



**Communication security
over the Internet**

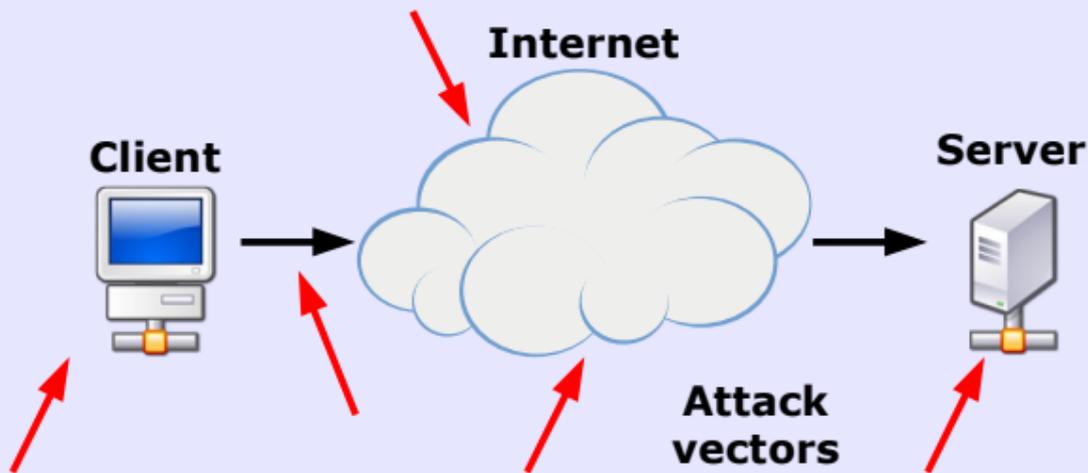
The big picture

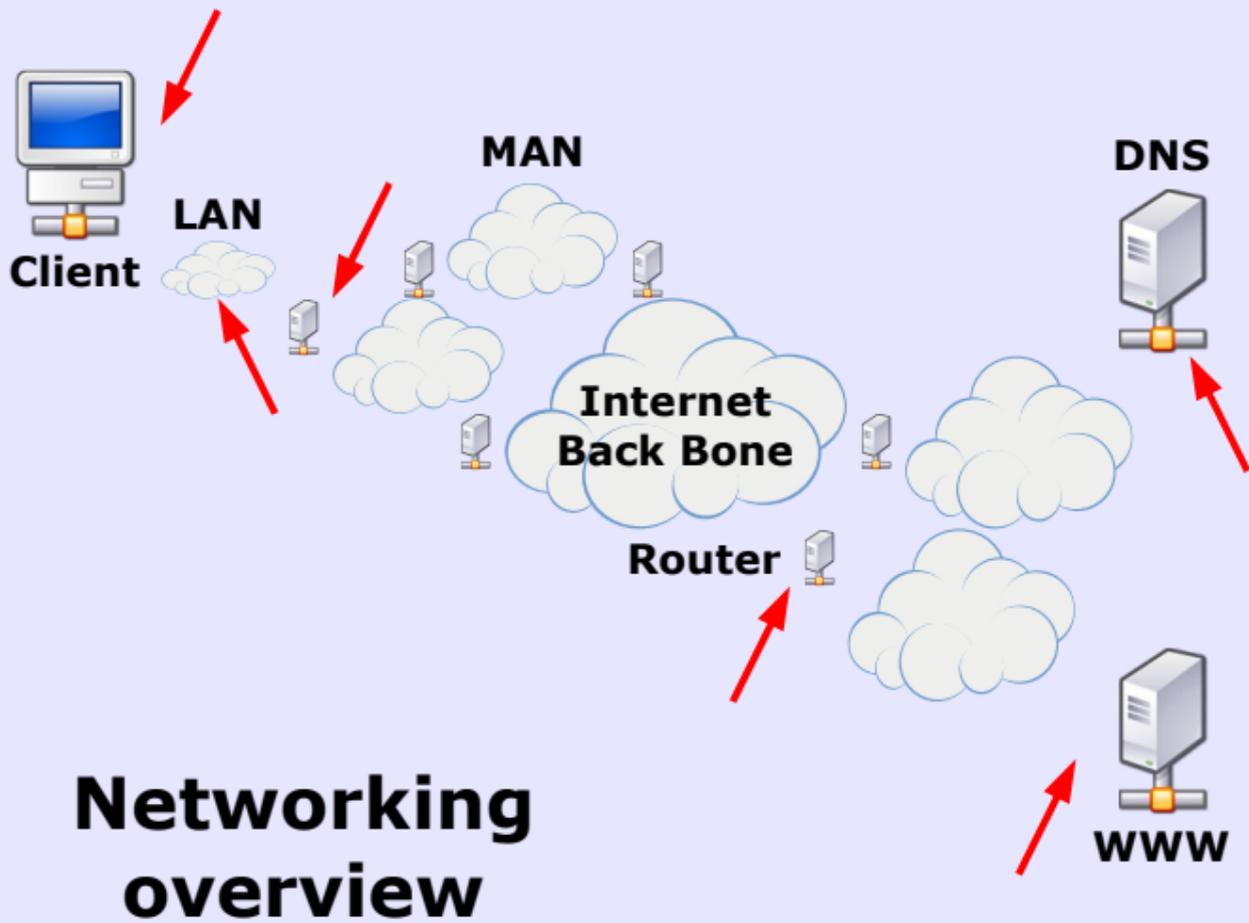


Me

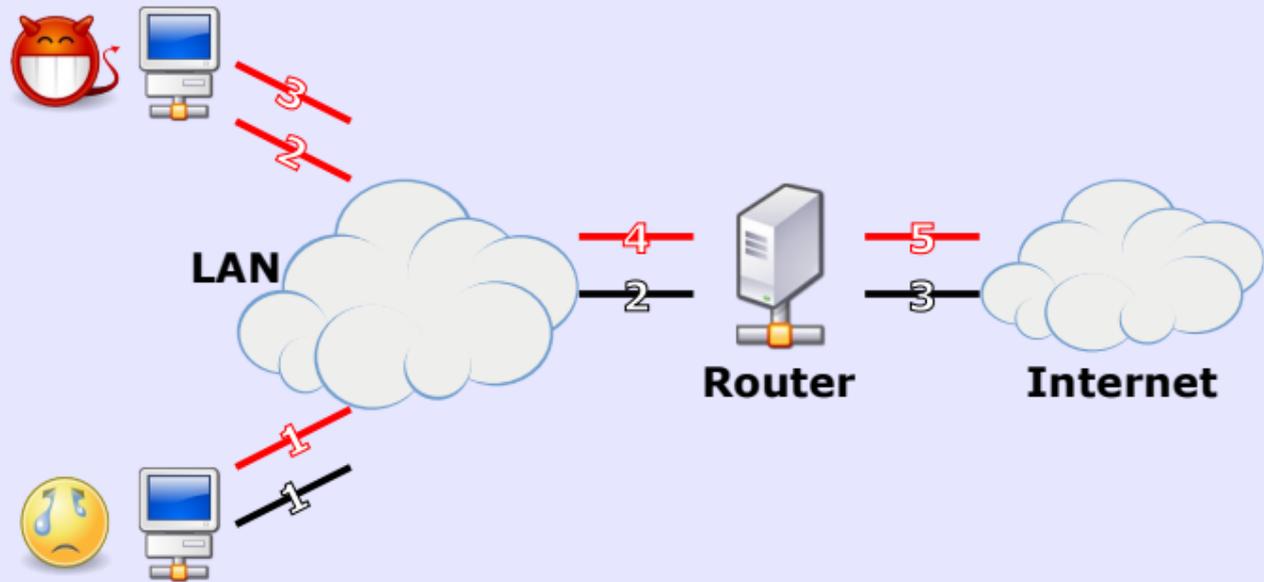


**Internet
Resource**

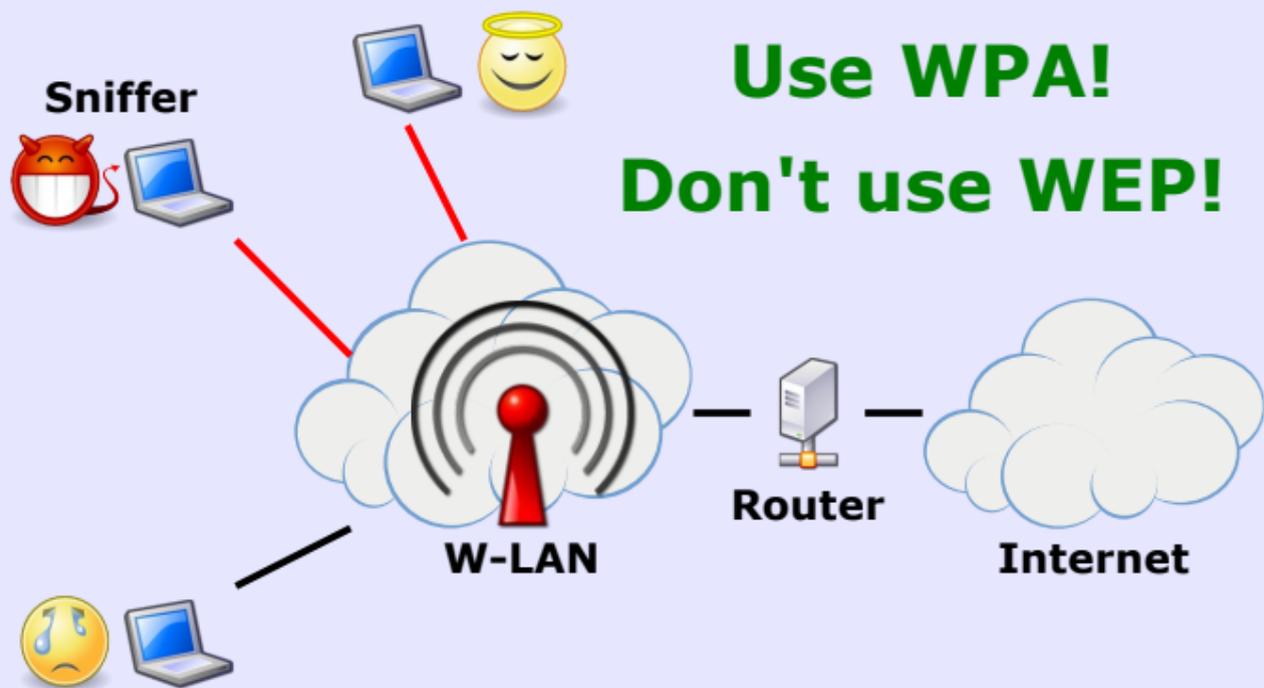




MITM (Man In The Middle)



AV: Spoofing



Use WPA!

Don't use WEP!

AV: Sniffing

Stream Content

```
POST /Wiki HTTP/1.1
Host: wiki.volution.ro
User-Agent: Mozilla/5.0 (X11; U; Linux i686 (x86_64); en-US; rv:1.9.2)
Gecko/20100207 Namoroka/3.6
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-us,en;q=0.5
Accept-Encoding: gzip,deflate
Accept-Charset: UTF-8,*
Keep-Alive: 115
Connection: keep-alive
Referer: http://wiki.volution.ro/Wiki?action=login
Content-Type: application/x-www-form-urlencoded
Content-Length: 82

action=login&name=Ciprian&password=this-is-not-my-
password&login=Login&login=LoginHTTP/1.1 200 OK
Transfer-Encoding: chunked
Content-Type: text/html; charset=utf-8
Vary: Cookie, User-Agent
```

Find Save As Print Entire conversation (36041 bytes)

