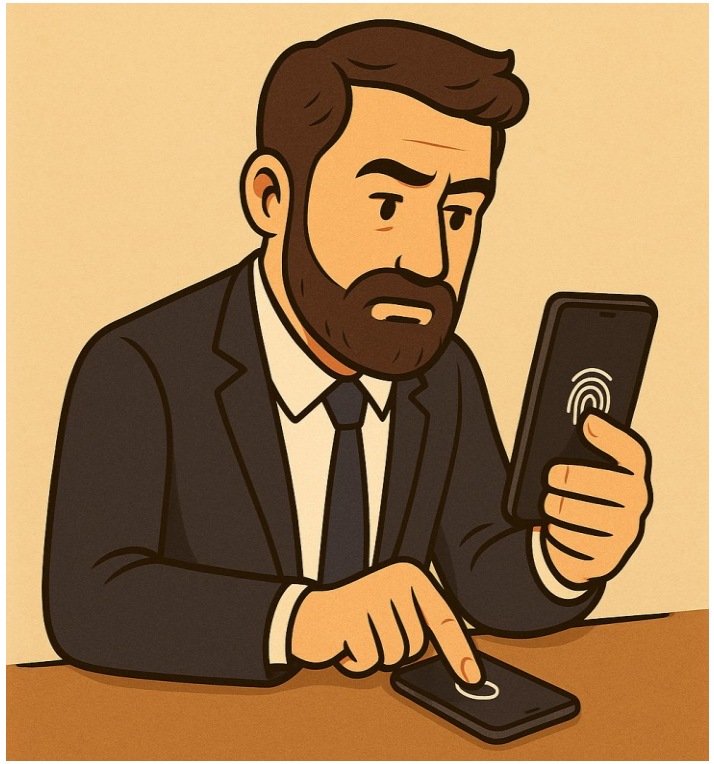
Authentisierung: Grundlagen und Perspektiven

Simran Tinani

cnlab Herbsttagung 2025 – FIDO2: einfach und sicher
Gleisarena, Zürich, 3. September 2025

cnlab

„Glaub mir, ich bin's wirklich!“ Authentisierung ist ein zeitloses Problem



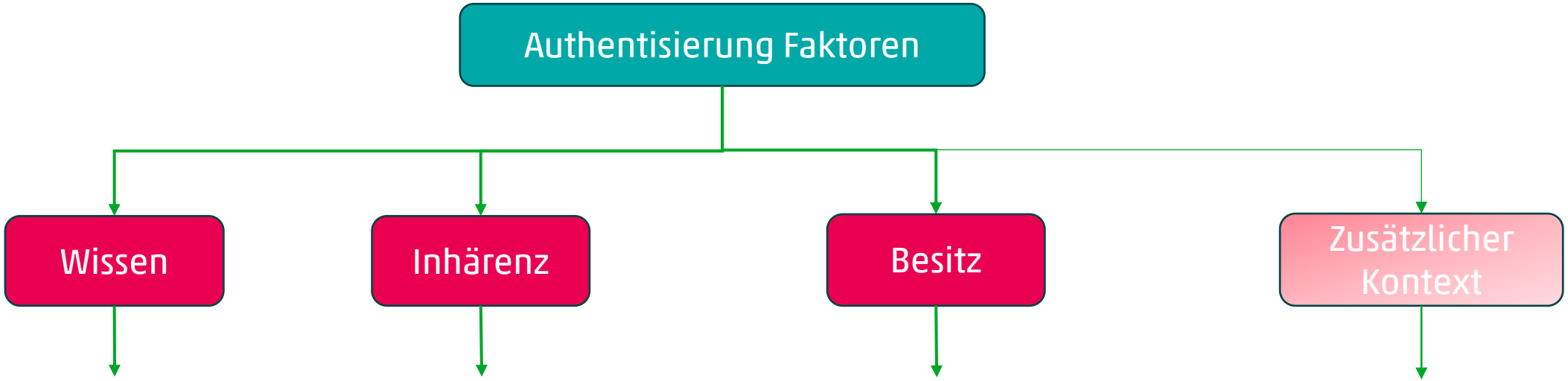
Ein heutiger Mensch authentisiert sich mit dem Fingerabdruck

Ein babylonischer Schreiber drückt vor 5.500 Jahren sein Siegel in Ton

Bilder sind KI-generiert.

Gängige Verfahren: Passwörter, Traditionelle MFA

Gängige Verfahren



- Passwort
- PIN
- Sicherheitsfragen

...

- Fingerabdruck
- Gesichtserkennung
- Iriserkennung
- Stimmerkennung

...

- OTP (Hard/Soft-Token, SMS)
- Push-Benachrichtigung
- Passkey
- Digitales Zertifikat (Smartcard, Gerät)

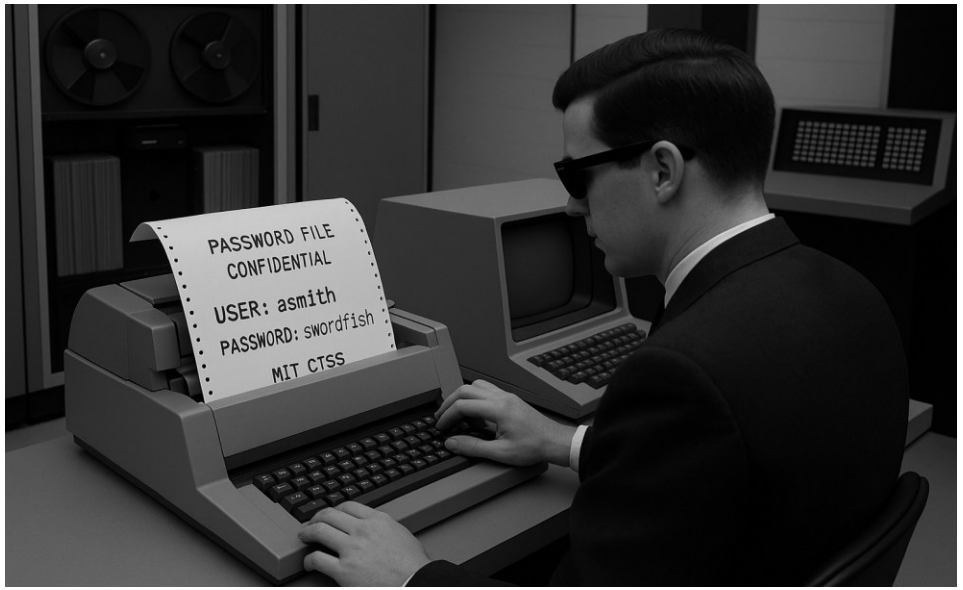
...

