Café digital

Senioren für Senioren LIESTAL

Ziel

- Förderung des Grundverständnisses der Datensicherheit
- Die verschiedenen Fachbegriffe soweit kennen, dass man weiss, worum es geht

Inhalt

- **Datensicherheit - warum wichtig?**
- **Die vier Basiselemente der Datensicherheit**
- **Virenschutz, kurzer Exkurs**
- **Schwerpunkt 2FA, was ist das überhaupt?**
- **2FA, Beispiele aus dem Alltag**
- **Erläuterung VPN**
- **VPN - Beispiele**
- **Zusammenfassung**
- **Quiz**

Datensicherheit - warum wichtig?

Senioren für Senioren LIESTAL

- Immer mehr Alltag online: E-Banking, E-Mail, Einkaufen, Billette SBB, Behördengänge etc.
- Persönliche Daten = wertvoll (für Kriminelle attraktiv)
- Betrugsversuche gezielt auf Senioren (Enkeltrick, Phishing-Mails, falsche Anrufe)
- Finanzielle & persönliche Folgen bei Datenverlust/-missbrauch
- Eigenes Verhalten = wichtigster Schutzfaktor

→ Datensicherheit (Data Security) bezeichnet den Schutz von Informationen vor unbefugtem Zugriff, Verlust, Diebstahl oder Beschädigung.

Safety versus Security

Der Begriff Sicherheit ist leider doppeldeutig, auf Englisch ist das präziser:

Datensicherheit im Sinne von **Safety** (Betriebssicherheit)

- Schutz vor unabsichtlichen Ereignissen
- z.B. Hardware-Defekt, Stromausfall, Naturereignis
- Gegenmassnahmen: Redundanz, Backup

Datensicherheit im Sinne von **Security** (Angriffssicherheit)

- Schutz vor absichtlichen Angriffen
- z.B. Hacker, Malware, Diebstahl

➔ **hier unser Thema**

4 Basiselemente der Datensicherheit

Data Security

Senioren für Senioren LIESTAL

Exkurs Virenschutz

Virenschutz (auch Antivirensoftware oder Antivirus) bezeichnet Software und Sicherheitsmassnahmen, die digitale Systeme vor schädlichen Programmen – sogenannter **Malware** – schützen.

Für Interessierte zum späteren Lesen

Obwohl der Name auf „Viren“ anspielt, decken moderne Virenschutzprogramme heute ein deutlich breiteres Spektrum an Bedrohungen ab:

- **Trojaner** (Trojanisches Pferd): Tarnt sich als nützliche oder harmlose Software (z. B. ein Spiel oder ein Installationsprogramm), schleust im Hintergrund jedoch unbemerkt Schadcode ein. Typische Ziele sind das Ausspähen von Daten oder das Öffnen von Hintertüren (Backdoors) für Angreifer. Im Gegensatz zu echten Viren verbreiten sich Trojaner nicht eigenständig durch Kopieren.
- **Ransomware**: Erpresst die Opfer, indem sie Dateien auf dem Computer oder dem Netzwerk verschlüsselt oder den Systemzugriff blockiert. Um wieder an die Daten zu gelangen, wird von den Kriminellen in der Regel ein Lösegeld (Ransom) gefordert – oft in Kryptowährungen.
- **Spyware**: Spioniert das Nutzerverhalten im Verborgenen aus. Sie zeichnet beispielsweise Tastatureingaben (Keylogging) auf, stiehlt Passwörter, sammelt Browser-Verläufe oder greift auf Webcam und Mikrofon zu, um die Daten an Dritte zu übermitteln.
- **Worms** (Würmer): Ähnlich wie Viren, aber mit einer entscheidenden Eigenschaft: Sie sind eigenständige Programme, die sich selbstständig über Netzwerke (wie das Internet oder lokale LANs) und Sicherheitslücken weiterverbreiten, ohne dass eine menschliche Interaktion oder eine infizierte Datei nötig ist.
- **Adware**: Short für Advertising-supported software. Sie zeigt unerwünschte Werbung an (z. B. aufdringliche Pop-ups, geänderte Startseiten im Browser oder manipulierte Suchergebnisse). Oft ist sie weniger zerstörerisch, aber extrem nervig und kann sensible Daten abgreifen oder als Einfallstor für gefährlichere Malware dienen. (u. a. Trojaner, Ransomware, Spyware, Worms und Adware).