Help

Filter Out This Stream

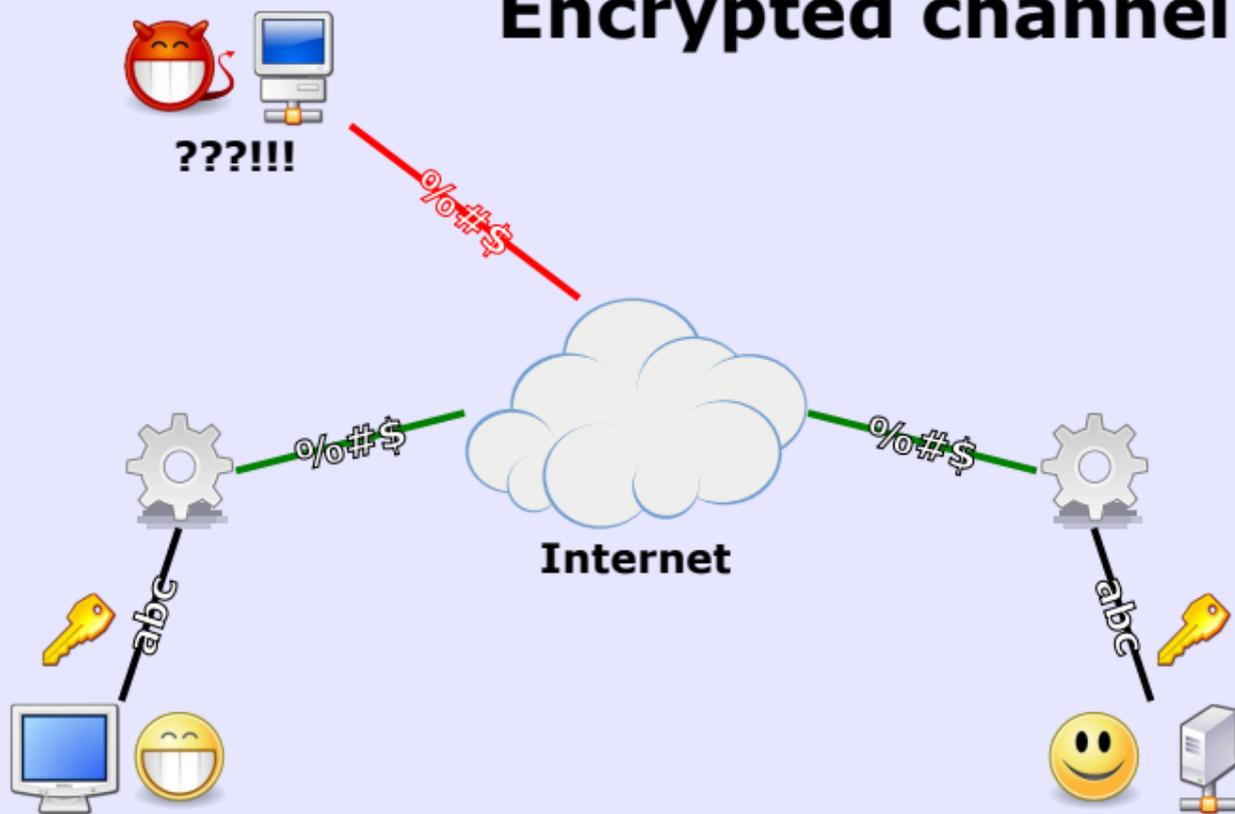
Close

HTTP network capture

Encryption



Encrypted channel



Stream Content

```
.....@...<..K.5..P..B..b.....#/b....p..7;B. .J.@X.....1.....).F  
(...>..&.....9.8...5.E.D.3.2...A...../.....  
.....wiki.volution.ro.#.$.;}.^..Dm@#....A#...  
$......f..i09)..r..>BS....4.?~.T..!W.....Q3..G..%  
3=.....L...m.....f...  
q.[.....i0.G...9).._.....].....1...  
%.....MN.u..M...J...F..K.*..q.....;F.ah...D......J.@X.....  
1.....).F(...>..5.....0  
.Z.u_@.....KY4..x...  
G...K.....n..`RH.....0.....7.o.....J.....6&.Zx6v2.  
[...f.ri)"..@..CuM.....s..)p...bQ@qR6.-L4.....+..  
(f.....K.q..7g.U.J...c...4..T.m.....@."...+`.q..o!9K.>..o..(..\t  
+`.....cZ...A. s...].A.s...s.C.U  
c.....QY..%.b..J#...0.{.>)  
+3..v~x0.3.....Ff./...Ct...Mn...M.....2@DH.....~.....^..R}.2.....#.t.0  
+4H.W;7.[\.;.d^.....B11...0ll|..~].p.....*..Y...3.....  
+.d/.`..N.....ptf..D.W&.E0a.^.-.5u...L\\...B.X..Y.  
[.....@.BBZ..r8.`.m.....d.../....._..j..5S*.....  
^8AM.'d..zo...3..8.....K.....PA|.....}.#R..  
[C.....B.....Y.....$|a.....a..3.cN.UC...  
..c.'..&...A.....1...y..I...L!&...?.8.....{...#.^o.L.....EQ.E0&.  
{%.r.;..oH...N.k.2
```

Find Save As Print Entire conversation (2008 bytes)

Help

Filter Out This Stream

Close

HTTPS Capture

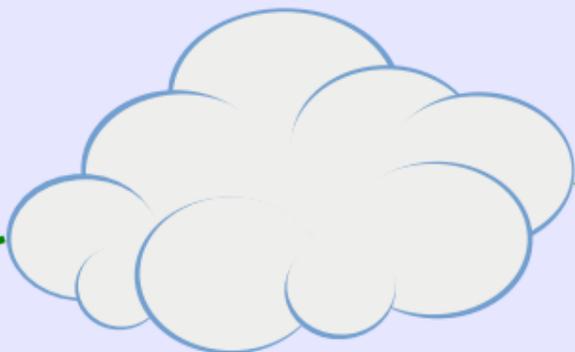
HTTPS (TLS/SSL)



