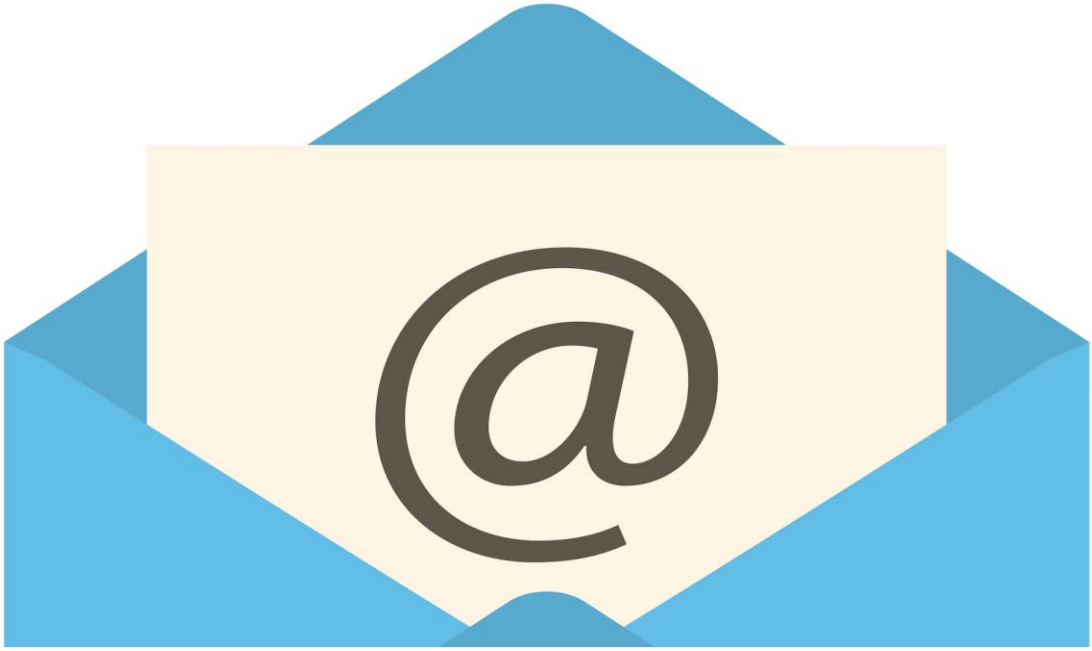
Copyright © September 2023

PERTEMUAN 12

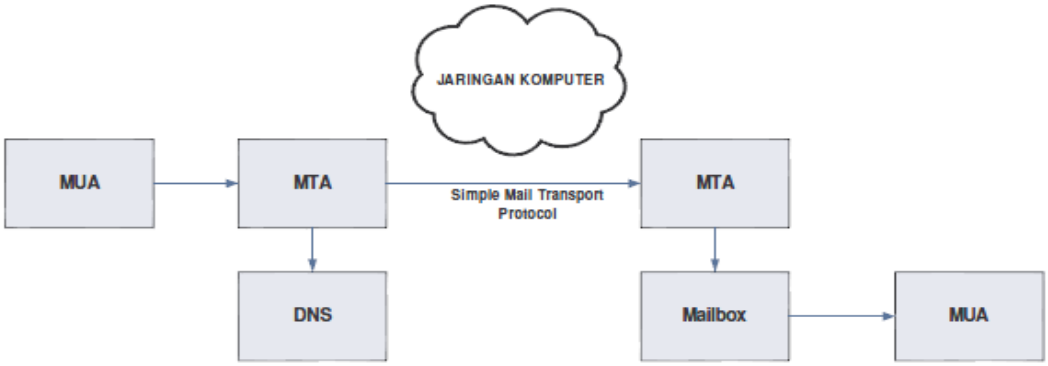
KEAMANAAN MAIL SERVER

A. Pengantar



- E-mail sudah digunakan orang sejak awal terbentuknya internet pada sekitar tahun 1969.
- Alamat e-mail merupakan gabungan dari nama user dan domain name ; user@domainname. Misalnya: dion@gmail.com.
- Proses pengiriman Email memanfaatkan protokol SMTP (Simple Mail Transport Protocol - bekerja di port 25) atau UUCP. Protokol SMTP hanya bekerja untuk berkomunikasi dengan server mail remote, tidak untuk server lokal.
- Sedangkan pengguna Email dapat membaca e-mailnya menggunakan protokol POP. Setiap pengguna memiliki 'mailbox' pada mail server tempat mail yang ditujukan kepada pengguna tersebut disimpan.
- Mail server hanya sebuah aplikasi yang berurusan dengan lalu lintas email, tidak secara langsung berhubungan dengan user yang akan berkirim email.
- Sistem email memiliki dua komponen
    i. Mail User Agent (MUA), Berhubungan dengan pengguna. Contoh: Pine, Eudora, Netscape, Outlook dan Pegasus.
