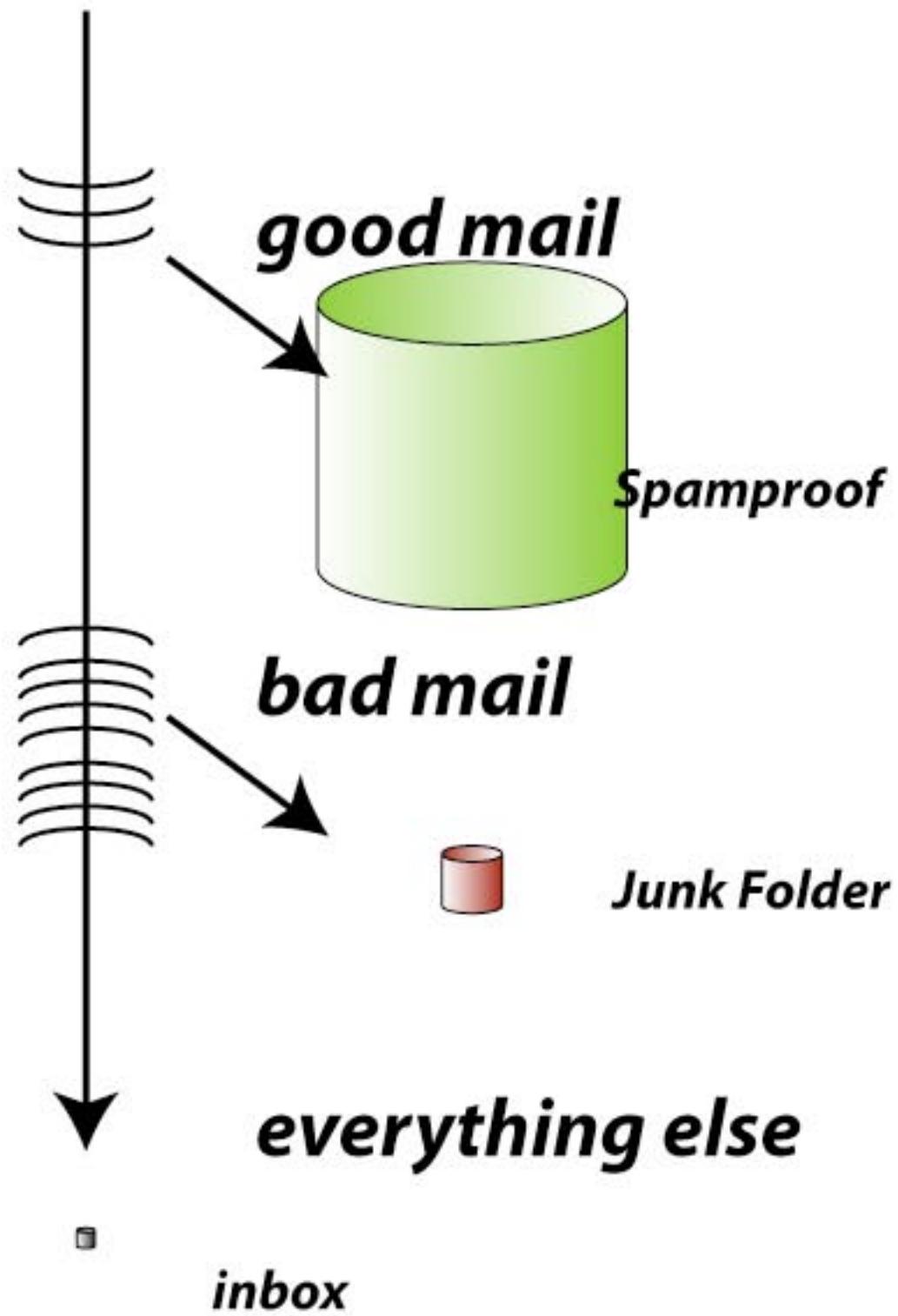




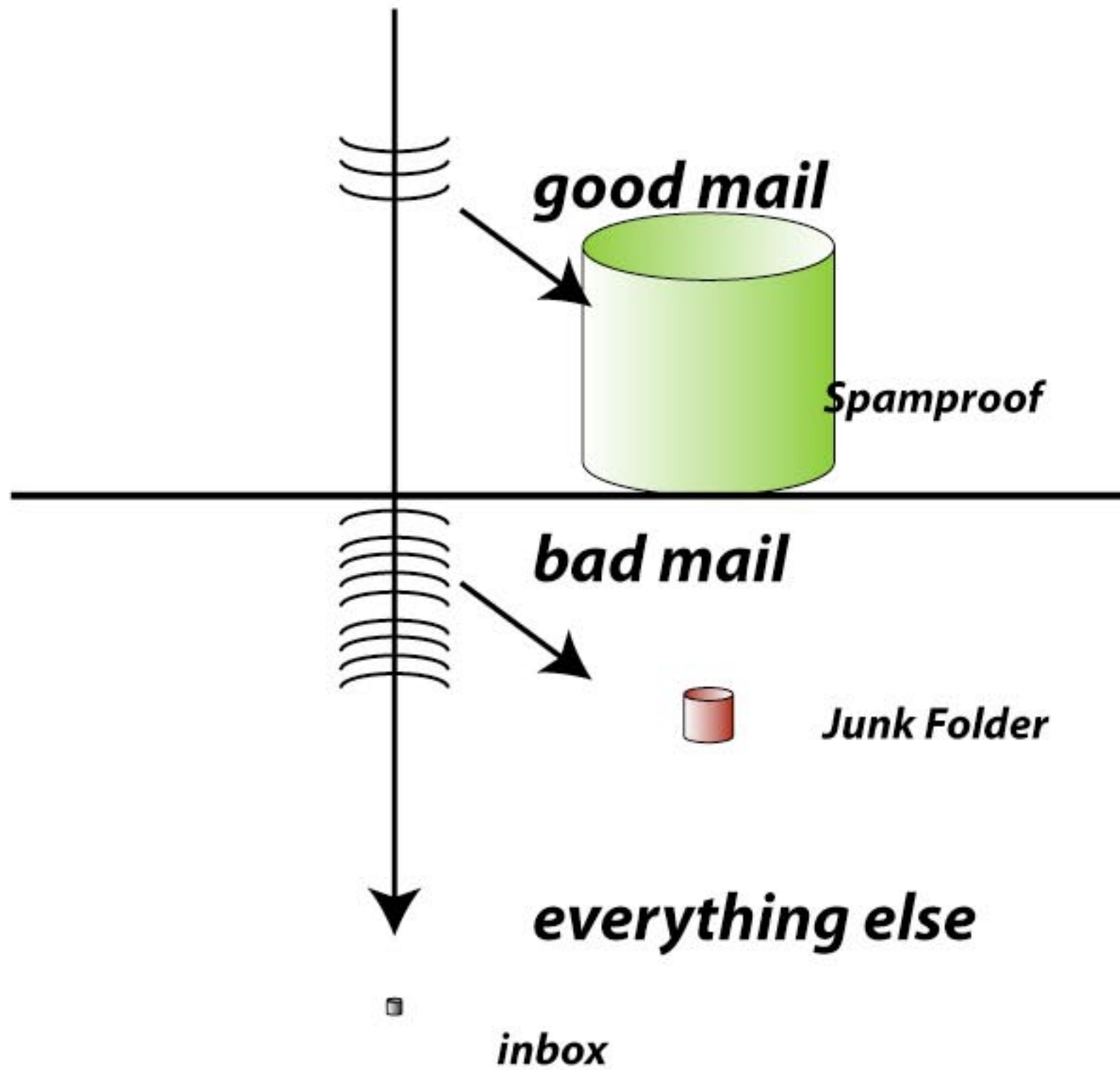
*medium future, 2006*

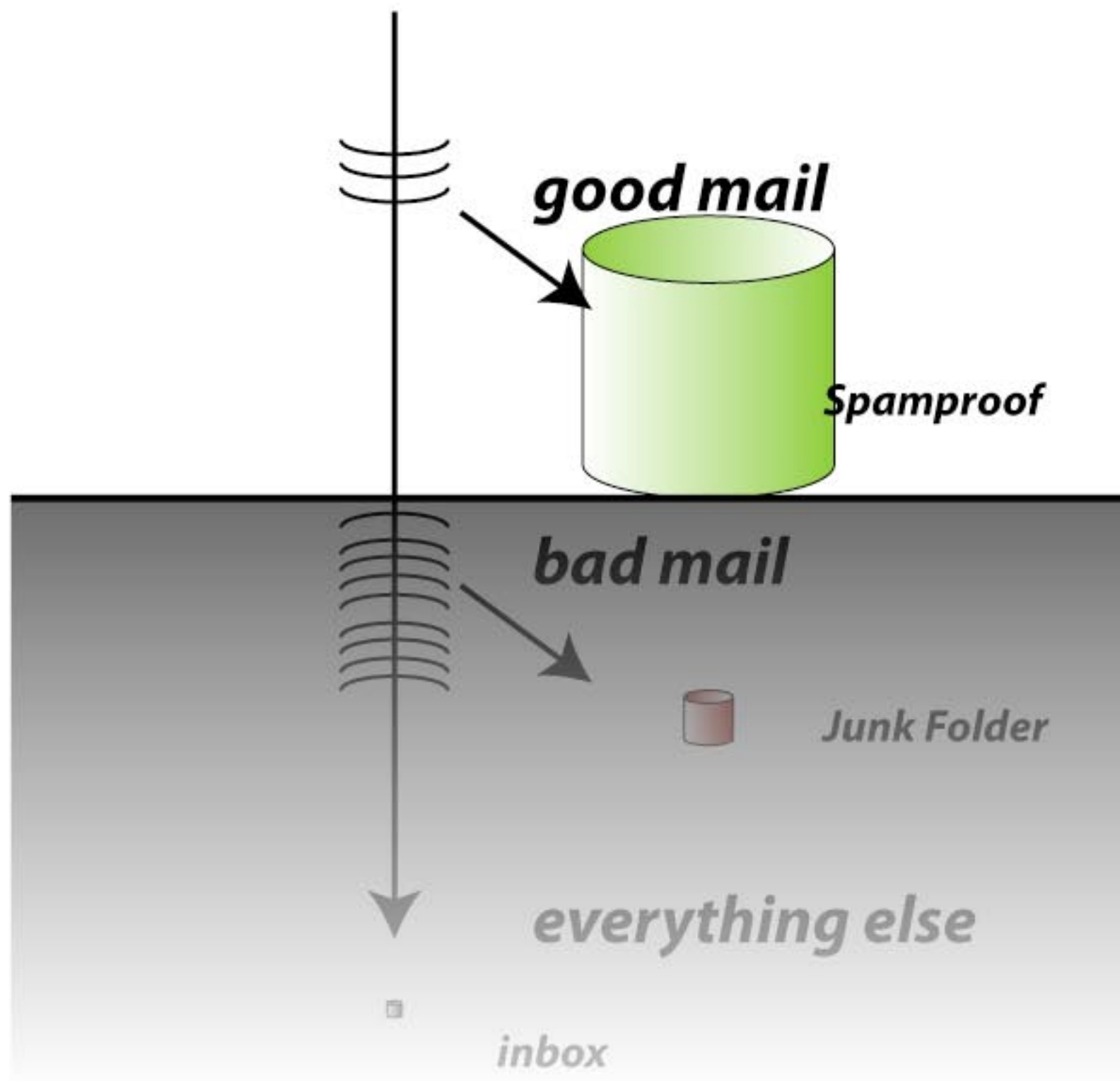


*far future, 2007....*



*far future, 2007....*





***close the Junk Folder  
and the Legacy Inbox***

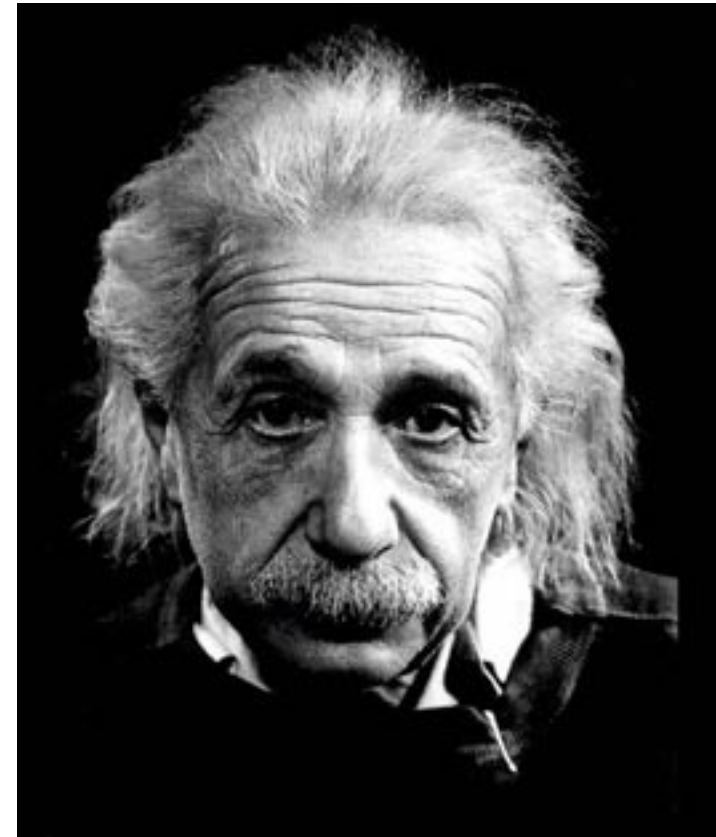
**If you want to stop getting spam, you have to stop accepting mail from strangers.**

**“The significant problems we face cannot be solved at the same level of thinking we were at when we created them.”**

**If you try to solve spam, you end up with things like content filtering and quarantine folders.**

**Spam is a phase to be outgrown.**

**Change people’s expectations. They are ready.**



# Reversals from the Paradigm Shift

*The opposite of every great idea is another great idea. –Niels Bohr*

mengwong@pobox.com 20040920

In the 21st century, if a message is not from an accountable sender, it should expect to be rejected.  
