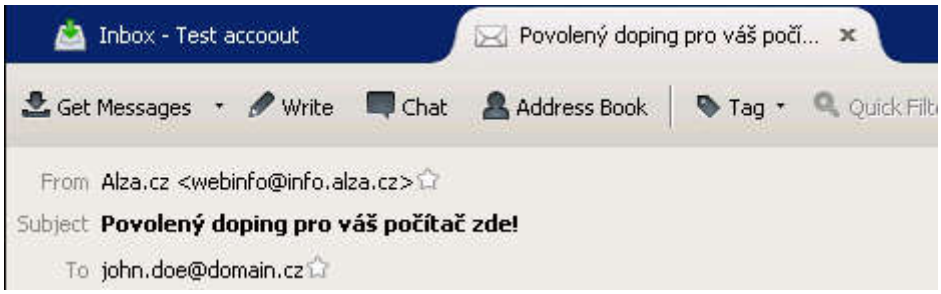
Thunderbird - replacing sender's address as potential security risk

1. Preconditions

- email address **john.doe@domain.cz** is only a name replacement of my test email account which exists on smtp server
- recipient **any.address@domain.com** is only a name replacement of my another test email account which exists on email server specified by domain's MX record
- a test message



  - **original sender - Alza.cz <webinfo@info.alza.cz>**
    (a newsletter ☺)
  - **original recipient - john.doe@domain.cz**

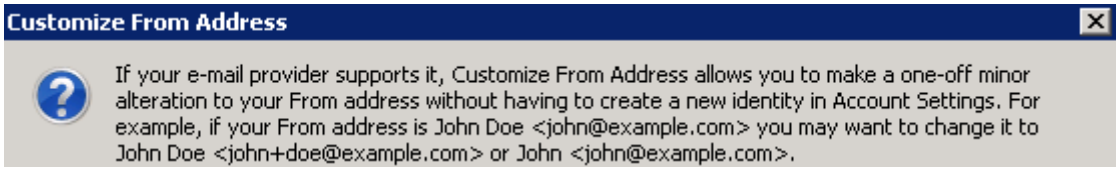
2. Forward an email by a common way

- recipient - any address
- sender - john.doe@domain.cz
- everything is OK, Sender is the same address as is entered in email account's configuration

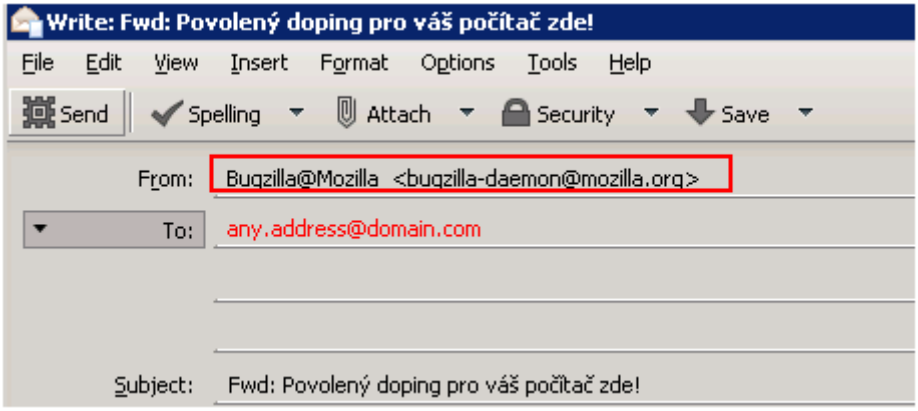
3. Forward an email using a feature "editing of From" (CHANGE SENDER'S ADDRESS WITH USER'S INTERACTION)

3a) compose a message by clicking to a button Forward

- recipient - any address
- sender - expand dropdown and click to Customize from address

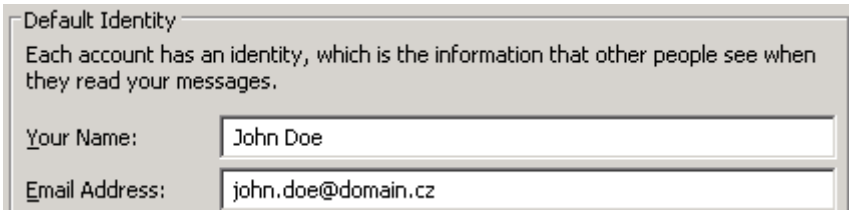


- In contrary text above we will change NAME AND DOMAIN instead of mentioned **name** → bugzilla-daemon@mozilla.org



