

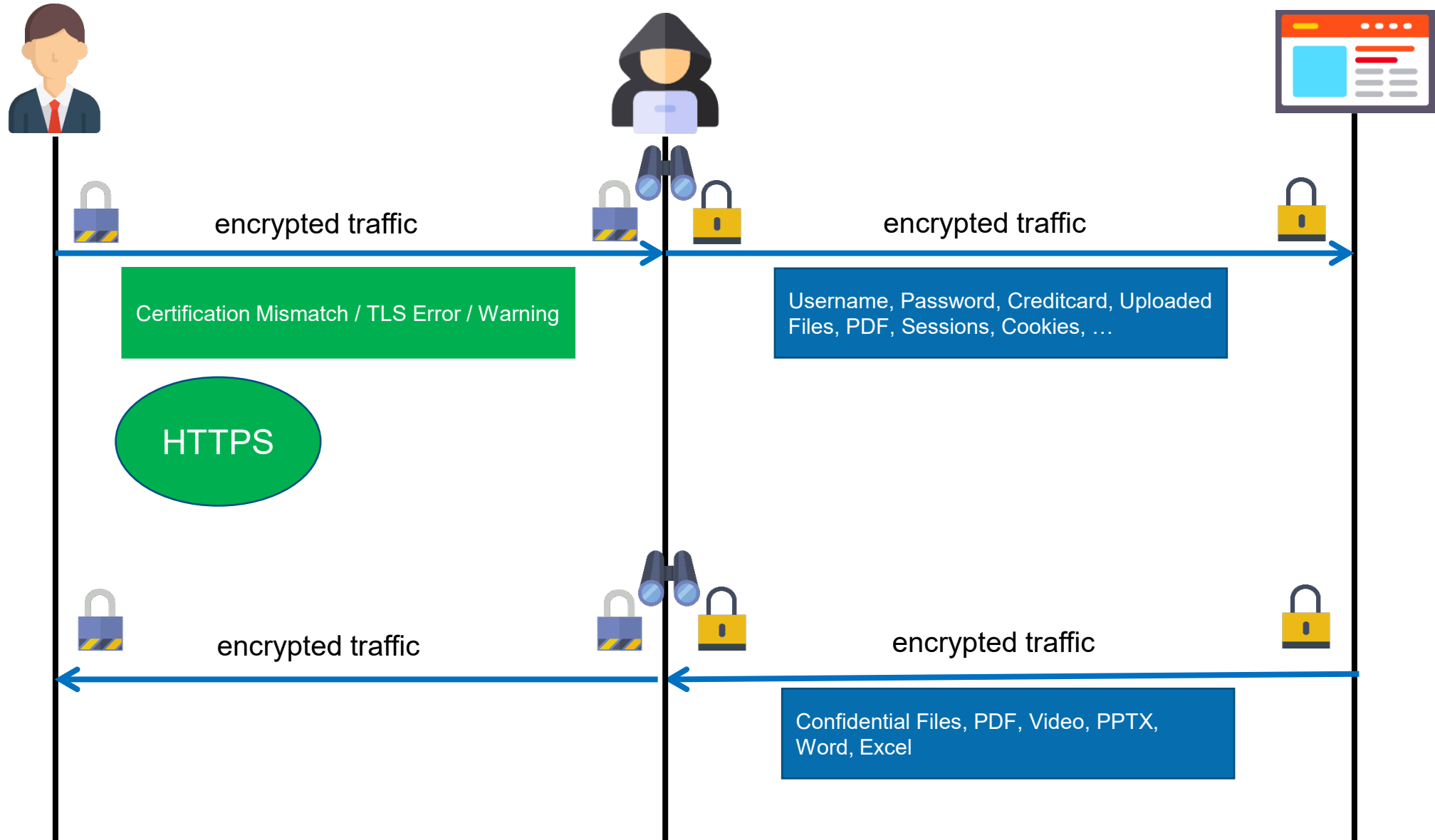


Man in the Middle Attacks

HTTPS

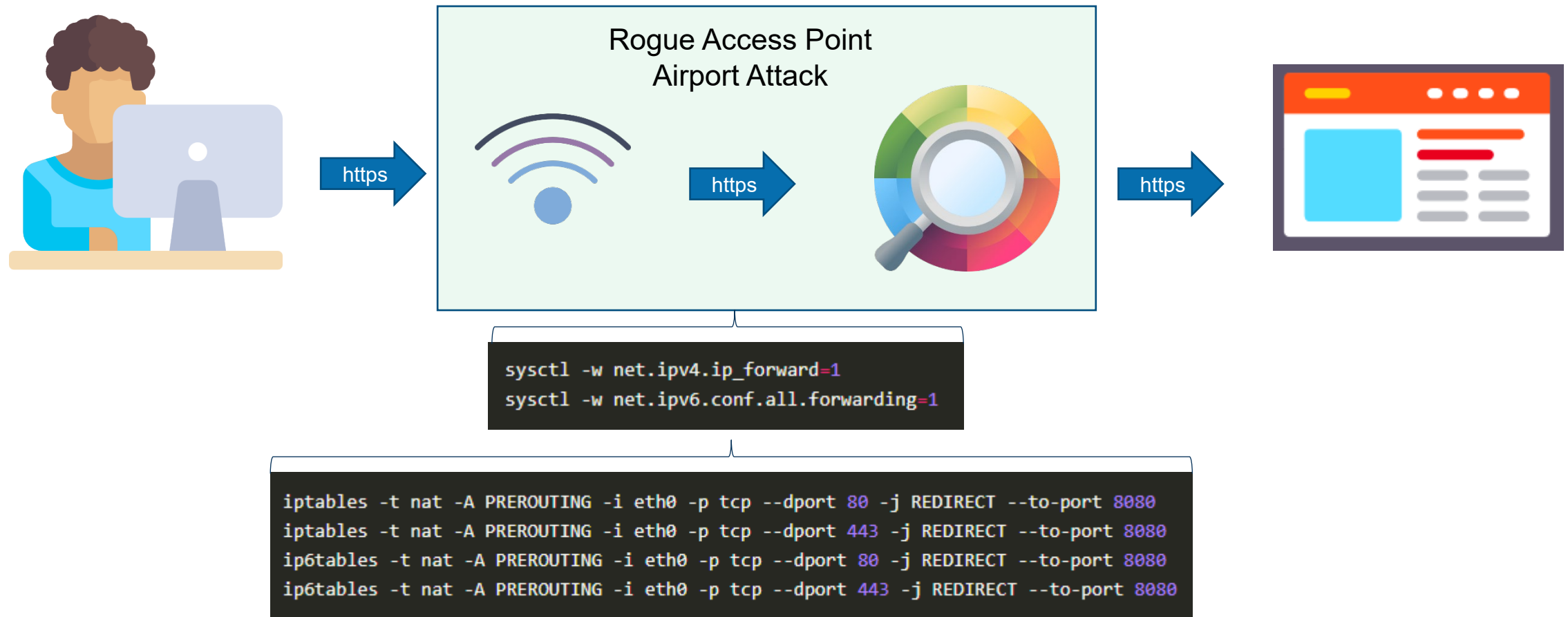
HS2024 Cyber Defense

Man in the Middle – Intercepting - Encrypted Traffic

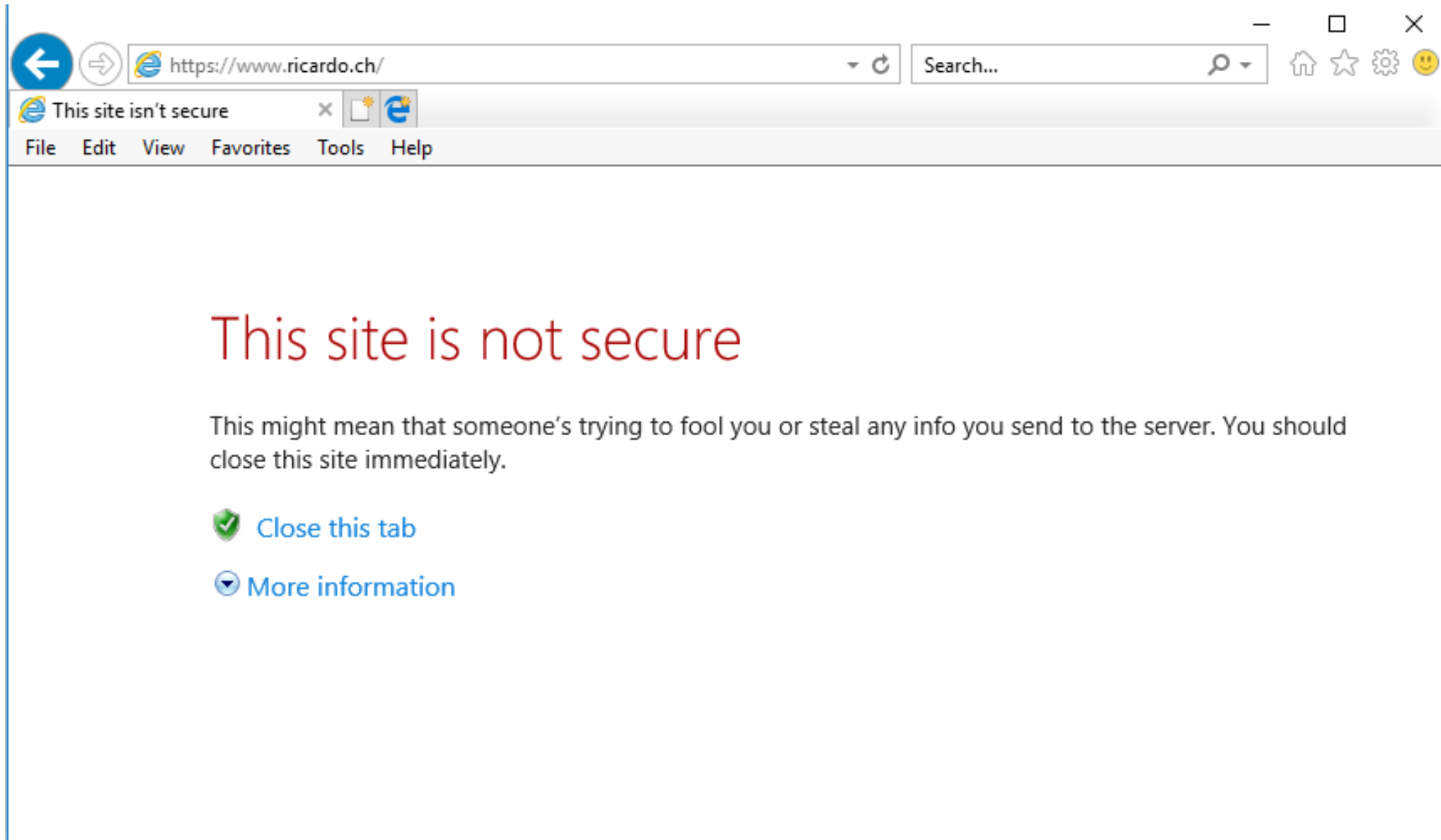