Exkurs Virenschutz

Abhängig vom verwendeten Betriebssystem (Operating System - OS):

- Microsoft Windows: Windows Defender ist meist vorinstalliert, genügt.
- Apple (Mac und iOS): nicht nötig (Sandbox)
- Android: Google Play Store ist sicher (Vorsicht beim Sideloading!)

Zweifaktor - Authentifizierung 2FA

Senioren für Senioren LIESTAL

«Ein Passwort alleine ist wie ein einfacher Haustürschlüssel – 2FA ist der zusätzliche Sicherheitsriegel.»

Was ist 2FA?

- Anmeldung in zwei Schritten statt nur einem.
- Kombination aus Wissen (Passwort) und Besitz (Smartphone/SMS-Code/App).

Warum ist 2FA nötig?

- Passwörter können gestohlen, erraten oder durch Datenlecks bekannt werden.
- Auch wenn jemand Ihr Passwort hat, kommt er ohne den zweiten Faktor nicht ins Konto.

Wie funktioniert 2FA in der Praxis? Drei Varianten:

- SMS-Code: Sie bekommen einen 6-stelligen Code per SMS geschickt.
- Authenticator-App: Eine App auf dem Handy generiert alle 30 Sekunden einen neuen Code (z. B. Google/Microsoft Authenticator, SwissID).
- Push-Nachricht: Eine Bestätigungsanfrage ploppt auf dem Handy auf („Sind Sie das?“ → „Ja“ antippen).

Zweifaktor - Authentifizierung 2FA

Tipps für den Alltag

- Bei wichtigen Konten aktivieren (E-Mail, E-Banking, Online-Shopping, WhatsApp).
- Keine Angst: Man muss den zweiten Code oft nur bei neuen Geräten oder in grösseren Abständen eingeben.

Beispiel Geldabheben am Bankautomaten

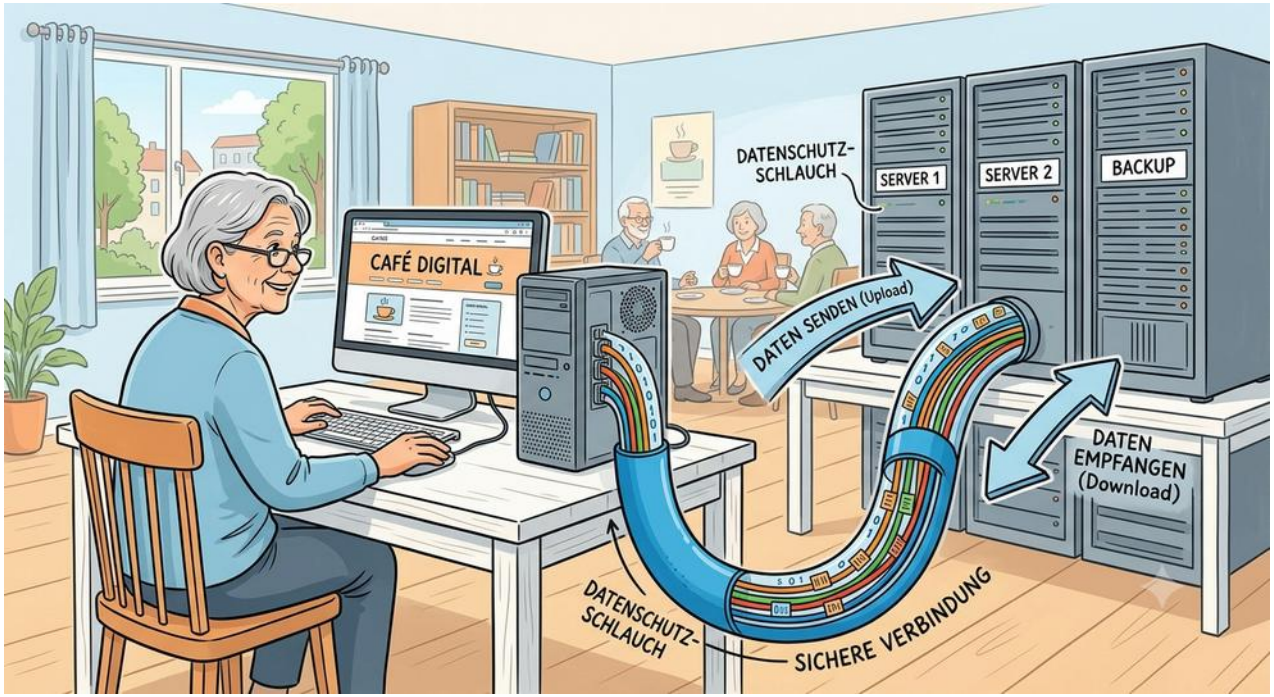
- Faktor 1 (Besitz): Die EC-/Bankkarte.
- Faktor 2 (Wissen): Die PIN.
- Ohne Karte bringt die PIN nichts – und ohne PIN bringt die Karte nichts.
- 2FA macht genau das Gleiche im Internet!