3b) Send a message via smtp server

- to accept sending of email, most of properly configured smtp servers (include gmail, outlook.com … …) require using same **MAIL FROM** and **domain** (email address) which was **used for authentication**. In this case a Thunderbird uses as **MAIL-FROM** email address taken from an identity section

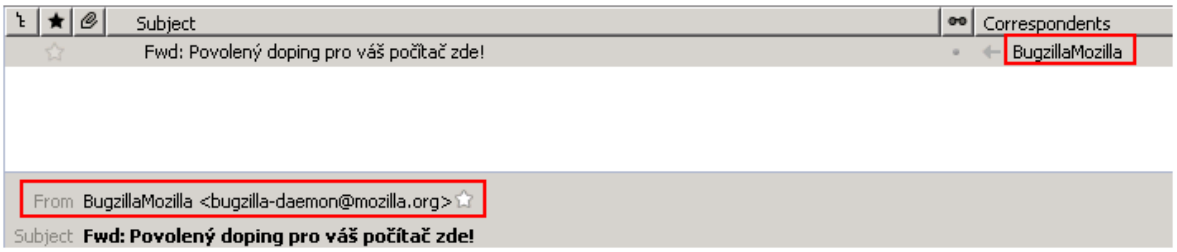


- a message is sent without any problem because Thunderbird DOES not use and address bugzilla-daemon@mozilla.org before DATA command.

```
20160503 10:33:41.341 smtpin sid=pkZh1s0040jifNx01 smtp=AUTH:235 status=2.7.0 method=CRAM-MD5 username=john.doe@domain.cz ......
20160503 10:33:41.341 smtpin sid=pkZh1s0040jifNx01 TRACE => [235 2.7.0 ... authentication succeeded\r\n]
20160503 10:33:41.341 smtpin sid=pkZh1s0040jifNx01 global=TRANSACTION-WAIT state=CMD cmd=AUTH
20160503 10:33:41.343 smtpin sid=pkZh1s0040jifNx01 TRACE <= [MAIL FROM:<john.doe@domain.cz> BODY=8BITMIME SIZE=51147\r\n]
20160503 10:33:41.343 smtpin sid=pkZh1s0040jifNx01 smtp=MAIL:250 status=2.1.0 msg="<john.doe@domain.cz> sender ok"
20160503 10:33:41.343 smtpin sid=pkZh1s0040jifNx01 TRACE => [250 2.1.0 <john.doe@domain.cz> sender ok\r\n]
20160503 10:33:41.346 smtpin sid=pkZh1s0040jifNx01 TRACE <= [RCPT TO:<any.address@domain.com>\r\n]
20160503 10:33:41.346 smtpin sid=pkZh1s0040jifNx01 smtp=RCPT:250 status=2.1.5 msg="<any.address@domain.com> recipient ok"
20160503 10:33:41.346 smtpin sid=pkZh1s0040jifNx01 TRACE => [250 2.1.5 <any.address@domain.com> recipient ok\r\n]

20160503 10:33:41.347 smtpin sid=pkZh1s0040jifNx01 TRACE <= [DATA\r\n]
20160503 10:33:41.347 smtpin sid=pkZh1s0040jifNx01 TRACE => [354 enter mail, end with "." on a line by itself\r\n]
20160503 10:33:41.347 smtpin sid=pkZh1s0040jifNx01 global=TRANSACTION-DATA state=WAIT-DATA cmd=DATA
20160503 10:33:41.472 smtpin sid=pkZh1s0040jifNx01 smtp=DATA:250 status=2.0.0 id=pkZh1s0040jifNx01kZhv2 size=51147 ......
```

3c) check mailbox (what common user will see)