    ii. Mail Transfer Agent (MTA), Yang melakukan pengiriman email. Contoh: sendmail, qmail, Exim, postfix, Mdaemon, exchange.

Copyright © September 2023



Gambar 2 - Alur Pengiriman Email

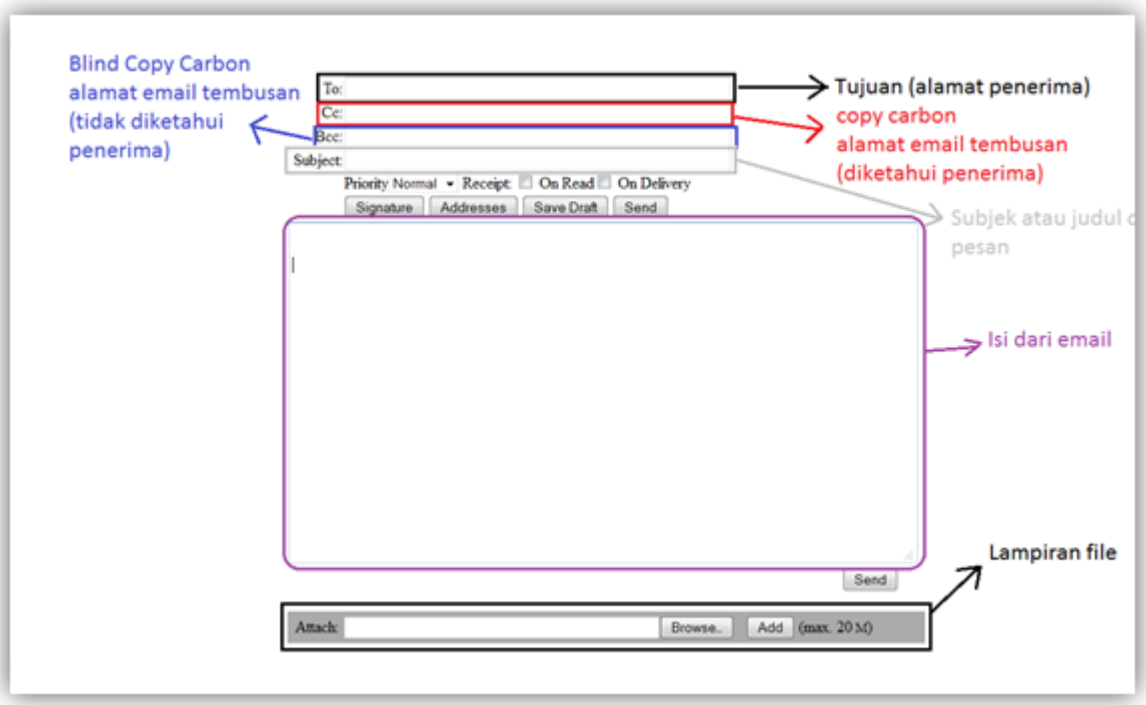
Penjelasan :

- MUA = Mail User Agent (Email Client : Thunderbird, Outlook, SquirellMail)
- MTA = Mail Transfer Agent (Email Server : Postfix, Qmail, Exim, Sendmail)
- DNS = Domain Name Server (BIND, PowerDNS, MyDNS)

B. Komponen Email

- *Envelope*, atau amplop. Ini digunakan oleh MTA untuk pengiriman. Envelope ditandai dengan dua buah perintah SMTP :
  MAIL from: tukul@students.ee.itb.ac.id
  RCPT to: susan@lskk.itb.ac.id
- *Header*, digunakan oleh *user agent*. Ada kurang lebih sembilan field header, yaitu: Received, Message-Id, From, Date, Reply-To, X-Phone, X-mailer, To dan Subject. Setiap field header berisi sebuah nama yang diikuti oleh sebuah titik dua (:), dan nilai dari field header tersebut.
- *Body* merupakan isi pesan dari pengirim ke penerima.