AV: Phishing



my-bank.com

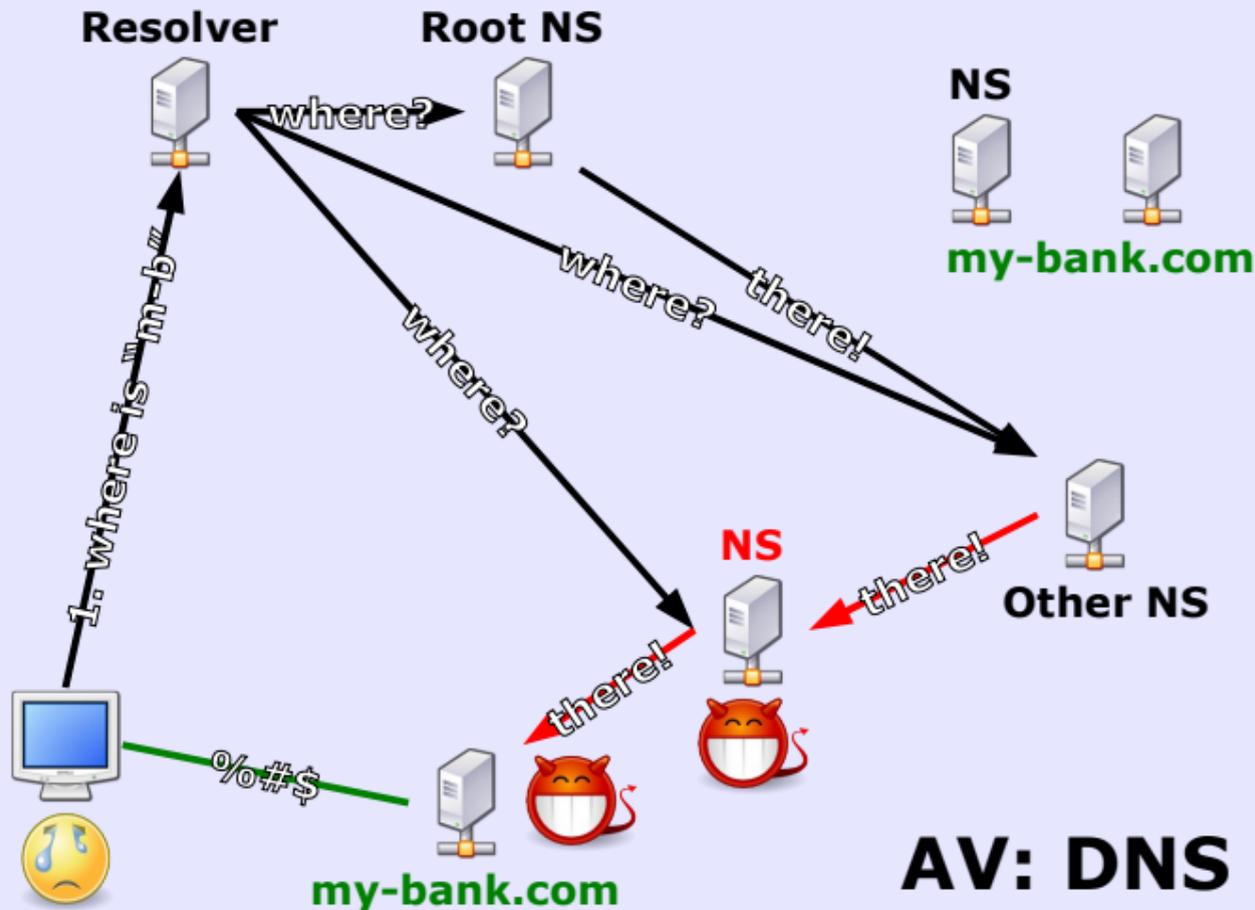


%0#\$\$

%0#\$\$

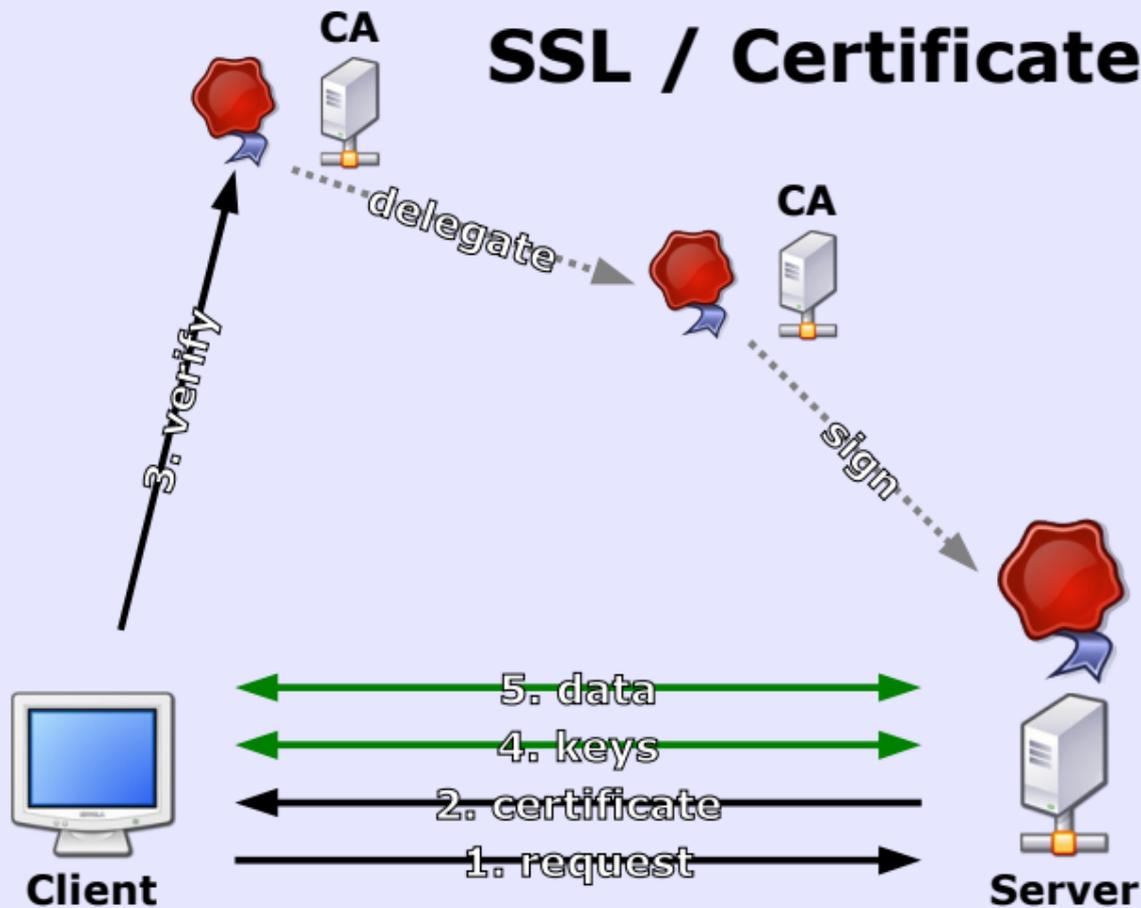


my-bamk.com



AV: DNS

SSL / Certificates



SSL in action (1)

The image shows a screenshot of a web browser window displaying the Raiffeisen Online login page. The browser's address bar shows the URL `https://www.raiffeisenonline.ro/eBankingWeb/logi`. The page features the Raiffeisen Bank logo and the slogan "Reușim împreună." (We succeed together). The main heading is "Bun venit la Raiffeisen Online" (Welcome to Raiffeisen Online). Below this, there is a message in Romanian: "Daca doresti sa accesezi Raiffeisen Online, te rugam sa consulți secțiunea 'Cum devii client' de pe www.raiffeisenonline.ro pentru a vedea care sunt condițiile pe care trebuie să le îndeplinești pentru a putea adera la serviciul de Internet Banking oferit de Raiffeisen Bank. Te rugăm să introduci Codul tau de utilizator." (If you want to access Raiffeisen Online, we ask you to consult the section 'How do you become a client' on www.raiffeisenonline.ro to see what conditions you need to fulfill to be able to join the Internet Banking service offered by Raiffeisen Bank. We ask you to enter your user code.) Below the message is a text input field labeled "Cod utilizator:" (User code) and a yellow "Continua" (Continue) button. At the bottom of the page, there is a "Done" status bar. The browser's system tray icons are visible in the bottom right corner.

File Edit View History Bookmarks Tools Help

raiffeisenonline.ro https://www.raiffeisenonline.ro/eBankingWeb/logi

Raiffeisen Online

Raiffeisen BANK

