HINTERGRUND

ONLINE-BANKING-BETRUG: RISIKEN ERKENNEN UND SICHERHEIT ERHÖHEN

Die Stiftung Konsumentenschutz hat eine Recherche zu Betrugsfällen im Bereich des Online-Bankings durchgeführt. Im Gespräch mit Andreas Wüscher von der Schaffhauser Kantonalbank hat der «Bock» erfahren, wie die Bank solche Betrugsfälle angeht und wie Betroffene sich verhalten sollen.

Auch über TWINT ist es möglich, Opfer eines Betrugs zu werden. Bild: Salome Zulauf

GESELLSCHAFT
SCHAFFHAUSEN

Ginevra Lo Piccolo

Betrugsfälle beim Online-Banking sind nichts Neues. Mit dem technischen Fortschritt werden solche Betrugsversuche jedoch immer raffinierter. Die Stiftung Konsumentenschutz hat untersucht, wie Banken im Falle eines Betrugs reagieren. Dabei zeigte sich, dass die meisten nicht rund um die Uhr erreichbar sind. Wer Opfer eines Betrugs wird, muss sich in der Regel an die Öffnungszeiten der Bank halten, um Hilfe zu erhalten. Das gilt insbesondere für Betrugsfälle am Wochenende oder abends. Betrügerinnen und Betrüger nutzen diese Kommunikationslücke zwischen Banken und Kundschaft aus, um Schaden anzurichten.

Andreas Wüscher, Leiter des Service- und Beratungscenters der Schaffhauser Kantonalbank, erklärte im Interview mit dem «Bock», welche Massnahmen in einem solche Fall ergreifen werden und wie Betroffene bestmöglichst handeln sollten.

«Bock»: *Welche Bankbetrugsarten treten aktuell am häufigsten auf?*
Andreas Wüscher: Derzeit beobachten wir insbesondere Phishing – etwa über gefälschte Webseiten, E-Mails oder SMS – sowie Social Engineering per Telefon, auch «Spoofing» genannt. Zunehmend verbreitet ist auch Betrug über mobile Bezahldienste wie TWINT, etwa in Form fingierter Post Paketbenachrichtigungen mit QR-Codes, auch «Quishing» genannt. Zudem stellen wir vereinzelt Enkeltricks, falsche Polizisten, Romance Scam oder Schockanrufe fest.

Gibt es eine Kundengruppe, die besonders häufig von Betrugsversuchen betroffen ist und falls ja, wieso?
Wüscher: Es gibt Tendenzen, dass ältere oder digital weniger versierte Personen anfälliger sind. Jedoch stellen wir auch fest, dass digital sehr affine Personen Opfer werden können. Es hängt also viel mehr von der persönlichen Situation ab als von der Erfahrung oder dem Wissen. Ein Zusammenhang zeigt sich insbesondere, wenn Opfer unter Druck agieren. Sei es, weil sie unter Druck gesetzt werden oder weil sie rasch etwas erledigen wollen. Zudem stellen wir auch fest, dass gerade jüngere Nutzer verlockende Angebote auf Social-Media-Plattformen oder Online-Marktplätzen kaufen möchten. Doch ist das Angebot zu gut, ist es vermutlich falsch.

Woran lässt sich erkennen, dass ein Betrugsfall vorliegt?
Wüscher: Insbesondere, wenn etwas überraschend passiert, sollte man vorsichtig agieren, zum Beispiel bei unaufgeforderter Kontaktaufnahme durch angebliche Behörden, Banken oder nicht bekannte Familienangehörige. Die Kontaktaufnahme erfolgt häufig telefonisch, kann aber auch per E-Mail, SMS oder über andere Kanäle erfolgen. Die Personen fordern in der Regel zum sofortigen Handeln auf und setzen Betroffene unter emotionalen Druck. Sie verlangen beispielsweise eine sofortige Geldüberweisung, die Preisgabe von Login-Daten oder die Installation einer Fernzugriffssoftware. Dabei erklären sie gerne auch, dass sie einen Betrug verhindern möchten – und schon haben sie die Falle gestellt. Deshalb sind ungewöhnliche Transaktionen oder Bargeldbezüge immer sehr kritisch zu hinterfragen.