Copyright © September 2023



Copyright © September 2023

C. Contoh Email

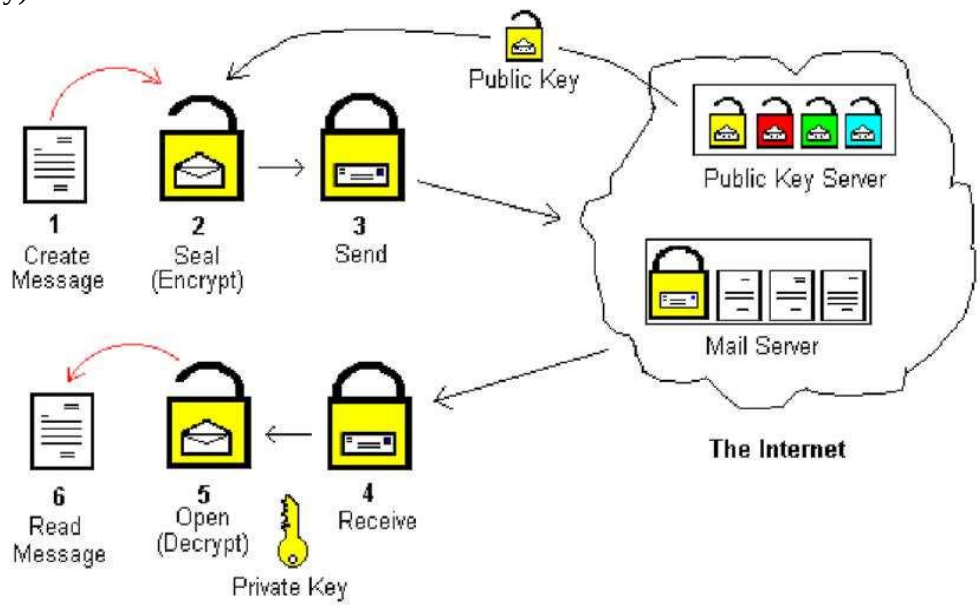
```
From: "Jimmy" <jimmy@tabloidpcplus.com>
        To: "Anton" <anton@bsi.ac.id>
        References: <WorldClient-F200506212027.AA27280044@bsi.ac.id>
        Subject: Re: Tanya mengenai workshop PC Plus
        Date: Wed, 22 Jun 2005 11:01:01 +0700

Return-path: <jimmy@tabloidpcplus.com>
Received: from mail.ub.net.id ([202.146.0.14])
        by bsi.ac.id ([202.183.1.20])
        with SMTP (MDaemon.PRO.v6.7.8.R)
        for <anton@bsi.ac.id>; Wed, 22 Jun 2005 11:26:15 +0700
Received: (qmail 26119 invoked by uid 1006); 22 Jun 2005 10:43:18 +0700
Received: from jimmy@tabloidpcplus.com by mail by uid 89 with qmail-scanner-1.22-st-qms
 (clamdscan: 0.73. spamassassin: 2.63.  Clear:RC:1(127.0.0.1):.
 Processed in 2.007306 secs); 22 Jun 2005 03:43:18 -0000
X-Antivirus-MYDOMAIN-Mail-From: jimmy@tabloidpcplus.com via mail
X-Antivirus-MYDOMAIN: 1.22-st-qms (Clear:RC:1(127.0.0.1):. Processed in 2.007306 secs
Process 26113)
Received: from mail.ub.net.id (HELO infokomputer.com) ()
  by mail.ub.net.id with SMTP; 22 Jun 2005 10:43:16 +0700
Received: from jimmy
        by infokomputer.com
        (MDaemon.PRO.v6.8.4.R)
        with ESMTP id 21-md50000000164.tmp
        for <anton@bsi.ac.id>; Wed, 22 Jun 2005 11:08:23 +0700
Message-ID: <00a901c576df$00cf3010$79260f0a@jimmy>
From: "Jimmy" <jimmy@tabloidpcplus.com>
To: "Anton" <anton@bsi.ac.id>
References: <WorldClient-F200506212027.AA27280044@bsi.ac.id>
Subject: Re: Tanya mengenai workshop PC Plus
Date: Wed, 22 Jun 2005 11:01:01 +0700
MIME-Version: 1.0
Content-Type: text/plain;
        charset="Windows-1252"
Content-Transfer-Encoding: 7bit
X-Priority: 3
X-MSMail-Priority: Normal
X-Mailer: Microsoft Outlook Express 6.00.2600.0000
```