Man in the Middle – HTTPS Interception - Encrypted Traffic

Transparent Proxy

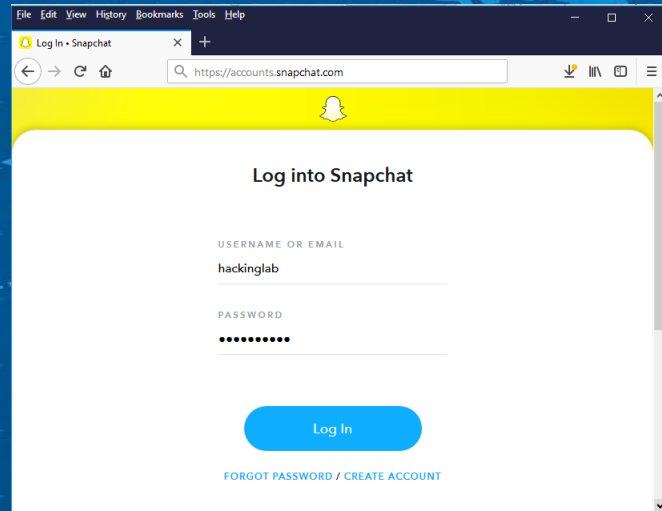


Man in the Middle – Intercepting - Encrypted Traffic



Offline Phishing

Offline Phishing



Username & Password

