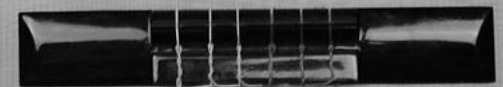


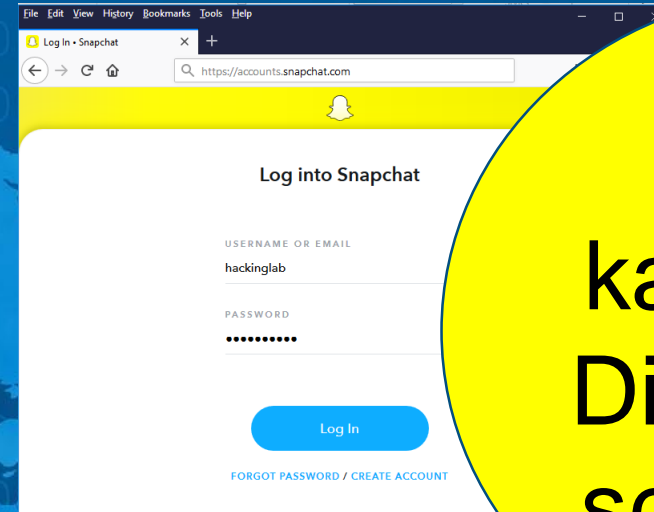
Phishing



Phishing Angriff (Offline)



Benutzername
Passwort



Wie
kannst Du
Dich davor
schützen?

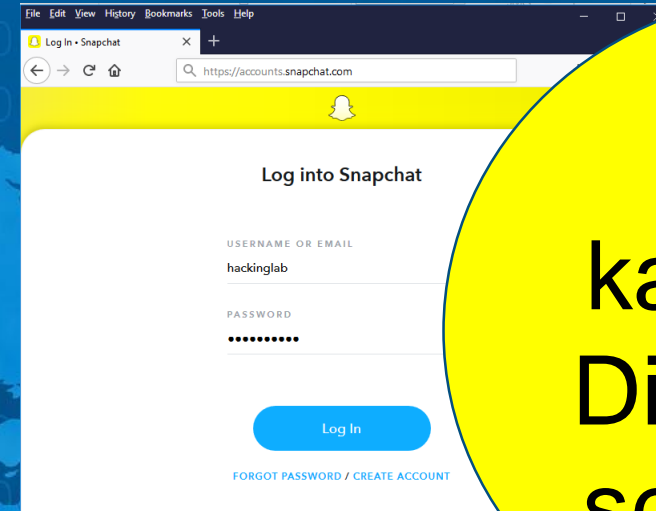
Benutzername
Passwort



Der Hacker erstellt eine
Seite, die genau gleich
aussieht wie das Original



Phishing Angriff (Online)



Wie
kannst Du
Dich davor
schützen?

Der Hacker macht eine
Weiterleitung (keine
Kopie) der Opfer Seite

Wie gut schützt Dich ein langes und komplexes Passwort, wenn jemand auf einen Phishing Angriff reinfällst?

Da Du Dein Passwort bei der fremden Seite eingibst und der Hacker dieses mithört, ist in diesem Fall egal, wie gut Dein Passwort ist. Du gibst es ja ein, der Hacker liest mit

Schützt Dich ein zweiter Faktor bei der Anmeldung (SMS) im Falle von Phishing?

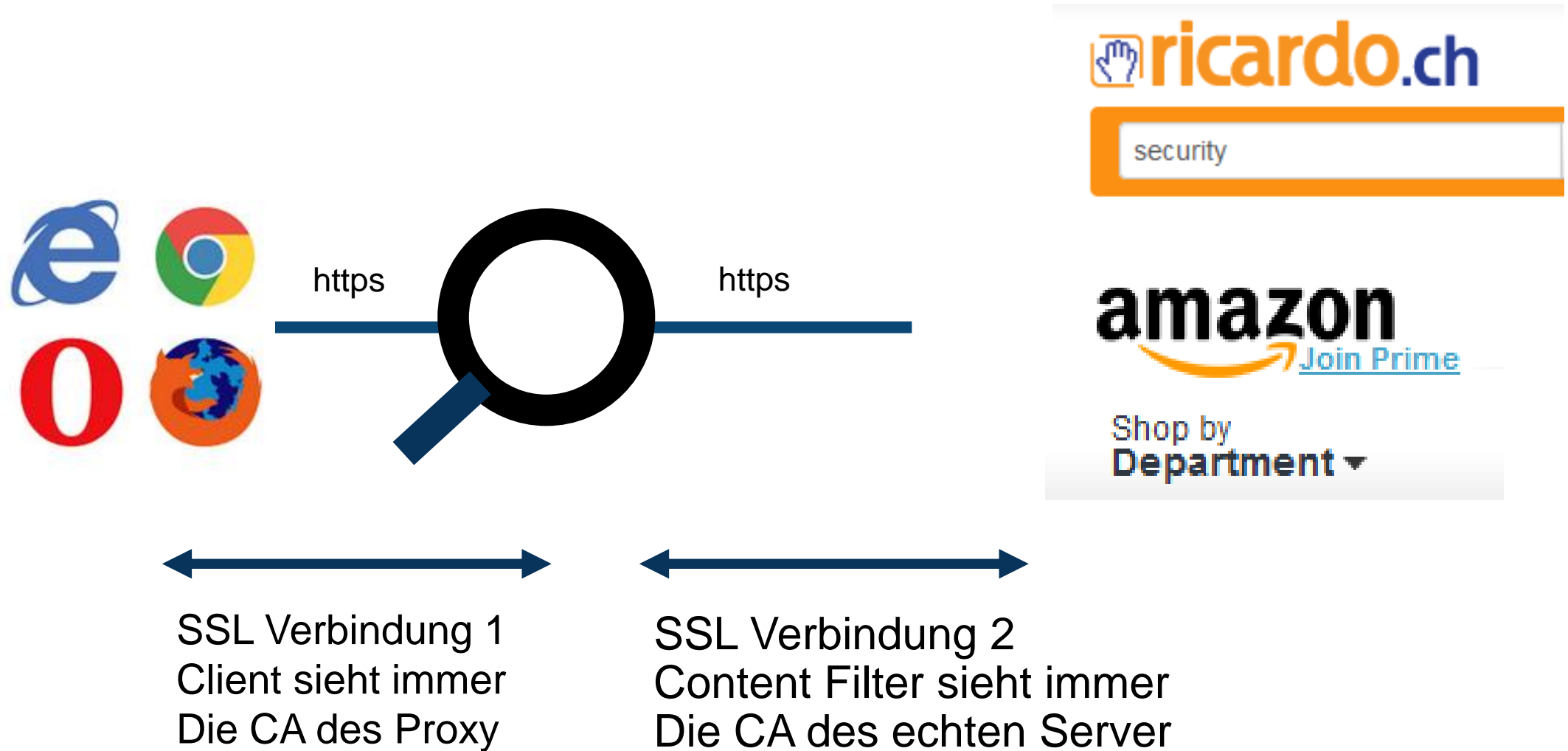
Es kommt darauf an....
Bei Online Phishing sicherlich nicht

Wie kann der Benutzer bemerken, dass er auf einer Phishing Seite ist?