D. Penyadapan Email (Confidentiality Problem)

- Email seperti kartu pos (postcard) yang dapat dibaca oleh siapa saja. Terbuka.
- Email dikirimkan oleh MTA ke “kantor pos” terdekat untuk diteruskan ke “kantor pos” berikutnya. Hopping. Sampai akhirnya di tujuan.
- Potensi penyadapan dapat terjadi di setiap titik yang dilalui.

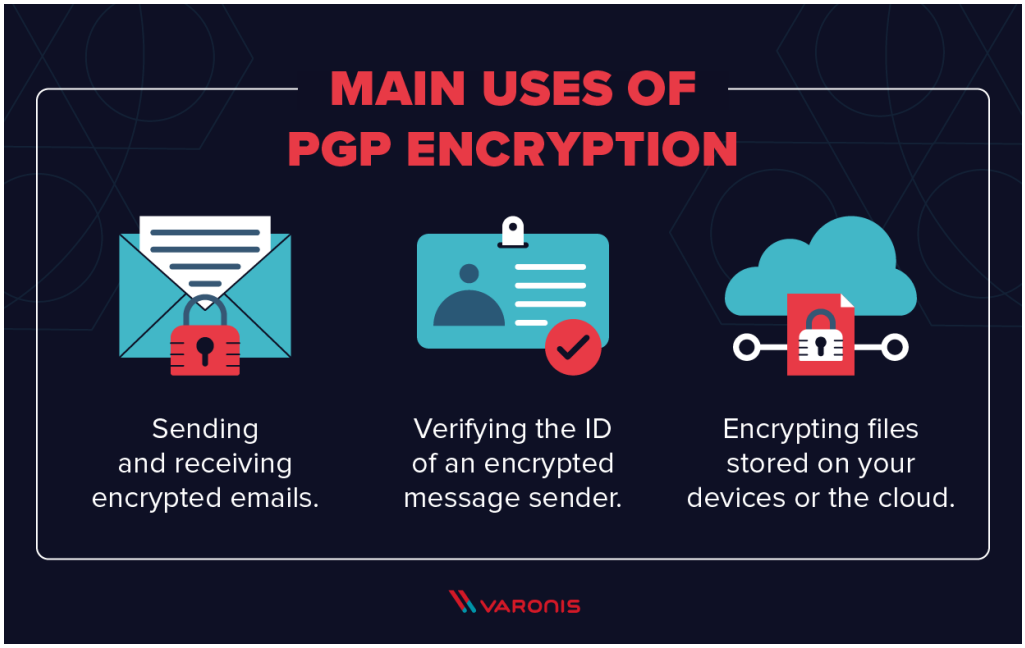
Copyright © September 2023

E. Proteksi Terhadap Penyadapan
Menggunakan enkripsi untuk mengacak isi surat. Contoh proteksi: PGP (Pretty Good Privacy)