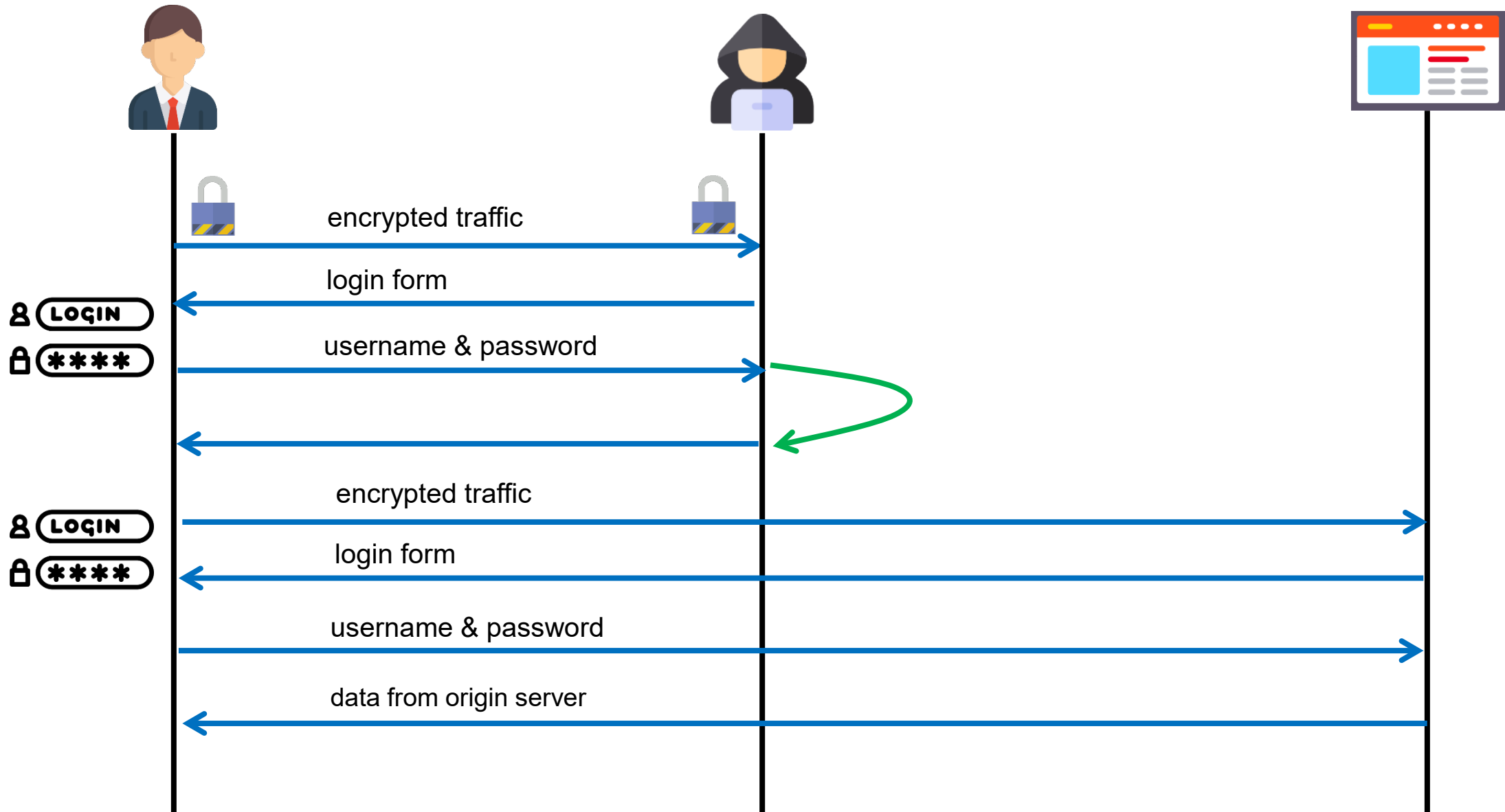
Redirect to Origin

Username & Password

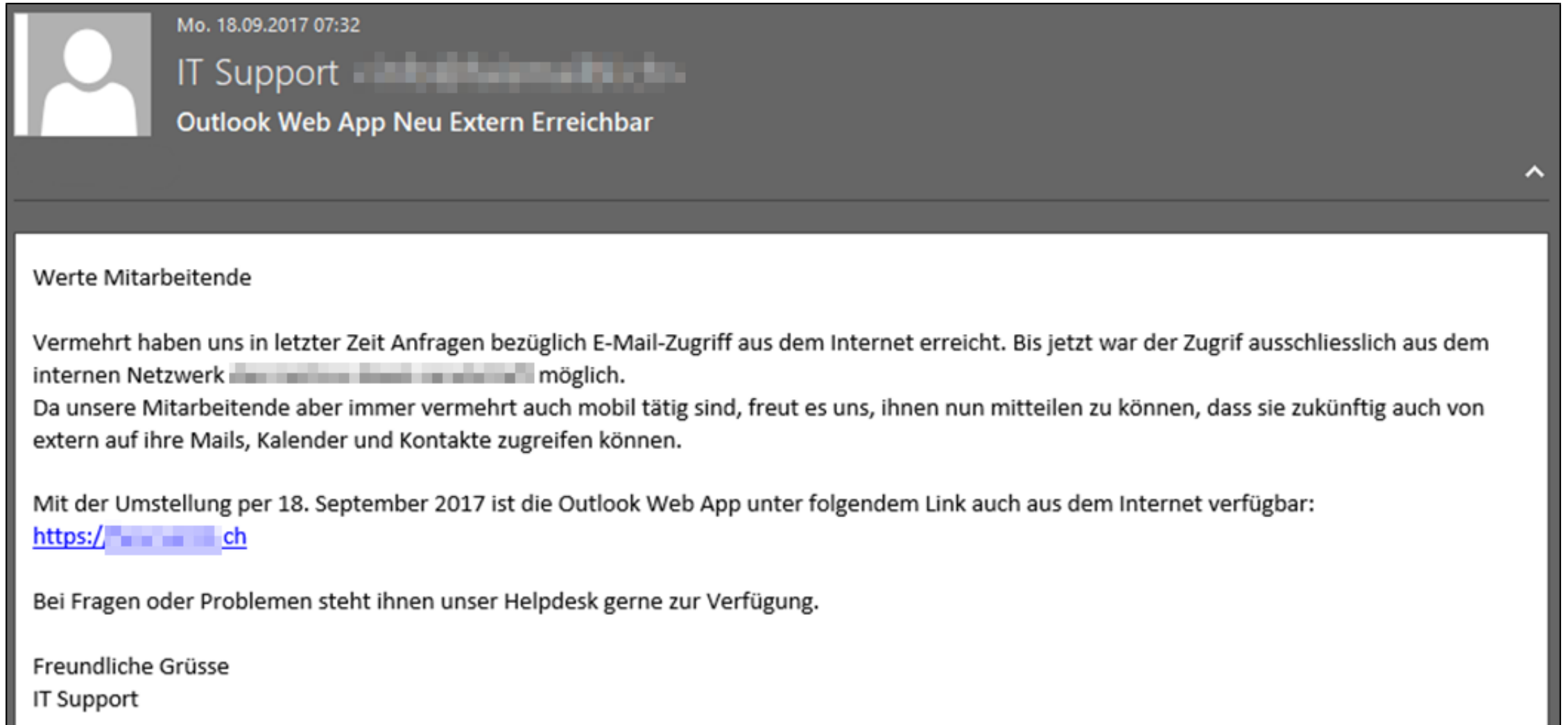
Offline (fake) copy of the original



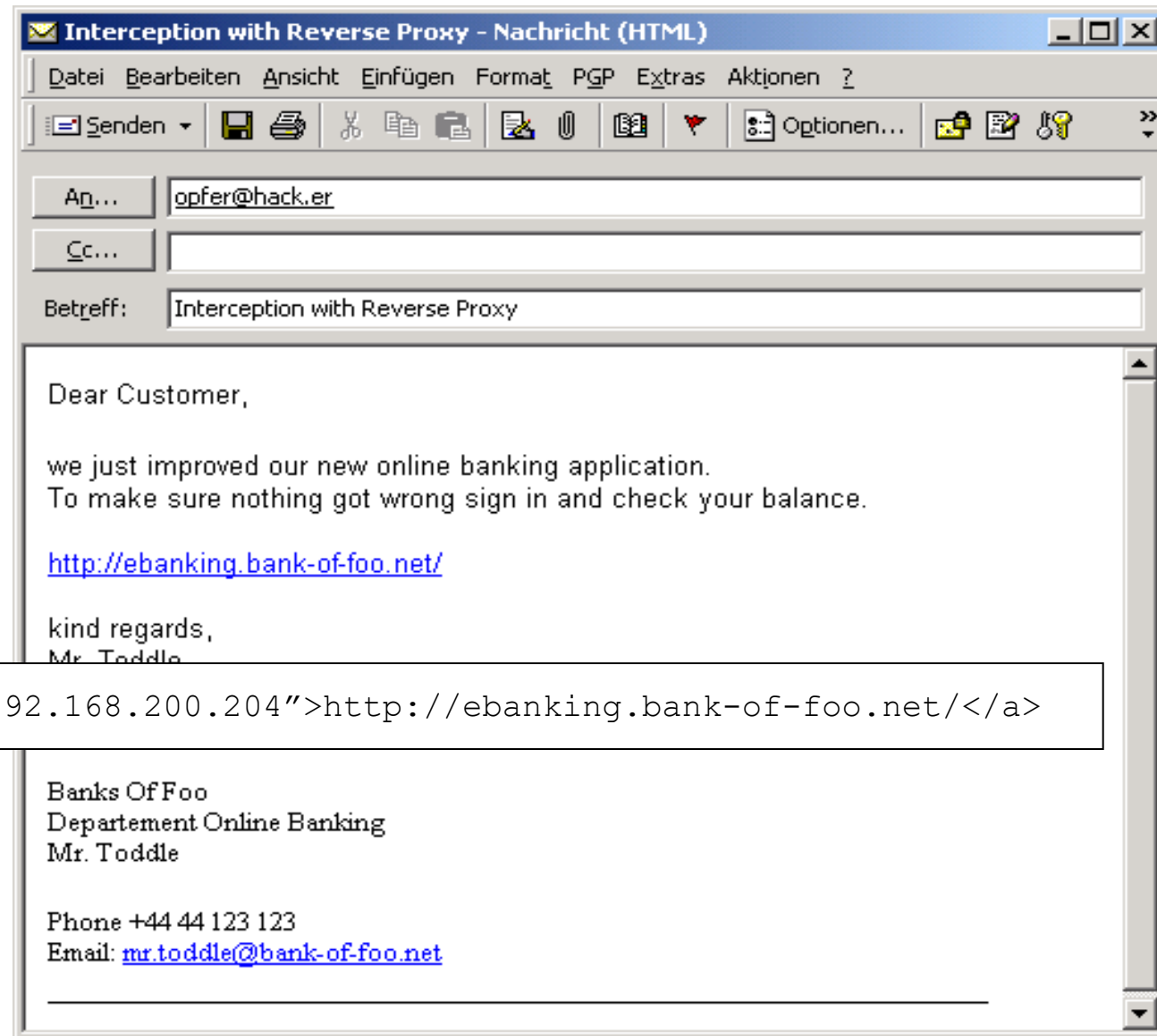
Man in the Middle – Offline Phishing – Fake https page