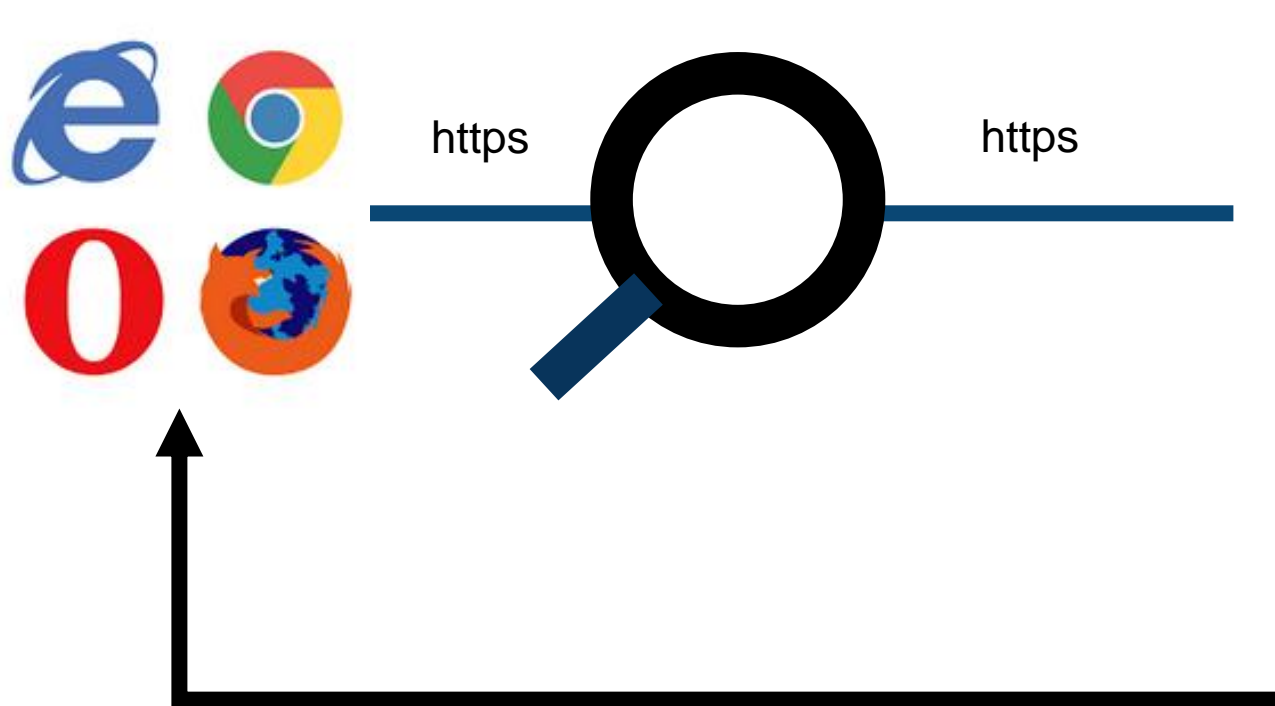


Überprüfung der **URL**
Überprüfung **https**

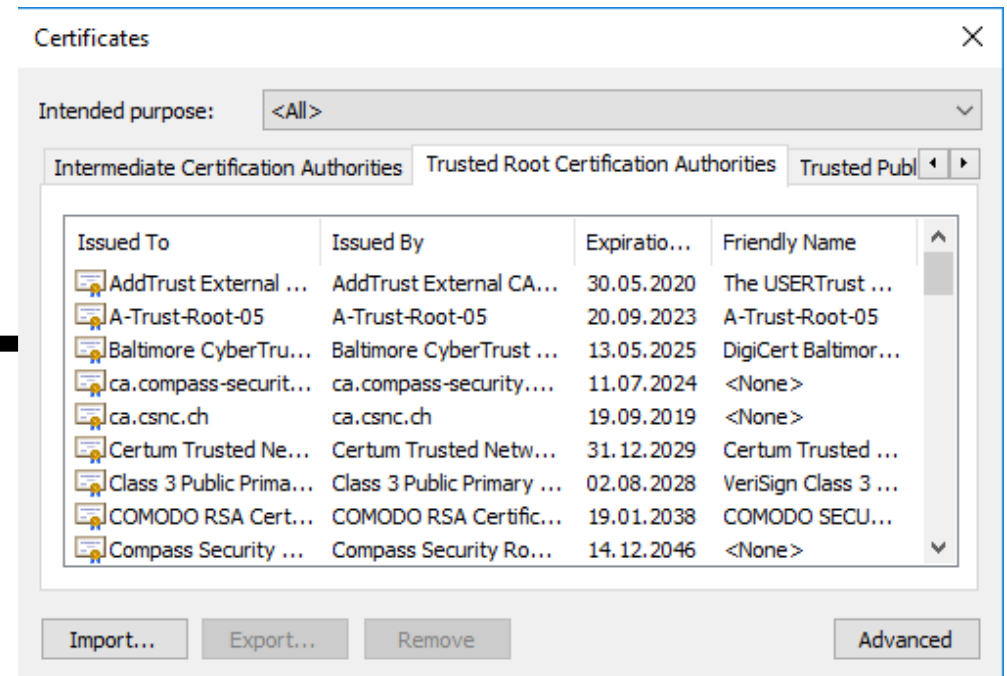
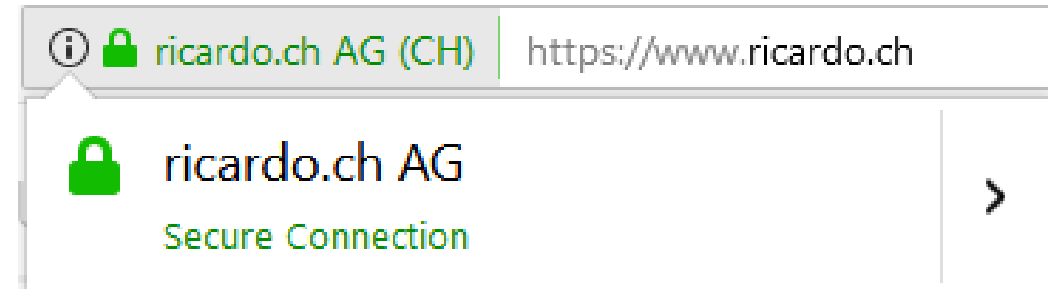
Online Phishing ist dasselbe Prinzip wie der Web Content Filter