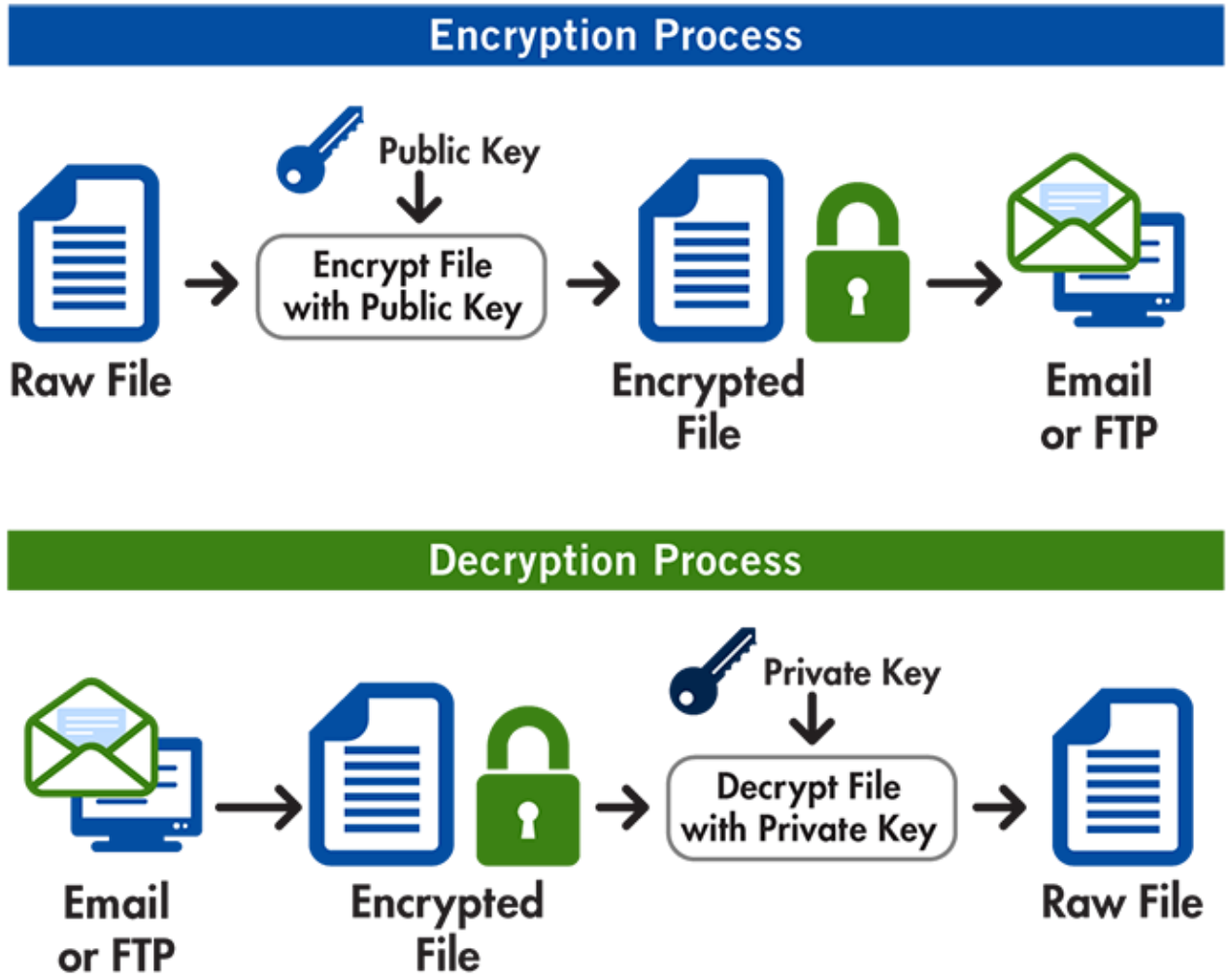


F. Pretty Good Privacy
Pretty Good Privacy (PGP) adalah suatu program / protokol enkripsi yang menyediakan fasilitas enkripsi (penyandian) dan autentikasi untuk layanan electronic mail dan penyimpanan file. PGP diciptakan oleh Phil Zimmerman pada tahun 1991. Telah digunakan dalam berbagai perusahaan untuk melindungi transfer data via email maupun penyimpanan berkas. PGP adalah aplikasi free open source. Zimmerman sebagai pencipta PGP menyebarkan aplikasi yang dia buat secara bebas.

