Vorsicht Kartenbetrug: So können Sie sich schützen!

Das Einkaufen im Internet ist grundsätzlich sicher. Kartenverarbeiter und Banken investieren viel in ihre Sicherheitssysteme. Trotzdem gelingt es Betrügern immer wieder, ihren Opfern Geld zu stehlen. Bei der jüngsten Betrugsmasche aktivieren die Opfer unbewusst ein mobiles Zahlungssystem. Marcel Drescher, Head Fraud Services des UBS Card Center, erläutert wie Betrüger beim Digital Wallet Fraud vorgehen und wie man sich davor schützen kann.

Was sind digitale Zahlungssysteme?

Dabei handelt es sich um elektronische Zahlungsinformationen, die anstelle einer Plastikkarte auf einem digitalen Medium für die Nutzung gespeichert werden. Das kann zum Beispiel in Form eines digitalen Portemonnaies, eines sogenannten «Wallet», auf dem Smartphone oder auf Smartwatches sein. Somit kann das entsprechende Gerät als Kredit- oder Debitkarte für Zahlungen eingesetzt werden.

Welche Betrugsarten kommen beim Online-Shopping am häufigsten vor?

Häufig werden persönliche Karteninformationen, die Sie bei Händlern rechtmässig für eine Zahlung einsetzen, zu einem späteren Zeitpunkt aufgrund eines Datenlecks gestohlen und für missbräuchliche Zwecke verwendet.

Eine weitere verbreitete Betrugsart ist das Erschleichen von persönlichen Karteninformationen und den entsprechenden elektronischen Zugangsmitteln über das Versenden von Phishing-E-Mails. Bei solchen E-Mails gaukeln Ihnen die Betrüger beispielsweise vor, dass noch eine kleine Gebühr für die Zustellung eines Pakets ausstehend ist. Sie werden aufgefordert, diese Zahlung über einen Link, der in der E-Mail mitgeschickt wurde, zu tätigen. Der Link führt allerdings auf eine gefälschte Webseite. Wenn Sie dort Ihre persönlichen Kartendaten eingeben und dann auch noch den Zugangscode preisgeben, den Sie separat via SMS oder Benachrichtigung erhalten haben, können die Betrüger über Ihr Geld verfügen.

Die Betrüger erschleichen sich oft die benötigten Daten über eine verschickte Phishing-E-Mail.

Was ist ein Digital Wallet Fraud?

Bei dieser Betrugsart versuchen Betrüger, in ihrer eigenen Wallet-App die Daten einer Drittperson missbräuchlich zu registrieren, damit sie im Anschluss mit ihrem Gerät missbräuchliche Zahlungen im Geschäft, Restaurant oder im Internet durchführen können.

Wie gehen Betrüger bei dieser Betrugsart vor?

Die Betrüger erschleichen sich oft die benötigten Daten über eine verschickte Phishing-E-Mail. Die Opfer geben ihre Daten unter der Annahme preis, dass sie der Zahlungsaufforderung in der Phishing-E-Mail nachkommen. Zudem geben sie auch den Zugangscode für die Bestätigung der Wallet Registrierung weiter, der ihnen separat via SMS an ihre registrierten Handynummern zugeschickt wurde. Dies erfolgt durch die Eingabe des Codes auf der gefälschten Webseite. Mit diesen Informationen verfügen die Betrüger nun über alle Daten, die für die erfolgreiche Registrierung notwendig sind.

Wo kann ich mich über Phishing-Mails informieren und wie erkenne ich diese?

Die wichtigsten Informationen können Sie unter www.card-security.ch, www.cybercrimepolice.ch oder auf den entsprechenden Seiten Ihrer Bank oder Ihres Kartenherausgebers abrufen.

Was muss ich tun, wenn ich meine Kartendaten und elektronischen Zugangsmittel doch weitergegeben habe?

Lassen Sie sofort die Karte sperren und weisen Sie darauf hin, dass Sie persönliche Kartendaten oder Zugangscodes weitergegeben haben. Eine Sperrung kann auch über die Web-Services der Kartenherausgeber direkt und schnell erfolgen. Nach erfolgter Kartensperrung ist die Karte vor weiterem Missbrauch geschützt. Missbräuchliche Transaktionen, die vor der Sperrung erfolgt sind, können leider nicht mehr rückgängig gemacht werden.

Wie kann ich mich vor Angriffen auf meine Debit- und Kreditkarten schützen?

Der beste Schutz ist gewährleistet, wenn Sie die Meldungen vom Kartenherausgeber, die Sie via SMS oder anderen Benachrichtigungen erhalten, vollständig und genau lesen. Wenn eine Zahlung über eine kleine Gebühr ausgeführt wird, in der SMS jedoch steht, dass es sich um den Bestätigungscode für die Registrierung der Kreditkarte XY für eine digitale Zahllösung handelt, dann darf der Code unter keinen Umständen weitergegeben werden.

Ausserdem ist es sehr empfehlenswert, einen Benachrichtigungsdienst für Ihre Kartenzahlungen zu aktivieren, sobald Transaktionen mit einer Karte durchgeführt worden sind. Damit behalten Sie stets den Überblick und verhindern, dass mehrere missbräuchliche Transaktionen innert kürzester Zeit erfolgen können. Falls Sie eine solche Nachricht über eine unbekannte Transaktion erhalten, sollten Sie die Karte sofort sperren lassen und den Kartenherausgeber kontaktieren.

Kontaktieren Sie auch den Kartenherausgeber, wenn Sie bei einer Zahlungsaufforderung Zweifel haben. Er kann Ihnen weiterhelfen und Sie möglicherweise vor einem Datenmissbrauch bewahren.

Bin ich für finanzielle Schäden haftbar, die durch Kartenbetrug entstehen?

Hier geht es um die Frage der Sorgfaltspflicht: Hat der Kunde seine akzeptierten Pflichten gemäss den Allgemeinen Geschäftsbedingungen eingehalten, wird er für den entstandenen Schaden entschädigt. Das ist zum Beispiel der Fall, wenn die persönlichen Daten über ein Datenleck gestohlen wurden.

Hingegen erhält der Kunde keinen Schadenersatz, wenn er seine persönlichen Kartendaten via Link aus einer Phishing-E-Mail weitergibt. Der Kunde hat den Schaden bis zu dem Zeitpunkt zu tragen, an dem die Karte durch ihn oder durch den Kartenherausgeber gesperrt wurde. Deswegen ist es wichtig, vor der Weitergabe von Freigabecodes genau zu prüfen, wofür diese Freigabe erteilt wird. Achten Sie genau darauf, was Sie freigeben, so etwa, welchen Betrag und und bei welchem Händler.

Marcel Drescher, Head Fraud Services UBS Card Center

Marcel Drescher und sein Team kümmern sich um Betrugsfälle im Zusammenhang mit Kredit- und Debitkarten für die Bank UBS und weitere Schweizer Kartenherausgeber.