- GPS-Standort
- IP-Addresse
- Zeitzone
- Tippmuster, Mausmuster
- Touchscreen-Verhalten

...

Passwörter: Leicht zu merken heisst leicht zu knacken

- **1961**: MIT-Betriebssystem CTSS führte als erstes Login-Kommando Passwort-Abfrage ein.
- **1962:** Ein Nutzer entdeckt, wie man das Passwortverzeichnis ausdrucken kann.
- Seitdem läuft's mit der IT-Sicherheit… so mittel.

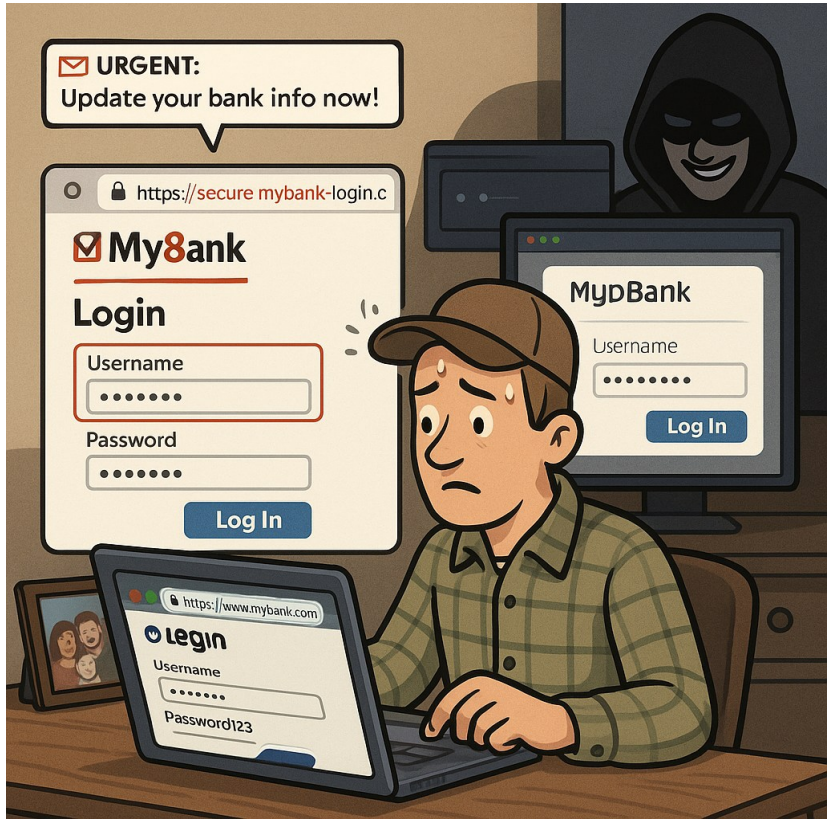


Allan Scherr holte sich per manipuliertem Punch-Card-Befehl die komplette Passwortdatei und teilte sie mit Freunden.

Bilder ist KI-generiert

Schwächen des Passworts

Schwache Credentials und schwacher Schutz



Phishing

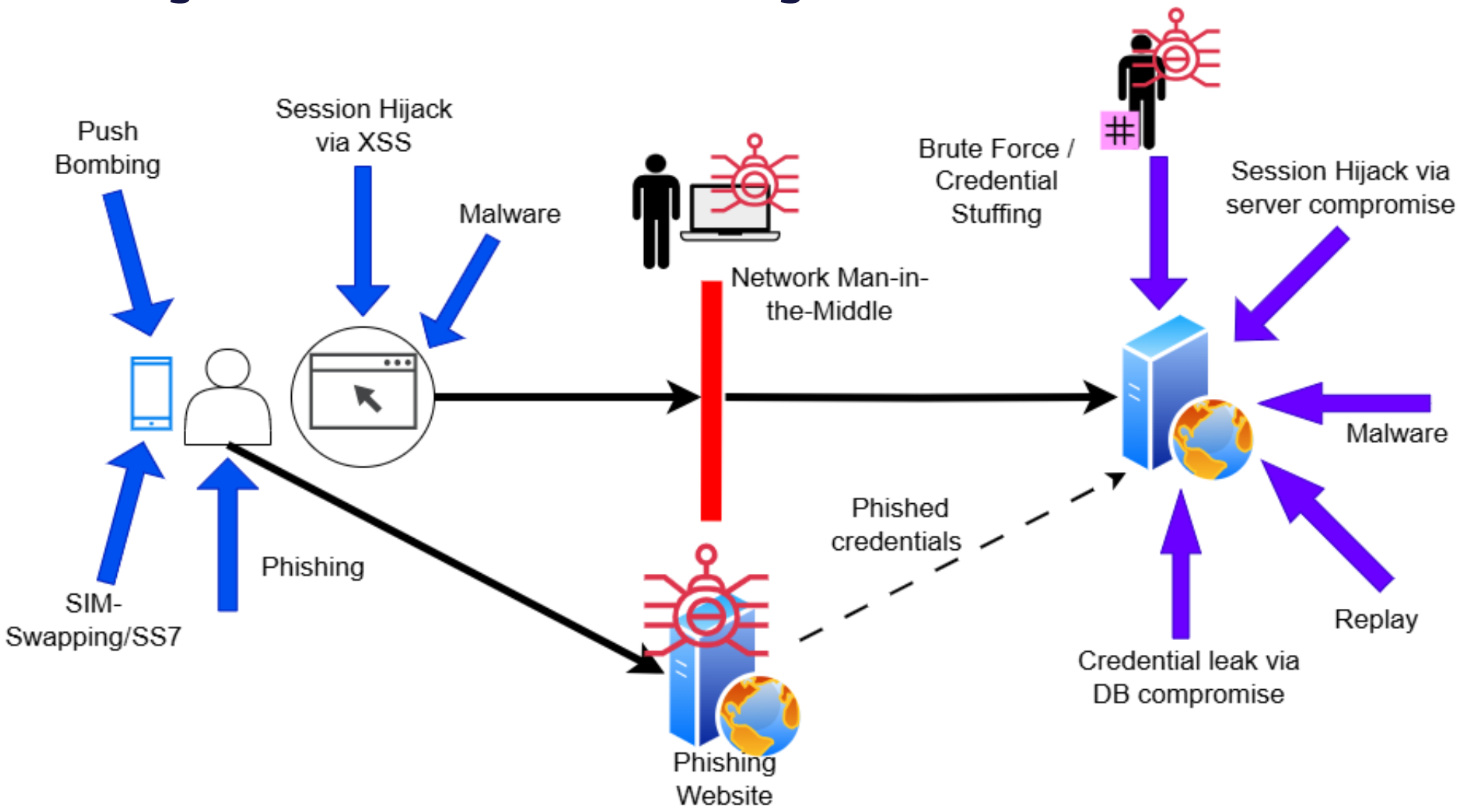
Bilder sind KI-generiert.