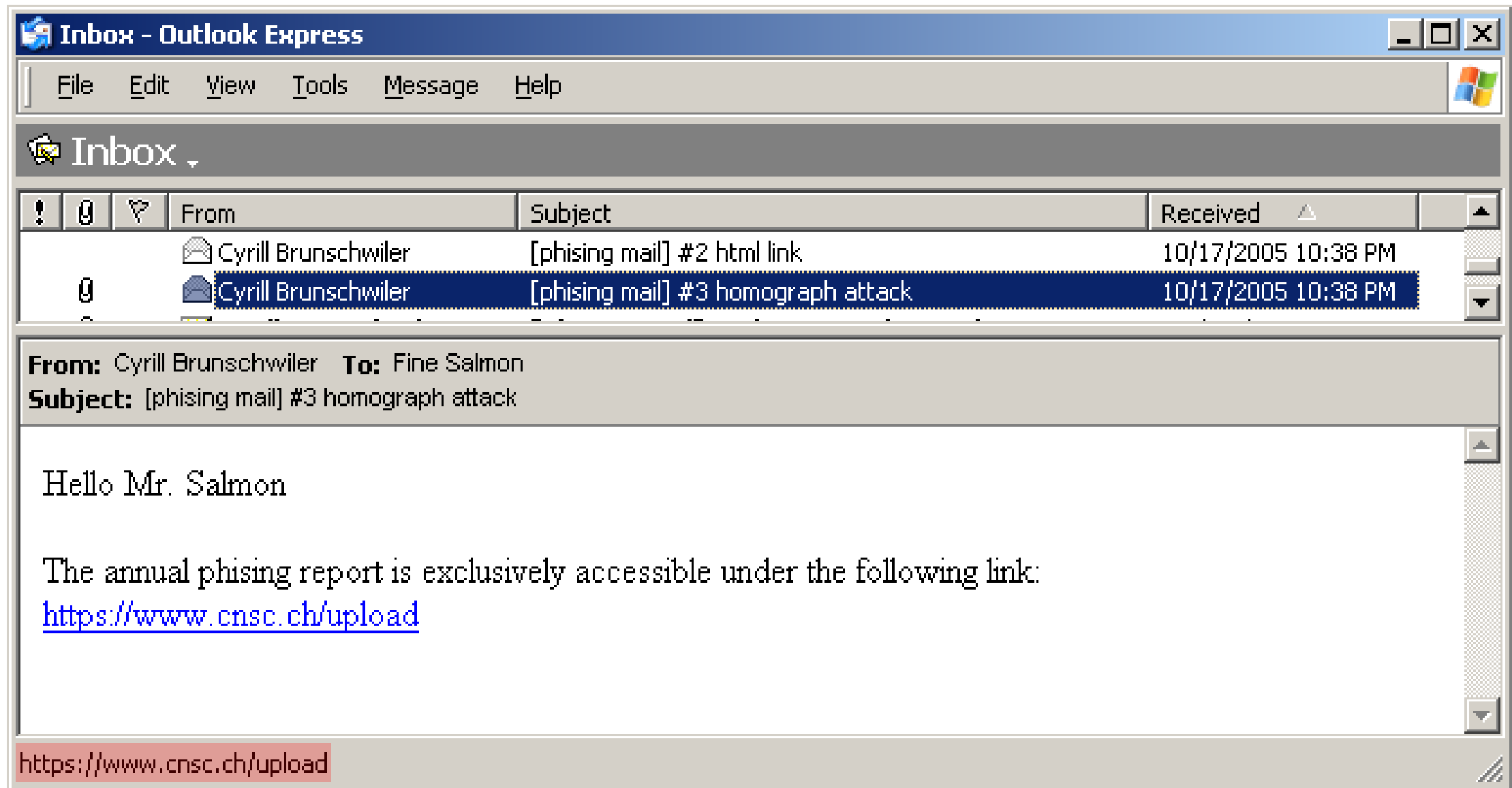
Why the victim is visiting the fake site



Why the victim is visiting the fake site

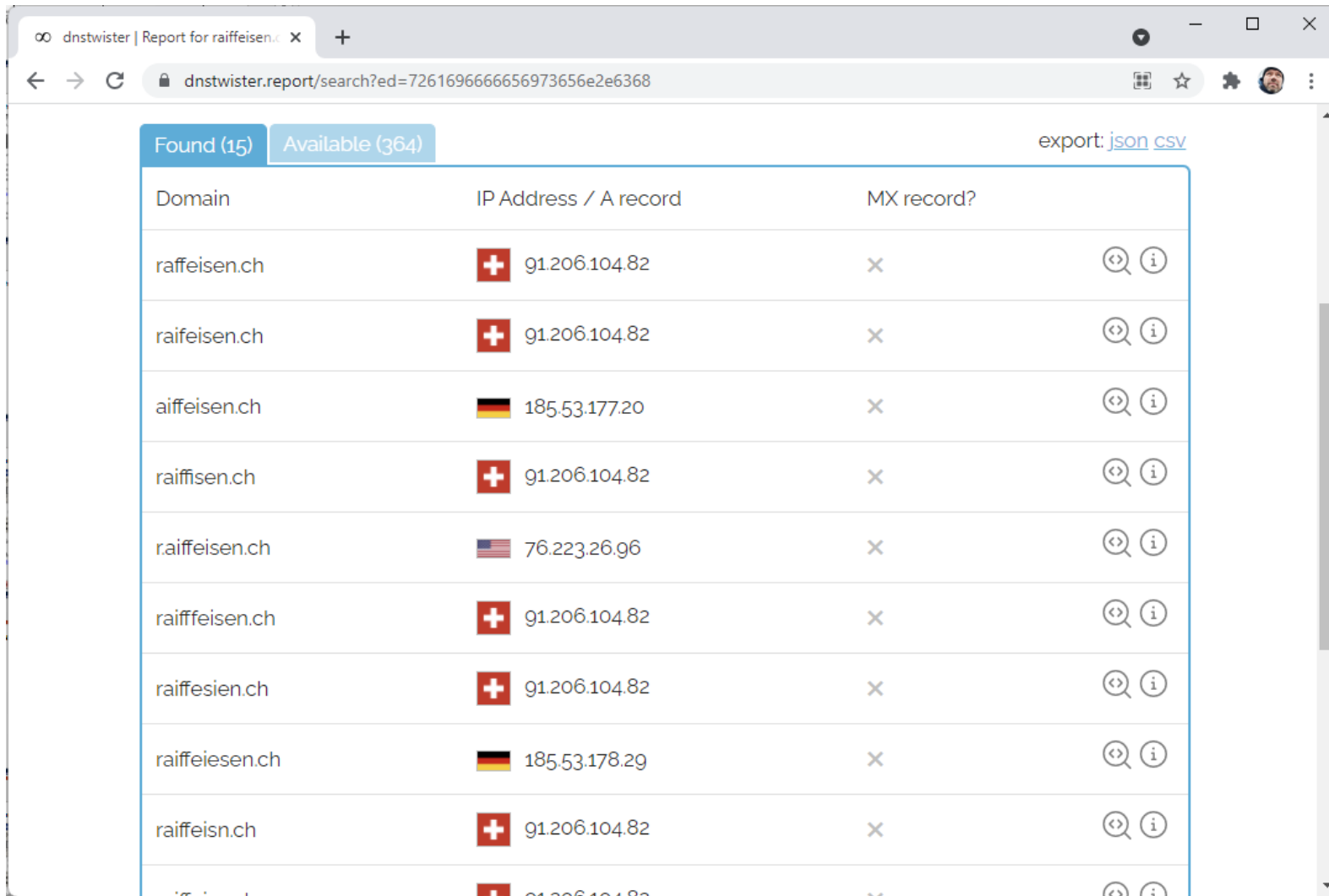


Homograph Attack (cnsc instead of csnc)












