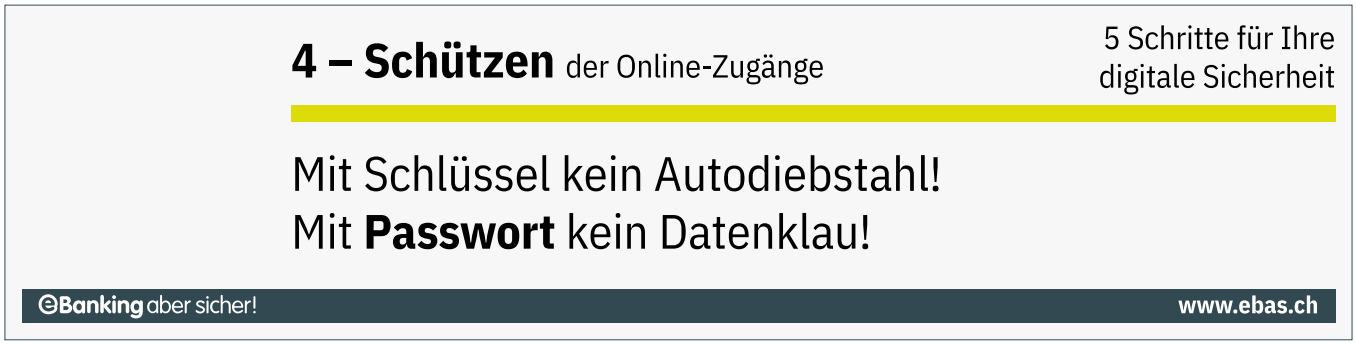
4 – Schützen der Online-Zugänge

Verschliessen Sie die Türe, wenn Sie das Haus oder die Wohnung verlassen? Schützen Sie auch Ihre Geräte und Online-Zugänge vor fremdem Zugriff.

Wichtigste Merkpunkte:

- Schützen Sie Ihren Computer und mobilen Geräte (Smartphones, Tablets etc.) vor unbefugtem Zugriff und sperren Sie den Bildschirm, wenn Sie nicht aktiv am Gerät arbeiten.
- Verwenden Sie sichere Passwörter (mind. 10 Zeichen lang, aus Ziffern, Gross- und Kleinbuchstaben sowie Sonderzeichen bestehend).
- Benutzen Sie nicht überall dasselbe Passwort, sondern für verschiedene Angebote verschiedene Passwörter.
- Aktivieren Sie nach Möglichkeit die sogenannte Zwei-Faktor-Authentifizierung.



Geräte vor unbefugten Zugriff absichern

Schützen Sie alle Ihre Geräte mit einem Zugangsschutz. Gerade bei Notebooks, Tablets und Smartphones sind Verlust und Diebstahl weitaus grössere Gefahren als beim Heim-PC.

Vergewissern Sie sich deshalb, dass insbesondere bei Ihren mobilen Geräten die automatische Bildschirmsperre mittels Code, Passwort, Fingerabdruck oder Gesichtserkennung eingeschaltet ist.

Zudem sollten Sie die Daten auf Ihrem Mobilgerät verschlüsseln. Dies gilt insbesondere auch für Zusatzspeicher wie externe Festplatten oder USB-Sticks. So verunmöglichen Sie Unbefugten den Zugriff auf Ihre Daten und Apps über Fremdsysteme.

iPhone/iPad

Unter Einstellungen/Touch ID & Code können Sie das Gerät mit einem Zahlencode oder Passwort schützen sowie Fingerprints hinterlegen. Beim iPhone X lässt sich unter Einstellungen/Face ID & Code die Gesichtserkennung konfigurieren. Die Daten werden beim iPhone bzw. iPad automatisch verschlüsselt abgespeichert.

Android

Je nach Gerät können Sie die Codesperre unter Einstellungen/Sicherheit einstellen. Aktivierung Sie unter Verschlüsselung & Anmeldedaten zudem die Verschlüsselung Ihrer Daten – wo nötig auch für Zusatzspeicher.

