Digitaler Schutz

- Kinder werden von ihren Eltern geschützt
- Beim Überqueren einer Straße schauen wir ob sie frei ist
- Wir sind wachsam wenn wir draußen unterwegs sind
- Wir schützen uns beim Sex mit fremden Partnern
- Wohnungstür/Auto/Fahrrad wird abgeschlossen

Und so können wir die Liste weiterführen……

Aber was ist wenn wir digital unterwegs sind?

- Viele gehen ungeschützt ins Internet
- Viele geben ihre Daten preis
- Viele nutzen keine Passwörter
- Und so weiter und so weiter

Woran liegt das?

- Ist es Unwissenheit?
- Ist es Gleichgültigkeit?
- Ist es Unvermögen?

Wohl von jedem etwas.

Wir schützen uns analog, also warum nicht auch digital?

Dabei gibt es so viele Möglichkeiten sich digital zu schützen.

Aber gleich vorne weg – Es gibt keinen 100%igen Schutz!

Was können wir tun bzw. was wird für uns getan?

Zu Hause:

Firewall im Router
Passwortschutz

Unterwegs:

Firewall im Handy
Passwortschutz

Aber wir müssen auch etwas tun!

- **Gastnetzwerk einrichten:** Für Besucher, um dein Hauptnetzwerk zu schützen.
- **Firmware-Updates:** Halte den Router immer auf dem neuesten Stand.
- **Antiviren-Software:** Installiere eine vertrauenswürdige Antiviren-Lösung auf allen Geräten.
- **Firewall aktivieren:** Nutze die integrierte Firewall deines Betriebssystems.
- **Regelmäßige Updates:** Installiere Sicherheitsupdates für Betriebssysteme und Apps sofort.
- **Starke Passwörter:** Nutze lange, einzigartige Passwörter für jedes Konto.
- **Passwort-Manager:** Verwende Tools wie z.B. KeePass, um Passwörter sicher zu speichern.
- **Zwei-Faktor-Authentifizierung (2FA):** Aktiviere 2FA, wo immer möglich.
- **Kameras & Mikrofone:** Deaktiviere oder klebe sie ab, wenn nicht in Gebrauch.
- **Smart-Home-Geräte:** Ändere Standard-Passwörter und deaktiviere unnötige Funktionen.
- **Regelmäßige Backups:** Sichere wichtige Daten auf externen Festplatten oder in der Cloud.
- **Verschlüsselung:** Nutze Tools wie VeraCrypt für sensible Daten.
- **Phishing erkennen:** Sei vorsichtig bei verdächtigen E-Mails oder Links.
- **Öffentliches WLAN meiden:** Nutze stattdessen dein mobiles Datenvolumen
- **Hotspot-Sicherheit:** Deaktiviere automatische WLAN-Verbindungen und vergiss Netzwerke nach der Nutzung.
- **Bildschirmsperre:** Nutze PIN, Muster oder biometrische Sperren (Fingerabdruck/Gesichtserkennung).
- **Ortungsdienste:** Aktiviere sie nur bei Bedarf und prüfe App-Berechtigungen.
- **Diebstahlschutz:** Aktiviere Funktionen wie „Mein Gerät suchen“ (Android/iOS) und Fernlöschung.
- **Verschlüsselung:** Aktiviere die Geräteverschlüsselung (z. B. FileVault auf Mac, BitLocker auf Windows).
- **Sensible Daten:** Speichere sie nicht unverschlüsselt auf dem Gerät. Nutze sichere Cloud-Dienste mit Ende-zu-Ende-Verschlüsselung.
- **USB-Sticks & externe Datenträger:** Nutze sie nur von vertrauenswürdigen Quellen und verschlüssle sie.
- **HTTPS:** Achte auf das Schloss-Symbol in der Adresszeile.
- **Messenger:** Nutze verschlüsselte Dienste wie Signal oder Threema.
- **E-Mails:** Vermeide das Öffnen von Anhängen oder Links aus unbekannten Quellen.
- **Backup:** Sichere regelmäßig deine Daten, falls das Gerät verloren geht.
- **Notfallkontakte:** Hinterlege eine vertrauenswürdige Person, die im Notfall auf wichtige Konten zugreifen kann.
- **Shoulder Surfing:** Gib Passwörter oder PINs nicht in der Öffentlichkeit ein.
- **Geräte nie unbeaufsichtigt lassen:** Auch nicht im Hotelzimmer oder Café.
- **Tipp:** Nutze eine separate SIM-Karte oder ein Zweitgerät für Reisen, um das Risiko bei Verlust zu minimieren.

Links zum Thema Sicherheit auf www.pc-phone-treff.de:

https://pc-phone-treff.de/2025/06/01/virenschutz/

https://pc-phone-treff.de/2024/10/27/moegliche-schutzmassnahmen/

https://pc-phone-treff.de/div/Sicheres%20Smartphone.pdf

Firewall:

Windows	Mac	Android	iOS	Linux
X	X	X	-	X

Virenschutz:

Programm	Windows	Mac	Android	iOS	Linux
ClamAV	-	-	-	-	**x**
Avira	**x**	**x**	**x**	**x**	-
Panda	x	x	x	x	-
TotalAV	x	x	x	x	-
BitDefender	x	x	x	x	x
Sophos	x	x	x	x	x
Norton360	x	x	x	x	-
Kaspersky	x	-	x	x	x
McAfee	x	x	x	x	x

Immer aktuell bleiben: Nur ein aktuelles System ist ein sicheres System.

Daten bitte, aber sparsam: Daten nur preisgeben, wenn unbedingt erforderlich.

Backup / Sicherungskopie: Zeitnah/Zeitgleich auf externen Laufwerken.

Programme / Apps: Nur von seriösen Anbietern/Herstellern/Quellen.

Sperre: PIN, Passwort, Muster oder Fingerabdruck nutzen.

Virenschutz / Firewall: 1x pro Gerät.

ENDE