DNSTwist

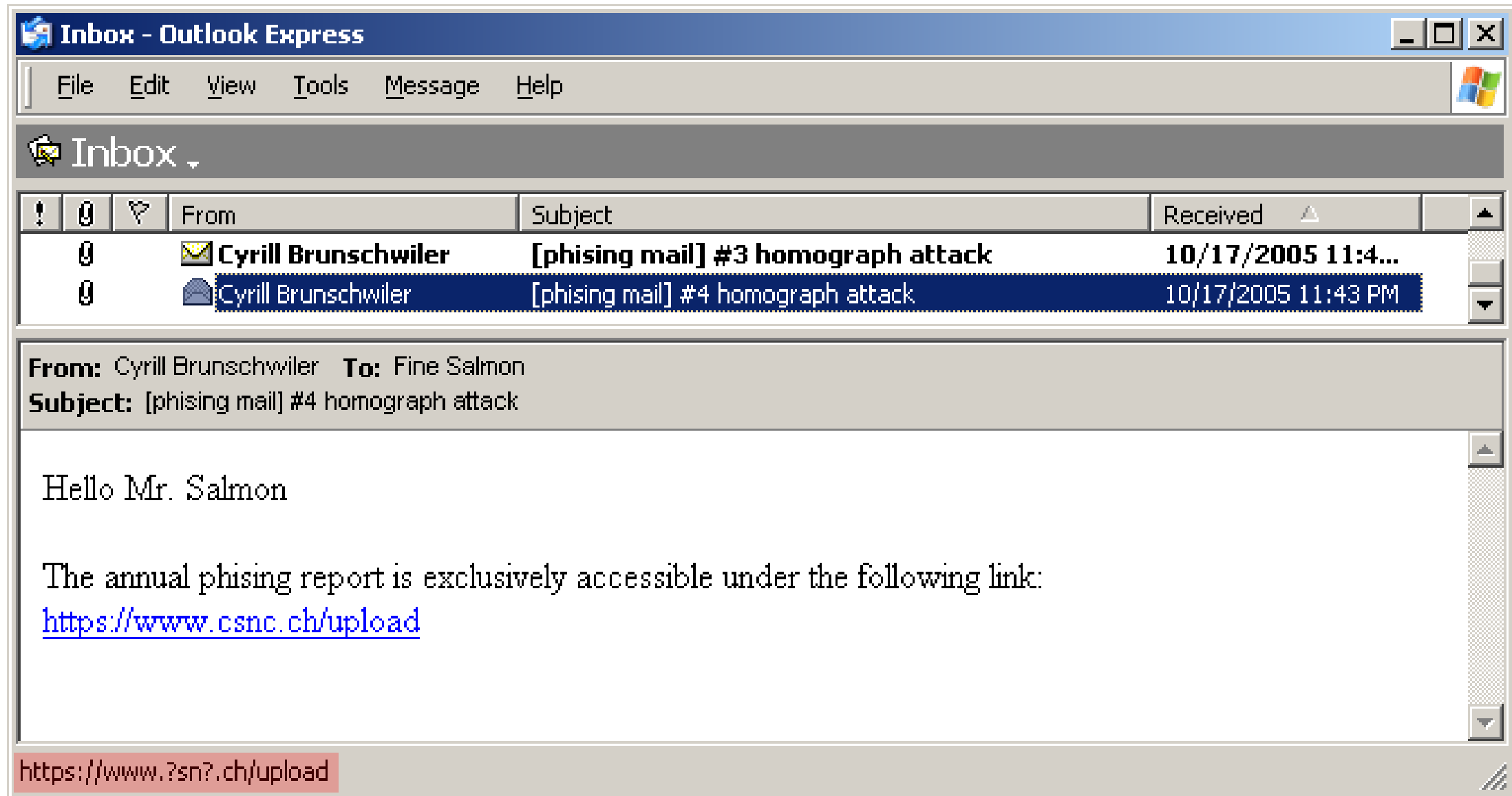
<https://dnstwister.report/>



Found (15) Available (364) export: [json](#) [csv](#)

Domain	IP Address / A record	MX record?
raiffeisen.ch	 91.206.104.82	×
raiffeisen.ch	 91.206.104.82	×
aiffeisen.ch	 185.53.177.20	×
raiffisen.ch	 91.206.104.82	×
raiffeisen.ch	 76.223.26.96	×
raiff Eisen.ch	 91.206.104.82	×
raiffesien.ch	 91.206.104.82	×
raiffeiesen.ch	 185.53.178.29	×
raiffeisn.ch	 91.206.104.82	×

Homograph Attack (punny code)



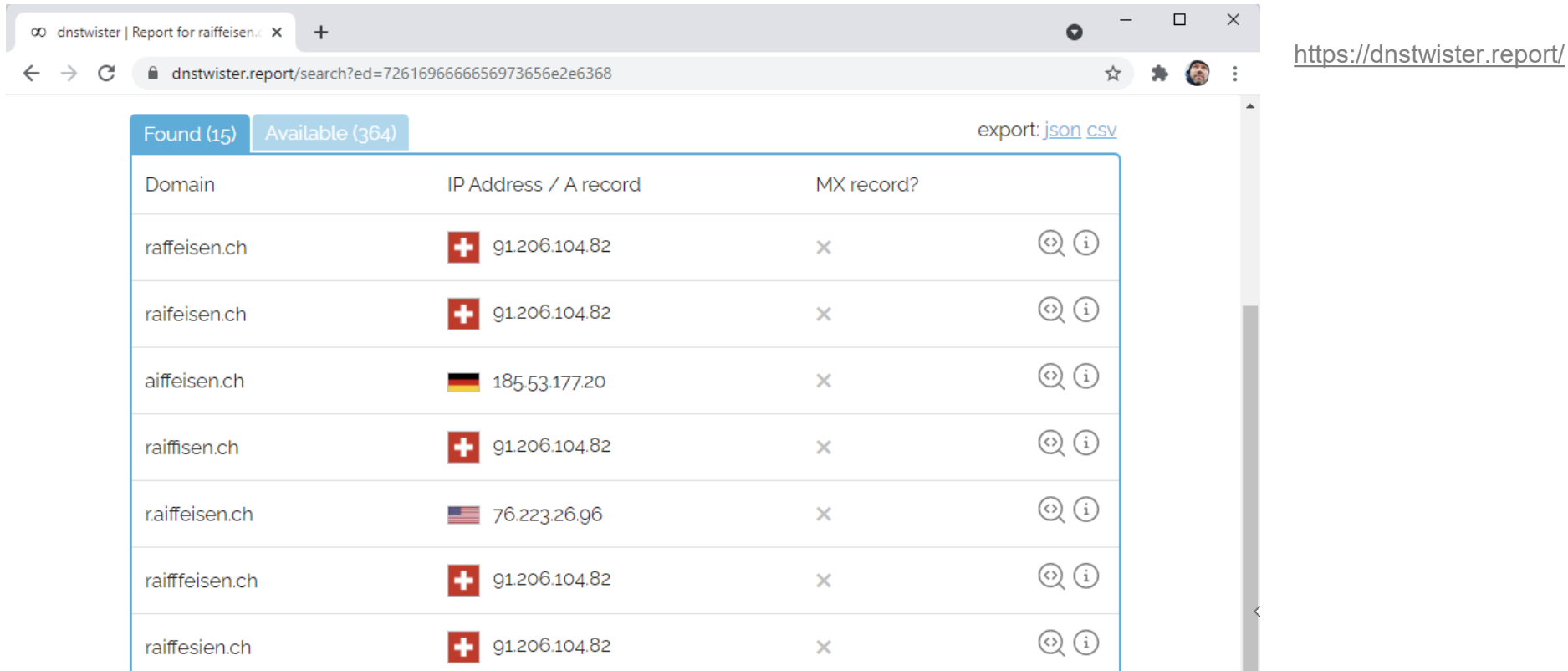
Mitigation Offline Phishing

User Awareness Training

2FA - Two factor authentication

Monitoring similar domain registrations as the own domain (dnstwists)

Being able to block certain websites or domains in case of emergency










dnstwister | Report for raiffeisen.ch

dnstwister.report/search?ed=72616966666569736556e2e6368

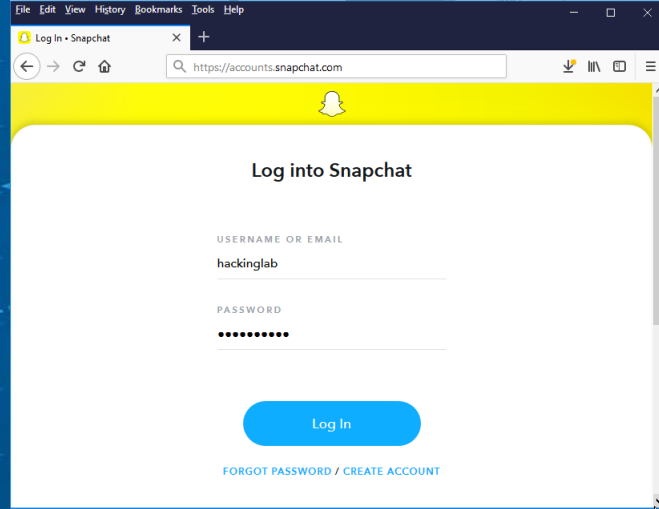
https://dnstwister.report/

Found (15) Available (364) export: [json](#) [csv](#)

Domain	IP Address / A record	MX record?
raiffeisen.ch	 91.206.104.82	×
raifeisen.ch	 91.206.104.82	×
aiffeisen.ch	 185.53.177.20	×
raiffisen.ch	 91.206.104.82	×
r.aiffeisen.ch	 76.223.26.96	×
raifffeisen.ch	 91.206.104.82	×
raiffesien.ch	 91.206.104.82	×

