

A hacker's perspective on 'confidential' data exchanges via E-mail

AIBL Luncheon
Navixia - Patrick Zwahlen
@navixia - @pzwahlen - paz@navixia.com
November 26th, 2021

E-mails

(1971 – present)

[\[Search\]](#) [\[txt|html|pdf|bibtex\]](#) [\[Tracker\]](#) [\[Email\]](#) [\[Diff1\]](#) [\[Diff2\]](#) [\[Nits\]](#)

Obsoleted by: [221](#)

Unknown

NETWORK WORKING GROUP

Richard W. Watson

Request for Comments #196

SRT-ARC

NIC 7141

July 20, 1971

Categories: A.5, D.7

Obsoletes: none

Updates: none

A MAIL BOX PROTOCOL

The purpose of this protocol is to provide at each site a standard mechanism to receive sequential files for immediate or deferred printing or other uses. The files for deferred printing would probably be stored on intermediate disk files, although details of how a file is handled, stored, manipulated, or printed at a site are not the concern of this protocol.

[\[Search\]](#) [\[txt|html|pdf|bibtex\]](#) [\[Tracker\]](#) [\[Email\]](#) [\[Diff1\]](#) [\[Diff2\]](#) [\[Nits\]](#)

Obsoleted by: [221](#)

Unknown

NETWORK WORKING GROUP
Request for Comments #196
NIC 7141
Categories: A.5, D.7
Obsoletes: none
Updates: none

Richard W. Watson
SRT-ARC
July 20, 1971

A MAIL

November 1981

The purpose of this protocol is to provide a standard mechanism to receive deferred printing or other information that would probably be stored on a remote site. Details of how a file is handled at a site are not the concern of this protocol.

Information Sciences Institute
University of Southern California
4676 Admiralty Way
Marina del Rey, California 90291

(213) 822-1511

[RFC 788](#)

**November 1981
Simple Mail Transfer Protocol**


An e-mail is a postcard...




... in an envelope



Senders and recipients

-  There are two senders
 - The one on the envelope
 - The one on the postcard

-  And two recipients
 - The one on the envelope
 - The one on the postcard

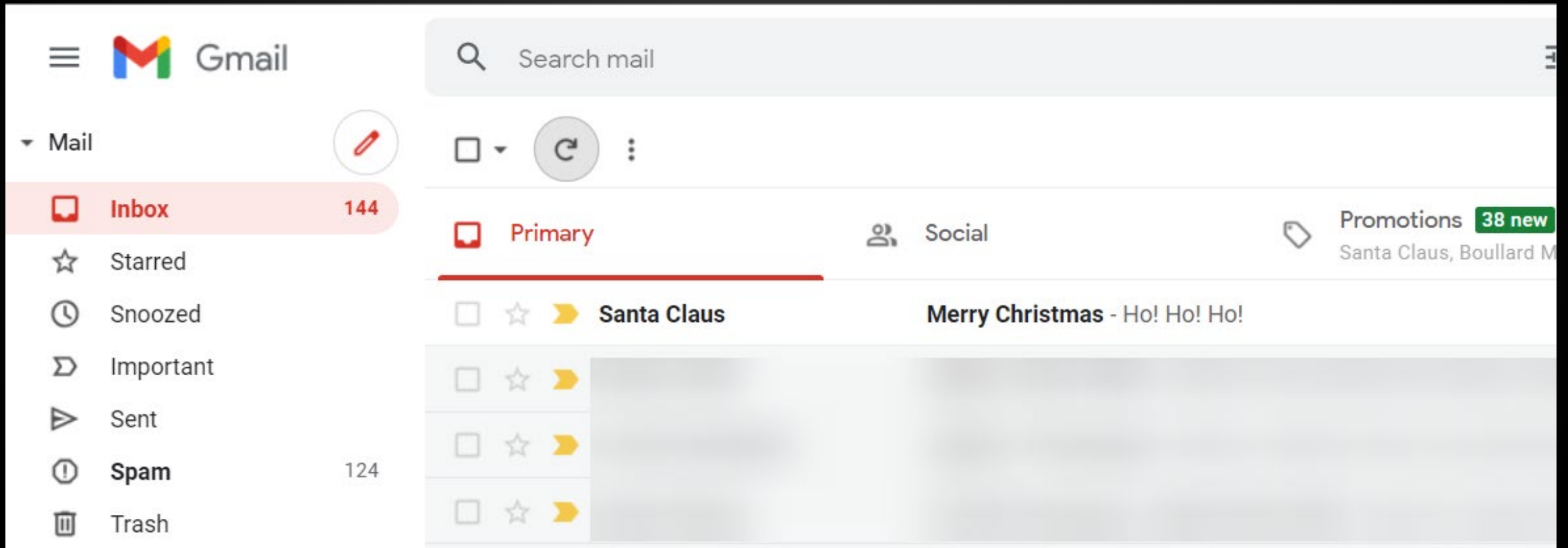
Mail impersonation demo

```
[nsp@dmz74 ~]$ █
```