Reușim împreună.

Bun venit la Raiffeisen Online

Reușim împreună.

Cod utilizator:

Continua

Raiffeisen Online nu-ti va solicita niciodata toate cifrele din seria cardului tau de debit sau pinul acestuia.
Nu da curs nici unei cereri de divulgare a elementelor de identificare (Cod utilizator, parola, PIN)

Done



General



Media



Permissions



Security

SSL in action (2)

Web Site Identity

Web site: **www.raiffeisenonline.ro**
Owner: **This web site does not supply ownership information.**
Verified by: **VeriSign Trust Network**

[View Certificate](#)

Privacy & History

Have I visited this web site before today? **No**
Is this web site storing information (cookies) on my computer? **Yes**
Have I saved any passwords for this web site? **No**

[View Cookies](#)

[View Saved Passwords](#)

Technical Details

Connection Encrypted: High-grade Encryption (3DES-EDE-CBC 168 bit)

The page you are viewing was encrypted before being transmitted over the Internet. Encryption makes it very difficult for unauthorized people to view information traveling between computers. It is therefore very unlikely that anyone read this page as it traveled across the network.

SSL in action (3)

General Details

This certificate has been verified for the following uses:

SSL Server Certificate

SSL Server with Step-up

Issued To

Common Name (CN)	www.raiffeisenonline.ro
Organization (O)	RAIFFEISEN BANK S.A.
Organizational Unit (OU)	ITC
Serial Number	77:C7:3D:33:42:E2:CB:FC:96:11:65:1F:0C:8F:77:12

Issued By

Common Name (CN)	<Not Part Of Certificate>
Organization (O)	VeriSign Trust Network
Organizational Unit (OU)	VeriSign, Inc.