Online Phishing

Online Phishing



Username
Password

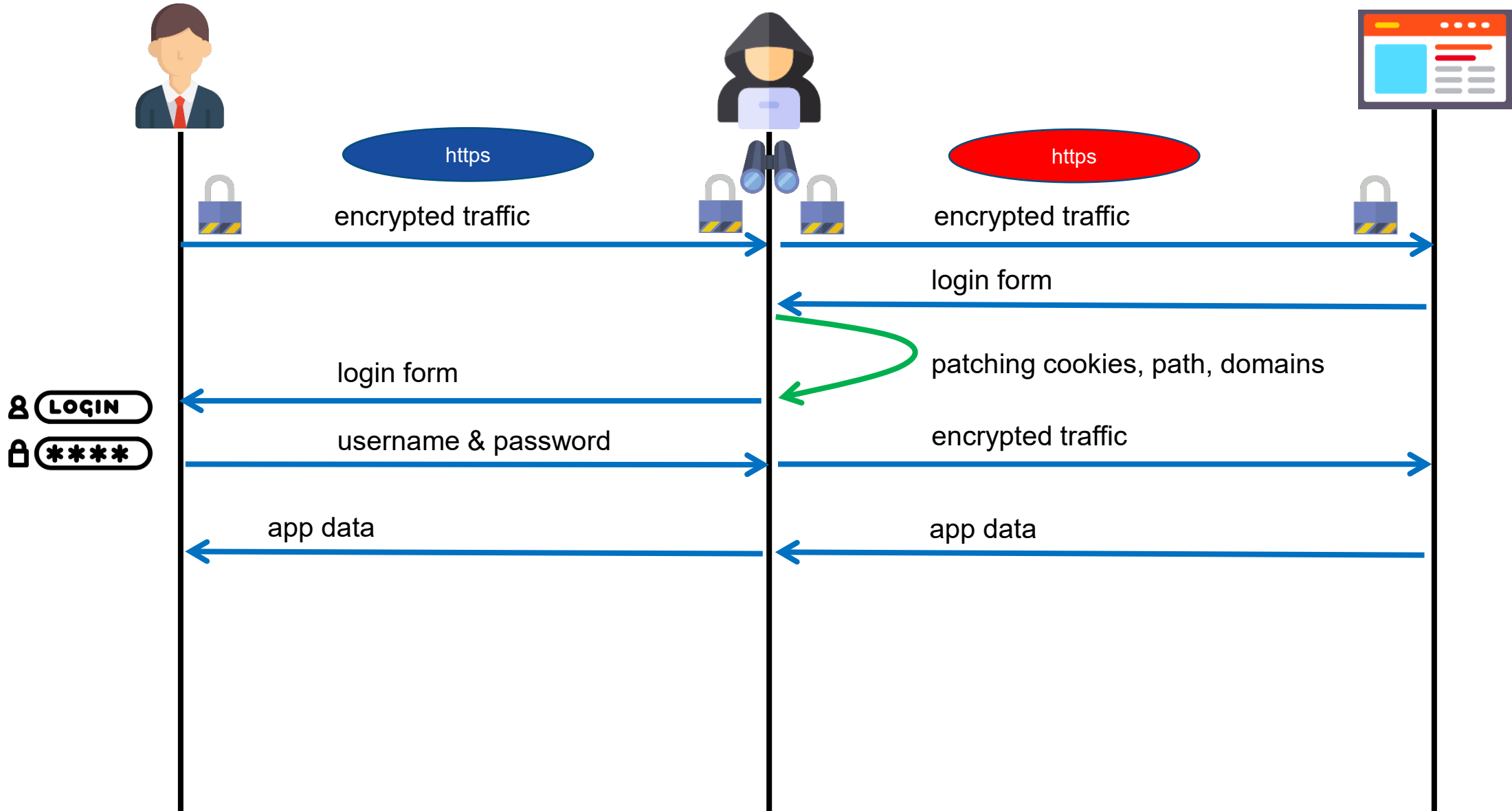


Username
Password

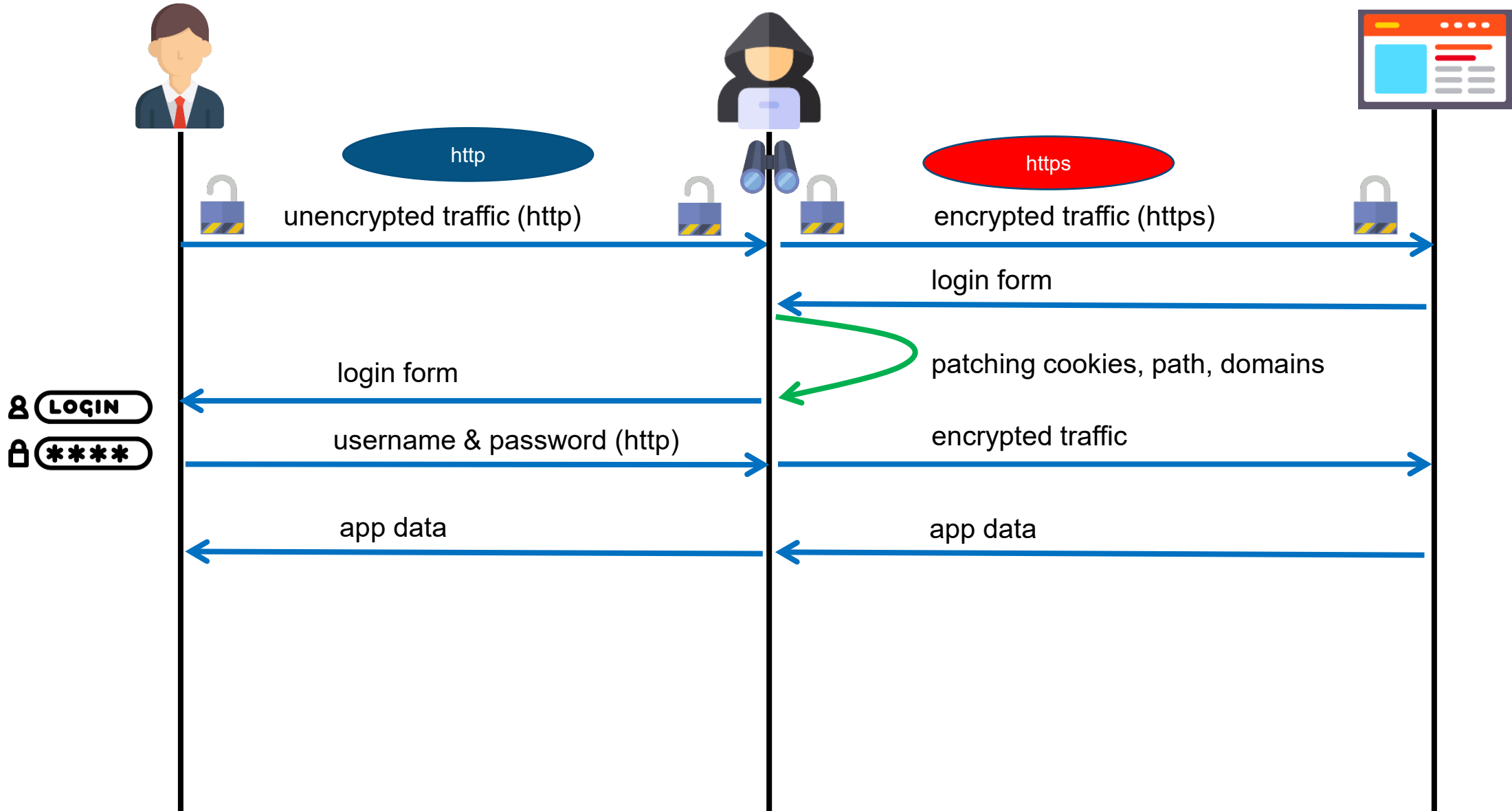
Hacker is «forwarding»
to origin (reverse proxy)



Man in the Middle – Online Phishing – https²https



Man in the Middle – Online Phishing – http²https



Is 2FA protecting against this attack?



No, it is not

HTTPS MitM Mitigation

Certification Transparency

Certificate Transparency Monitoring

Certificate Transparency is an open framework which helps log, audit and monitor publicly-trusted TLS certificates on the Internet. This tool lets you search for certificates issued for a given domain and subscribe to notifications from Facebook regarding new certificates and potential phishing attacks.

