

22.05.2026

«Bequemlichkeit» das grösste Sicherheitsrisiko

In der modernen digitalen Welt ist Zeit die wertvollste Währung. Alles muss sofort, intuitiv und mit möglichst wenig Aufwand erfolgen. Die Banken haben auf diesen Wunsch reagiert und das E-Banking so benutzerfreundlich wie nie zuvor gestaltet. Doch genau in diesem Streben nach maximalem Komfort liegt eine unterschätzte Gefahr. Während die technischen Sicherheitssysteme der Finanzinstitute heute Festungen gleichen, bleibt der Mensch die Variable, die durch den Wunsch nach Bequemlichkeit oft die Tore öffnet.

Der psychologische Konflikt zwischen Sicherheit und Komfort

Sicherheit und Bequemlichkeit stehen sich in der Informationstechnologie meist völlig gegensätzlich gegenüber. Echte Sicherheit erfordert oft zusätzliche Schritte, bewusstes Innehalten und eine gewisse kognitive Anstrengung. Doch unser Gehirn ist darauf programmiert, Energie zu sparen und den Weg des geringsten Widerstands zu gehen. Dies führt dazu, dass Sicherheitsmassnahmen oft als störende Barrieren wahrgenommen werden, die es zu umgehen oder so schnell wie möglich hinter sich zu bringen gilt.

Ein klassisches Beispiel ist die Wahl des Passworts. Ein kryptisches, langes Passwort, das man sich mühsam merken muss, wird zugunsten einer einfachen, vertrauten Kombination verworfen. Noch gefährlicher wird es, wenn aus reiner Bequemlichkeit dasselbe Passwort für alle Dienste verwendet wird. Kriminelle wissen das: Ein einziger erfolgreicher Angriff auf einen unsicheren Online-Shop kann so zum Generalschlüssel für das gesamte digitale Leben eines Nutzers werden.

Wenn Schnelligkeit vor Gründlichkeit geht

Die grösste Bedrohung entsteht jedoch im Moment der Transaktion. Moderne Betrugsmaschinen wie das [Social Engineering](https://www.ebas.ch/social-engineering/) (<https://www.ebas.ch/social-engineering/>) zielen exakt auf unsere Neigung ab, Dinge schnell und ohne langes Nachdenken zu erledigen. Wenn eine Push-Nachricht auf dem Smartphone erscheint, die zur Freigabe einer Zahlung auffordert, neigen viele dazu, den Bestätigungsknopf fast reflexartig zu drücken. In der Eile wird oft übersehen, ob der Betrag, der Empfänger oder der Zeitpunkt der Anfrage überhaupt plausibel sind.

Betrüger nutzen diese «Klick-Mentalität» gezielt aus. Sie setzen ihre Opfer unter Zeitdruck oder täuschen eine gewohnte Routine vor. Wer in einem stressigen Moment schnell eine vermeintliche Sicherheitsprüfung bestätigt, hat oft schon verloren. Dabei ist gerade diese kurze Unterbrechung – das bewusste Lesen einer SMS-Bestätigung oder das Überprüfen der URL im Browser – der entscheidende Schutzwall gegen den Verlust des eigenen Vermögens.

Ein Plädoyer für die «bewusste Unbequemlichkeit»

Um sich effektiv zu schützen, müssen Nutzer lernen, eine gewisse Unbequemlichkeit als Qualitätsmerkmal von Sicherheit zu akzeptieren. Das Einrichten eines Passwort-Managers, das konsequente Nutzen der Zwei-Faktor-Authentifizierung (2FA) oder das manuelle Eintippen einer Bank-URL, anstatt auf einen Link in einer E-Mail zu klicken, sind kleine Investitionen an Zeit, die einen immensen Schutz bieten.

Die Technik allein reicht nicht aus. Wahre digitale Resilienz entsteht erst durch ein gesundes Mass an Misstrauen und die Bereitschaft, den Komfort kurzzeitig hintenanzustellen. Sicherheit im Netz ist kein Zustand, sondern ein ak-

tiver Prozess. Wer bereit ist, den «extra Schritt» zu gehen, macht es den Kriminellen schwerer, als es jede Firewall allein könnte. Am Ende ist ein wenig Aufwand ein kleiner Preis für die Gewissheit, dass das eigene Geld sicher bleibt.

Mögliche Schutzstrategien

Um der Falle der Bequemlichkeit zu entgehen, helfen bereits kleine Verhaltensänderungen, die Ihre Sicherheit massiv erhöhen.

- **Bewusste Entschleunigung:**

Führen Sie Entscheidungen niemals unter Zeitdruck durch. Nehmen Sie sich die Zeit und schauen Sie es sich genau an.

- **Strikte Passwort-Disziplin:**

Verwenden Sie einzigartige, komplexe [Passwörter \(https://www.ebas.ch/4-schuetzen-der-online-zugaenge/\)](https://www.ebas.ch/4-schuetzen-der-online-zugaenge/), das Sie bei keinem anderen Dienst nutzen. Ein Passwort-Manager hilft Ihnen dabei, die Übersicht zu behalten, ohne dass die Sicherheit unter der Bequemlichkeit leidet.

- **Konsequente Zwei-Faktor-Authentifizierung (2FA):**

Aktivieren Sie die zusätzliche Bestätigung auf einem zweiten Gerät überall dort, wo es möglich ist. Betrachten Sie diesen Zusatzschritt nicht als Hindernis, sondern als Ihre wichtigste digitale Lebensversicherung gegen [Identitätsdiebstahl \(https://www.ebas.ch/identitaetsdiebstahl/\)](https://www.ebas.ch/identitaetsdiebstahl/).

- **Automatisierung:**

Überlassen Sie die Sicherheit nicht Ihrem Gedächtnis. Aktivieren Sie automatische [Updates \(https://www.ebas.ch/3-vorbeugen-mit-software-updates/\)](https://www.ebas.ch/3-vorbeugen-mit-software-updates/) für Ihr Betriebssystem, Ihren Browser und Ihre Apps, damit kritische Sicherheitslücken sofort geschlossen werden, ohne dass Sie aktiv daran denken müssen.

- **Kritische Distanz zu Komfort-Features:**

Funktionen wie FaceID- oder Fingerabdruck-Logins sind komfortabel, verleiten aber zu reflexivem Handeln. Hinterfragen Sie jede biometrische Abfrage kurz, um nicht versehentlich einen fremden Zugriff zu autorisieren.