Sichere Passwörter

Passwörter sind nach wie vor die gängigsten und am meisten verwendeten Schlüssel im elektronischen Umfeld. Sie schützen den Zugriff auf sensible und private Daten. Durch ein paar einfache Regeln im Umgang mit Passwörtern sind Sie besser geschützt.

6 Regeln zum sicheren Passwort - verwenden Sie...

- mindestens 10 Zeichen
- Ziffern, Gross- und Kleinbuchstaben sowie Sonderzeichen
- keine Tastaturfolgen wie z.B. «asdfgh» oder «45678»
- kein Wort einer bekannten Sprache, d. h. das Passwort sollte keinen Sinn machen
- nicht überall dasselbe Passwort
- speichern Sie Ihr Passwort nicht unverschlüsselt ab

Nachfolgend ist beschrieben wie Sie auf einfache Art und Weise ein sicheres Passwort erstellen und es sich auch merken können:

- Nehmen Sie einen Satz, den Sie sich gut merken können, und bilden Sie Ihr Passwort mit den jeweiligen Anfangsbuchstaben und Ziffern:
  «**M**eine **T**ochter **T**amara **h**at **a**m **19. J**anuar **G**eburtstag**!**»
- So entsteht ein Passwort aus einer beliebigen Zeichenfolge, das Sie sich gut merken können:
  «**MTTha19.JG!**»

Passwort-Manager

In einem Passwort-Manager können Sie sämtliche Passwörter verschlüsselt abspeichern – und müssen sich dadurch nur noch ein einziges Passwort merken.

Windows

Für den Einsatz unter Windows empfehlen wir folgende, zum Teil kostenlose Passwort-Manager:

- KeePass (https://www.keepass.info)
- Password Safe (https://www.passwordsafe.de)
- SecureSafe (https://www.securesafe.com)
- eWallet (https://www.iliumsoft.com)

macOS

Für den Einsatz unter Mac empfehlen wir folgende, zum Teil kostenlose Passwort-Manager:

- KeePassXC (https://keepassxc.org)
- SecureSafe (https://www.securesafe.com)
- eWallet (https://www.iliumsoft.com)

Smartphone und Tablet

Für den Einsatz auf dem Smartphone oder Tablet empfehlen wir folgende, zum Teil kostenlose Passwort-Manager:

- KeePass (https://www.keepass.info)
- Password Safe (https://www.passwordsafe.de)
- SecureSafe (https://www.securesafe.com)
- eWallet (https://www.iliumsoft.com)

Zwei-Faktor-Authentifizierung

Zusätzlich zu einem sicheren Passwort sorgt die sogenannte Zwei-Faktor-Authentifizierung für noch mehr Sicherheit. Dabei wird beim Login zusätzlich zum ersten Sicherheitselement (meistens ein Passwort) ein zweites, unabhängiges Sicherheitselement abgefragt. Dies kann beispielsweise ein Code sein, der auf ein Mobiltelefon geschickt oder direkt auf diesem generiert wird.

Mittlerweile bieten nebst Finanzinstituten auch viele weitere Online-Dienstleister (z.B. Google, Facebook) eine Zwei-Faktor-Authentifizierung an. Nutzen Sie diese für eine erhöhte Sicherheit. Eine Beschreibung der verschiedenen bei Finanzinstituten eingesetzten Verfahren finden Sie hier (https://www.ebas.ch/category/23).

Wurde mein Online-Zugang gehackt?

Kontrollieren Sie, ob das Passwort eines Ihrer Online-Konten gehackt wurde:

https://haveibeenpwned.com (https://haveibeenpwned.com)

Auf der kostenlosen Plattform «Have I Been Pwned» können Sie herausfinden, ob Ihre Login-Daten zu einem Online-Konto kompromittiert oder bei einer Datenpanne veröffentlicht wurden. Geben Sie hierzu Ihren entsprechenden Benutzernamen oder Ihre E-Mail-Adresse und niemals das zu prüfende Passwort ein!

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
Schritt 5 – Aufpassen (https://www.ebas.ch/5-aufpassen-und-wachsam-sein/)