Kreditkartenbetrug: Bank Cornèr

Ein Aargauer Rentner verlor durch Betrug rund 10 000 Franken. Die Kreditkarten-Herausgeberin Cornèrcard weigert sich, einen Teil der Summe zu übernehmen. Das Beispiel zeigt, welche Risiken Kunden im Internet eingehen.

Andreas Bolliger (Name geändert) aus einer Gemeinde im Bezirk Baden AG sagt von sich, er sei «ein vorsichtiger Mensch». Umso mehr ärgert es ihn, dass er auf ein betrügerisches E-Mail hereingefallen ist und dadurch viel Geld verloren hat.

Das Unheil beginnt im vergangenen November. Bolliger vergisst, die Handyrechnung von Sunrise zu bezahlen. Das holt er einen Monat später mit der Dezemberrechnung nach. Zufälligerweise erreicht ihn am 26. Dezember beim Skifahren im Berner Oberland ein vermeintliches E-Mail von Sunrise. Darin heisst es, er habe die Rechnung für den Monat November doppelt bezahlt.

> *«Wenn ein Rentner sein Zahlverhalten massiv ändert, müsste Cornèrcard reagieren»*
>
> Nicolas Mayencourt,
> Experte für Cyber-Sicherheit

Der 73-Jährige meint, er habe erneut gepatzt, und füllt das verlinkte Formular für eine Rückerstattung aus. Dabei gibt er auch seine Kreditkartendaten und seine Mobiltelefonnummer an. Das Absenden funktioniert aber nicht: Das Formular bleibt hängen, und Bolliger muss abbrechen. Als etwas später ein angebliches Bestätigungsmail von Sunrise eintrifft, glaubt er, es habe doch noch geklappt.

Stutzig wird Bolliger erst, als sein Smartphone am 27. Dezember spätnachmittags keine Verbindung mehr hat. Deshalb sucht er am nächsten Tag den Sunrise-Shop in Interlaken BE auf. Dort machen ihn die Sunrise-Angestellten darauf aufmerksam, dass seine Handynummer von einem anderen Gerät verwendet werde. Bolliger schwant Böses. Er lässt die Nummer wieder auf sein eigenes Handy übertragen und ruft darauf den Kundendienst seiner Kreditkartenherausgeberin Cornèrcard an.

Von dessen Sicherheitsabteilung erfuhr er, was geschehen war: Betrüger hatten seine Kreditkarte dazu benutzt, bei der Kryptowährungsbörse Binance.com in Litauen Geldtransfers durchzuführen. Am 28. Dezember zwischen 0.58 und 3.38 Uhr hatten sie in elf Tranchen 10 263 Franken überwiesen. Die Transaktionen hatten die Täter alle per SMS-Code autorisiert. Es war ihnen gelungen, in das Sunrise-Konto von Bolliger einzudringen und seine Handynummer über eine digitale SIM-Karte auf ein fremdes Gerät zu übertragen. So konnten die Kriminellen alle SMS-Codes des Cornèrcard-Sicherheitssystems abfangen und die Zahlungen in Bolligers Namen bestätigen.

