Starkes Passwort & Co.

Wie Sie Ihre Online-Zugänge vor unbefugtem Zugriff schützen können

Ihre Polizei und die Schweizerische Kriminalprävention (SKP) – eine interkantonale Fachstelle der Konferenz der kantonalen Justiz- und Polizeidirektorinnen und -direktoren (KKJPD), in Zusammenarbeit mit der Hochschule Luzern und «eBanking – aber sicher!»

So wie Sie die Türe verschliessen, wenn Sie das Haus oder die Wohnung verlassen, so sollten Sie auch Ihre Geräte und Online-Zugänge vor fremdem Zugriff schützen.

Wichtigste Merkpunkte:

- Schützen Sie Ihren Computer und Ihre mobilen Geräte (Smartphones, Tablets etc.) vor unbefugtem Zugriff und **sperren Sie den Bildschirm,** wenn Sie nicht aktiv am Gerät arbeiten.
- Verwenden Sie **starke Passwörter** (mind. 12 Zeichen lang, aus Ziffern, Gross- und Kleinbuchstaben sowie Sonderzeichen bestehend).
- Benutzen Sie nicht überall dasselbe Passwort, sondern für verschiedene Angebote **unterschiedliche Passwörter.**
- Aktivieren Sie nach Möglichkeit die sogenannte **Zwei-Faktor-Authentifizierung.**

Wurde mein Online-Zugang gehackt?

Kontrollieren Sie, ob das Passwort eines Ihrer Online-Konten gehackt wurde. Auf **www.ebas.ch/haveibeenpwned** können Sie herausfinden, ob Ihre Login-Daten zu einem Online-Konto kompromittiert oder bei einer Datenpanne veröffentlicht wurden. Die Seite konsultiert den Datenbestand der bekannten Plattform **haveibeenpwned.com** und bereitet die Resultate für Sie in deutscher Sprache auf. Geben Sie hierzu Ihren entsprechenden Benutzernamen oder Ihre E-Mail-Adresse und niemals das zu prüfende Passwort ein!

www.ebas.ch/have-i-been-pwned

haveibeenpwned.com

Wie Sie Ihre Geräte gegen 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

- Zugriffssperre bis iPhone 9: Unter **Einstellungen/ Touch ID & Code** können Sie das Gerät mit einem Zahlencode oder Passwort schützen sowie Fingerprints hinterlegen.
- Zugriffssperre ab iPhone 10: Unter **Einstellungen/Face ID & Code** lässt sich die Gesichtserkennung konfigurieren.
- Beim iPhone bzw. iPad werden die Daten automatisch verschlüsselt.

Android

- Je nach Gerät können Sie die Zugriffssperre unter **Einstellungen/Sicherheit und Datenschutz** einstellen.
- Die Verschlüsselung können Sie unter **Einstellungen/ Sicherheit und Datenschutz/ Mehr Sicherheit und Datenschutz/Verschlüsselung & Anmeldedaten** aktivieren – wo nötig auch für Zusatzspeicher.

Wie Sie starke Passwörter erstellen

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.

Sechs Regeln für ein starkes Passwort

1. Mindestens 12 Zeichen
2. Ziffern, Gross- und Kleinbuchstaben sowie Sonderzeichen
3. Keine Tastaturfolgen wie z. B. «asdfgh» oder «45678»
4. Kein Wort einer bekannten Sprache. Das Passwort sollte keinen Sinn ergeben und in keinem Wörterbuch vorkommen.
5. Überall ein anderes Passwort
6. Speichern Sie Ihr Passwort nicht unverschlüsselt ab.

Nachfolgend ein Beispiel, wie Sie auf einfache Art und Weise ein starkes Passwort erstellen:

- 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 **M**eier **h**at **a**m **19. J**anuar **G**eburtstag**!**»
- So entsteht ein Passwort aus einer beliebig wirkenden Zeichenfolge, das Sie sich aber gut merken können: «**MTTMha19.JG!**»

Passwort-Manager

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

www.ebas.ch/step4

Video zum Passwort-Manager:

www.youtube.com/watch?v=dsfBqVNuIds

Zwei-Faktor-Authentifizierung

Zusätzlich zu einem starken 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 unter:

www.ebas.ch/beachten-sie-beim-anmelden

Video zur Zwei-Faktor-Authentifizierung:

www.youtube.com/watch?v=hWi4AqkdARI

Passkeys

Passkeys ersetzen Passwörter durch fortschrittliche Verschlüsselung und biometrische Daten. Diese neue Technologie bietet eine benutzerfreundliche und sichere Methode, auf Online-Konten zuzugreifen. Ein Passkey ist ein digitaler Schlüssel, bestehend aus einem öffentlichen und einem geheimen Schlüssel. Der geheime Schlüssel ist auf Ihrem Gerät gespeichert und durch PIN oder biometrische Daten wie Fingerabdruck oder Gesichtserkennung geschützt. Selbst wenn Ihr Gerät gestohlen wird, kann niemand ohne Ihre biometrischen Daten oder PIN auf Ihre Passkeys zugreifen. Erfahren Sie mehr über die Funktionsweise und das Erstellen eines Passkey unter:

www.ebas.ch/passkeys

Januar 2025

SKPPSC

Schweizerische Kriminalprävention
Haus der Kantone
Speichergasse 6
3001 Bern

www.skppsc.ch

Dieses Faltblatt entstand in Zusammenarbeit mit
der **Hochschule Luzern** und **«eBanking – aber sicher!»**.

www.ebas.ch | www.ebankingabersicher.ch

HSLU Hochschule Luzern

eBanking aber sicher!