Welche Schritte sollten Kundinnen und Kunden unternehmen, sobald ein Betrugsverdacht besteht?
Wüscher: Betroffene sollten sich umgehend telefonisch bei ihrer Bank melden. Dabei ist wichtig, dass sie die Telefonnummer selbständig wählen und sich nicht weiterverbinden lassen. Ausserhalb der Öffnungszeiten sind die gängigen Sperrhotlines zu kontaktieren (bei der Schaffhauser Kantonalbank beispielsweise Viseca für Karten und Twint). Das E-Banking kann durch mehrmalige Falscheingabe des Passworts gesperrt werden. Weiter ist der Kontakt zu den Betrügerinnen und Betrügern unbedingt abzubrechen und keine weiteren Zugangsdaten bekannt zu geben. Bei eingetretenem Schaden ist eine Anzeige bei der Polizei zu erstatten und gegebenenfalls die Versicherung zu informieren. Ist der Fall abgeschlossen und die Polizei hat alle Beweismittel gesammelt, empfehlen wir das betroffene Gerät durch eine fachkundige Person auf Schadsoftware prüfen zu lassen. Zusätzlich kann eine Meldung beim Bundesamt für Cybersicherheit BACS erfolgen.

> «DIE PERSONEN SETZEN BETROFFENE UNTER EMOTIONALEN DRUCK.»
>
> **Andreas Wüscher**
> Leiter des Service- und Beratungscenters der SHKB.

Und wie geht die Schaffhauser Kantonalbank bei einem bestätigten Betrugsfall vor?
Wüscher: Ist ein Betrugsfall bestätigt, sperren wir das entsprechende Konto sofort, untersuchen den Vorfall und unterstützen die betroffene Person bei den weiteren Schritten wie etwa bei der Anzeige bei der Polizei. Zudem prüfen wir, ob weitere Konten oder Zugänge sicherheitsrelevant betroffen sein könnten. Je nach Fall prüfen wir ergänzende Massnahmen, wie beispielsweise die komplette Löschung des E-Banking, die Sperrung von Karten, die Deaktivierung von TWINT und/oder die Sperrung weiterer Konten.

Wer trägt die finanzielle Verantwortung im Falle eines erfolgreichen Betrugs?
Wüscher: In aller Regel trägt die betroffene Person den entstandenen Schaden selbst. Üblicherweise ist es nämlich so, dass die betroffene Person leider grobfahrlässig gehandelt hat, in dem sie persönliche und daher streng geheim zuhaltenden Zugangsdaten einer Drittperson preisgegeben und/oder die entsprechenden Zahlungen selbst erfasst und ausgelöst hat. Auf diesem Weg von betroffenen Personen freigegebene Zahlungen kann eine Bank in der Regel nicht als betrügerische Transaktion erkennen und daher auch nicht verhindern. Aus diesem Grund ist eine Cyber Versicherung für jeden Haushalt empfehlenswert.

Ist bereits eine Tendenz erkennbar, beispielsweise eine Zunahme von Betrugsfällen in letzter Zeit und mit welchen neuen Betrugsformen ist künftig zu rechnen?
Wüscwher: Ja. Seit zwei Jahren beobachten wir eine deutliche Zunahme von digitalen Betrugsversuchen – sowohl in der Anzahl als auch in der Raffinesse. Die Täter agieren zunehmend professioneller und organisierter. Aufgrund der technologischen Entwicklung wie etwa künstlicher Intelligenz ist es schwierig, eine verlässliche Aussage zu machen. Heute sehen wir bereits, dass durch den Einsatz von KI Phishing Seiten für den Laien kaum mehr zu unterscheiden sind und auch betrügerische E-Mails oder gar Sprachnachrichten und Videos im Umlauf sind – sogenannte «Deep Fakes». Auch QR-Code-Betrug sowie manipulierte Banking-Apps dürften zunehmen. Mobile Zahlungsdienste geraten ebenfalls verstärkt in den Fokus.
Die Entwicklung der Betrugsformen ist nicht nur für Pwrivate relevant, sondern auch für Unternehmen. Zu denken ist dabei an die Bekannte «CEO-Fraud» Masche mittels Deep Fake. Ein gefälschter Anruf fordert zur dringewnden Zahlung / Handlung auf.