Search Subscriptions

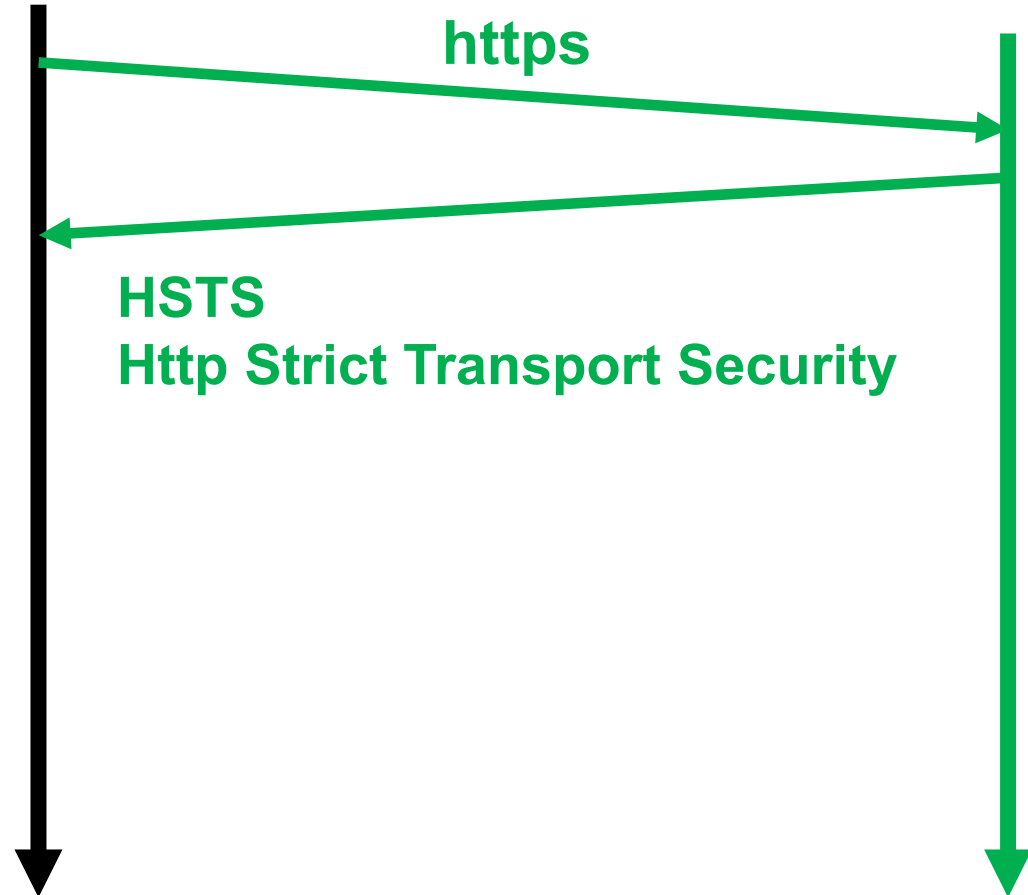
hslu.ch

Domains	Subject	Issuer	Validity	Certificate
hosting.hslu.ch	CN=hosting.hslu.ch	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3	Nov 01, 2018 - Jan 30, 2019	Show Details
hosting.hslu.ch	CN=hosting.hslu.ch	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3	Nov 01, 2018 - Jan 30, 2019	Show Details (CT Precertificate)
gerd.animation.hslu.ch	CN=gerd.animation.hslu.ch	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3	Oct 27, 2018 - Jan 25, 2019	Show Details (CT Precertificate)
gerd.animation.hslu.ch	CN=gerd.animation.hslu.ch	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3	Oct 27, 2018 - Jan 25, 2019	Show Details
jean.animation.hslu.ch	CN=jean.animation.hslu.ch	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3	Oct 27, 2018 - Jan 25, 2019	Show Details
jean.animation.hslu.ch	CN=jean.animation.hslu.ch	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3	Oct 27, 2018 - Jan 25, 2019	Show Details (CT Precertificate)
wiki.animation.hslu.ch	CN=wiki.animation.hslu.ch	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3	Oct 27, 2018 - Jan 25, 2019	Show Details
wiki.animation.hslu.ch	CN=wiki.animation.hslu.ch	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3	Oct 27, 2018 - Jan 25, 2019	Show Details

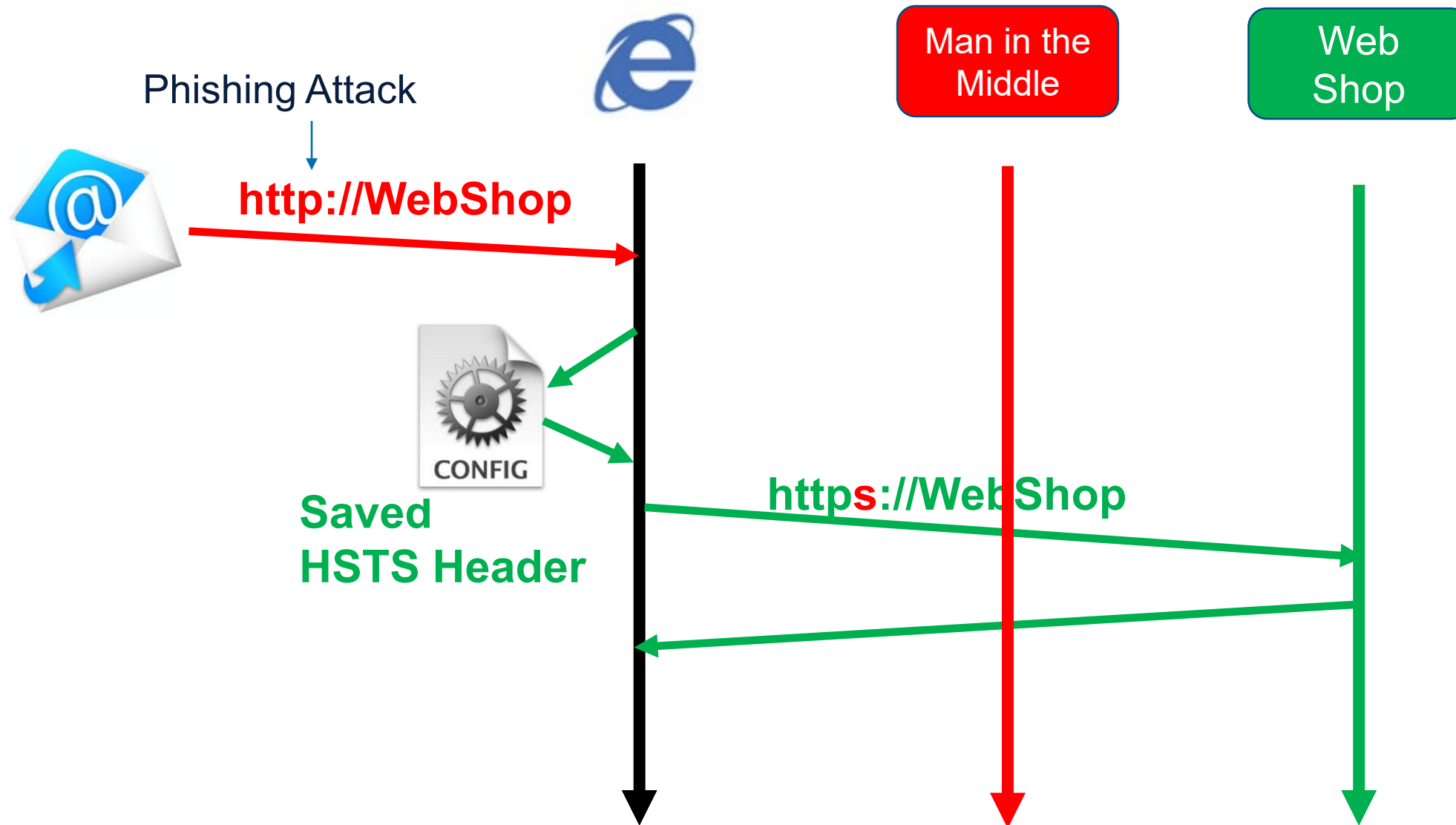
HSTS (http Strict Transport Security)



Saved
HSTS Header

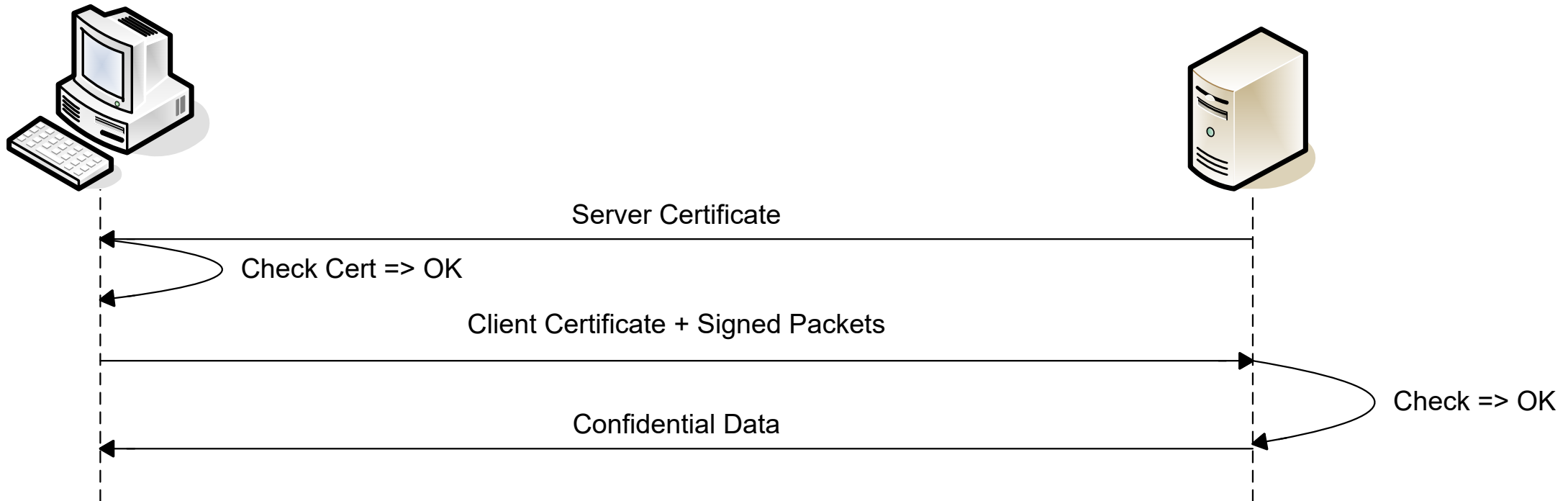


HSTS (http Strict Transport Security)



