Internetsicherheit für Senioren / Seniorinnen

Nachstehend geben wir Ihnen wichtige Tipps, wie Sie sicher im Internet unterwegs sind.

Grundlegende Sicherheitshinweise zum Surfen im Internet:

- Kaufen und installieren Sie Sicherheitsprogramme
- Installieren Sie regelmässig Updates
- Surfen Sie auf verschlüsselten Webseiten
- Nutzen Sie keine öffentlichen Netzwerke
- Bleiben Sie anonym. Geben Sie im Internet immer nur die Daten an, die unbedingt erforderlich sind. Erscheint Ihnen eine Seite nicht vertrauenswürdig, sollten Sie keine Informationen über sich preisgeben
- Laden Sie nichts aus unbekannten Quellen herunter
- Schützen Sie Ihr Heimnetzwerk

Tipps zur Passwortsicherheit:

- Ein Passwort sollte min. 10 Zeichen lang sein. Verwenden Sie eine Mischung aus grossen und kleinen Buchstaben, Zahlen und Sonderzeichen wie !?/% enthalten
- Geben Sie Ihre Passwörter nicht weiter
- Verwenden Sie nicht immer wieder dasselbe Passwort
- Speichern Sie Ihre Passwörter, wenn möglich in ein Passwort-Manager-Programm

Ratschlag: Auch für Ihr E-Mail-Konto ist ein starkes Passwort ratsam. Zusätzlich sollten Sie eine 2-Faktor-Authentisierung einrichten. Mithilfe dieser Methode wird z.B. ein Code an Ihr Smartphone gesendet, welchen Sie dann zusätzlich zur Anmeldung benötigen.

Sicherheit beim E-Banking:

- Geben Sie nie sensible Daten wir Geheimzahlen oder Transaktionsnummern heraus
- Nutzen Sie keine öffentlichen WLAN-Netze für das E-Banking
- Nutzen Sie keine fremden Geräte für das E-Banking
- Melden Sie sich nach dem E-Banking aus der App oder dem Browserfenster ab
- Setzen Sie ein Überweisungslimit, das die Summe der möglichen Überweisungen pro Tag einschränkt

Ratschlag: Bei Verdacht auf Betrug rufen Sie sofort die E-Bank-Hotline Ihrer Bank an

Sicherheitstipps zum Online-Shopping

- Schauen Sie im Impressum nach Informationen zum Shop-Betreiber
- Informieren Sie sich vorab über zusätzlich Kosten zu Versand, Rückgabe oder Stornierung
- Lesen Sie Bewertungen oder Erfahrungsberichte zum Online-Shop
- Nutzen Sie bei unbekannten Shops keine Zahlungsarten, bei denen Sie vor Erhalt der Ware zahlen müssen
- Legen Sie auch für ein Kundenkonto bei einem Online-Shop ein sicheres Passwort fest

Schutzeinstellungen für das Smartphone

- Verwenden Sie einen SIM-Karten-PIN, um den Zugang zu Ihrer SIM-Karte zu schützen
- Richten Sie ein Bildschirmsperre ein, zum Beispiel mit PIN, einem Muster oder Fingerabdrucksensor
- Führen Sie regelmässig Updates durch, um Sicherheitslücken zu schliessen
- Öffnen Sie keine Links von unbekannten Absendern
- Nutzen Sie keine öffentlichen WLAN-Netzwerke

E-Mail-Sicherheit und E-Mail Phishing

- Wenn Sie eine unerwartete E-Mail erhalten, sehen Sie sich dazu die E-Mail-Adresse genau an
- Öffnen Sie keine E-Mails von unbekannten Adressanten
- Prüfen Sie den Absender genau und unterlassen Sie es im Zweifelsfall, einen Link anzuklicken oder einen Anhang zu öffnen
- Phishing-Mails wirken heute oft täuschend echt, zeichnen sich aber durch Drohungen, Dringlichkeiten, Bitten oder Exklusivität aus
  Darin wird der Empfänger aufgefordert auf eine manipulierte Internet-Seite oder am Mobiltelefon persönliche Zugangsdaten wie Benutzername, Passwörter oder Kreditkarten-Angaben usw. mitzuteilen

Ratschlag: Wurden Sie Opfer einer Phishing Attacke, Beleidigungen oder Hassrede im Netz?
Melden Sie den Angriff beim Nationalen Zentrum Cybersicherheit NCSC und helfen Sie mit, dass Internet für uns alle sicherer zu machen. https://www.ncsc.admin.ch/ncsc/de/home.html

Und zu guter Letzt gewähren Sie einer Person, die Sie nicht kennen oder der Sie nicht vertrauen, niemals einen Online-Zugang auf Ihren Computer.