Sicher durchs Internet

Android Smartphones

1. Apps nur aus dem offiziellen App-Store herunterladen

Laden Sie Apps ausschließlich aus dem offiziellen App-Store herunter:

- Beim Android-Smartphone ist das der Google Play Store.

Warum?
Der Google Play Store kontrolliert die dort angebotenen Programme (Apps) – sie sind also in der Regel sicher.
Natürlich kann es auch hier mal schwarze Schafe geben, aber das Risiko ist deutlich geringer als auf anderen Seiten im Internet.

Achtung:
Viele Internetseiten sehen seriös aus und versprechen tolle kostenlose Apps oder besondere Funktionen. Sie verleiten zum schnellen Herunterladen. Es werden oft andere Formulierungen als „App Download“ gewählt.
Hier einige Beispiele:

- Sicherheits-Applikation installieren
- Sicherheitsmodul oder Erweiterungsmodul herunterladen
- Ihre Sitzung ist abgelaufen, bitte aktualisieren Sie die aktuelle App Version *hier*.

Klicken Sie hier nicht leichtfertig!

Sicher durchs Internet

Android Smartphones

2. Halten Sie Ihr Betriebssystem auf den aktuellen Stand

Updates sind unverzichtbar für Ihre Sicherheit.

Aktualisieren Sie regelmäßig Ihr Betriebssystem (also die Software, die auf Ihrem Handy läuft). Sollte ein Software-Update verfügbar sein, nehmen Sie sich die Zeit und aktualisieren Sie Ihr Handy.

- Öffnen Sie die Einstellungen auf Ihrem Smartphone
- Wählen Sie „Software-Update“ oder „System-Update“
- Tippen Sie auf „Nach Updates suchen“
- Falls ein Update verfügbar ist, tippen Sie auf „Herunterladen / Installieren“

Tipp: Machen Sie Updates dann, wenn Sie Ihr Smartphone nicht brauchen, und wenn es am Ladegerät angeschlossen ist und mit dem WLAN verbunden ist.

Tipp: **Automatische System-Updates aktivieren:**

- Öffnen Sie die Einstellungen auf Ihrem Smartphone
- Gehen Sie zu „Software Update“ oder „System-Update“
- Tippen Sie auf „Automatische Updates“ oder aktivieren Sie den Menüpunkt „Automatisch über WLAN laden“

3. Aktualisieren Sie regelmäßig Ihre Apps

Apps die nicht gepflegt, also regelmäßig aktualisiert werden, löschen sie besser. Nicht aktuelle Apps stellen ein Sicherheitsrisiko da.

So prüfen Sie, ob App-Aktualisierungen (Updates) verfügbar sind:

- Öffnen Sie die App Google Play Store
- Tippen Sie oben rechts auf Ihr Profilsymbol
- Wählen Sie „Apps und Geräte verwalten“
- Hier sehen Sie, welche Apps aktualisiert werden können
- Tippen Sie auf „Alle aktualisieren“

Tipp: Aktivieren Sie die automatischen Aktualisierungen (Updates) Ihrer installierten Apps.

So stellen Sie ein, dass Ihre Apps automatisch aktualisiert werden:

- Öffnen Sie die App Google Play Store
- Tippen Sie oben rechts auf Ihr Profil-Symbol
- Tippen Sie auf „Einstellungen“
- Wählen Sie Netzwerkeinstellungen
- Tippen Sie auf „Apps automatisch aktualisieren“
- Wählen Sie „Nur über WLAN“ (empfohlen, um mobiles Datenvolumen zu sparen).