Senders must be authenticated. Senders must also be known, reputable, or accredited.

## 20th century email

*The average message is good. Spam is the exception.*

*By default, accept a message unless we have a good reason to reject it.*

*Spammers evolve. The list of reasons to reject a message keeps growing.*

*Filter out spam based on content.*

*File suspected spam to a spam folder.*

*Spamfolders reduce reliability. Senders have to ask "did you get my mail?"*

*The biggest challenge in solving spam is reducing false positives.*

*End-users can send mail through any SMTP server, as anyone.*

*Expectation: strangers can email each other totally out of the blue.*

*Corporations, particularly sales accounts, are very sensitive to FPs, so the "default accept" paradigm will never go away entirely.*

## 21st century email

- 1 *The average message is spam. Ham is the exception.*
- 2 *By default, reject a message unless we have a good reason to accept it.*
- 3 *Good senders are relatively static. The list of reasons to accept a message stays short.*
- 4 *Filter in ham based on sender.*
- 5 *There is no spam folder.*
- 6 *If a message is accepted, senders can be confident it will be read.*
- 7 *If we can solve false positives perfectly, spam is solved as a side effect.*
- 8 *End-users have to phone home using 587 AUTH and send mail as themselves.*
- 9 *Expectation: strangers need to be generally reputable or else be introduced.*
- 10 *Humans, particularly children, are much more sensitive to false negatives, so "default reject" will eventually become dominant.*

The two paradigms will coexist for quite some time.

Mail that passes the 21st century challenge may end up in a "first-class" folder, giving it attention priority from the end-user.

Mail that does not meet 21st century criteria will be subject to the gauntlet of 20th century antispam techniques, and runs a greater risk of being filed (by mistake) to the spamfolder.

