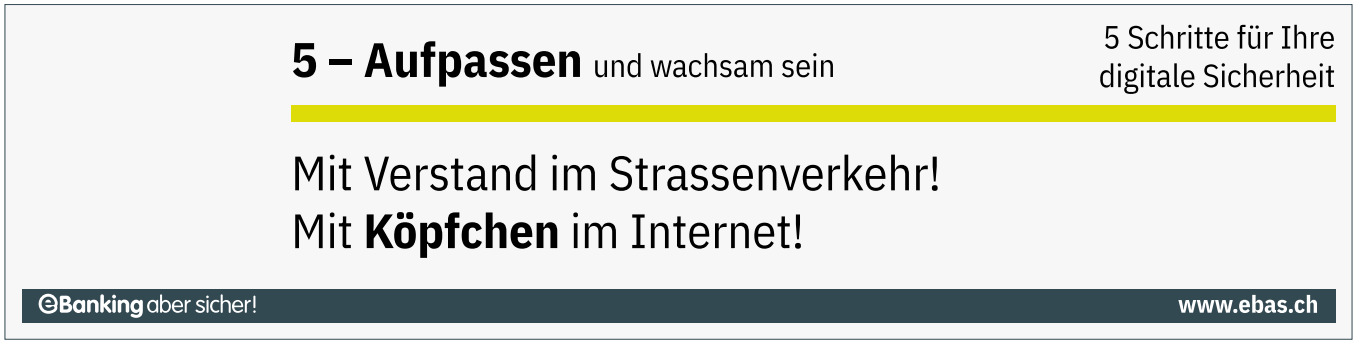
# 5 – Aufpassen und wachsam sein

**Glauben Sie alles, was Ihnen weisgemacht wird? Nehmen Sie Ihre Eigenverantwortung wahr und surfen Sie im Internet stets mit einer gesunden Portion Misstrauen.**

**Wichtigste Merkpunkte:**

- Seien Sie beim Surfen im Internet stets misstrauisch und überlegen Sie sich gut, wo und wem Sie Ihre persönlichen Informationen preisgeben.
- Finanzinstitute, Telekommunikations- und sonstige Dienstleistungsunternehmen fragen nie nach einem Passwort (weder per E-Mail, noch per Telefon) und verlangen auf diese Weise auch keinen Passwortwechsel.
- Beachten Sie bei der Verwendung von mobilen Geräten (Smartphones, Tablets) die gleichen Vorsichtsmassnahmen wie an Ihrem Computer zuhause.
- Holen Sie sich bei Unsicherheit oder Verdacht auf einen Angriff Unterstützung.




Mit den Schritten 1 bis 4 haben Sie Ihre Geräte und Online-Zugänge technisch sehr gut abgesichert. Oft bleibt allerdings das Verhalten der Benutzerin oder des Benutzers selbst das grösste Risiko und wird so zum Ziel von Angriffen – lassen Sie deshalb stets Ihren gesunden Menschenverstand walten.

## Schutz vor Phishing und Social Engineering

Beim Phishing (https://www.ebas.ch/phishing/) versuchen Betrüger in E-Mails oder am Telefon Ihr Vertrauen zu gewinnen, indem sie sich z. B. als Ihr Finanzinstitut ausgeben und Sie mit einem Link auf eine Website locken, die jener Ihres Finanzinstituts ähnlich sieht. Fallen Sie darauf herein und geben Ihre Zugangsdaten ein, können Kriminelle damit Ihr Konto plündern.

Oder bei Betrügerischen Supportanrufen (https://www.ebas.ch/betruegerische-supportanrufe/) werden Sie von einem angeblichen Mitarbeitenden von Microsoft oder einer IT-Support-Firma kontaktiert, welcher dann versucht, Zugriff auf Ihr Gerät zu erhalten.

**Denken Sie daran: Ein seriöses Finanzinstitut wird Sie niemals per E-Mail oder Telefon nach Ihren E-Banking-Zugangsdaten fragen.**

Die Grundlage für solche Angriffe finden Betrüger oft in Sozialen Medien und Netzwerken

(https://www.ebas.ch/soziale-medien-und-netzwerke/) . Seien Sie auch dort vorsichtig und überlegen Sie sich gut, welche Informationen Sie von sich preisgeben.

## Erhöhte Risiken bei mobilen Geräten

**Zugriffsrechte bei mobilen Apps**

Viele Apps räumen sich ohne erkennbaren Grund umfassende Rechte ein. Ein Zugriff auf beispielsweise Standortdaten, Adressbuch oder den Telefonstatus ist nicht bei jeder App notwendig. Prüfen Sie daher kritisch, ob die Zugriffsrechte zum Erfüllen der Funktionalität wirklich notwendig sind, und deaktivieren Sie nach Möglichkeit alle nicht benötigten Rechte.

Prinzipiell sollten Sie mit der Weitergabe Ihrer Ortsangaben sehr zurückhaltend sein: Meiden Sie Lokalisierungsdienste und speichern Sie keine Positionsangaben in Fotos, die Sie ins Internet laden. Diebe und Hacker könnten sich diese Informationen zunutze machen.

**Bei Verlust sofort sperren**

Verlorene oder gestohlene Geräte können Sie mithilfe verschiedener Apps aus der Ferne sperren. Dadurch sind Ihre persönlichen Daten auf dem Gerät gelöscht und nicht mehr aufzurufen. Doch Vorsicht: Derartige Befehle können ebenso von böswilligen Dritten genutzt werden. Achten Sie auch hier auf einen vertrauenswürdigen Anbieter. Nach erfolgter Geräte-Sperrung sollten Sie auch die SIM-Karte bei Ihrem Anbieter sperren lassen.

## Hilfe anfordern

Sind Sie unsicher, haben Sie den Verdacht auf einen Angriff oder sind Sie gar Opfer eines Angriffs geworden, zögern Sie nicht, sich Hilfe zu holen – beispielsweise:

- Bei Unklarheiten und Unsicherheiten im E-Banking kontaktieren Sie Ihr Finanzinstitut (https://www.ebas.ch/partner/) .
- Bei technischen Problemen oder Verdacht auf Malwarebefall, holen Sie sich Rat und Hilfe bei einem IT-Experten/IT-Supporter.
- Sind Sie Opfer eines Angriffes geworden, melden Sie diesen bei Ihrem Finanzinstitut (https://www.ebas.ch/partner/) und bei der Polizei (https://polizei.ch) .

*Schützen Sie Ihre Daten und alle Ihre Geräte mit den «5 Schritten für Ihre digitale Sicherheit»:*

*Schritt 1 – Sichern (https://www.ebas.ch/1-sichern-der-daten/)*
*Schritt 2 – Überwachen (https://www.ebas.ch/2-ueberwachen-mit-virenschutz-und-firewall/)*
*Schritt 3 – Vorbeugen (https://www.ebas.ch/3-vorbeugen-mit-software-updates/)*
*Schritt 4 – Schützen (https://www.ebas.ch/4-schuetzen-der-online-zugaenge/)*
***Schritt 5 – Aufpassen***