Validity

Issued On	04/06/2009
Expires On	04/07/2010

Fingerprints

SHA1 Fingerprint	99:12:79:4D:97:BE:D2:CB:1B:53:41:E4:18:72:36:0E:44:3A:F8:D0
MD5 Fingerprint	B2:67:2B:39:82:E0:85:23:70:62:48:F8:01:C0:60:44

Close

SSL in action (4)

The screenshot shows a web browser window with the following elements:

- Address Bar:** Contains the URL `https://www.raiffeisenonline.ro/eBankingWeb/logi` and a search bar with the text "Google".
- Page Header:** Features the Raiffeisen BANK logo on the left and the slogan "Reușim împreună." on the right.
- Warning Banner:** A yellow banner with the text "!!!FAKE EVIL PERSON DOING EVIL THINGS!!!".
- Main Content Area:**
 - Text: "Daca doresti sa accesezi **Raiffeisen Online**, te rugam sa consulți secțiunea "Cum devii client" de pe **www.raiffeisenonline.ro** pentru a vedea care sunt condițiile pe care trebuie să le îndeplinești pentru a putea adera la serviciul de Internet Banking oferit de Raiffeisen Bank. Te rugam sa introduci Codul tau de utilizator."
 - Text: "Cod utilizator:" followed by an input field.
 - Button: "▶ Continua".
 - Text: "Raiffeisen Online nu-ti va solicita niciodata toate cifrele din seria cardului tau de debit sau pinul acestuia. Nu da curs nici unei cereri de divulgare a elementelor de identificare (Cod utilizator, parola, PIN)!"
- Language Selection:** Three flags (UK, FR, RO) are visible on the right side of the main content area.
- Status Bar:** Shows the word "Done" on the left and a small icon on the right.



SSL missing in action ???!!!

The screenshot shows a web browser window with the following elements:

- Address Bar:** A red box highlights the address bar containing the URL `https://www.raiffeisenonline.ro/eBankingWeb/logi`. The domain `raiffeisenonline.ro` is also highlighted in blue.
- Page Header:** The Raiffeisen BANK logo is on the left, and the slogan "Reușim împreună." is on the right.
- Warning Message:** A yellow banner with a red border contains the text "!!!FAKE EVIL PERSON DOING EVIL THINGS!!!".
- Form:** Below the banner is a login form with the label "Cod utilizator:" and an input field. A yellow "Continua" button is below the input field.
- Footer:** At the bottom, there is a "Done" label on the left and a system tray area on the right with a red box around it, containing a battery icon and a network icon.



General



Media



Permissions



Security

Web Site Identity

Web site: **www.raiffeisenonline.ro**
 Owner: **This web site does not supply ownership information.**
 Verified by: **Evil Person**

[View Certificate](#)

Privacy & History

Have I visited this web site before today?
 Is this web site storing information (cookies) on my computer?
 Have I saved any passwords for this web site? **No**

[View Cookies](#)

[View Saved Passwords](#)

Technical Details

Connection Encrypted: High-grade Encryption (AES-256 256 bit)
 The page you are viewing was encrypted before being transmitted over the Internet. Encryption makes it very difficult for unauthorized people to view information traveling between computers. It is therefore very unlikely that anyone read this page as it traveled across the network.



???

Huh ???

???

General Details

This certificate has been verified for the following uses.

SSL Server Certificate

Issued To

Common Name (CN) www.raiffeisenonline.ro
Organization (O) FAKE RAIFFEISEN
Organizational Unit (OU) <Not Part Of Certificate>
Serial Number 01

Issued By

Common Name (CN) My Evil CA
Organization (O) Evil Person
Organizational Unit (OU) <Not Part Of Certificate>

Validity

Issued On 03/18/2010
Expires On 03/18/2011

Fingerprints

SHA1 Fingerprint DB:2B:A4:DA:B4:35:0F:41:C7:8C:D3:A0:9F:C0:51:8E:1A:34:1A:B1
MD5 Fingerprint F5:1C:C0:91:B6:0D:69:AA:F7:19:61:48:6D:57:A9:E0



Check "SHA1 Fingerprint"!!!

Don't rely on "MD5 Fingerprint"!!!

Close

The explanation!