Copyright © September 2023



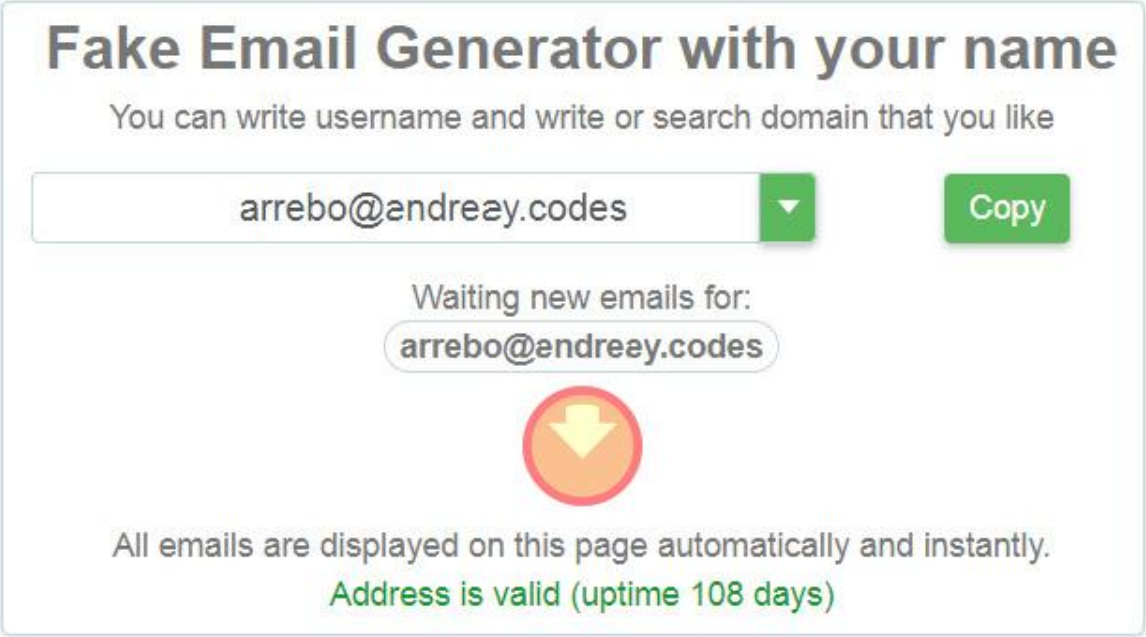
Copyright © September 2023



G. Email Palsu

- Mudah membuat email palsu dengan membuat header sesuka anda.
- Email palsu ini kemudian dikirimkan via MTA atau langsung via SMTP
- Aktivitas tercatat di server dalam berkas log.

Copyright © September 2023



H. Proteksi: Email Palsu
- Lihat header untuk mengetahui asal email dan Menggunakan digital signature.
- Namun keduanya jarang dilakukan