## **The two basic questions**

- 1) Do I recognize you? (Hi, Mom!)**
- 2) Are you really who you say you are?  
(Hey, you're not actually my mother.)**

## **The two basic questions**

- 1) Do I recognize you? (Hi, Mom!)**
- 2) Are you really who you say you are?**  
**(Hey, you're not actually my mother.)**

**“Are you a stranger?”**





## **The two basic questions**

- 1) Do I recognize you? (Hi, Mom!)**
- 2) Are you really who you say you are?  
(Hey, you're not actually my mother.)**

**“Are you a stranger?”**

- actually a very fine-grained question**
- have I sent mail to you before?**
- are you in my addressbook?**
- are you in my friends' addressbooks?**
- are you in my ISP's whitelist?**
- are you in a global reputation system?  
(e.g. [rating.cloudmark.com](http://rating.cloudmark.com))**
- have you been accredited?  
(e.g. Bonded Sender or Habeas)**

## **The two basic questions**

- 1) Do I recognize you? (Hi, Mom!)**
- 2) Are you really who you say you are?  
(Hey, you're not actually my mother.)**

**“Are you a stranger?”**

- these reduce to the First Contact problem**
- we value getting mail from strangers**
- spammers will pretend to be strangers**
- this is why we haven't solved spam yet**

## The two basic questions

- 1) Do I recognize you? (Hi, Mom!)
- 2) Are you really who you say you are?  
(Hey, you're not actually my mother.)

“Are you a stranger?”

- these reduce to the First Contact problem
- **we** value getting mail from strangers
- spammers will pretend to be strangers
- this is why we haven't solved spam yet

Wait a minute. Who is “we”?

## The two basic questions

- 1) Do I recognize you? (Hi, Mom!)
- 2) Are you really who you say you are?  
(Hey, you're not actually my mother.)

“Are you a stranger?”

- these reduce to the First Contact problem
- **we** value getting mail from strangers
- spammers will pretend to be strangers
- this is why we haven't solved spam yet

Wait a minute. Who is “we”?

- sales account at a corporation,  
worried about false positives

## The two basic questions

- 1) Do I recognize you? (Hi, Mom!)
- 2) Are you really who you say you are?  
(Hey, you're not actually my mother.)

“Are you a stranger?”

- these reduce to the First Contact problem
- **we** value getting mail from strangers
- spammers will pretend to be strangers
- this is why we haven't solved spam yet

Wait a minute. Who is “we”?

- sales account at a corporation,  
worried about false positives
- your 15 year old daughter  
more worried about false negatives

## The two basic questions

- 1) Do I recognize you? (Hi, Mom!)
- 2) Are you really who you say you are?  
(Hey, you're not actually my mother.)

“Are you a stranger?”

- these reduce to the First Contact problem
- **we** value getting mail from strangers
- spammers will **pretend** to be strangers
- this is why we haven't solved spam yet

Wait a minute. Who is “we”?

- sales account at a corporation,  
worried about false positives
- your 15 year old daughter  
more worried about false negatives

We want to make it  
hard for bad guys,  
easy for good guys.

## **The two basic questions**

**1) Do I recognize you? (Hi, Mom!)**

**2) Are you really who you say you are?  
(Hey, you're not actually my mother.)**



**Sender Authentication**



*How can we authenticate senders?*

## **IP-based schemes**

**Is the SMTP client a designated MX?**

*Forwarders need to do SRS.*

*Mailing lists don't have to do anything.*

## **Cryptography**

**Is the signature valid?**

*Forwarders don't have to do anything.*

*Mailing lists need to preserve content integrity.*

*How can we authenticate senders?*

## **IP-based schemes**

**Is the SMTP client a designated MX?**

*Forwarders need to do SRS.  
Mailing lists don't have to do anything.*

## **Cryptography**

**Is the signature valid?**

*Forwarders don't have to do anything.  
Mailing lists need to preserve content integrity.*

*What identity do we authenticate?*

## **Return-Path**

**RFC2821**

*Identity = sender  
Goal: stop joe-jobs  
and reject spam before DATA*

## **Header From:**

**RFC2822**

*Identity = author  
Goal: stop phishing  
and verify user-visible  
authorship information*

*How can we authenticate senders?*

## IP-based schemes

Is the SMTP client a designated MX?

*Forwarders need to do SRS.  
Mailing lists don't have to do anything.*

## Cryptography

Is the signature valid?

*Forwarders don't have to do anything.  
Mailing lists need to preserve content integrity.*

*What identity do we authenticate?*

## Return-Path

RFC2821

*Identity = sender  
Goal: stop joe-jobs  
and reject spam before DATA*

## Header From:

RFC2822

*Identity = author  
Goal: stop phishing  
and verify user-visible  
authorship information*