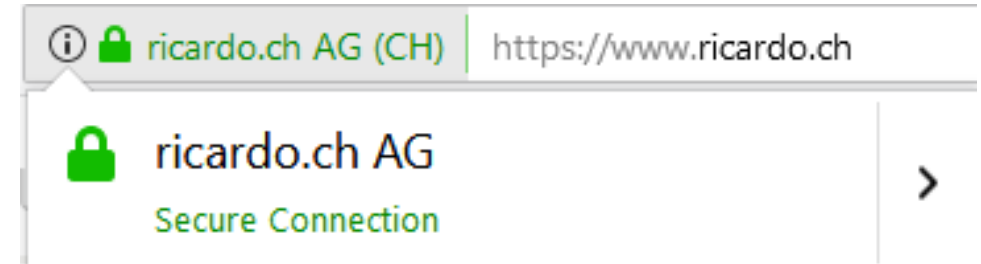
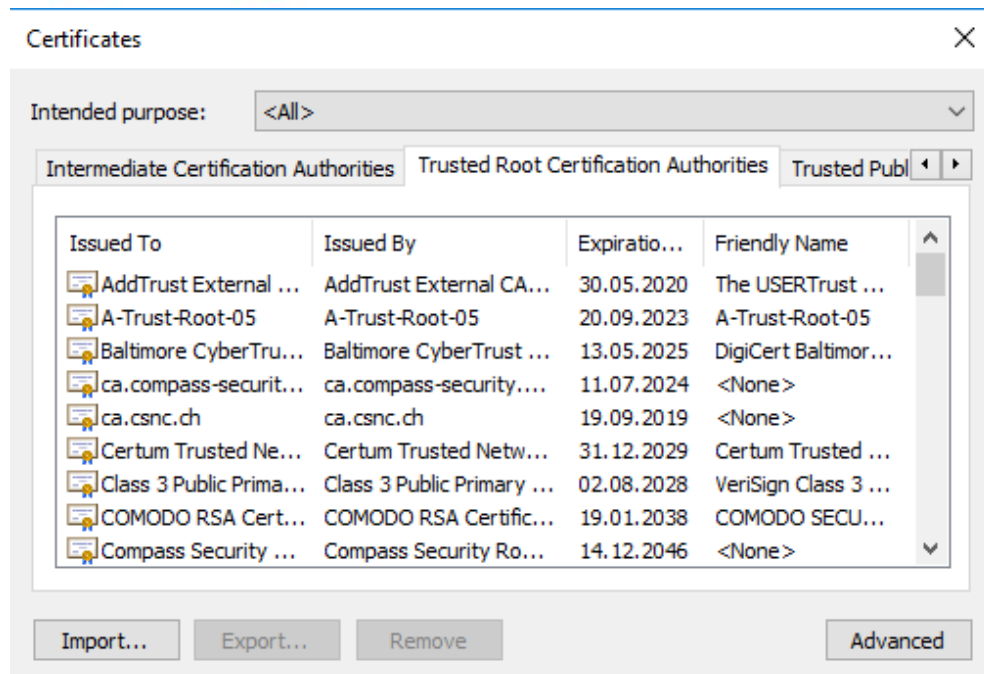
Online Phishing ist dasselbe Prinzip wie der Web Content Filter



Keine Warnung des Benutzers in diesem Fall, wenn die CA welches das TLS Certificate für die Webseite ausgestellt hast als vertrauenswürdige CA im PC hinterlegt ist