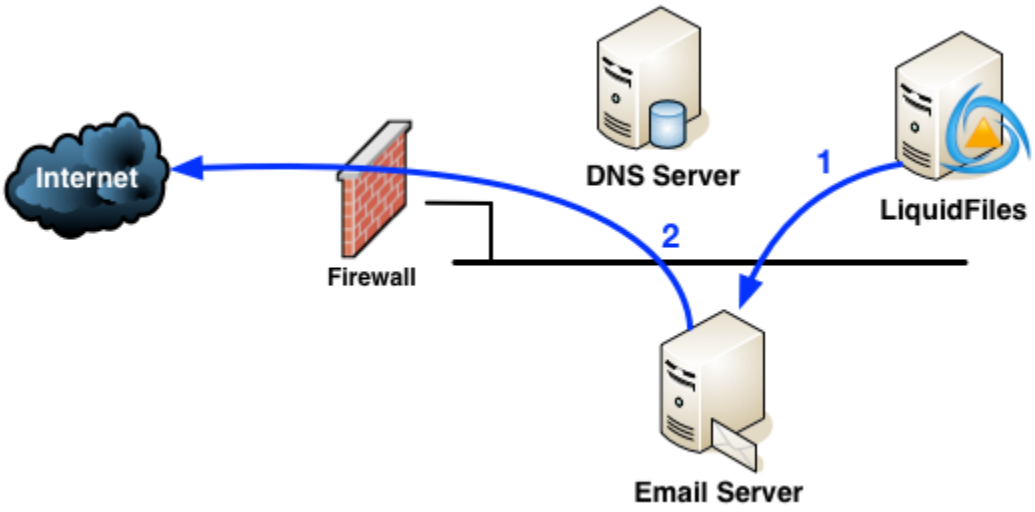
I. Spamming
- Spam adalah email sampah. Email yang masuk kedalam inbox kita yang berisi informasi yang sebenarnya tidak kita inginkan. Biasanya email spam berisi informasi produk, promosi atau iklan.
- Kadang spam juga berisi informasi-informasi bohong (hoax), penipuan atau bisa berupa fakta tetapi sudah dirubah sebagian sehingga validitasnya tidak dapat dijamin lagi.
- Proteksi: MTA dipasang proteksi terhadap spamming.

Copyright © September 2023

J. Mailbomb
- Biasanya email spam ini dikirimkan ke banyak alamat email oleh satu pihak 'spammer' dengan menggunakan apa yang disebut dengan istilah 'email bombing'. Satu email berisi pesan-pesan tertentu, semisal iklan atau hoax dlsb. dikirimkan ke banyak alamat email yang bisa didapat dari mailing list tertentu atau daftar alamat email yang dimiliki oleh 'spammer'.
- Proteksi: membatasi ukuran email, quota disk, menggunakan filter khusus.

K. Mail Relay
- Menggunakan server orang lain untuk mengirimkan email Akibat:
  i. Bandwidth orang lain terpakai untuk mengirim email tersebut (yang biasanya banyak)
  ii. Mengelabui penerima email
- Proteksi
  i. Mail Abuse Prevention System
     http://mail-abuse.org/
  ii. ORBZ – Open Relay Blackhole Zone
     http://www.orbz.org/
  iii. ORDB – Open Relay Database
     http://www.ordb.org/
  iv. RBL-type services
     http://www.ling.helsinki.fi/users/reriksso/rbl/rbl.html

Copyright © September 2023



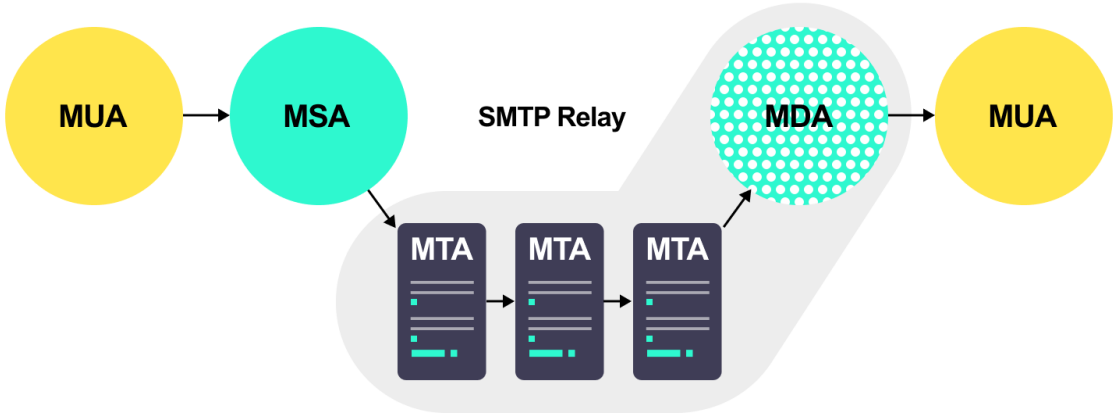
L. Mail User Agent (MUA)