Virtual Private Network - VPN

Ein VPN ist wie ein (undurchsichtiger) Tunnel für Ihre Daten – niemand sieht von aussen, woher sie kommen, was sie transportieren und wohin sie gehen.

Was ist ein VPN?

- Eine verschlüsselte Verbindung zwischen dem eigenen Gerät und dem Internet.
- Die echte IP-Adresse (der „digitale Absender“) wird verschleiert.



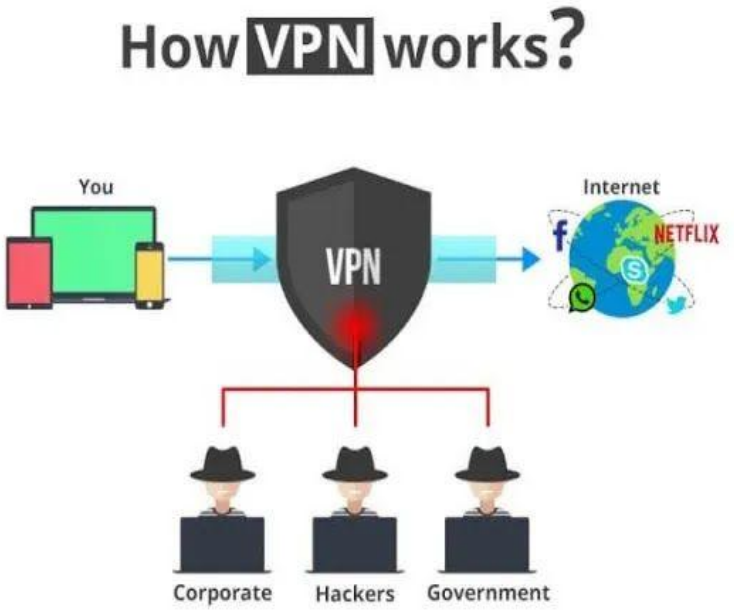
Virtual Private Network - VPN

Wann ist der Einsatz eines VPN sinnvoll?

- Schutz in öffentlichen WLANs: Verhindert, dass Fremde im Café, Zug oder Hotel Daten mitlesen.
- Privatsphäre: Internetanbieter und Werbenetzwerke können das Surfverhalten nicht leicht nachverfolgen.
- Reisen: Ermöglicht den Zugriff auf gewohnte Schweizer/Heimat-Dienste aus dem Ausland (z. B. Mediatheken/SRF/ARD).