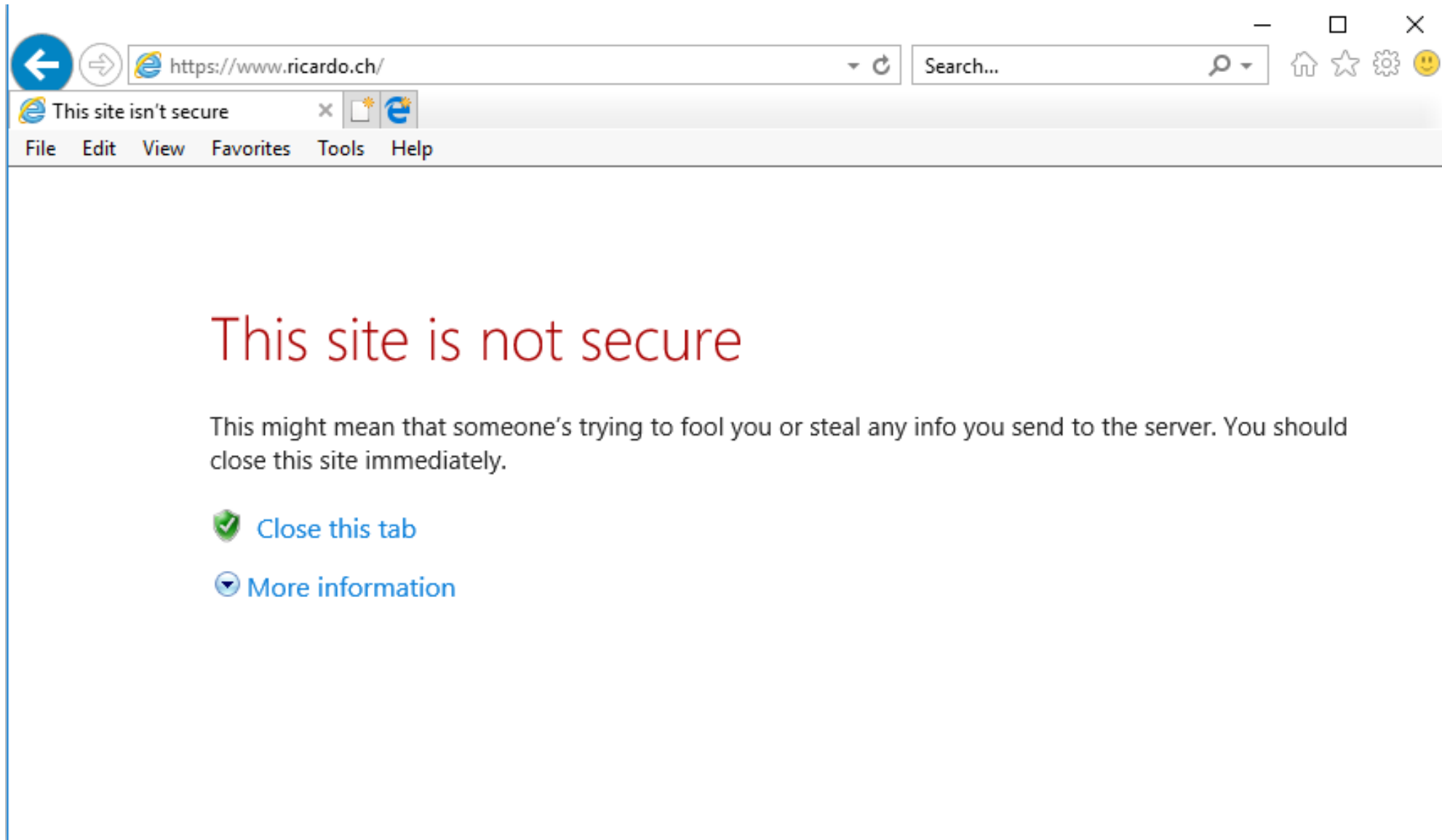


Funktionsweise Content Filter in der Firewall



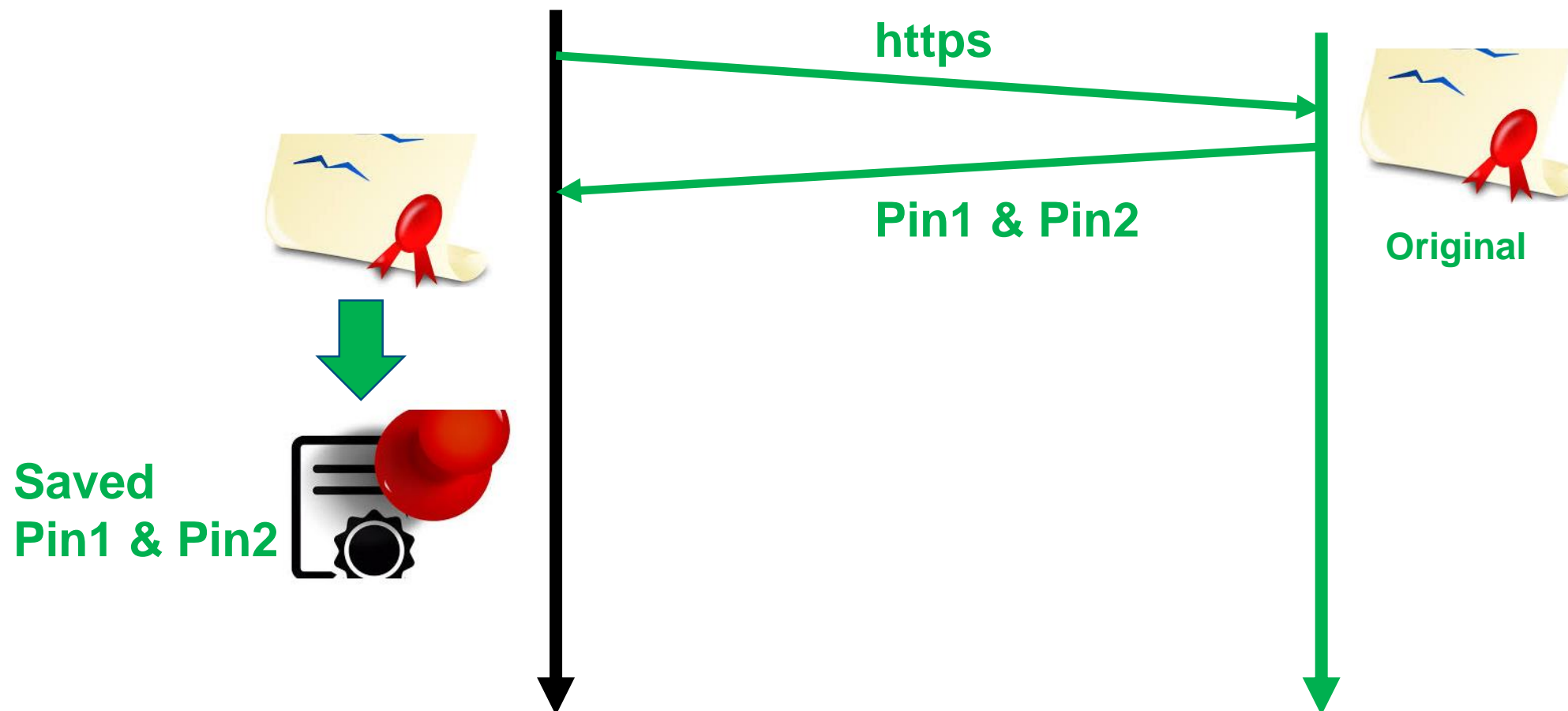
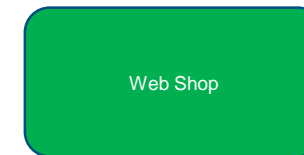
Kennen Sie diese Fehlermeldung?

Wenn die CA nicht im Trusted CA Store gespeichert ist ...