Die Sicherheitssysteme von Cornèrcard reagierten nicht

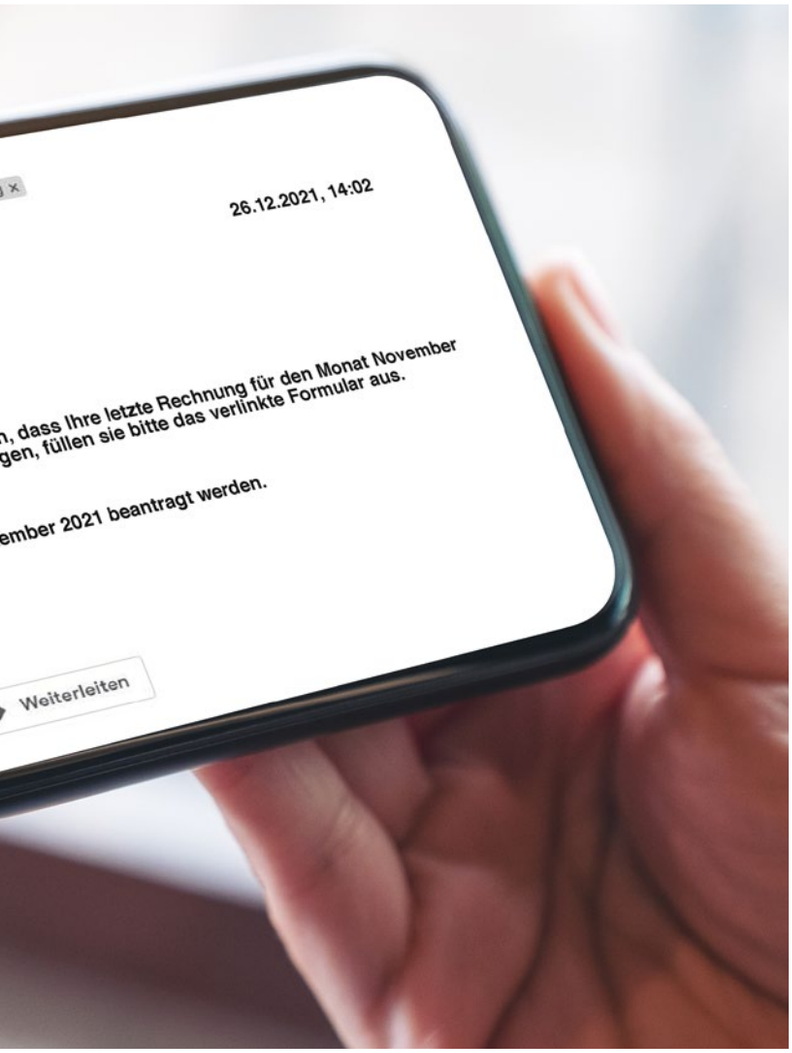
Cornèrcard schreibt dem Rentner Anfang Februar: Alle Transaktionen seien durch die Eingabe des korrekten SMS-Codes autorisiert worden. Deshalb bestehe «keine Möglichkeit, den Betrag beim entsprechenden Internethändler zu beanstanden und eine Rückerstattung einzufordern». Zudem verweist Cornèrcard auf die allgemeinen Geschäftsbedingungen. Darin heisst es, alle nach Durchführung der Autorisierung vorgenommenen Kartenbelastungen würden «dem betreffenden Karteninhaber zugerechnet, der sie vorbehaltlos als rechtsgültig und verbindlich akzeptiert». Für allfällige Missbräuche durch Dritte übernehme Cornèrcard «keine Verantwortung».

GETTY IMAGES MONTAGE

Das Phishing-Mail: Damit gelang es den Betrügern, die Herrschaft über die Kredit

Andreas Bolliger ist sich bewusst, dass er einen Fehler machte. Er ist grundsätzlich bereit, die Konsequenzen zu tragen. Andererseits findet er, dass Cornèrcard eine Mitschuld trifft. Denn die Sicherheitssysteme der Kreditkartenherausgeberin hätten nicht funktioniert. Bolliger argumentiert: Wenn ein Rentner über Jahre hinweg mit seiner Kreditkarte monatliche Umsätze im tiefen dreistelligen Bereich tätige und dann plötzlich mitten in der Nacht in hoher Kadenz auf einer Kryptowährungsbörse in

stiehlt sich aus Verantwortung



karte und das Mobiltelefon des Opfers zu erlangen

So schützen Sie sich vor Phishing-Attacken

■ Misstrauen Sie E-Mails, SMS, Telefonanrufen oder Websites, die Sie auffordern, Kartendaten, Passwörter, Einmal-Codes oder persönliche Daten bekanntzugeben. Informieren Sie sich über aktuelle Vorkommnisse beim Nationalen Zentrum für Cybersicherheit: **Ncsc.admin.ch**

■ Sind Sie unsicher, ob eine Anfrage vertrauenswürdig ist, vergewissern Sie sich mit einem Telefonanruf auf die offizielle Nummer des Unternehmens. Bringen Sie diese Nummer via Suchmaschine in Erfahrung.