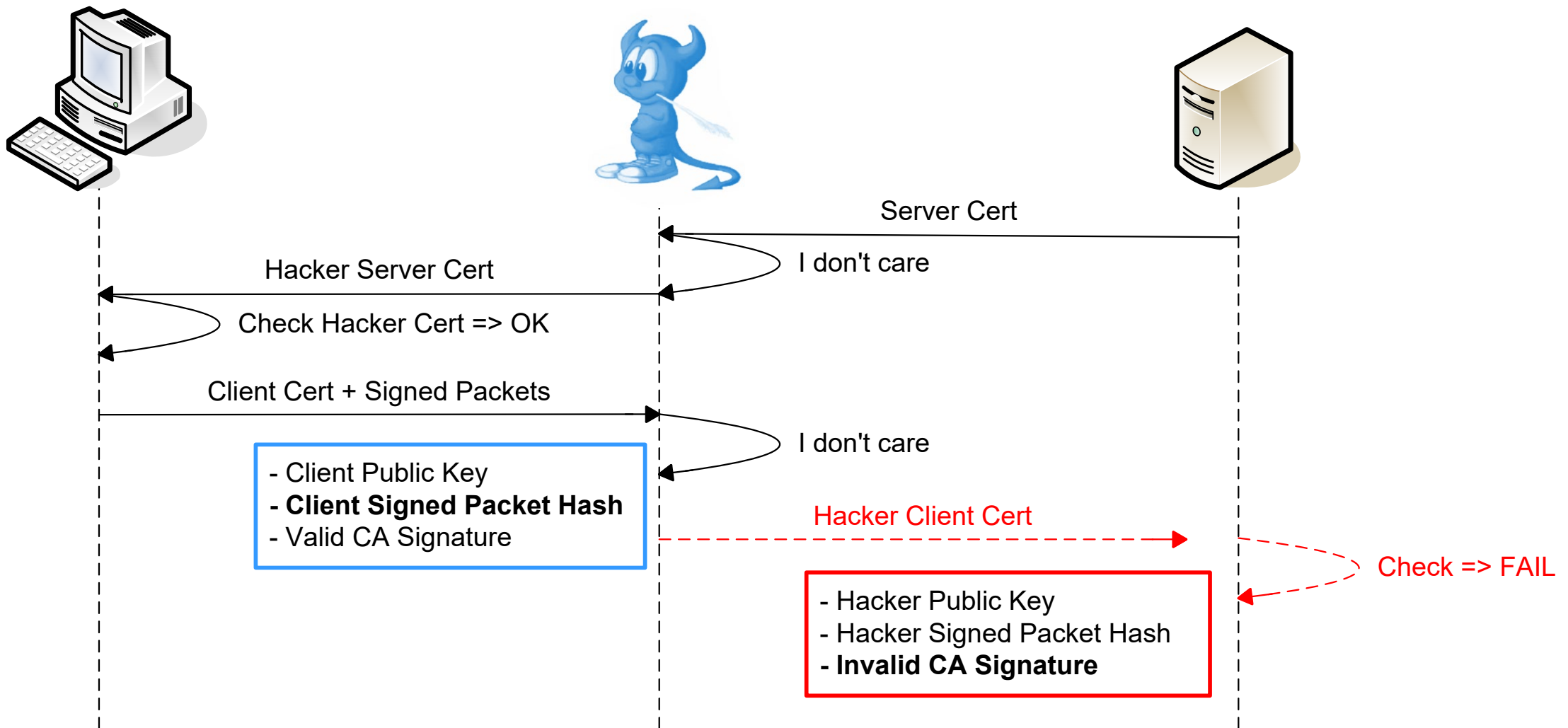
SSL/TLS & Mutual Authentication

Schematic Authentication – use of Client Certificates



SSL/TLS & Mutual Authentication

Man-In-The-Middle Attack fails



MitM Protection – FIDO2

<https://www.youtube.com/watch?v=ce5IHjfYmwQ>

Slides shown in this
video available

FIDO2 Challenge Response Protocol

Key pair (*public key*, *secret key*)

Authenticator



Client



public key

Relying Party



challenge, "**Origin**" (1)



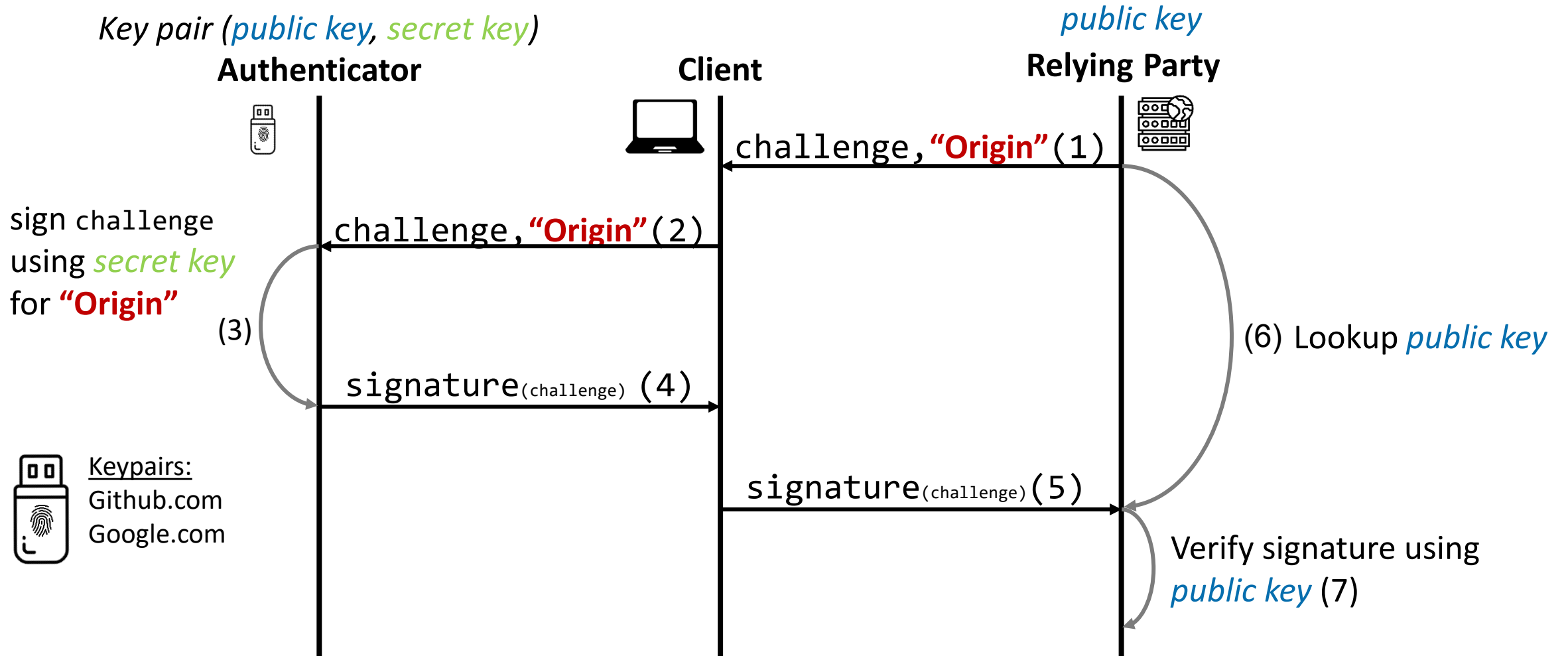
Keypairs:
Github.com
Google.com

26:28 / 37:32

compass-security.com



FIDO2 Challenge Response Protocol



Mitigation Phishing

- Mutual Authentication (Client Certificates, Server Certificates)
- FIDO2
- User Awareness Training
- Monitoring similar domain registrations as the own domain (dnstwists)
- Being able to block certain websites or domains in case of emergency