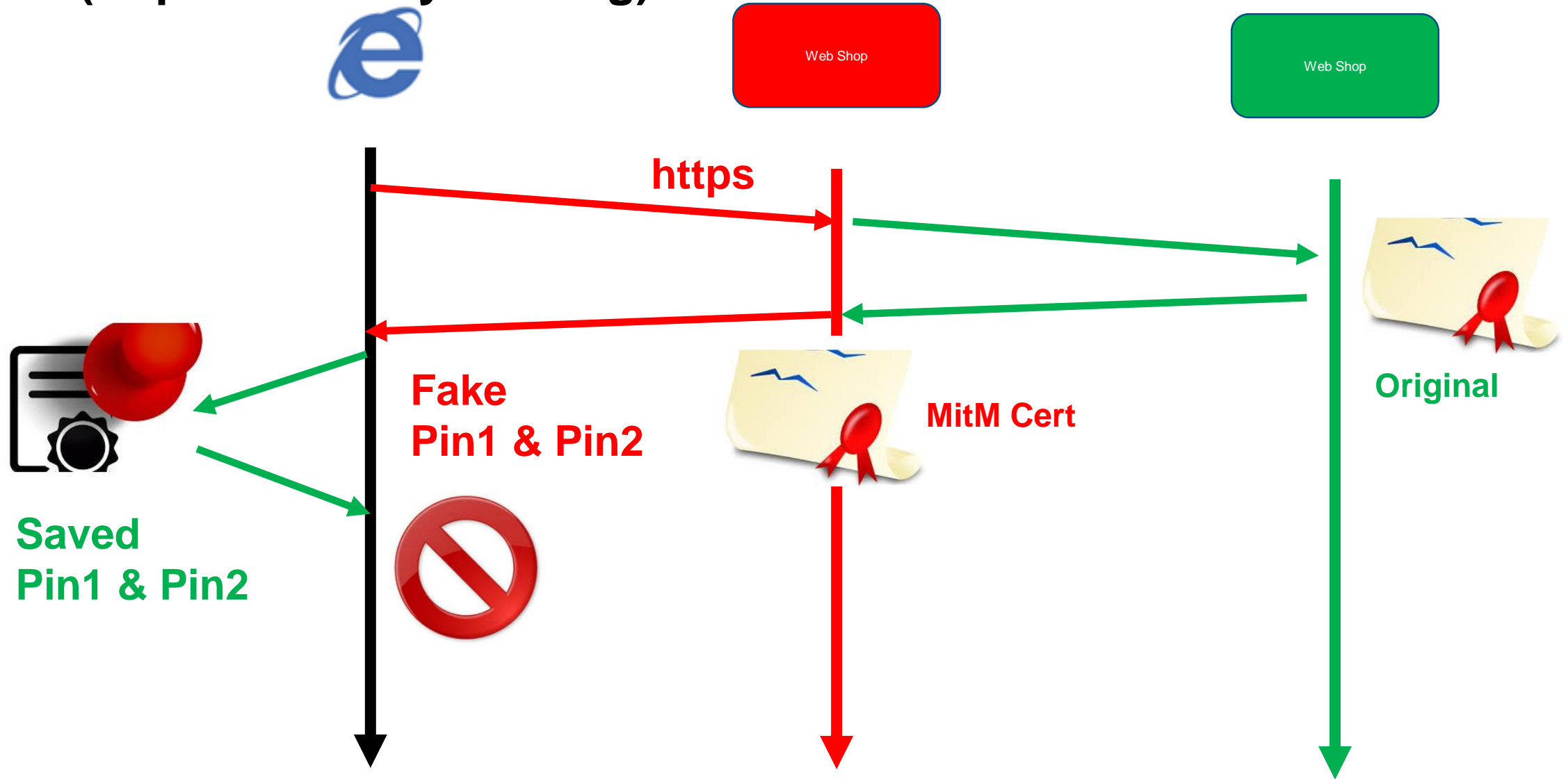


Schutz vor SSL MitM

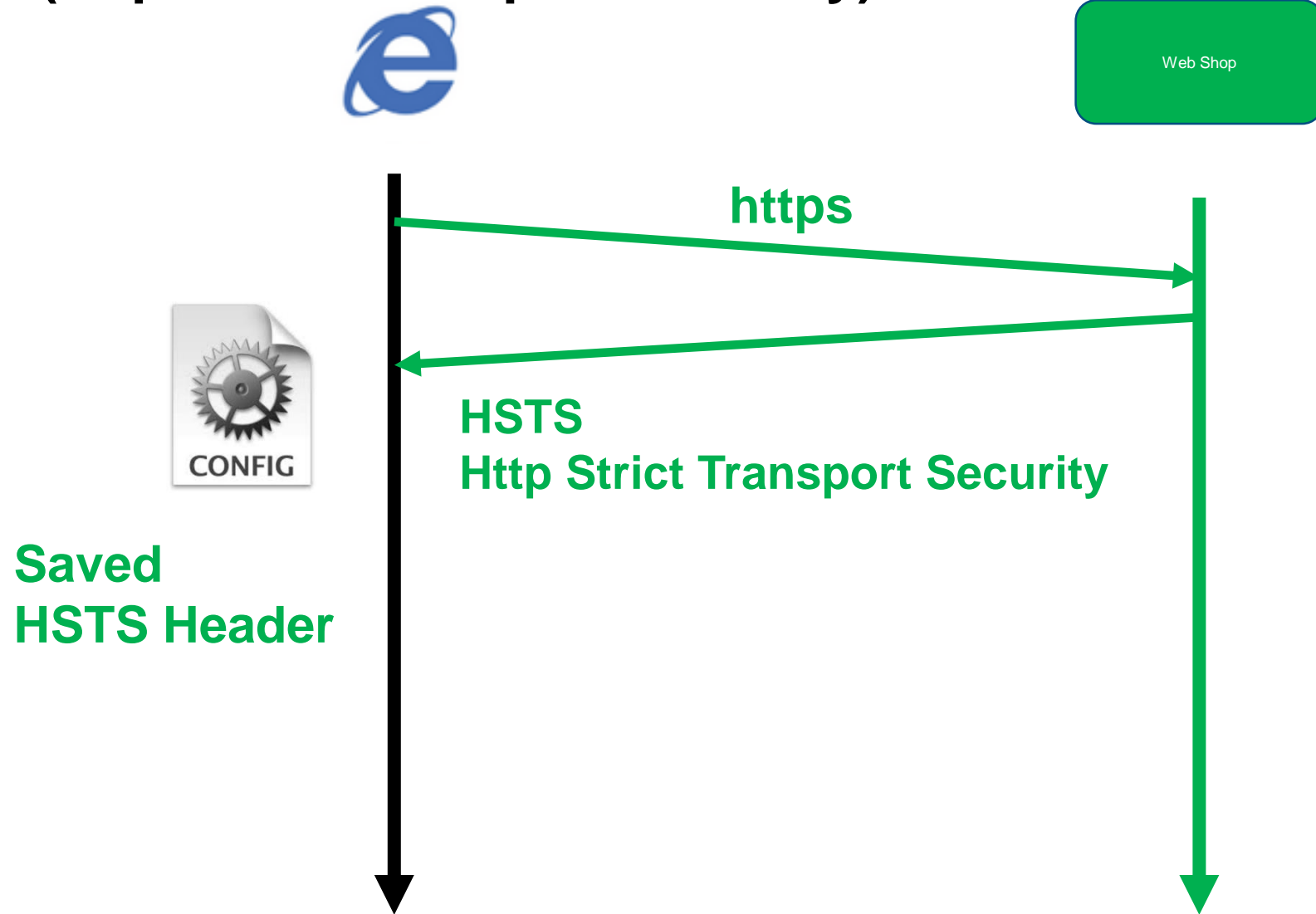
HPKP (http Public Key Pinning)