Traditionelle MFA: Unabhängige zweite Faktoren

Faktor	Angriffe
SMS-OTP	▪ SS7 ▪ SIM-Swapping / SIM-Kloning ▪ SMS-Lesen durch andere Apps ▪ MitM, MitB ▪ Serverkompromittierung (Seed-Diebstahl) ▪ **Phishing**
(Software-, Hardware-) TOTP	▪ MitM, MitB ▪ Serverkompromittierung (Seed-Diebstahl) ▪ **Phishing**
Push-Notifikation	▪ MitM, MitB ▪ Push-Bombing ▪ **Phishing**

Angriffspunkte

Bekannte Angriffe bei der Authentisierung



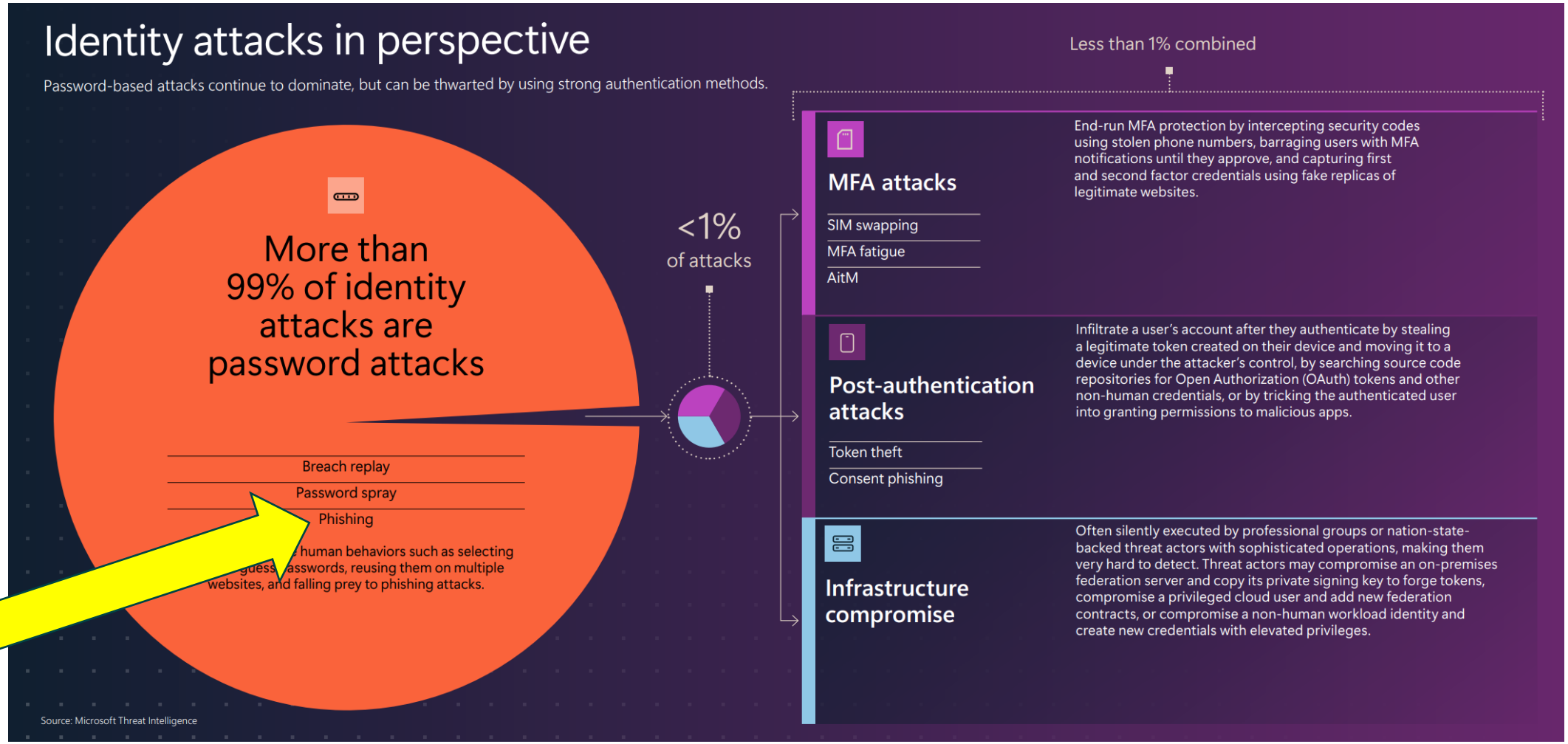
Phishing: ein grosses Problem schwacher Authentisierungsmechanismen

- Täuschung, um Nutzer zur Preisgabe vertraulicher Informationen zu bewegen
- Klassisches Phishing: Phishing-Webseite zeigt ein Login-Formular, sammelt Credentials
- Echtzeit-Phishing: Angreifer leitet Credentials in Echtzeit vom User weiter an den Server
- Grundursachen:
  - **Wiederverwendbare** und **übertragbare** Credentials
  - **Keine Bindung** zwischen Domänen und Credentials
  - **Benutzer** können echte und gefälschte Domains/URLs **nicht zuverlässig unterscheiden**
- *Mehrere Faktoren ≠ Phishing-Schutz*