Was kann ein VPN nicht?

- Es ersetzt keinen Virenscanner
- Es schützt nicht vor Betrugs-E-Mails (Phishing), wenn man selbst Daten auf gefälschten Seiten eingibt.



Virtual Private Network - VPN

Analogie zur Post

- Normales Surfen im öffentlichen WLAN ist wie eine Postkarte: Der Kellner, der Nachbartisch oder ein Post-Beamter könnte theoretisch mitlesen.
- Ein VPN steckt die Nachricht in einen undurchsichtigen Briefumschlag.

Site-to-Site VPN

VPN einrichten

- Nur vertrauenswürdige, bekannte Anbieter nutzen (kostenlose Gratis-VPNs verkaufen oft Nutzerdaten).
- Einfach per App auf Smartphone oder Tablet mit einem Klick ein- und ausschalten.

Virtual Private Network - VPN

Im Ausland:

- Gewisse Web-Applikationen sind auf bestimmte Länder beschränkt (z.B. die meisten TV-Sender)
- Sie sitzen im Hotel in Spanien und möchten die Tagesschau SRF schauen. Das VPN „versetzt“ Ihren Standort digital zurück nach Hause (der SRF Server «glaubt», Sie sitzen in der Schweiz).

VPN - Anbieter auswählen

- Die goldene Regel: Wenn ein VPN-Dienst völlig kostenlos ist und keine Einschränkungen hat, bezahlt man meist mit seinen persönlichen Daten.
- Strenge „No-Logs“-Politik: Der Anbieter speichert nicht ab, welche Websites besucht werden. Seriöse Anbieter lassen dies regelmässig von unabhängigen Prüfern (Audits) bestätigen.
- Firmensitz: Standorte ausserhalb der USA oder der EU (wie die Schweiz oder Panama) bieten oft einen besseren rechtlichen Schutz für Kundendaten.
- Bedienung: Gute Anbieter bieten einfache Ein-Klick-Apps für Windows, Mac, Android und iOS, die sich wie ein Lichtschalter ein- und ausschalten lassen.

Virtual Private Network - VPN

VPN - Anbieter

- **Proton VPN (Schweiz)**
  Besonderheit: Firmensitz in der Schweiz mit sehr strengen Datenschutzgesetzen.
  Vorteile: Bietet eine dauerhaft kostenlose Version (ohne Datenlimit, allerdings mit eingeschränkter Serverauswahl/Geschwindigkeit). Sehr transparent, quelloffener Code (Open Source) und unabhängige Sicherheitsaudits.
  Ideal für: Einsteiger, die erst einmal kostenlos testen möchten, sowie datenschutzbewusste Nutzer.

- **Mullvad VPN (Schweden)**
  Besonderheit: Maximale Anonymität und einfache Preisstruktur.
  Vorteile: Kostet pauschal 5 € pro Monat (keine Abo-Falle, jederzeit kündbar). Man benötigt für die Registrierung nicht einmal eine E-Mail-Adresse – das System generiert lediglich eine zufällige Kontonummer.
  Ideal für: Nutzer, die maximale Privatsphäre ohne unübersichtliche Rabatt-Abos suchen.

- **NordVPN (Panama)**
  Besonderheit: Einer der weltweit bekanntesten und grössten Anbieter.
  Vorteile: Sehr schnelle Verbindungen, benutzerfreundliche Apps für PC, Smartphone und Tablet. Bietet viele Zusatzfunktionen wie integrierten Schutz vor schädlichen Websites.
  Ideal für: Allrounder, Streaming (z. B. Schweizer Fernsehen im Ausland schauen) und einfache Handhabung.

Zusammenfassung

Senioren für Senioren LIESTAL

1. Datensicherheit: Safety versus Security
2. Die vier Basiselemente der Datensicherheit (Security)
3. Exkurs Virenschutz
4. 2FA
5. VPN