HPKP (http Public Key Pinning)



HSTS (http Strict Transport Security)



HSTS (http Strict Transport Security)

HTTP, kein HTTPS



http://WebShop



**Saved
HSTS Header**

https://WebShop

Man in the Middle

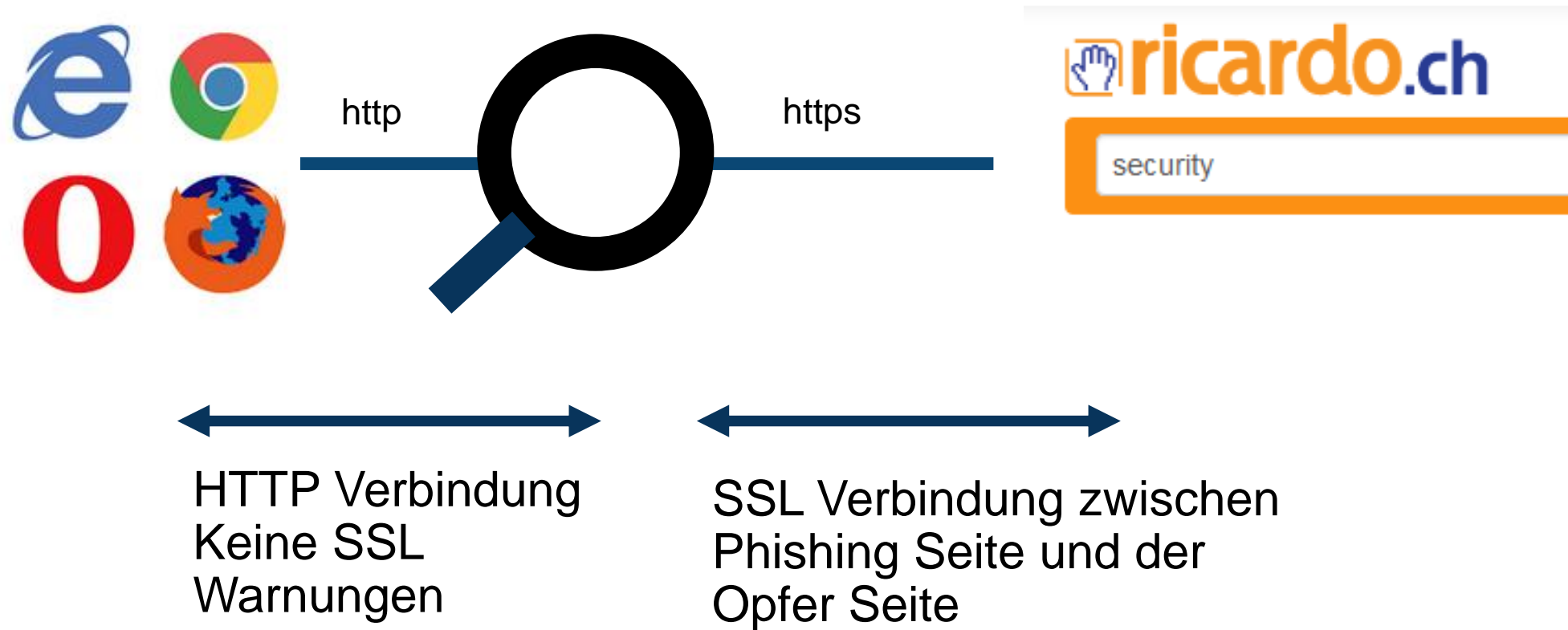
Web Shop

Was heisst das für Hacker?

Falls man einen Virus auf einem PC des «Opfers» hat, dann wäre es wohl geschickt, man würde präventiv einen Eintrag einer «Hacked CA» in den PC konfigurieren. Das würde später die Warnungen im Browser deaktivieren.

Phishing Seiten ohne SSL anbieten. Dann gibt es auch keine SSL Warnung
(Reverse Proxy Case)