Andreas Wüscher, Leiter des Service- und Beratungscenters SHKB. Bild: zVg.

SCHUTZMASSNAHMEN

- Keine Links in unerwarteten SMS oder E-Mails anklicken
- TWINT-Zahlungen nur über vertrauenswürdige Quellen tätigen
- Keine persönlichen oder Bankdaten am Telefon preisgeben
- QR-Codes beim Scannen gut hinterfragen: Stimen Angaben im E-Banking mit Angaben auf Einzahlungsschein überein? Ist der Link vertrauenswürdig?
- Banking-Apps nur aus offiziellen App-Stores laden
- Sicherheitssoftware aktuell halten
- Zwei-Faktor-Authentifizierung aktivieren
- Kein Geld an unbekannte Personen überweisen oder Bargeld übergeben

«EN ERHOLSAME TAG DIREKT AM RHY»

GASTKOLUMNE
SCHAFFHAUSEN

Yannick Vögele, Schaffhauser Kantonalbank

Sie fragen sich bestimmt, was hat «en Tag am Rhy» mit einer Finanzkolumne zur Vermögensanlage zu tun?

Es ist ganz einfach:
Beides macht grossen Spass und ist erholsam, wenn Sie die wichtigsten Grundsätze berücksichtigen.
Sie stehen mit Ihrer Familie an der Lindlipromenade und warten darauf, in den Weidling Ihrer Freunde einzusteigen. Währenddessen geniessen Sie den natürlichen Schatten der Bäume, während sich die Sonne im Rhein spiegelt. Lange haben Sie sich auf diesen Tag gefreut und deshalb alles akribisch geplant: Ihr Rucksack ist für ein Picknick am Schaaren gepackt, Badetuch und Sonnencrème sind dabei. Sie haben für heute bewusst keine weiteren Termine vereinbart, damit Sie den Tag auf und am Rhy voll und ganz geniessen können. Niemand möchte diesen besonderen Tag verlassen, wenn es gerade am schönsten ist. Das wäre sehr ungünstig.

Gleiches gilt für Ihre Vermögensanlage:
Planen Sie vorausschauend und bringen Sie Zeit mit. So müssen Sie die Finanzmärkte nicht zu einem ungünstigen Zeitpunkt verlassen.

Das Picknick ist verzehrt und nun wird es Zeit für den ersten «Schwumm» des Tages. Sie schwimmen gegen die Strömung, während sich der Körper langsam von der Hitze abkühlt. Im Augenwinkel sehen Sie eine Wiffe - ein vertrautes Bild aus Ihrer Jugend. Damals sind Sie voller Elan darauf zu geschwommen und hinaufgeklettert. Heute verzichten Sie schmunzelnd auf dieses grosse Risiko. Lieber freuen sich stattdessen auf eine entspannte Runde Boggia mit Ihren Kindern. Zurück am Ufer wird Ihnen klar: der Risikoappetit ist individuell – und verändert sich mit der Zeit.

Deshalb gilt:
Berücksichtigen Sie auch bei Ihrer Vermögensanlage Risiken, die Ihrem Risikoappetit entsprechen. Nach der Runde Boggia treiben Sie mit dem Weidling in Richtung Lindli zurück. Zufrieden bewundern Sie den herrlichen Sonnenuntergang über dem Rhein – gemeinsam mit Ihrer Familie und Ihren Freunden.

Der Tag war ein voller Erfolg:
Sie haben gut geplant und unnötige Risiken umschifft. Das ist mein persönliches Erfolgsrezept für «en Tag am Rhy» und meine nachhaltige Vermögensanlage. So kann man mit Zuversicht in die Zukunft blicken – und sich unterwegs immer wieder erholen.

Ich wünsche Ihnen einen erholsamen Spätsommer und viel Freude bei der Vermögensanlage.