Phishing ist einfacher als andere Angriffe

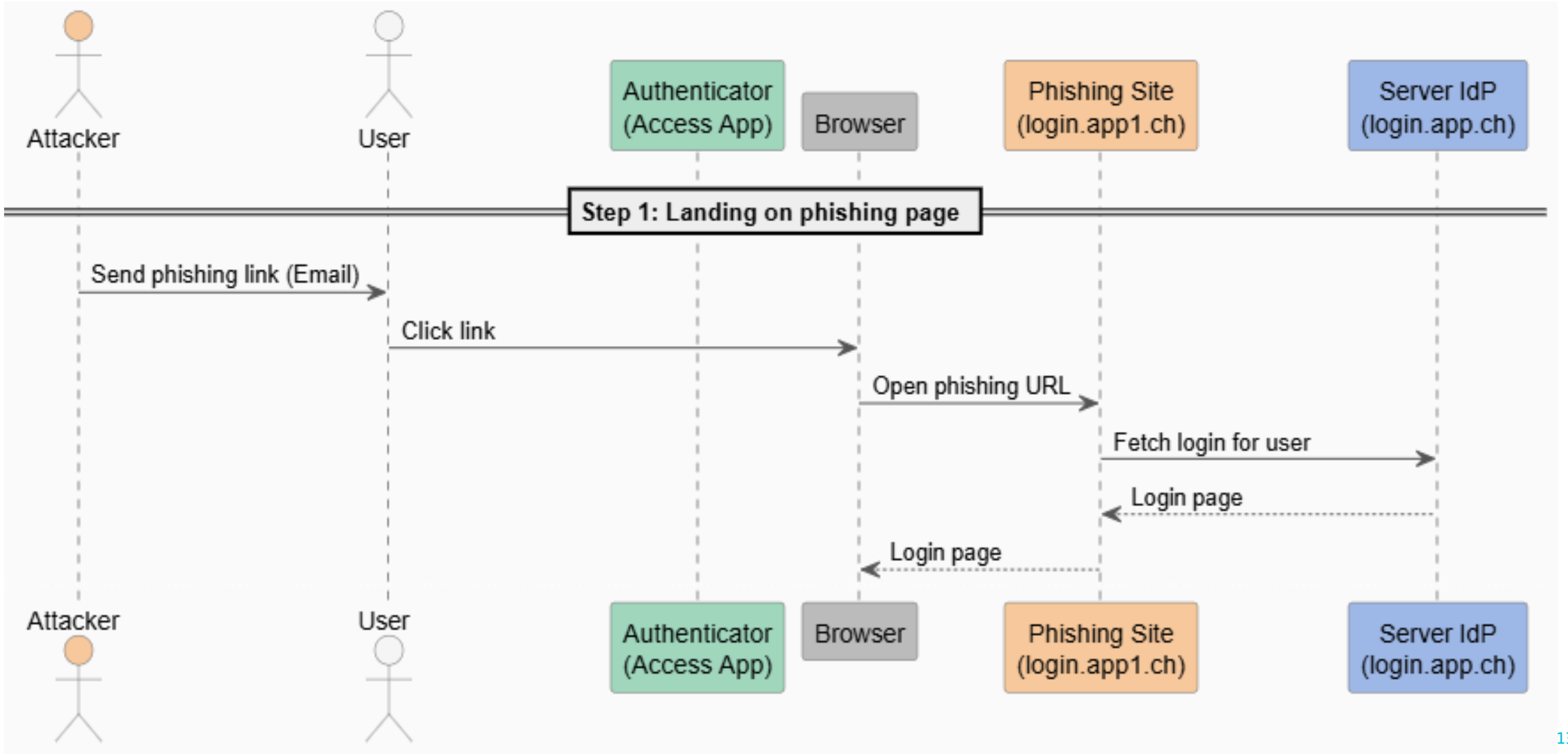
- **Phishing**: täuscht *den Benutzer* → die **falsche Webseite** wirkt echt (ähnlicher URL, gleiche Grafik)
  - Der Benutzer wird auf die gefälschte Seite gelockt (z. B. per E-Mail, Link, gefälschte Domäne).
  - Menschen haben Mühe, gefälschte URLs und gefälschte Webseiten zu erkennen.
- **Network MitM** (Server Impersonation): täuscht *den Browser* (Client) → die **falsche Verbindung** wirkt echt
  - Der Datenverkehr muss zuerst über den Angreifer umgeleitet werden (z. B. über manipuliertes DNS, BGP Hijack)
  - Der Angreifer muss ein gültiges Zertifikat für den Server präsentieren (Browser prüft)
- **Session Hijack**: täuscht *die Anwendung* (Server)→ die **falsche Identität** wirkt echt (findet nach der Authentisierung statt)
  - Der Angreifer muss an das Session-Token des Benutzers gelangen (z. B. XSS, unsichere Cookies, Abhören ohne TLS).
  - Moderne Browser haben Mechanismen, das zu verhindern