■ Viele Kreditkartenfirmen bieten Apps an. Nutzen Sie diese, um Ihre Transaktionen zu überprüfen, in Echtzeit Informationen über Einkäufe zu erhalten oder die Kreditkarte bei Nichtgebrauch zu sperren.

■ Schützen Sie Ihr Smartphone und Ihren Computer vor fremden Zugriffen, indem Sie die Sicherheitsupdates ausführen, einen Virenscanner installieren und das Gerät durch Passwort oder biometrische Daten absichern.

■ Wenn Sie die Kreditkarte selten brauchen und nur tiefe Monatsumsätze erreichen, dann verlangen Sie bei der Kartenherausgeberin eine Senkung der Ausgabenlimite.

■ Durch Datenlecks und Hackerangriffe sind Millionen von Passwörtern in Umlauf geraten. Ob Ihr Passwort bekannt ist, erfahren Sie möglicherweise unter: **Leakchecker.uni-bonn.de** oder **Checktool.ch**

■ Überprüfen Sie stets die Monatsrechnung Ihrer Kreditkarte und beanstanden Sie allfällige Fehler bei der Kartenherausgeberin innert 30 Tagen ab Rechnungserhalt.

GETTY IMAGES

Litauen Tausende von Franken einzahle, müsste Cornèrcard Verdacht schöpfen.

Das sieht auch Nicolas Mayencourt, Gründer der Berner Cybersecurity-Firma Dreamlab Technologies AG, so: «Wenn ein Rentner sein Zahlverhalten plötzlich so massiv ändert und auf einer Kryptoplattform tätig wird, müsste bei Cornèrcard ein rotes Lämpchen aufleuchten.» Bei so hohen Transaktionen innert kurzer Zeit hätte die Kreditkartenherausgeberin die Zahlungen auf Eis legen und den Kunden für Abklärungen anrufen müssen. Deshalb ist Mayencourt der Meinung, dass Cornèrcard eine Mitschuld trägt und einen grösseren Anteil am Schaden übernehmen sollte.

Wenig Verständnis zeigt der Experte für IT-Sicherheit auch gegenüber der Haltung von Cornèrcard, jede per SMS-Code autorisierte Zahlung sei quasi durch den Karteninhaber erfolgt.

Unklar bleibt, wie es die Betrüger geschafft haben, in das Sunrise-Konto einzudringen. Der Kantonspolizei Zürich ist das Phishing-Mail bekannt. Cybersecurity-Experte Mayencourt kann sich vorstellen, dass die Betrüger das Passwort aus einer Datenbank mit gehackten Passwörtern bezogen haben.

Was den Kriminellen zudem half: Sunrise reduzierte das Sicherheitsniveau für den Wechsel von SIM-Karten für einige Wochen. So konnten die Täter im Online-Konto von Bolliger die Telefonnummer der bestehenden SIM-Karte auf die E-SIM-Karte eines fremden Geräts übertragen, ohne dass ein weiterer Sicherheitscheck erfolgte. Das änderte Sunrise laut Sprecher Rolf Ziebold am 16. Februar. Ziebold erklärt, Sunrise habe die Sicherheitsvorkehrungen unabhängig vom Fall Bolliger wieder verstärkt.

Cornèrcard ist nicht bereit, einen grösseren Teil des Schadens von Bolliger zu übernehmen. «Aus Kulanzgründen» erliess sie ihm nur die entstandenen Transaktionsgebühren und -spesen in der Höhe von 500 Franken. Bolliger kündigte Ende Februar seine Kreditkarte per sofort. **Thomas Lattmann**