4. Öffentliches WLAN nur mit Vorsicht

Wenn Sie ein öffentliches WLAN nutzen:

- Keine Passwörter eingeben
- Keine Bankgeschäfte machen
- Keine persönlichen Daten eingeben

Vermeiden Sie es, sich automatisch mit öffentlichen WLAN´s zu verbinden (z.B. im Hotel oder in einem Einkaufszentrum).
Diese Funktion lässt sich so ausschalten:

- Öffnen Sie die Einstellungen
- Wählen Sie „Verbindungen“
- Wählen Sie das öffentliche WLAN aus
- Suchen Sie den Punkt „automatisch erneut verbinden“ und deaktivieren Sie diese Funktion. (ggf. in den Einstellungen / Zahnradsymbol neben dem Namen des WLAN´s)

Sicher durchs Internet

Android Smartphones

5. Achten Sie auf sichere Internetseiten (http**s**://)

Wenn Sie eine Internetseite (mit dem Browser, also nicht per App) aufrufen, achten Sie auf die Adresszeile.
Die Adresse sollte mit http**s**:// beginnen (das „s“ steht für „sicher“ englisch: „secure“).

Besonders wichtig bei:

- Online-Einkäufen
- Seiten, auf denen Sie sich einloggen
- Formularen, in denen Sie Daten eingeben

Achtung bei QR-Codes:
Ein QR-Code ist wie ein Link, der für Ihr Handy lesbar ist. Sie scannen ihn – und landen direkt auf einer Internetseite.
QR-Codes sind praktisch – aber schauen Sie sich die Adresse trotzdem genau an. Beginnt sie mit https://?

- Ein QR-Code allein richtet noch keinen Schaden an.
- Gefährlich wird es erst, wenn Sie dort persönliche Daten eingeben sollen.

Tipp:
Wenn Sie sich unsicher sind, geben Sie die Adresse lieber selbst ein.

6. Starke Passwörter nutzen

- Verwenden Sie lange Passwörter (mindestens 10 Zeichen).
- Kombinieren Sie Buchstaben, Zahlen und Sonderzeichen.
- Verwenden Sie für jede Seite ein anderes Passwort.

Das wichtigste Passwort, ist das Passwort zu Ihrer E-Mail-Adresse. Denn darüber lassen sich fast alle anderen Passwörter zurücksetzen.

Wie können Sie sich Ihre Passwörter merken?

- Sie können einen Passwortmanager nutzen.
- Sie notieren Ihre Passwörter auf Papier und bewahren diese nicht am Handy, sondern sicher zu Hause auf.

Zwei-Faktor-Authentifizierung (2FA) aktivieren

Sichern Sie Ihre Zugänge, nicht nur durch Ihr Passwort, sondern durch einen weiteren Beweis, dass es sich wirklich um Sie handelt. Das wird die Zwei-Faktor-Authentifizierung genannt. Ein weiterer Beweis kann z.B. sein: Eine SMS mit Code empfangen, eine Nachricht bestätigen z.B. in einer App, eine E-Mail mit Code erhalten.

Sicher durchs Internet

Android Smartphones

Vorteil: Selbst wenn jemand Ihr Passwort kennt, kann er sich nicht einloggen – weil der zweite Beweis fehlt.

Die Einstellung, um die Zwei-Faktor-Authentifizierung (2FA) einzurichten, ist Anbieterabhängig. Sie finden diese in den Konto- oder Passwort-Einstellungen des jeweiligen Anbieters, z.B. bei Ihrem E-Mail Anbieter unter Login & Sicherheit. Sie können die 2FA nur dort aktivieren, wo der Anbieter sie anbietet.

Bei vielen Anbietern, wie z.B. bei allen Banken ist die 2FA Anmeldung gesetzlich vorgeschrieben. Sie kommen hier also nicht drum rum diese auch zu nutzen.

Viele Anbieter von E-Mail Konten, bieten es freiwillig an. Und hier würde ich es dringlich empfehlen die 2FA auch einzurichten, denn das Passwort Ihrer E-Mail sollte bestmöglich geschützt sein.

7. Keine Links aus E-Mails oder SMS anklicken

Phishing-Gefahr! Lieber direkt auf die Webseite gehen.
Phishing ist ein Kunstwort aus „Passwort“ und „Fischen“. Kriminelle versuchen, mit gefälschten Nachrichten an Ihre Daten zu kommen.