- a message was sent from **bugzilla-daemon@mozilla.org**

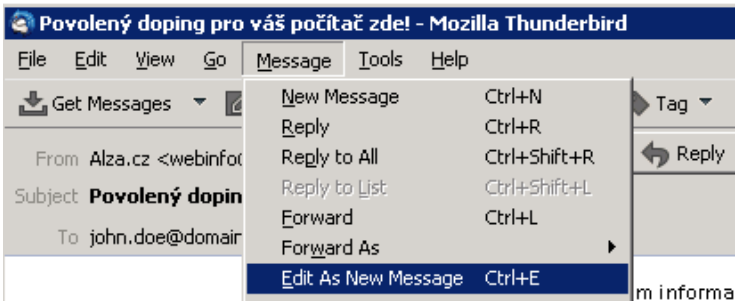
→ without analyze of a message's sources a common user have no opportunity how to find out a real sender (return path)

3d) Check a message's header to find out envelope sender

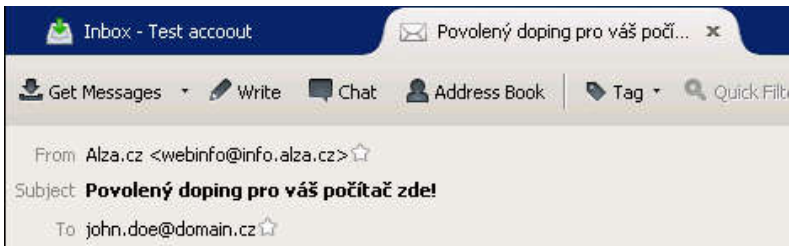
- a "real sender" - john.doe@domain.cz
- faked sender - bugzilla-daemon@mozilla.org

4. Forward/answer email using function Edit as new message (CHANGE SENDER'S ADDRESS WITHOUT USER'S INTERACTION)

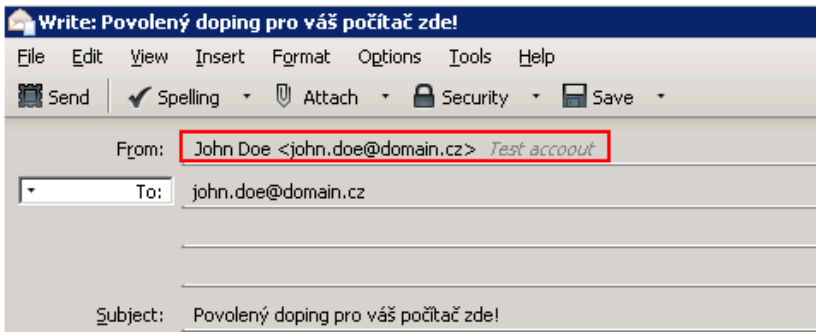
4a) compose a message



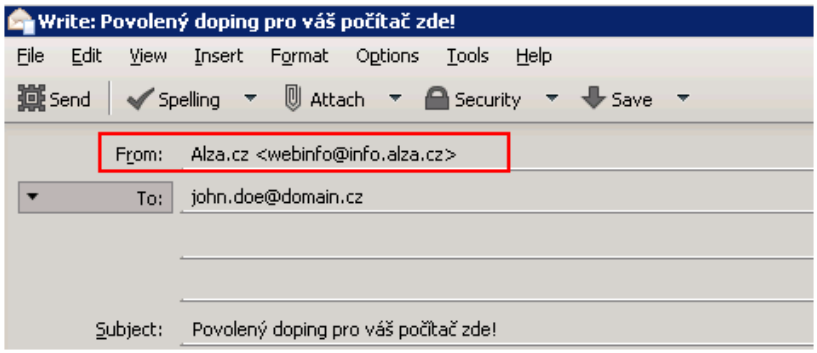
- in contrary to previous Thunderbird version an original sender replaces From:
  - original message



- Thunderbird 38.7.2 - From is the same as email account's address - **a correct behavior**



- Thunderbird 45 - From is the same as original messages' sender **= sender will be faked**



Because common users are not taking care about From address on compose window, they will only change a recipient in the field To and send email.

5. EXPECTED BEHAVIOR

1. Compose message as new

- previous version's behavior

2. Edit from

- this one is a potential security risk because it allows **very easy way** faking sender's address. So it can be used by spammers of for purposes of stealing personal data using trusted sender's address….
- **I'm proposing to reject this feature as potential security risk**