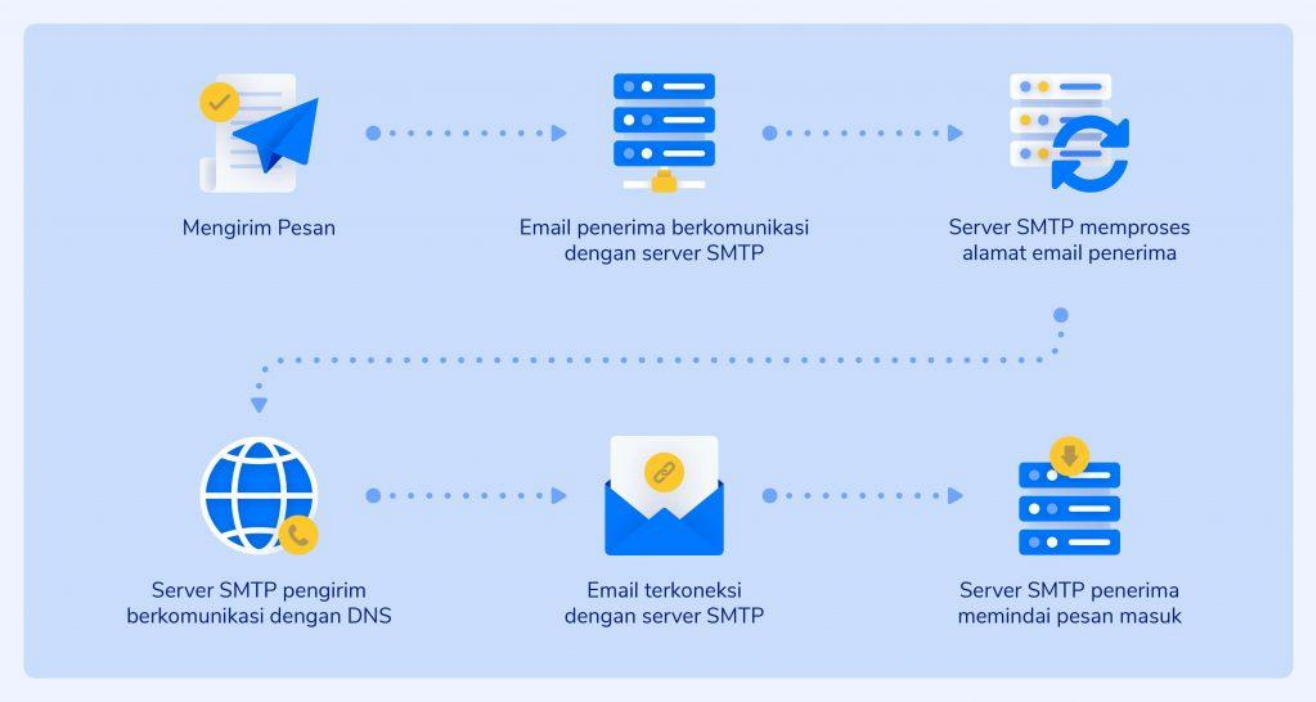
- MUA adalah aplikasi yang digunakan untuk menyusun, mengirim, dan menerima email. Contoh MUA misalnya adalah Yahoo, Gmail, Outlook, dan layanan email yang lain.
- Beberapa MUA bisa tampak lebih grafis, seperti Evolution, Thunderbird, dan Outlook, atau memiliki interface yang berbasis teks sederhana seperti Mutt.

M. Mail Transport Agent (MTA)

- MTA merupakan salah satu komponen mail server yang bertugas menerima dan mengirim email dari komputer yang satu ke komputer yang lain. MTA memainkan peranan penting dalam sistem penanganan pesan internet. Beberapa tugas MTA antara lain:
  i. Menerima email.
  ii. Meminta catatan mail exchange dan memilih server email untuk mentransfer email.
  iii. Mengirim pesan respons otomatis jika pesan gagal sampai tujuan.

Copyright © September 2023



N. Mail Delivery Agent (MDA)

- MDA adalah sebuah software komputer yang bertanggung jawab mengantarkan email dari MTA sever. MDA juga dikenal sebagai LDA atau Local Delivery Agent. Beberapa MTA dapat mengisi peran MDA ketika mereka menambahkan pesan email baru ke file pesan pengguna lokal.