Wie schütze ich mich im Internet?

Verwende verschiedene Passwörter

Vermeide unbedingt überall das gleiche Passwort zu verwenden. Wenn du überall das gleiche Passwort verwendest, können Hacker womöglich nicht nur Zugriff auf einen deiner Accounts erhalten, sondern womöglich auf mehrere oder im schlimmsten Fall sogar alle.
Am besten du verwendest hierfür einen Passwort Manager. Ein Passwort Manager hilft dir bei der Verwaltung deiner Passwörter und hilft dir diese sicher zu speichern.
Beispiele für Passwort-Manager:

🔗 https://1password.com/de/
🔗 https://www.dashlane.com
🔗 https://www.lastpass.com/de

Verwende verschiedene Email Adressen

Registriere dich nicht überall mit der gleichen Email-Adresse. Durch deine Email-Adresse ist es recht einfach deine diversen Accounts, deiner Person zuzuordnen. Einzelne Email-Anbieter (z.B.: GMX) ermöglichen die Erstellung von Alias-Adressen. Hierfür kann man sich weitere Email-Adressen anlegen, die kein eigenes Postfach haben, sondern lediglich eine Weiterleitung auf deine eigentliche Email-Adresse darstellen. Außerdem hast du den Vorteil, wenn du für jede Registrierung eine eigene Email-Adresse verwendest, dann kannst du (falls dir unerwünschte Newsletter, Spam, etc. zugesendet werden) jederzeit die Email-Adresse wieder löschen oder Emails von dieser Email-Adresse mit Regeln in deinem Email-Programm relativ einfach aussortieren. Außerdem weißt du dadurch eventuell, welche der Webseiten auf der du dich registriert hast deine Daten preisgegeben hat, verkauft hat oder gehacked wurde, wenn du plötzlich unerwartete Emails erhältst.

Wusstest du dass du dir bei Prowect eigene Email-Adressen anlegen kannst (mit deiner eigenen Wunschdomain)?

🔗 https://www.prowect.com/services#hosting-services

Achte auf eine verschlüsselte Verbindung

Wenn du im Internet surfst, solltest du unbedingt darauf achten, dass du bei Webseiten, bei denen du womöglich deine Daten preisgibst (beispielsweise indem du dich registrierst oder über ein Kontaktformular, etc.) immer eine verschlüsselte Verbindung verwendest.
Ob eine verschlüsselte Verbindung besteht erkennst du daran dass du eine Webseite mit `https://` aufrufst. (Achtung: `http://` ist nicht verschlüsselt!)
Oft wird eine verschlüsselte Verbindung im Browser auch speziell gekennzeichnet. (z.B.: durch ein Schlosssymbol 🔒)

Erkenne Spam- & Phisingmails

Hin und wieder erhältst du Emails mit mysteriösen Links, unerwünschter Werbung oder einer Aufforderung zur Bekanntgabe deiner Bankdaten oder Eingabe deiner Zugangsdaten.
Falle auf diese Art von Emails auf keinen Fall herein! Ignoriere sie, lösche sie und lass dich auf keinen Fall erpressen.
Tipp: Du kannst oft in deinem Mail-Programm verschiedene Regeln definieren und eventuell bestimmte Emails aussortieren. (z.B.: von einem bestimmten Absender oder abhängig von einem bestimmten Inhalt)

Gib deine Daten nicht preis

Versuche auf Webseiten, auf denen du dich registrierst so wenig Daten wie möglich preis zu geben. Du brauchst keine Namen erfinden oder irgendwelche Fantasiedaten eintragen, aber versuche wirklich nur die Pflichtfelder auszufüllen.
Somit schützt du deine Daten und womöglich auch deine Identität.

Lade nichts herunter von mysteriösen Drittanbietern

Oft bieten dir diverse Webseiten oder Streaming-Plattformen den Download von Software oder Filmen, etc. an. Denke daran dass das Stehlen bzw. Nutzen von kostenpflichtiger Software oder kostenlose Streamen von Kinofilmen illegal ist und somit auch strafrechtliche Folgen haben kann.
Die Ersteller bzw. Betreiber dieser Webseiten wollen durch ihre Inhalte - lediglich Besucher anlocken.
Versuche solche Dienste zu vermeiden und lade nichts herunter, wenn du dir nicht sicher sein kannst, ob es nicht womöglich eine Schadsoftware sein könnte oder ein Virus der in dein System eingeschleust werden kann.

Achtung: oft ist ein Download oder eine Interaktion deinerseits gar nicht notwendig, auch der Besuch bzw. der Aufruf einer bestimmten Webseite, kann bereits gravierende Folgen haben.

Verwende eine Firewall

(D)eine Firewall schützt dich davor, dass ggf. bestimmte Zugriffe auf deinen PC nicht möglich sind. Du solltest daher unbedingt deine Firewall aktivieren und nur jene Verbindungen erlauben die du auch erlauben möchtest. Solltest du feststellen dass womöglich Verbindungen bestehen, die du gar nicht möchtest, kannst du diese auch explizit deaktivieren bzw. blockieren.

Verwende eine Virenschutzsoftware

Überall kann ein Virus lauern - hinter jeder Webseite, hinter jedem Button, in jeder Datei, in jeder Email. Sichere dich ab, indem du dir eine Virenschutzsoftware installierst und lasse sie auch regelmäßig dein System nach Viren scannen. So kannst du ggf. erhaltene oder versehentlich heruntergeladene Viren entdecken und diese beseitigen (lassen).
Beispiele für Virenschutzsoftware:

🔗 https://www.avira.com/de
🔗 https://www.kaspersky.de
🔗 https://at.norton.com
🔗 https://www.mcafee.com

Checkliste

	Aktuelle Virenschutzsoftware installiert
	Aktuellen Virenscan durchgeführt (innerhalb der letzten 30 Tage)
	Firewall aktiviert
	Firewall Regeln definiert (für eingehende & ausgehende Verbindungen)
	Passwort-Manager installiert und in Verwendung
	Unterschiedlicher Passwörter verwendet bzw. kürzlich erneuert/geändert (in den letzten 30 Tagen)