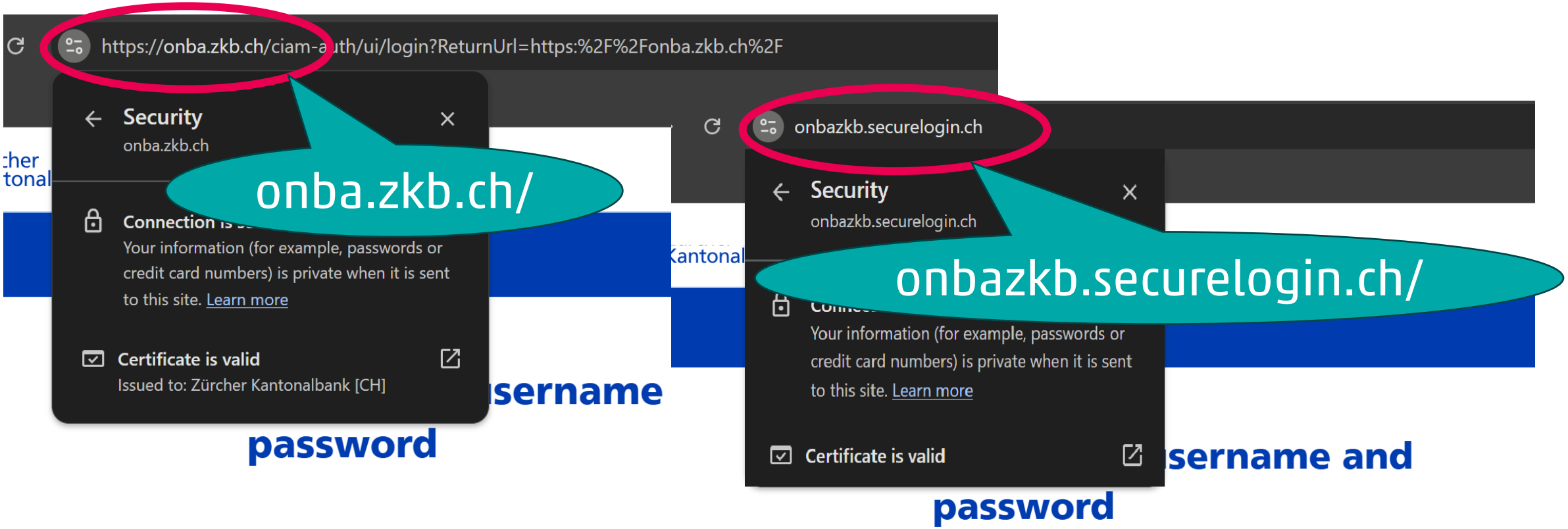
Microsoft Digital Defense Report 2024: >99% Angriffe betreffen Passwörter



https://www.microsoft.com/en-us/security/security-insider/threat-landscape/microsoft-digital-defense-report-2024

Real-Time Phishing: Landung auf der Phishing-Seite





password

Username

The username is your contract number.

Password

Forgot your password?

username and password

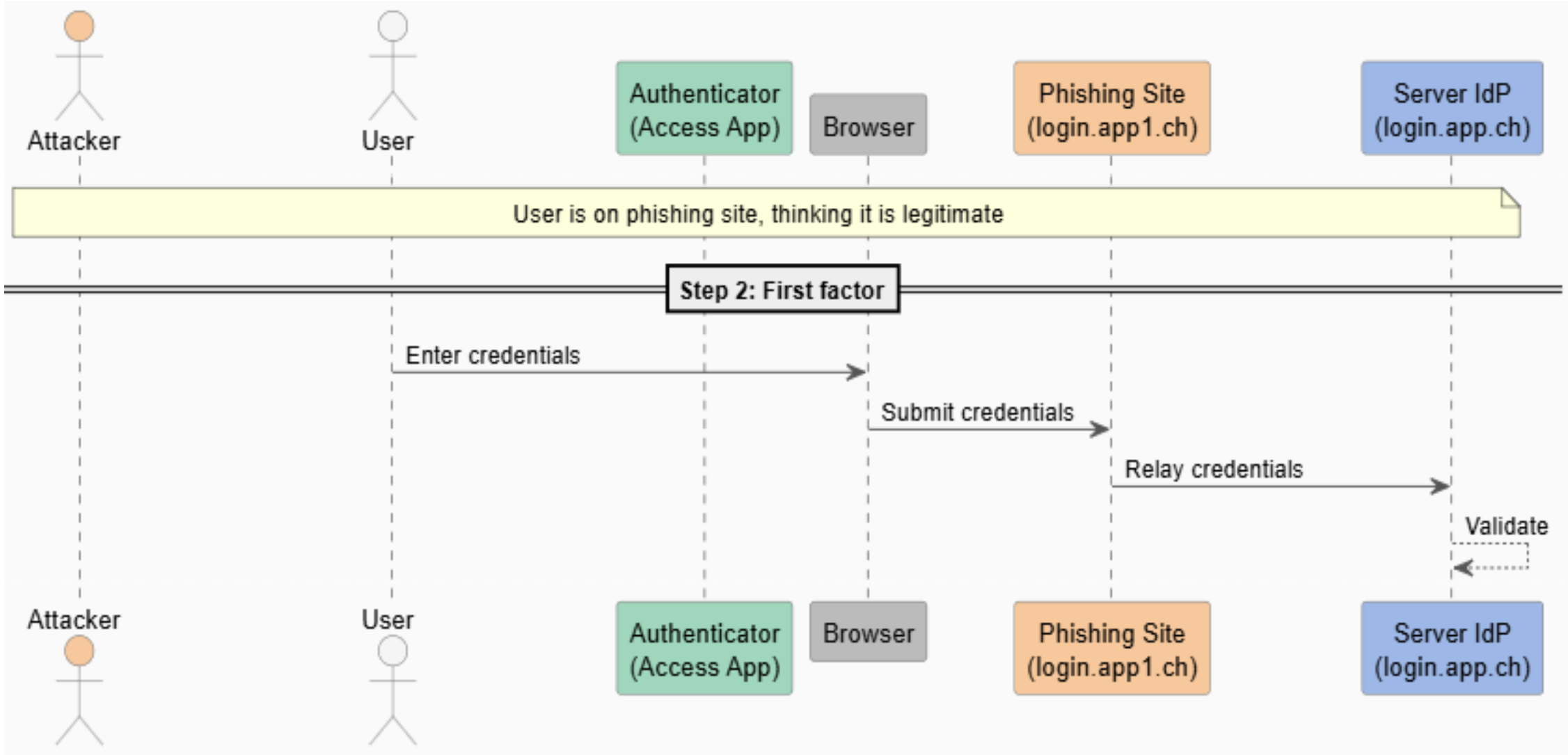
Username

The username is your contract number.

