KARTENZAHLUNGEN SIND SICHER.

Debit- und Kreditkarten sind sehr sichere und beliebte Zahlungsmittel, die häufig genutzt werden. Das lockt auch Betrüger:innen an. Phishing-Angriffe nehmen zu. Dabei gehen die Täter:innen immer raffinierter und professioneller vor, sodass die Opfer keinen Verdacht schöpfen.

Die meisten Kartendelikte können Sie durch Einhalten weniger Grundregeln selbst verhindern. Achten Sie darauf!

Zum Wissenstest

Mehr zum Thema Kartensicherheit:
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!

Ihre Polizei

card security

WAS IST PHISHING?

Phishing ist aktuell die häufigste Betrugsmasche bei Debit- und Kreditkarten. Fast jeder Kartenbetrug beginnt mit einer Phishing-Nachricht. Dabei gehen die Täter:innen sehr geschickt vor.

Sie tarnen ihre Nachrichten beispielsweise als Mitteilungen einer Bank, einer Kartengesellschaft oder eines Lieferservices und kontaktieren die Empfänger:innen via SMS, WhatsApp, E-Mail usw. Die Opfer werden aufgefordert, einem Link in der Nachricht zu folgen. Dieser führt auf eine gefälschte Website. Dort sollen die Opfer persönliche Informationen preisgeben.

Sobald die «Phisher» die Daten haben, heben sie Geld ab oder kaufen mit der Karte online ein. Wer nicht auf der Hut ist, verliert rasch sehr viel Geld.

Wer auf Phishing-Mails reagiert und Zugangsdaten oder Codes weitergibt, setzt sich einer grossen Gefahr aus: Wenn die Sorgfaltspflichten verletzt wurden, haften die Karteninhaber:innen in der Regel für den Schaden selbst.

TIPPS GEGEN PHISHING-ANGRIFFE

Absender prüfen.
Wenn Sie unsicher sind, ob es sich um eine Phishing-Nachricht handelt, prüfen Sie die E-Mail-Adresse des Absenders. Kennen Sie diese Person? Ist die E-Mail-Adresse glaubwürdig? Fragen Sie beim offiziellen Absender, zum Beispiel bei der Bank oder dem Lieferservice, nach.

Keine Zugangsdaten weitergeben.
Ihre Bank oder Ihr Kartenanbieter kontaktiert Sie nie, um vertrauliche Informationen oder Zugangsdaten abzufragen. Auch über ungewöhnliche Konto- oder Kartenbewegungen informieren die Finanzinstitute nie via E-Mail. Antworten Sie nicht auf solche Anfragen.

Fehler suchen.
Prüfen Sie, ob eine unerwartete Mail echt ist. Achten Sie auf falsche Logos, Schreibfehler oder falsche Firmennamen. Es lohnt sich, genau hinzuschauen.

Nicht unter Zeitdruck handeln.
Werden Sie misstrauisch, wenn Sie jemand unter Zeitdruck setzt oder mit schwerwiegenden Folgen droht. Typisch für Phishing-Mails ist, dass kurze Fristen gesetzt werden oder Ihnen mit strafrechtlichen Folgen gedroht wird.

Links überprüfen.
Öffnen Sie keine Links oder Anhänge, wenn Sie den Absender nicht kennen und auch keine Nachricht erwarten. Es könnte sich um einen Link zu einer gefälschten Website oder um einen Anhang mit Schadsoftware handeln.

Tippen Sie Links zu Websites immer selbst ein. Prüfen Sie, ob es sich um die offizielle URL des Unternehmens handelt. Überlange Links sollten Sie misstrauisch machen. Vertrauenswürdige Websites beginnen mit «https://».

Nur bezahlen, wenn Sie sicher sind.
Geben Sie Ihre Karteninformationen und Sicherheitsnummern nur dann an, wenn Sie eine Zahlung tätigen wollen.

Karten-App aktivieren.
Aktivieren Sie die App Ihres Kartenanbieters. Damit reduzieren Sie das Betrugsrisiko. Sie können jede Zahlung prüfen und müssen sie teilweise auch nochmals bestätigen (3-D Secure).

Jede Zahlung prüfen.
Kontrollieren Sie jede Zahlungsaufforderung genau und prüfen Sie den Zahlungsempfänger. Geben Sie Zahlungsbestätigungen erst frei, wenn Sie den Betrag und den Händlernamen kontrolliert haben.

Codes nie weitergeben.
Geben Sie Bestätigungscodes nie weiter. Mit einem Bestätigungscode können Täter:innen weitere Services, zum Beispiel ein mobiles Zahlungssystem wie Google Pay, einrichten und von Ihrem Konto Geld stehlen.

Shops überprüfen.
Prüfen Sie auf Websites immer die allgemeinen Geschäftsbedingungen des Händlers und achten Sie auf Gütesiegel wie zum Beispiel «Trusted Shops».

Geräte aktualisieren.
Veraltete Programme auf dem Computer oder dem Smartphone sind ein Sicherheitsrisiko. Aktualisieren Sie Ihre Geräte regelmässig und schliessen Sie mit Updates mögliche Sicherheitslücken. Nutzen Sie auch Antiviren und Sicherheitssoftware.

Anzeige erstatten.
Wenn Sie Opfer einer Phishing-Attacke geworden sind, lassen Sie Ihre Debit- und Kreditkarte sofort sperren oder ändern Sie die Zugangsdaten zu sämtlichen Konten. Erstatten Sie Anzeige bei der Polizei.