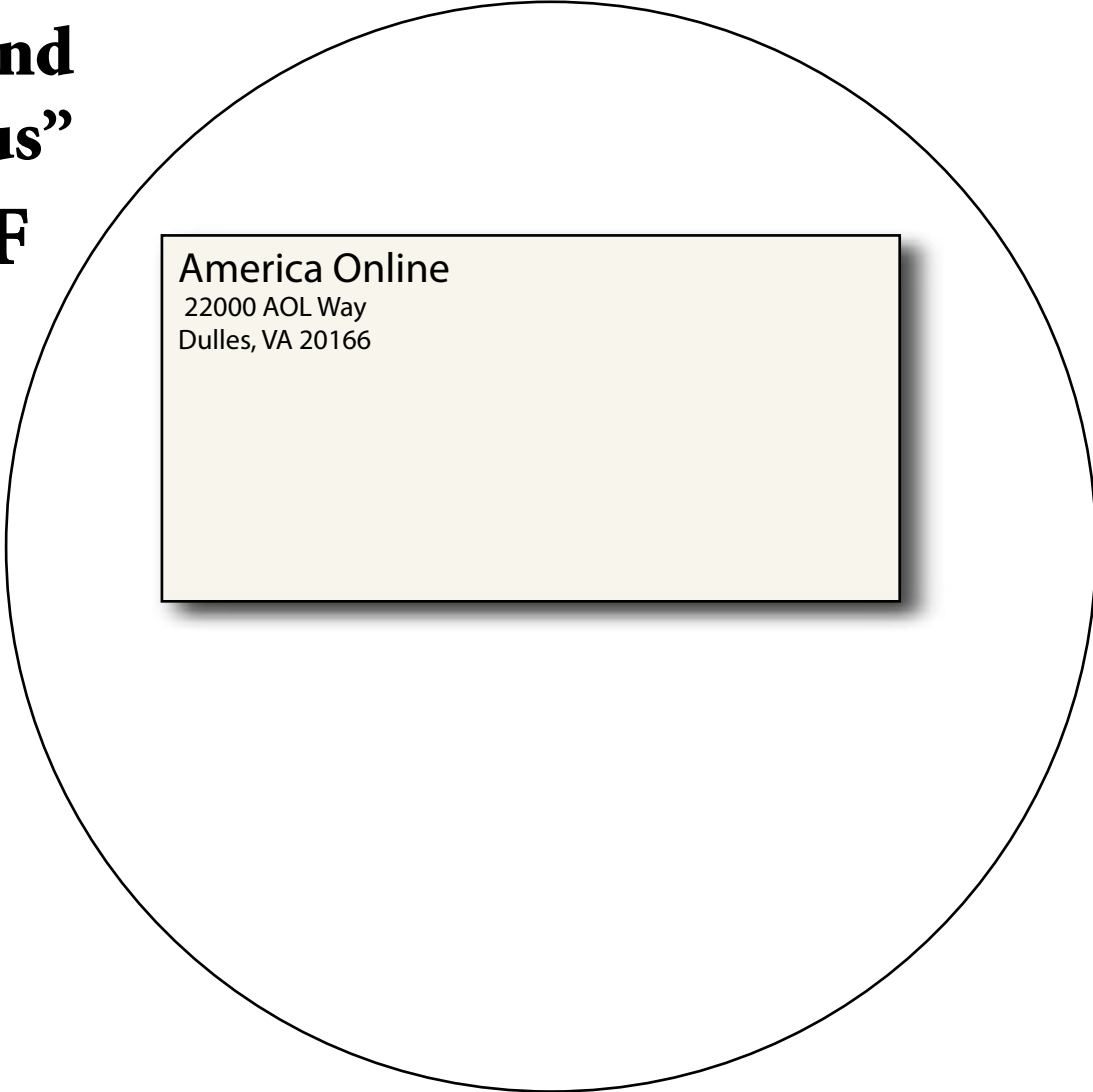
SPF

Sender-ID

DomainKeys, IIM

PGP, S/MIME, etc

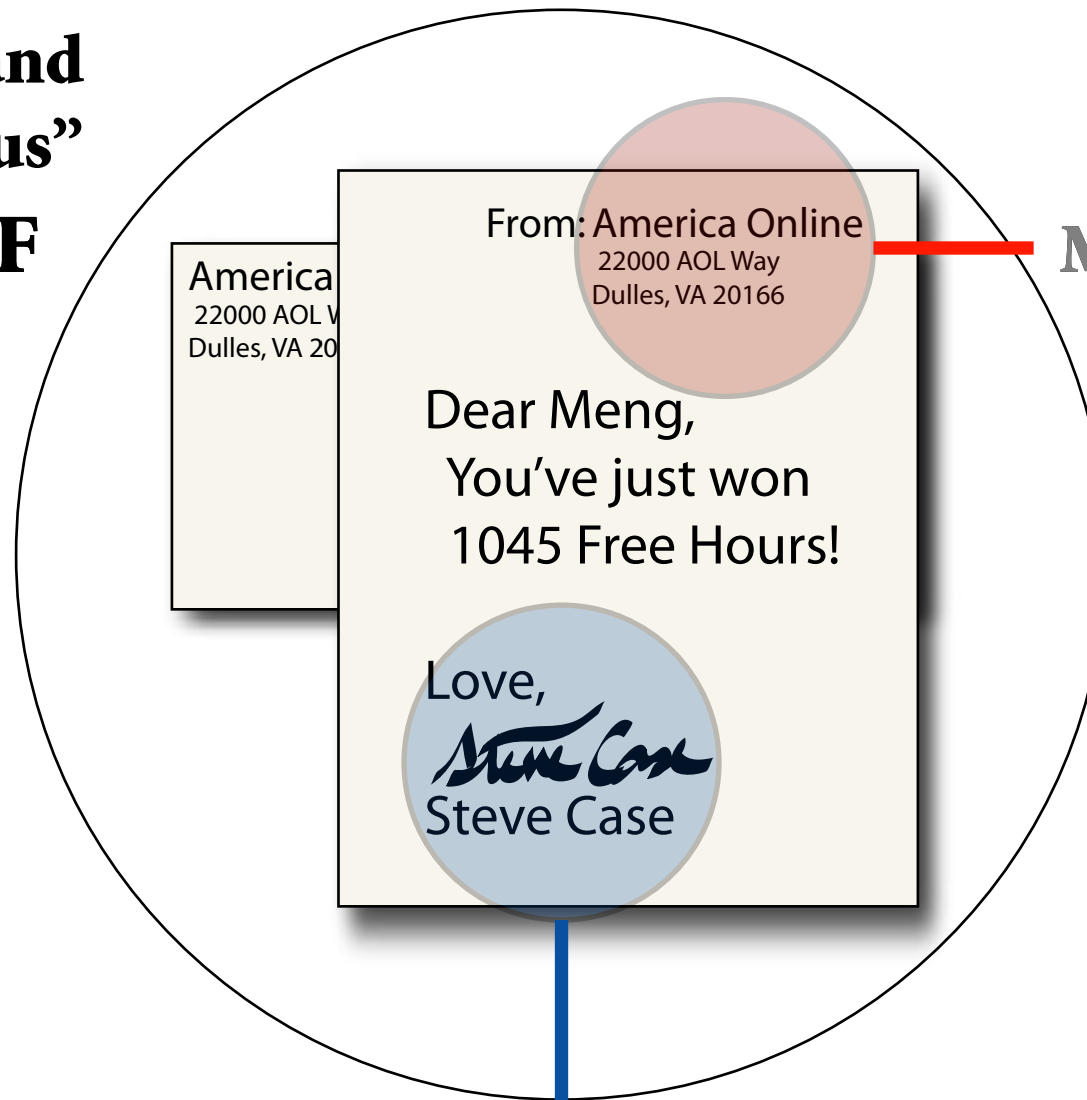
**fights joe-jobs and  
“you sent us a virus”  
SPF**