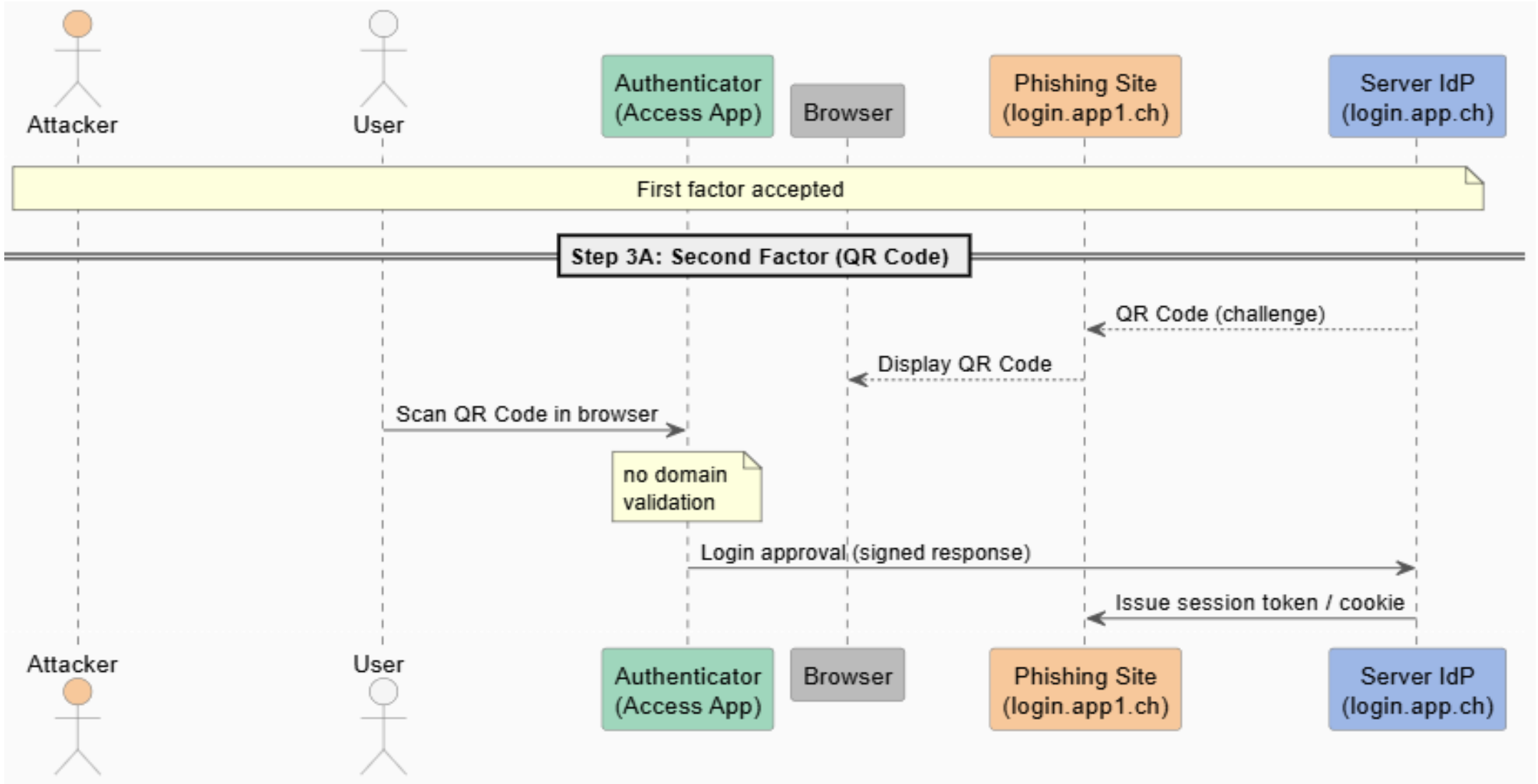
Password

Forgot your password?