Your Certificates People Servers Authorities Others

You have certificates on file that identify these certificate authorities:

Certificate Name	Security Device	
Equifax Secure Global eBusiness CA-1	Builtin Object Token	▲
Equifax Secure eBusiness CA-1	Builtin Object Token	
▼ Evil Person		
My Evil CA	Software Security Device	☰
▼ GeoTrust Inc.		
GeoTrust Primary Certification Authority	Builtin Object Token	
GeoTrust Global CA	Builtin Object Token	
GeoTrust Global CA 2	Builtin Object Token	
GeoTrust Universal CA	Builtin Object Token	
GeoTrust Universal CA 2	Builtin Object Token	▼

Edit... Import... Export... Delete... OK

Email security

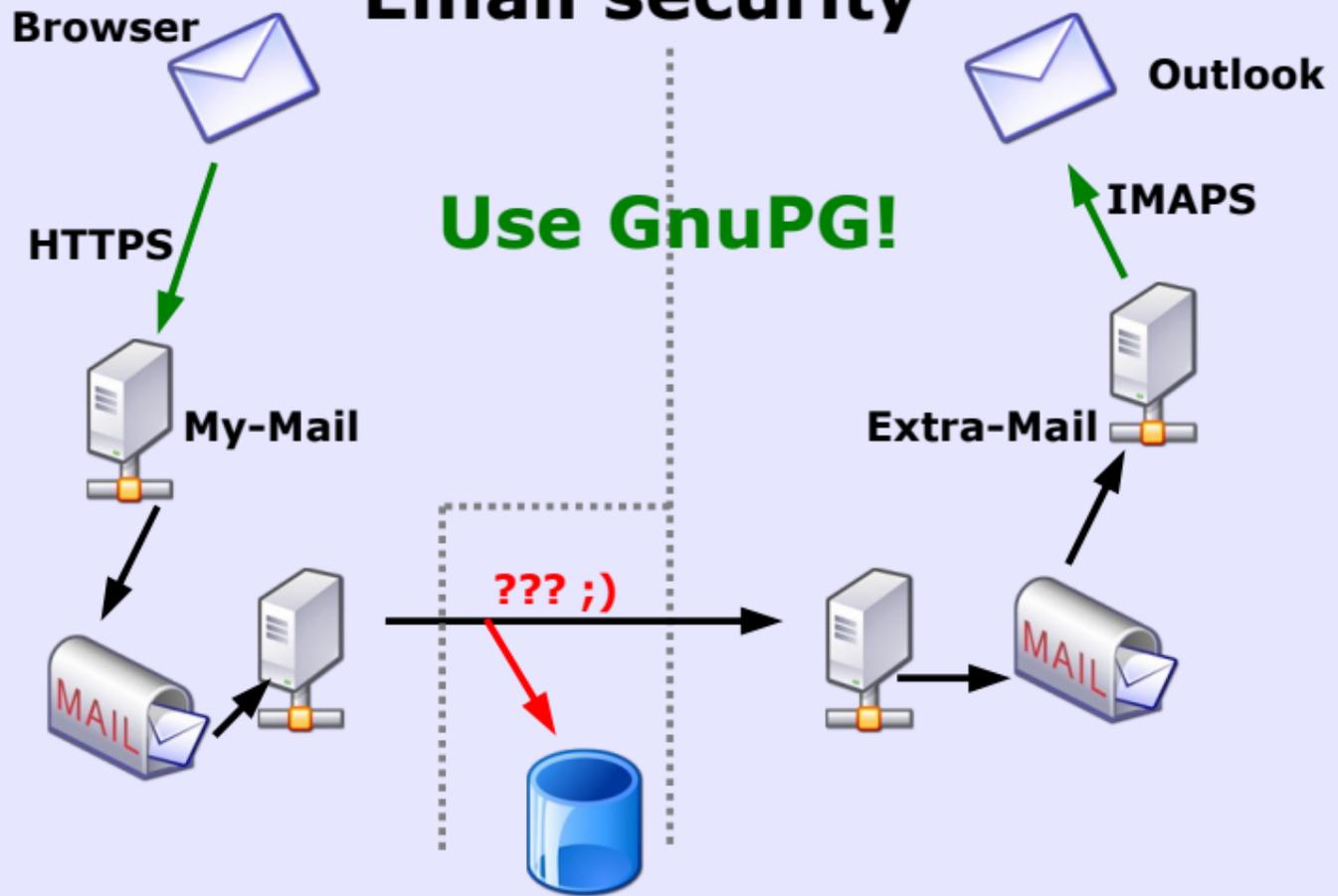
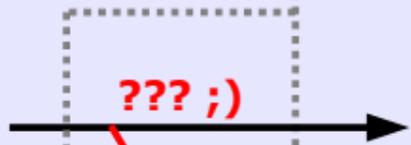
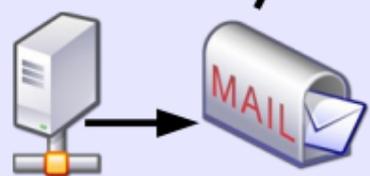
Browser 

 Outlook

HTTPS

Use GnuPG!

IMAPS



Keep focus!