America Online  
22000 AOL Way  
Dulles, VA 20166

**fights joe-jobs and  
“you sent us a virus”**

**SPF**



**Microsoft  
Caller-ID  
for Email**

**fights phishing scams**

**Cryptographic Schemes**

**Yahoo DomainKeys**

**PGP or S/MIME**

# Sender ID

**fights joe-jobs and  
“you sent us a virus”**

**SPF**

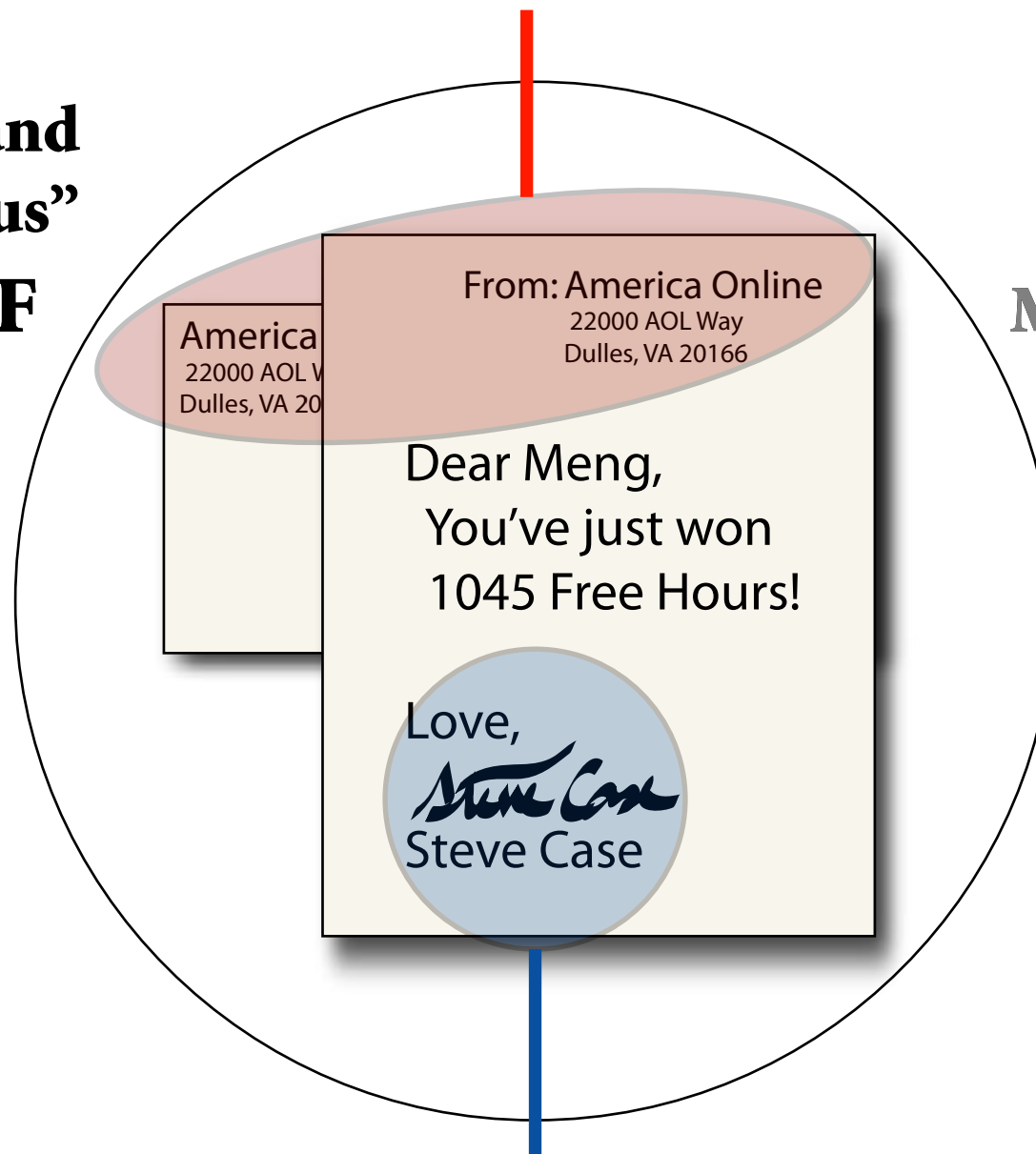
**Microsoft  
Caller-ID  
for Email**

**fights phishing scams**

**Cryptographic Schemes**

**Yahoo DomainKeys**

**PGP or S/MIME**



# Many Identities, Many Proposals...

## MTAMark, Selective Sender

evaluate(client-ip)

## CSV, SPF run against the HELO

spf\_evaluate(client-ip, helo-domain)

## SPF Classic

spf\_evaluate(client-ip, return-path)

## SPF run against the headers = SenderID

spf\_evaluate(client-ip, PRA)

## Yahoo! DomainKeys, Cisco IIM, crypto

evaluate(From header, content)

TCP/IP provides client-ip

HELO mx.example.com

MAIL FROM:<user@example.com>

RCPT TO:<recipient>

DATA

Sender: <user@example.com>

From: <user@example.com>



## **The Internet Engineering Task Force and the MARID Working Group**

- **March 2004, MARID working group formed**
- **Six months of bickering followed**

## **The Internet Engineering Task Force and the MARID Working Group**

- **March 2004, MARID working group formed**