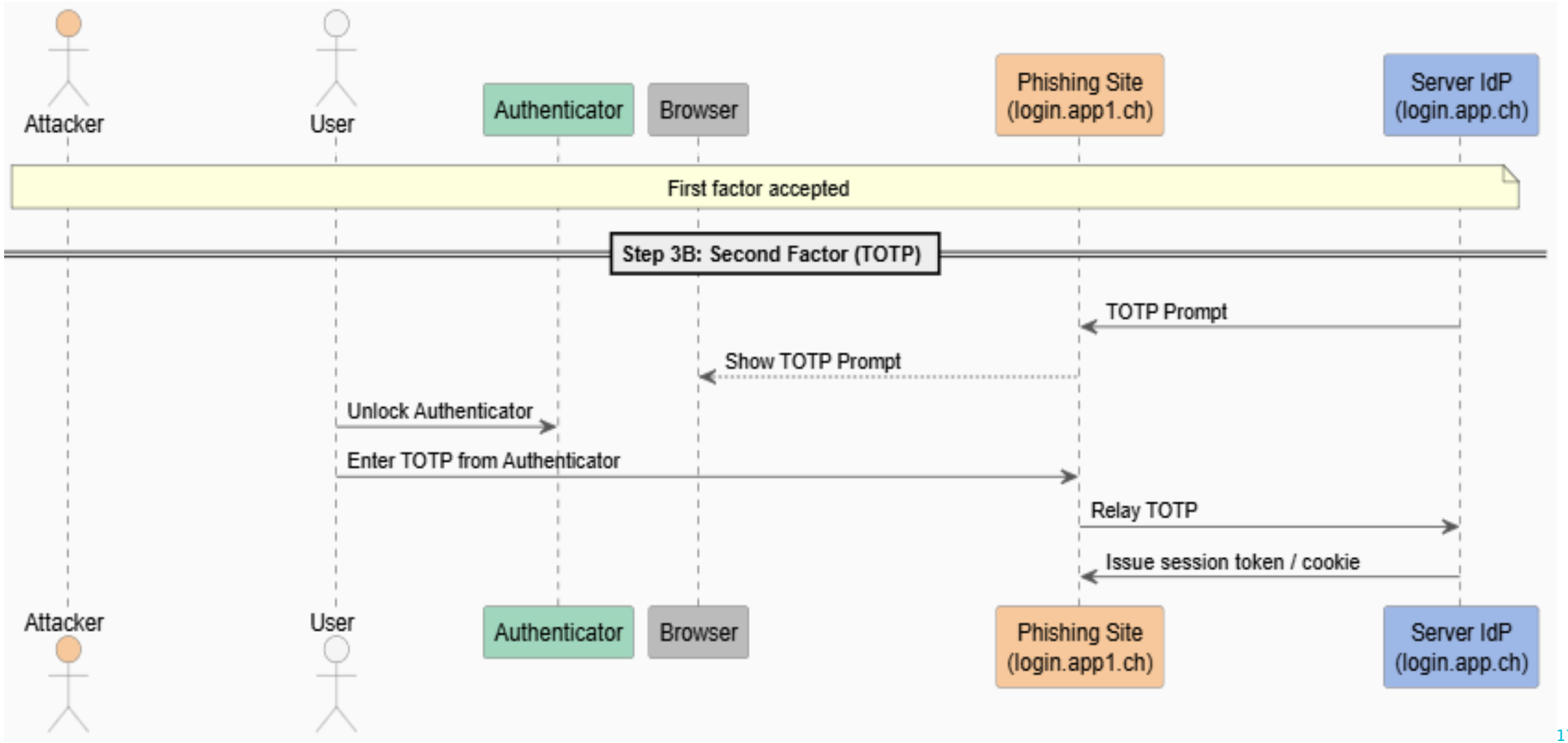
Real-Time Phishing: Erster Faktor



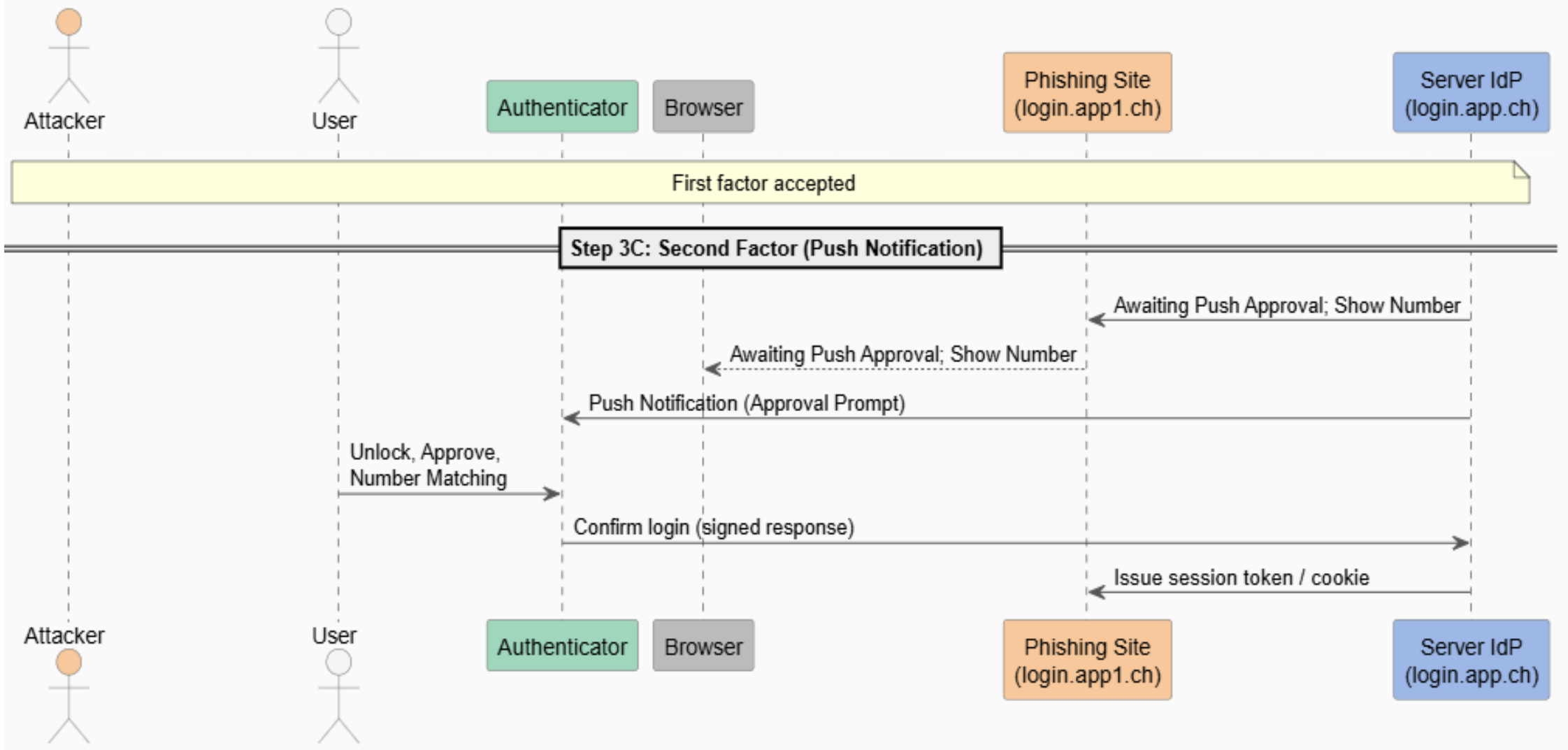
Real-Time Phishing: Fall QR-Code als 2. Faktor



