Checkliste Verbraucherschutz

Das Themenfeld des Verbraucherschutzes wird in vielen Bereichen rund um den sicheren Einstieg mit Smartphone und Tablet gestreift.
Hier haben wir eine kleine Checkliste zusammengestellt, damit Sie einen Überblick haben, worauf Sie zu Ihrem persönlichen Schutz besonders achten sollten.

- [ ] **Ich halte mein Gerät aktuell.**
Prüfen Sie das Betriebssystem des Smartphones oder Tablets sowie alle installierten Apps regelmäßig auf Updates und installieren Sie diese. So sind Sie und Ihre Daten bestmöglich geschützt.

- [ ] **Ich erstelle für jedes Benutzerkonto ein individuelles und sicheres Passwort.**
Das Passwort sollte aus mindestens zehn Zeichen bestehen und Groß- und Kleinbuchstaben, Zahlen und Sonderzeichen enthalten.

- [ ] **Ich lade Apps nur aus vertrauenswürdigen Quellen wie dem App Store (bei Apple-Geräten) oder Play Store (bei Android-Geräten) herunter** – diese Apps werden auf Schadsoftware geprüft.

- [ ] **Ich lösche SMS, WhatsApp-Nachrichten oder E-Mails, wenn mir der Absender nicht bekannt ist oder nicht vertrauenswürdig erscheint.**

- [ ] **Ich öffne bei E-Mails von unbekannten Personen keine Anhänge und begutachte auch bei bekannten Personen den Anhang kritisch, wenn etwas verdächtig erscheint.**

Haben Sie keine Angst – das meiste, was Sie mit Tablet und Smartphone erleben können, ist positiv. Zu Ihrem eigenen Schutz sollten Sie dabei einfach auf diese Dinge achten.

☐ **Wenn sich jemand am Telefon als Bekannte oder Verwandter ausgibt, aber nicht eindeutig als diese Person erkennbar ist, werde ich skeptisch und lege auf.**
Rufen Sie die Person unter der Ihnen bekannten Nummer an. So können Sie prüfen, ob wirklich diese Person bei Ihnen angerufen hat.

☐ **Ich verrate sensible Daten wie Passwörter oder PINs nicht am Telefon oder über Messenger oder E-Mail.**
Diese Daten werden niemals von Ämtern oder Banken über die oben genannten Wege angefordert, und auch Staatsanwaltschaften oder Ordnungsämter fordern nicht telefonisch zu einer Zahlung auf.

☐ **Ich tippe in verdächtigen SMS, Messenger-Nachrichten oder E-Mails keine Links an.**
Werden Sie in einer E-Mail aufgefordert, Ihre Zugangsdaten – insbesondere für Online-Banking, aber auch für soziale Netzwerke oder Online-Shops – einzugeben oder diese über einen Link zu aktualisieren, handelt es sich sehr wahrscheinlich um einen Betrugsversuch. Wurden Sie mit vollständigem Namen angesprochen (lediglich die Angabe Ihrer E-Mail-Adresse ist nicht ausreichend)? Sind die vollständigen Angaben des (angeblich) anschreibenden Unternehmens angegeben? Sind Sie bei diesem Unternehmen überhaupt Kunde bzw. haben Sie an einem entsprechenden Gewinnspiel überhaupt teilgenommen? Ist die angeschriebene E-Mail-Adresse jene, die bei dem Dienst registriert ist? Trifft eines davon nicht zu, löschen Sie die E-Mail. Im Zweifelsfall: Suchen Sie über eine Suchmaschine Hinweise zu dem Aufruf oder rufen Sie das Unternehmen an und fragen Sie, ob die E-Mail von dort kommt. Nutzen Sie dazu keinesfalls eine in der Nachricht selbst angegebene Telefonnummer.

Haben Sie keine Angst – das meiste, was Sie mit Tablet und Smartphone erleben können, ist positiv. Zu Ihrem eigenen Schutz sollten Sie dabei einfach auf diese Dinge achten.

☐ **Ich verschicke niemals Geld oder Wertgegenstände und gebe keine Kontodaten weiter – egal ob mich jemand per E-Mail, Messenger-Nachricht, Telefon oder in einem Dating-Portal darum bittet.**
Die Aufforderung Geld an (scheinbare) Bekannte in Not zu schicken ist eine weit verbreitete Betrugsmasche. Dies gilt auch (und ganz besonders) für Bekannte aus dem Online-Dating.

☐ **Beim Online-Shopping achte ich darauf, nur bei seriösen Anbietern zu kaufen.**
Passt die angebotene Ware zum Namen der Internetseite? Ist ein Impressum vorhanden? Sind die Preise realistisch (im Vergleich zu anderen Anbietern)? Gibt es mehrere Zahlungsmöglichkeiten (nicht nur Vorkasse)? Sind die Texte auf der Internetseite fehlerfrei (Rechtschreibung, Grammatik)? ...

☐ **Beim Online-Dating achte ich auf meinen persönlichen Schutz, da ich nie genau wissen kann, mit wem ich es zu tun habe.**
Achten Sie darauf, nur Plattformen zu nutzen, bei denen sich die Nutzerinnen und Nutzer verifizieren müssen. Geben Sie nicht zu viele persönliche Daten preis. Vor einem ersten Treffen sollten immer Telefonate und Videoanrufe stattfinden.

Haben Sie keine Angst – das meiste, was Sie mit Tablet und Smartphone erleben können, ist positiv. Zu Ihrem eigenen Schutz sollten Sie dabei einfach auf diese Dinge achten.