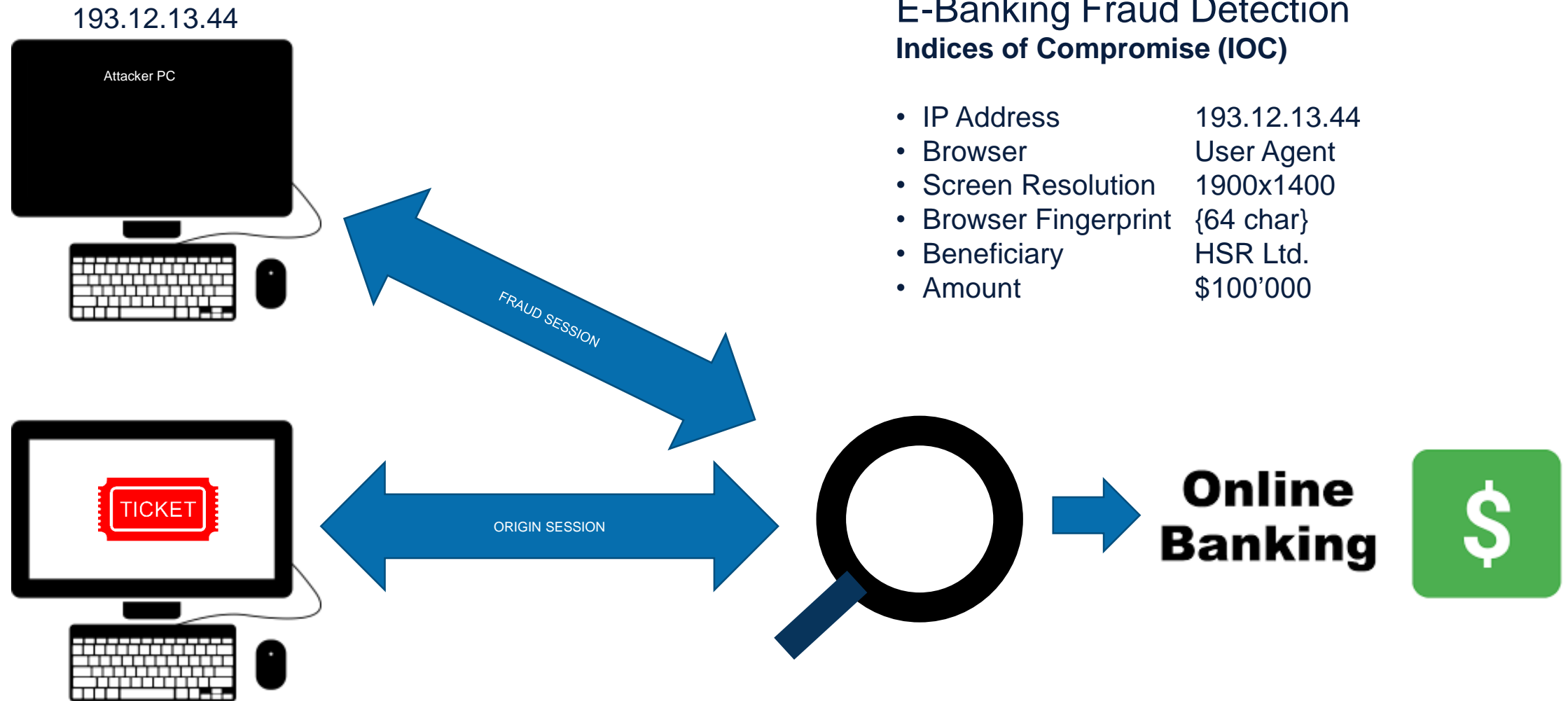
Phishing Seite ohne SSL?