Real-Time Phishing: Fall TOTP als 2. Faktor



Real-Time Phishing: Fall Push-Benachrechtigung als 2. Faktor



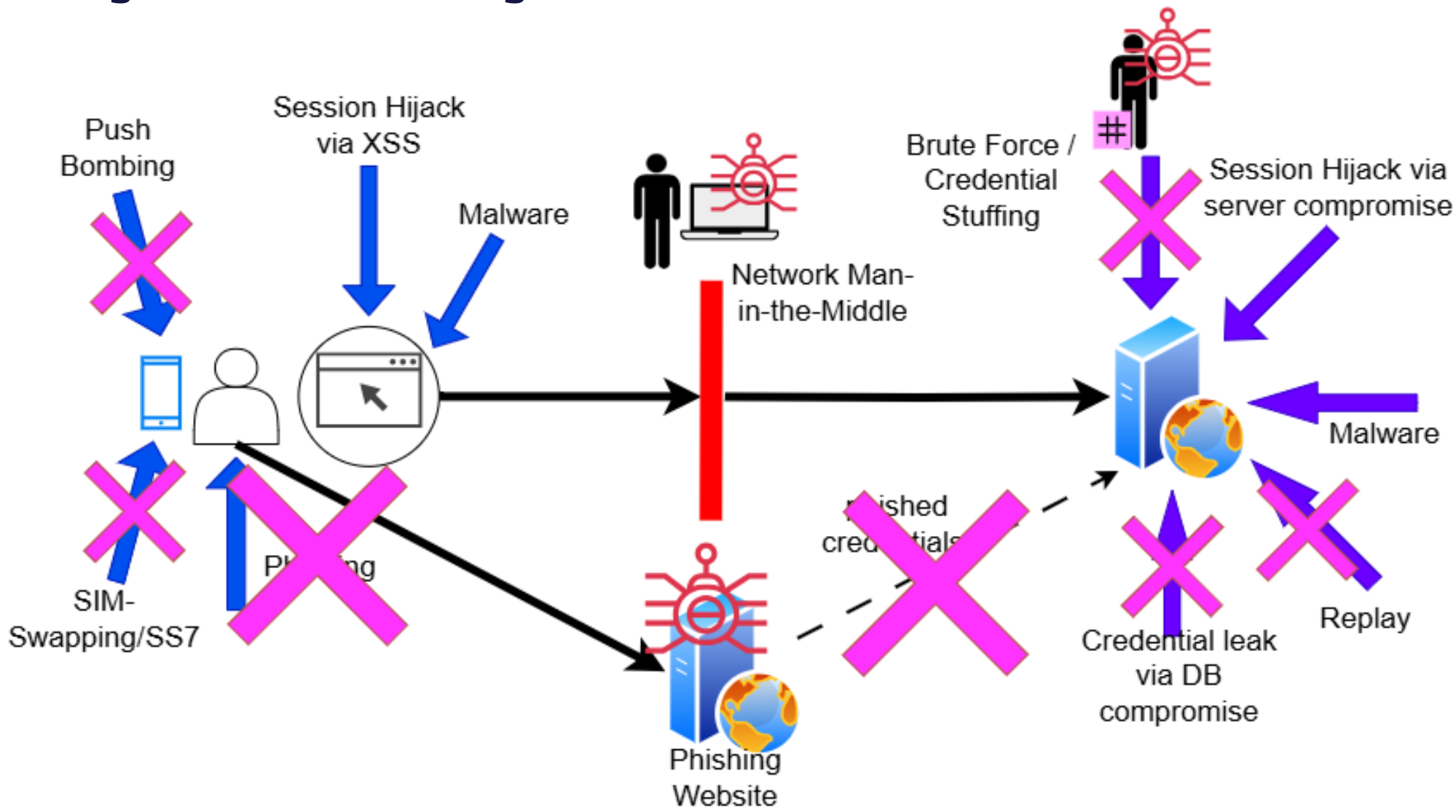
Echtzeit-Phishing ist einfach!

- **Evilginx[1]:** open-source MitM Framework für Echtzeit-Phishing
- Fängt die Kommunikationsnachrichten zwischen Benutzer und Server ab, verändert sie bei Bedarf und leitet sie in beide Richtungen weiter
- Spart Angreifern Zeit und Aufwand: proxyt echte Webseiten täuschend echt und fängt automatisch Zugangsdaten samt Session-Token ab
- Wirkt gegen alle MFA-Mechanismen ohne Domänen-Bindung (und ohne Kanal-Bindung)

[1] *https://github.com/kgretzky/evilginx2*
Bilder ist KI-generiert

Warum FIDO2?

Auswirkung von FIDO2 auf Angriffe



Klassifizierung von Authentisierungsverfahren (NIST SP 800-63B)

AAL	Zulässige Authentifizierungsarten	Sicherheitsanforderungen
AAL1 (basic confidence)	▪ Passwort ▪ Look-up Secret ▪ Out-of-Band (OOB) ▪ Single-Factor OTP (SF-OTP) ▪ Multi-Factor OTP (MF-OTP) ▪ Single-Factor Cryptographic (SF-Krypto) ▪ Multi-Factor Cryptographic (MF-Krypto)	Multi-Factor empfohlen, nicht notwendig
AAL2 (high confidence)	▪ Ein Multi-Factor-Authenticator (MF-OTP, MF-Krypto) ODER ▪ Zwei Single-Factor Authenticators (mind. ein „Besitz-Faktor“)	▪ Multi-Factor notwendig ▪ Mindestens ein Phishing-resistenter Faktor
AAL3 (very high confidence)	▪ Multi-Factor Cryptographic Authenticator (MF-Crypto) ODER ▪ Single-Factor Cryptographic + (Passwort oder Biometrie)	▪ Multi-Factor notwendig ▪ Kryptografischer Nachweis notwendig ▪ Nicht exportierbarer privater Schlüssel ▪ Phishing-Resistenz notwendig ▪ Authentisierungsabsicht

Zusammenfassung: Warum FIDO2?

- ✓ Starke beweisbare Authentisierung mit kryptographischen Signaturen
- ✓ „Intrinsisch“ mehrfaktorig (AAL2): Besitz (Authenticator) + User-Verifikation (PIN oder Biometrie)
- ✓ Echtzeit-Phishing-Schutz:
  - ❖ Credentials sind **nicht frei übertragbar** (Private Key bleibt auf dem Authenticator)
  - ❖ Login-Daten sind **nicht wiederverwendbar** (Jeder Login braucht eine neue Signatur)
  - ❖ **Domänen-Bindung**: Ein Credential gilt nur für eine Domäne
  - ❖ **Technische URL-Prüfung:** Der Browser gibt die wirkliche Login-URL zum Authenticator

Vielen Dank für Ihre Aufmerksamkeit_

Simran Tinani
simran.tinani@cnlab.ch
+41 55 536 22 30

info@cnlab-security.ch
+41 55 214 33 40

cnlab security AG
Obere Bahnhofstrasse 32b
CH-8640 Rapperswil-Jona
Switzerland

cnlab