Typische Maschen:

- Gefälschte E-Mails von „Banken“ oder „Online-Shops“
- Nachrichten über angebliche Paketlieferungen
- SMS oder WhatsApp-Nachrichten mit Links
- „Hallo Mama, ich habe ein neues Handy…“

Wichtig:

- Klicken Sie niemals auf Links in solchen Nachrichten
- Geben Sie keine Daten ein
- Überweisen Sie niemals Geld, ohne sich abzusichern

Wenn Sie unsicher sind, rufen Sie den Absender unter der Ihnen bekannten Nummer an – nicht unter der Nummer aus der Nachricht!

Wenn Sie eine E-Mail oder eine SMS / WhatsApp oder einen Anruf von „Ihrer Bank“ bekommen und es heißt:

- Ihr Konto wurde gehackt
- Sie müssen sofort etwas tun
- Sie sollen Daten preisgeben oder auf einen Link klicken

Sicher durchs Internet

Android Smartphones

LEGEN SIE AUF ❗ KLICKEN SIE NIEMALS AUF LINKS ❗
GEBEN SIE KEINE DATEN AM TELEFON PREIS ❗

Rufen Sie Ihre Bank nur unter der offiziellen Telefonnummer an – also die Nummer, die Sie aus dem Telefonbuch kennen oder von Ihrer Bankkarte. Oder gehen Sie direkt in die Filiale.

🛑 Das gleiche gilt für Anrufe oder E-Mails von Telefonanbieter, die behaupten Ihr Anschluss wird gesperrt!

🛑 Ebenso für Paket Lieferanten,
auch wenn es angeblich sehr eilig ist Zollgebühren zu bezahlen!

🛑 Und auch wenn Sie angeblich etwas gewonnen haben!

KLICKEN SIE NICHT ❗
UND AM TELEFON KEINE DATEN NENNEN ❗

8. Unbekannte Online-Shops? Genau prüfen!

Sie sehen ein tolles Angebot in einem unbekannten Internet-Shop? Dann prüfen Sie vorher ganz genau:

- Handelt es sich um eine verschlüsselte sichere Seite mit http**s**://?
- Ist der Preis vielleicht zu schön um wahr zu sein?
- Gibt es ein vollständiges Impressum mit Adresse?
- In Deutschland ist ein vollständiges Impressum Pflicht. Nur ein Postfach oder eine E-Mail Adresse ist nicht ausreichend.
- Gibt es Bewertungen? – Nicht nur die Bewertungen auf der Seite des Shops, prüfen Sie lieber Google Bewertungen, Verbraucherzentralen oder andere unabhängige Foren.
- Welche Bezahlmöglichkeiten werden angeboten? Vorsicht bei Vorkasse. Gibt es AGB´s und ein Rückgaberecht?
- Schauen Sie hier: Fake-Shop-Check: www.fakeshop-finder.de (Verbraucherzentrale)

Tipp: Im Zweifel lieber auf den Kauf verzichten – und auf Nummer sicher gehen.

9. Stimmen, Bilder und Videos können gefälscht sein – seien Sie skeptisch

Was Sie hören und sehen, muss nicht echt sein.
Durch sogenannte „Künstliche Intelligenz“ (KI) lassen sich inzwischen Stimmen, Fotos und ganze Videos fälschen und sehen täuschend echt aus.

Was bedeutet das für Sie?

- Sie könnten ein Video sehen, in dem ein bekannter Mensch etwas sagt – das er nie gesagt hat.
- Sie könnten einen Anruf mit der Stimme Ihrer Tochter bekommen – der nicht von ihr stammt.
- Sie könnten ein Foto sehen, das aussieht wie eine echte Szene – das aber am Computer erstellt wurde.
- Diese Technik ist beeindruckend, aber leider auch für Betrüger zugänglich.

Glauben Sie nicht alles, nur weil es echt aussieht oder sich vertraut anhört. Im Zweifel: nachfragen, prüfen, misstrauen.

10. Persönliche Daten: Nur so viel wie nötig

Geben Sie nur das preis, was wirklich nötig ist.

- Geburtsdatum, Adresse, Telefonnummer – das alles ist wertvoll für Betrüger.
- Je weniger bekannt ist, desto sicherer sind Sie.

Regel: So viel wie nötig – so wenig wie möglich.