So schütze ich mich.

» Nachrichten von Unbekannten misstrauen.
» Nie auf Links klicken oder Anhänge öffnen.
» Immer Absender-E-Mail und URL prüfen.
» Nur über offizielle Websites einloggen (nicht via Links).
» Webbrowser und Betriebssystem aktuell halten.
» Nie Login- und Kartendaten herausgeben.
» Starke Passwörter und Zwei-Faktor-Authentifizierung nutzen.
» Benachrichtigungsdienst aktivieren, um bei Zahlungen Nachricht zu erhalten.
» Transaktionen und Zahlungen prüfen.

Teste dein Wissen!

Was kann ich ausserdem noch tun?

» Sich bei der Bank oder dem Kartenherausgeber über Sicherheitsfunktionen der Karte informieren.
» Nur Kartenfunktionen aktivieren, die im Alltag tatsächlich genutzt werden.
» Bei Diebstahl Anzeige erstatten.

Mehr zum Thema Kartensicherheit unter
www.card-security.ch

SKPPSC Schweizerische Kriminalprävention
Prévention Suisse de la Criminalité
Prevenzione Svizzera della Criminalità

Ihre POLIZEI
Votre POLICE
La vostra POLIZIA
Kantonale und Städtische Polizeikorps
Corps de police cantonaux et municipaux
Corpi di polizia cantonali e comunali

#ufpasse

Vorsicht Phishing!

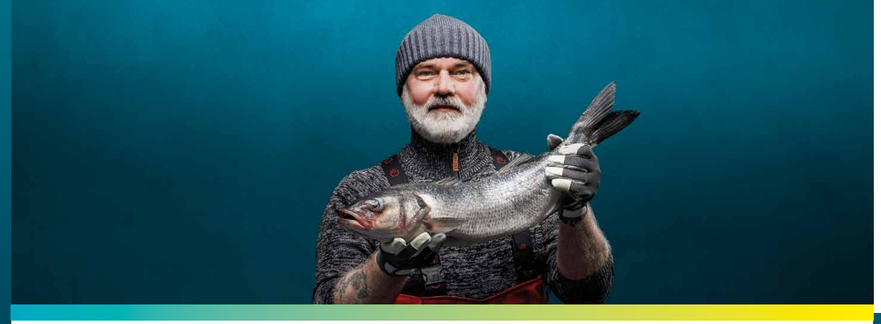
Schütze dich vor Kartenmissbrauch.

card security

Ihre Polizei

#ufpasse vor diesen BETRUGS-ARTEN

Debit- und Kreditkarten sind sehr sichere und beliebte Zahlungsmittel, die häufig genutzt werden. Das lockt auch Betrüger und Betrügerinnen an. Sie versuchen mit immer neuen Betrugsmaschen ihren Opfern Geld zu stehlen. Die meisten Kartendelikte können verhindert werden, wenn sich Kartenbesitzerinnen und Kartenbesitzer an wenige Grundregeln halten.



Phishing

Phishing-Angriffe unterscheiden sich oftmals in ihrer Aufmachung und Tonalität. Das Prinzip dahinter ist jedoch immer dasselbe. Die potenziellen Opfer erhalten Nachrichten via E-Mail, Handy oder Social Media. Diese sehen aus wie von einer Bank, der Kartengesellschaft oder einem Lieferservice. Die Opfer werden aufgefordert, dem Link in der Nachricht zu folgen. Wer auf den Link klickt, kommt auf eine gefälschte Website und soll dort persönliche Informationen preisgeben. Wer hier nicht aufpasst, verliert viel Geld.

Pharming

Pharming ist mit Phishing verwandt. Nutzerinnen und Nutzer geben eine korrekte Webadresse ein und werden unbemerkt auf eine gefälschte Website umgeleitet. Dies geschieht mithilfe eines Virus oder eines Trojanischen Pferds. Wie beim Phishing werden die Opfer dann aufgefordert, persönliche Daten und Karteninformationen einzugeben. Mit diesen Informationen können die Betrüger oder Betrügerinnen schliesslich problemlos Geld stehlen. Die Betrugsart wird «Pharming» genannt, weil im Hintergrund oft ganze Server-Farmen mit gefälschten Webseites betrieben werden.

Carding

Bei Carding nutzen Täterinnen oder Täter gestohlene oder gefälschte Karteninformationen, um online einzukaufen oder Geld am Bancomaten abzuheben. Sie bevorzugen Karten oder Online-Shops, die mangelhaft geschützt sind. Die benötigten Daten wurden vorgängig durch Phishing-Betrug, Datenschutzverletzungen oder Skimming illegal gesammelt und im Darknet verkauft. Die Opfer bemerken den Betrug erst, wenn bereits Geld gestohlen worden ist. Zwischen dem Datendiebstahl und dem eigentlichen Betrug können oft Monate verstreichen.

Scamming

Bei Scamming versuchen Betrügerinnen oder Betrüger ihre Opfer mit verlockenden Angeboten zu ködern. Alle Avancen zielen darauf ab, die Opfer unter Vorwänden dazu zu bringen, Vorauszahlungen zu leisten. Scamming hat viele Gesichter: Betrug mit vorgetäuschter Liebe (Romance Scam), Betrug mit falschen Geldversprechen (Investment Scam), Betrug mit Wohnungsangeboten (Flatmate Scam), Betrug mit dem Traumjob (Employment Scam) oder Lottogewinn-Versprechen (Lottery Scam).