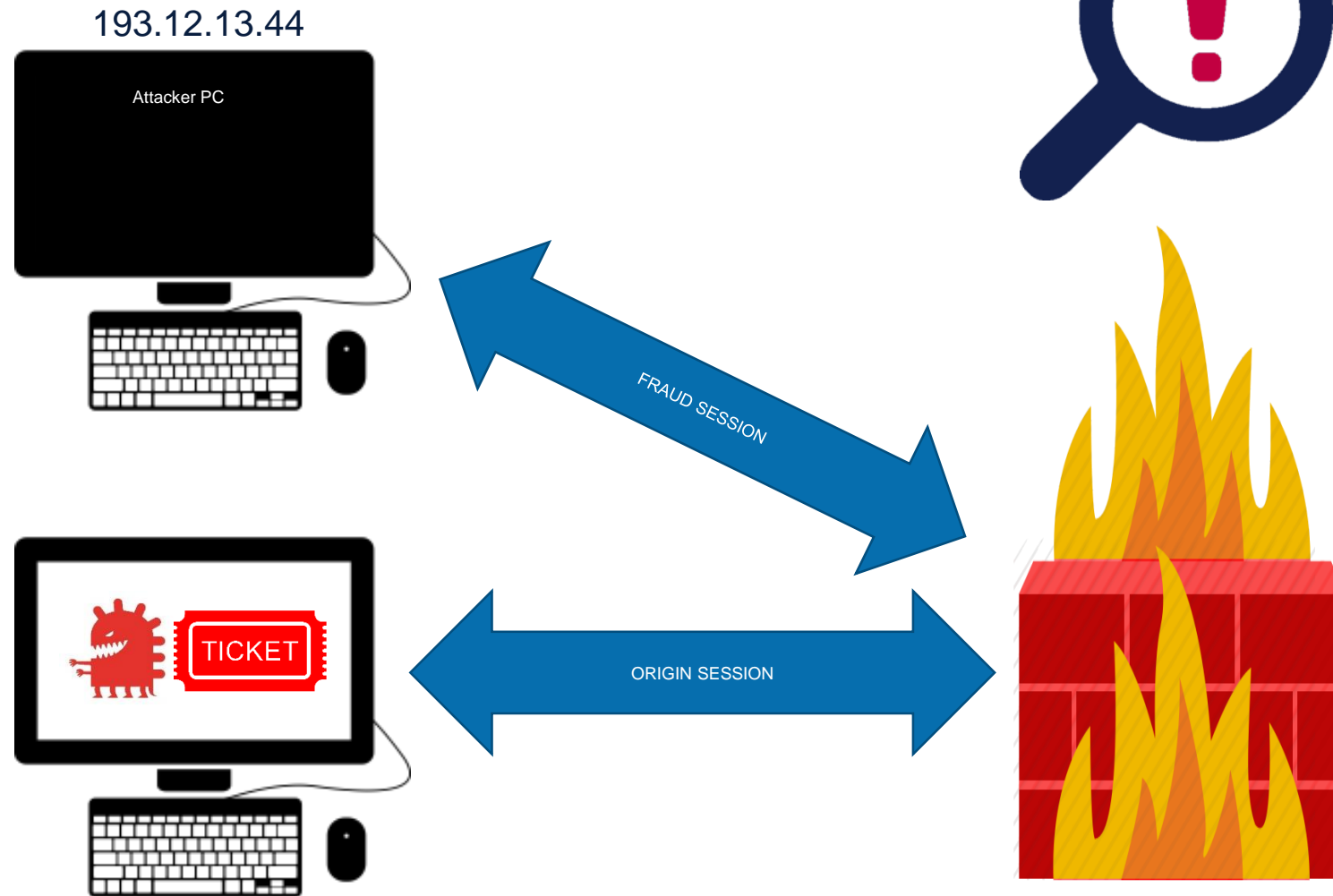
Erkennen von Phishing Angriffen

Fraud Detection

E-Banking Online Phishing Angriffe



E-Banking Attack Session Hijacking



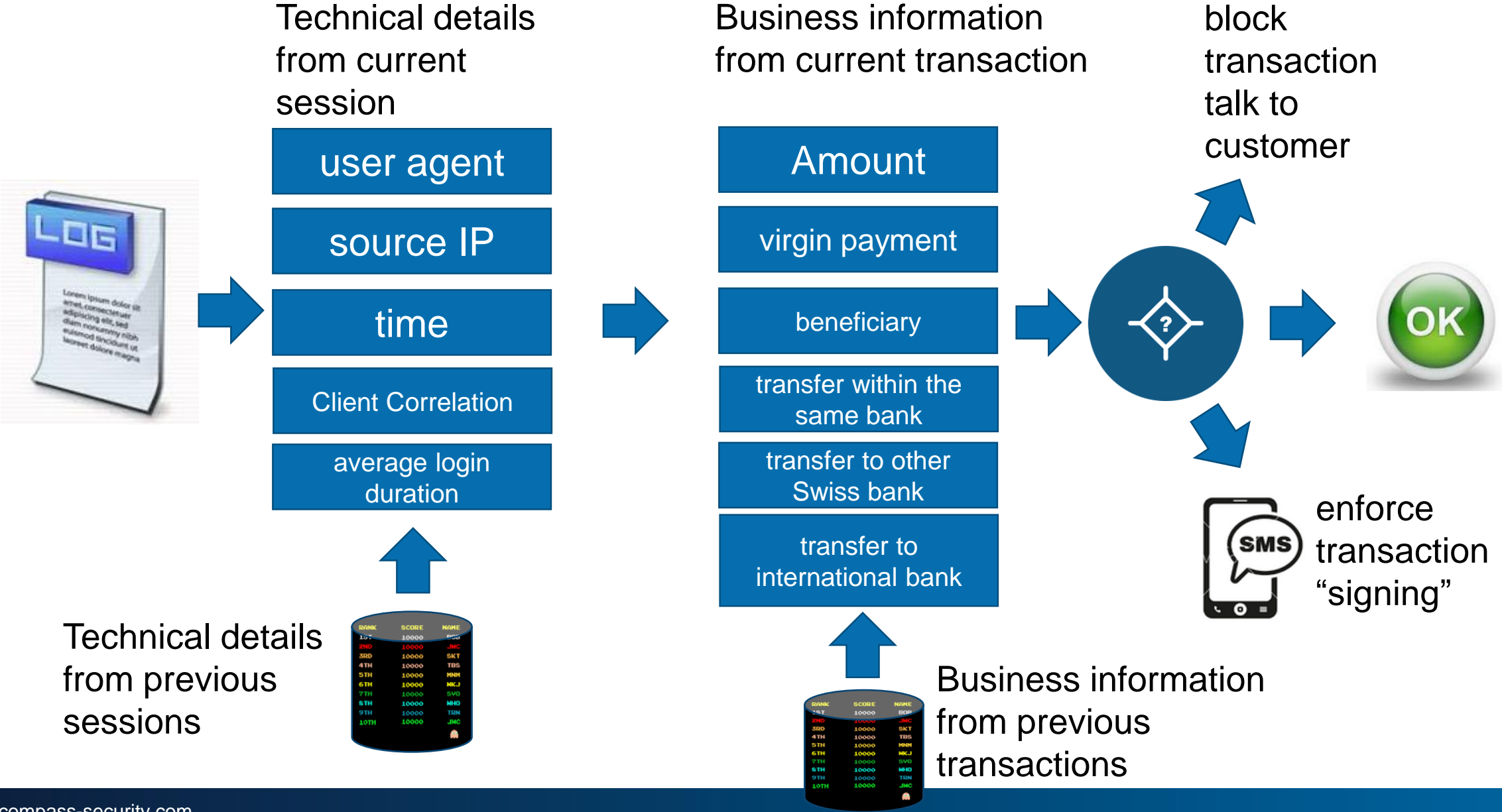
E-Banking Fraud Detection Indices of Compromise (IOC)

- | | |
|-----------------------|--------------|
| • IP Address | 193.12.13.44 |
| • Browser | User Agent |
| • Screen Resolution | 1900x1400 |
| • Browser Fingerprint | {64 char} |
| • Beneficiary | HSR Ltd. |
| • Amount | \$100'000 |

**Online
Banking**



Fraud Detection System

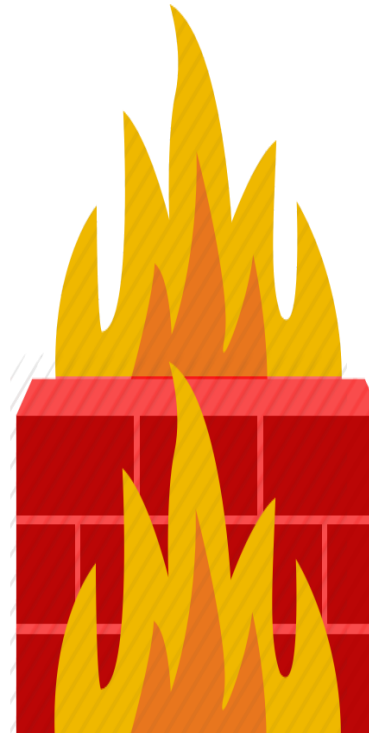
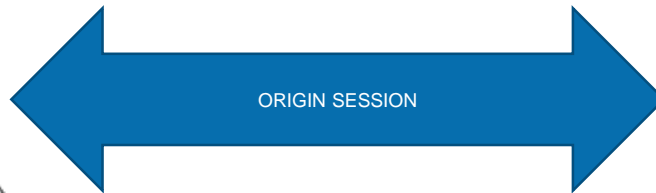
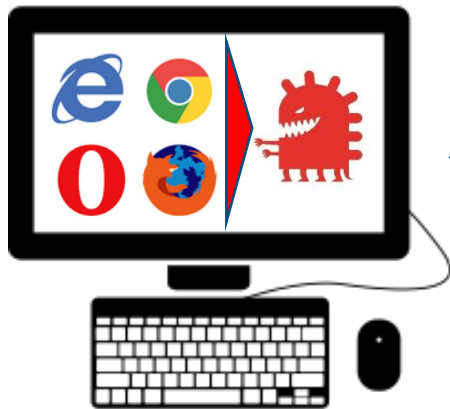


Man-in-the-Browser Attack



E-Banking Fraud Detection Indices of Compromise (IOC)

- Clickstream Analysis
- Outliner Detection
- Keystroke Typing Speed
- URL Frequency Analysis



**Online
Banking**