- **Six months of bickering followed**

**“Children, what’s your favourite colour?”**

**– “Blue!”**

**– “Yellow!”**

**– “No, you’re wrong!”**

**– “No, you’re stupid!”**

**also known as “My saliva tastes better than yours”**

## The Internet Engineering Task Force and the MARID Working Group

- March 2004, MARID working group formed
- Six months of bickering followed
- laws are like sausage:  
you don't want to see how they're made



## The Internet Engineering Task Force and the MARID Working Group

- March 2004, MARID working group formed
- Six months of bickering followed
- laws are like sausage:  
you don't want to see how they're made
- the sausage exploded in October
- “No consensus: let the market decide.”



## **Why did MARID fail?**

- **“here are six proposals, let’s choose the best one”**
- **“everybody fight”**
- **“oh, look, there’s no consensus.”**

## Why did MARID fail?

- “here are six proposals, let’s choose the best one”
- “everybody fight”
- “oh, look, there’s no consensus.”

## Project Cheeseplate: learning from MARID’s mistakes

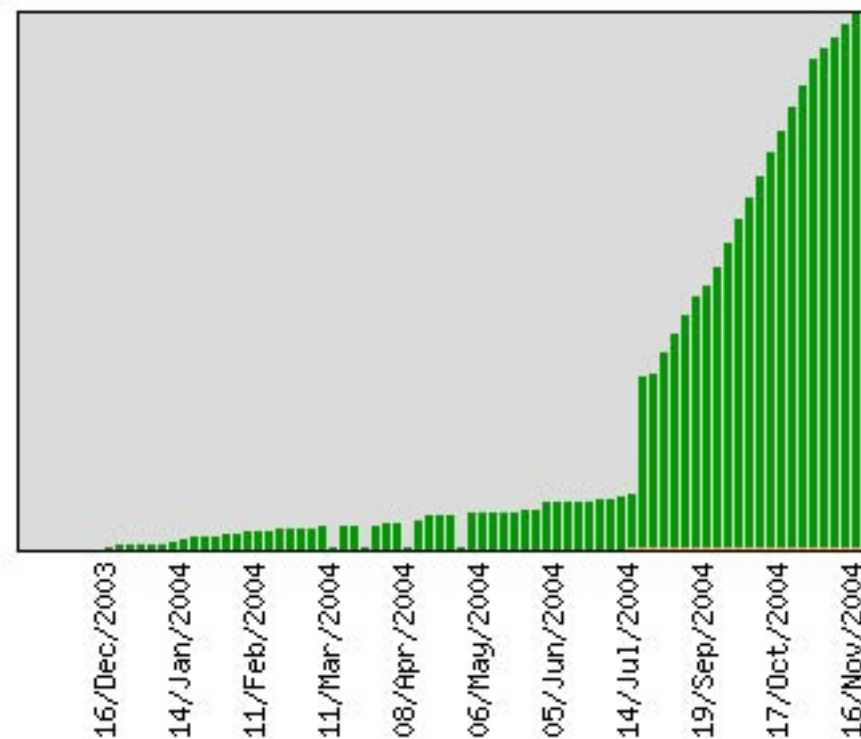
- “here are six proposals, let’s do them all”
- “everybody play nicely together”
- not everybody will like everything
- as long as everybody likes something