Mail impersonation demo

```
250 mx74.lesz.ch
mail from: <evil@hacker.org>
250 2.1.0 Ok
rcpt to: <patrick.zwahlen@gmail.com>
250 2.1.5 Ok
data
354 End data with <CR><LF>.<CR><LF>
From: Santa Claus <santa@north.org>
Subject: Merry Christmas

Ho! Ho! Ho!
.
250 2.0.0 Ok: queued as EAB21C00D43
```



The screenshot shows the Gmail interface. At the top left, there is a menu icon, the Gmail logo, and the word "Gmail". Below this is a "Mail" section with a dropdown arrow and a red pencil icon. The "Inbox" is highlighted in red and shows 144 messages. Other folders include "Starred", " Snoozed", " Important", " Sent", " Spam" (with 124 messages), and " Trash". On the right side, there is a search bar labeled "Search mail". Below the search bar are icons for a dropdown menu, a refresh button, and a vertical ellipsis. The main content area shows the "Primary" tab selected, with "Social" and "Promotions" (38 new) also visible. A red horizontal line is under the "Primary" tab. The first email in the list is from "Santa Claus" with the subject "Merry Christmas - Ho! Ho! Ho!". Below it are three more email entries, which are blurred.

alice@alice.com





bob@bob.com

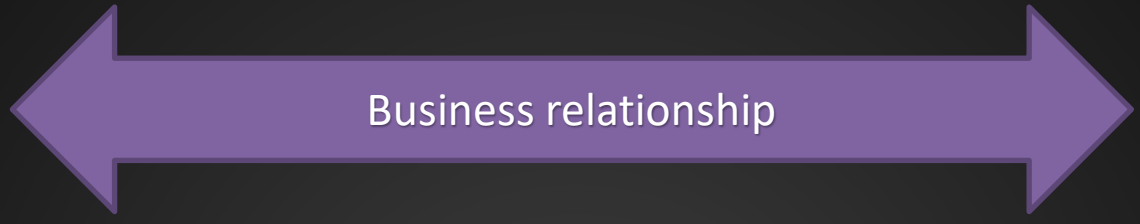


charlie

Legacy problems

-  Alice will receive SPAM
 - No solution!
-  Alice will receive external emails coming from @alice.com
 - The root cause for impersonation scams
 - Solution: disable spoofing & add banner for external e-mails

alice@alice.com



Business relationship



bob@bob.com



charlie

alice@alice.com



bob@bob.com



From: alice@alice.com
To: bob@bob.com



charlie

alice@alice.com

bob@bob.com



From: alice@alice.com
To: bob@bob.com



charlie

Solutions

Sender authentication

- **SPF**: Sender Policy Framework
 - Which server can send e-mails as @alice.com
- **DKIM**: Domain Key Identified E-mail
 - Cryptographic signature of the sender's domain

Policy decision

- **DMARC**: Domain-based Message Authentication, Reporting & Conformance
 - What to do if SPF and/or DKIM fail

New kid on the block

- **ARC**: Authenticated Received Chain

alice@alice.com



bob@bob.com








From: alice@a1ice.com
To: bob@bob.com

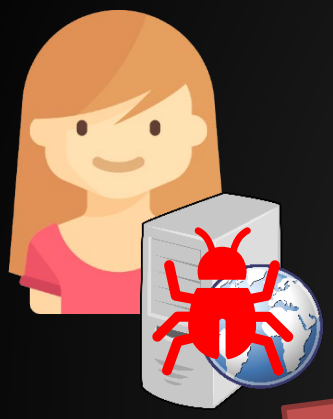


charlie

Look-alike domains

-  It is regular SPAM again!
-  No silver-bullet solution
-  Train users
-  Add a banner to e-mails coming from the outside
-  Machine-learning might help at some point