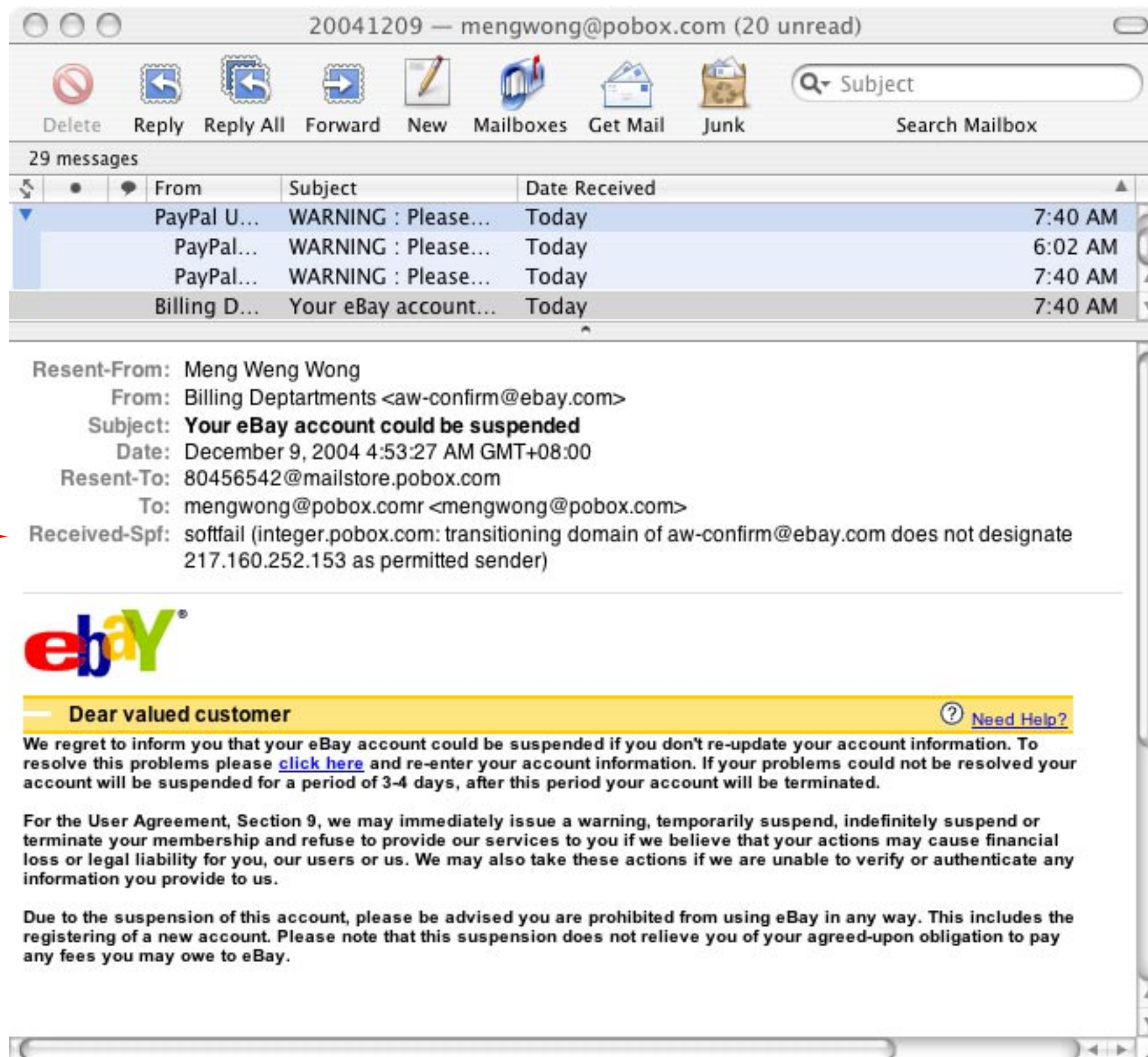
## **Sender Authentication bottom line:**

- **SPF is the most widely adopted technology to date**
- **20% of all internet email is covered by SPF records**
- **most MTA and antispam products can check SPF**
- **Microsoft expected to go live with Sender ID in Hotmail, Outlook, Exchange**
- **Cryptographic solutions still maturing: people want DK and IIM to merge**
- **Members of MAAWG have agreed to publish SPF records by end Q4 2004**
- **MAAWG collectively covers about 250 million mailboxes (<http://www.maawg.org/>)**





This stuff is actually working.



## **Next Steps**

- **everybody publish SPF records today**
- **expect to do other things as well, including crypto**
- **receivers should start using SPF results as part of a spam scoring solution**
- **opensource: upgrade your MTAs or download patches**
- **commercial MTAs: ask your vendor about SPF and other antispam standards**
- **forwarding and hosting providers need to think about SRS and header prepending**
- **whitepaper has specific deployment advice. <http://spf.pobox.com/whitepaper.pdf>**

## **Collaboration and Industry Involvement**

- **APCAUCE in Kyoto 18–25 Feb   <http://www.apricot.net/>**
- **ISPcon and Inbox Event in 2005**
- **ISPs consider joining MAAWG   <http://www.MAAWG.org/>**
- **if you run an opensource MTA, help fund development of Cheeseplate**
- **(SPF project budget to date: US\$3,000)**

## **Collaboration and Industry Involvement**

- **APCAUCE in Kyoto 18–25 Feb** <http://www.apricot.net/>
- **ISPcon and Inbox Event in 2005**
- **ISPs consider joining MAAWG** <http://www.MAAWG.org/>
- **if you run an opensource MTA, help fund development of Cheeseplate**
- **(SPF project budget to date: US\$3,000)**

**THANK YOU!**

<http://spf.pobox.com/>

<http://spf.pobox.com/whitepaper.pdf>

<http://spf.pobox.com/slides/20041210-sg/>

<http://inbox.mengmail.com/>

[mengwong@pobox.com](mailto:mengwong@pobox.com)