alice@alice.com

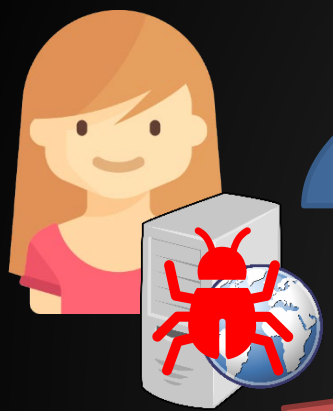


bob@bob.com



charlie

alice@alice.com







From: alice@alice.com
To: bob@bob.com

bob@bob.com



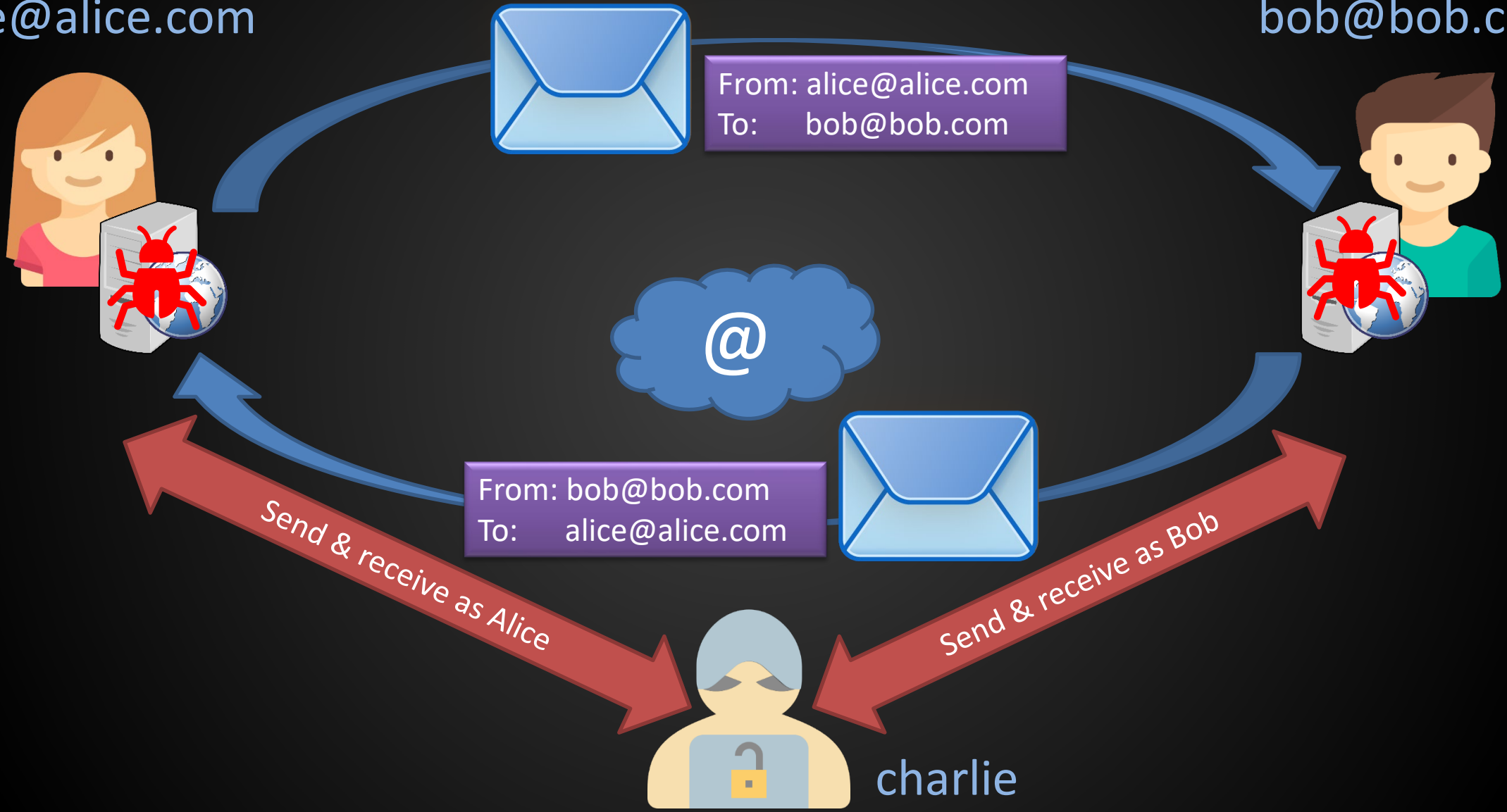
charlie

Compromised e-mail server






-  Charlie can observe the e-mails flow
-  Charlie can send “legitimate” e-mails as “Alice”
-  SPF, DKIM & DMARC are useless
-  Bob cannot technically detect the issue

alice@alice.com

bob@bob.com



Take aways

-  E-mail was never designed for today's use cases
-  E-mail is hard to authenticate and therefore, non-repudiation is hard too
-  E-mail encryption is still not a thing
-  Your messaging service is critical and must be highly protected (even in the cloud)
-  Your strongest password should be the one protecting your e-mails

THANK YOU !

