Merkblatt

Internet und E-Banking: So schützen Sie sich vor Betrug

Darum geht es

Die Zahl der Betrugsfälle steigt von Jahr zu Jahr – das ist besorgniserregend. Internetkriminelle werden immer raffinierter. Deshalb wird es immer schwieriger, einen Betrug oder einen Angriff auf das Bankkonto oder die Kreditkarte rechtzeitig zu erkennen. Viele Betrüger nutzen psychologische Tricks und setzen ihre Opfer unter Druck. Im schlimmsten Fall erhalten sie so Zugang zu Passwörtern und Bankdaten sowie zu sensiblen und sehr persönlichen Informationen. Dieses Merkblatt zeigt Ihnen auf, welche Methoden besonders verbreitet sind und wie Sie sich vor Betrug schützen können.

E-Banking – Vorsicht vor Phishing-Attacken

Heute erledigen viele Schweizer ihre Bankgeschäfte am PC, Tablet oder Smartphone. Die Banken unternehmen grosse Anstrengungen, um ihren Kunden sichere E-Banking-Systeme zur Verfügung zu stellen. Die meisten Angriffe richten sich nicht gegen die Banken selbst, sondern gegen die Geräte ihrer Kunden. Besonders verbreitet sind folgende Methoden.

Phishing: Phishing bedeutet so viel wie «Passwörter fischen». Dabei versuchen Kriminelle, an vertrauliche Daten von Bankkunden und so an ihre Ersparnisse zu gelangen. Analysen der Schweizerischen Kriminalprävention (SKP) zeigen, dass Phishing-Angriffe sehr unterschiedlich ablaufen können. Dennoch gibt es typische Merkmale, wie der folgende Ablauf zeigt:

- Betrüger versenden gefälschte E-Mails, in denen sie sich beispielsweise als Bankmitarbeitende ausgeben. In diesen E-Mails wird den Kundinnen und Kunden vorgegaukelt, dass ihre Kontoinformationen und Zugangsdaten nicht mehr sicher oder aktuell seien – und darum über den in der E-Mail angegebenen Link aktualisiert werden müssten.
- Der angegebene Link führt allerdings nicht auf die Originalseite der Hausbank, sondern auf eine gefälschte Webseite, die der Originalseite täuschend ähnlichsieht. Alle persönlichen Daten, die man dort eingibt, gelangen direkt zu den Betrügern.
- Mit den gestohlenen Zugangsdaten tätigen Kriminelle dann blitzschnell Überweisungen – oft über mehrere zehntausend Franken, die sie den Konten ihrer Opfer belasten. Diese Gelder sind oft verloren.

Tipps: Achten Sie auf diese Punkte, wenn Sie Ihr E-Banking nutzen

Halten Sie sich an die gängigen Verhaltensempfehlungen, um Ihr E-Banking sicher zu nutzen. Hier finden Sie die wichtigsten Regeln übersichtlich zusammengefasst.

- Geben Sie die Adresse zur Anmeldeseite Ihres E-Bankings immer manuell in die Adresszeile Ihres Browsers ein. Suchen Sie die Seiten nicht über Suchmaschinen wie Google, Bing, etc.
- Falls Sie unsicher sind, ob Sie sich auf der richtigen Login-Seite befinden, schauen Sie darauf, dass eine sichere SSL-Verbindung besteht (https://, Schloss-Symbol).
- Die richtige Internetadresse wird entweder neben dem Schloss-Symbol oder nach einem Klick auf das Schloss-Symbol angezeigt.
- Achten Sie darauf, dass die Internetadresse der Login-Seite korrekt geschrieben ist. Betrüger ändern oft nur einzelne Buchstaben in der Adresse ab.
- Unterbrechen Sie den Anmeldeprozess und die Verbindung sofort, falls ein Systemunterbruch auftritt (z. B. ein plötzlich auftretender weisser Bildschirm) oder wenn ungewöhnliche Fehlermeldungen erscheinen (z. B. «Das System ist derzeit überlastet. Bitte haben Sie etwas Geduld und probieren Sie es später noch einmal»).
- Unterwegs sollten Sie Ihr Login und Passwort verdeckt eingeben. Vermeiden Sie, dass Ihnen jemand über die Schultern blickt.
- Benutzen Sie Ihr E-Banking nur von bekannten und sicheren Geräten aus. Öffentliche Internetgeräte in Hotels sind beispielsweise dafür nicht geeignet.
- Kontaktieren Sie sofort Ihre Bank, wenn Ihnen etwas sonderbar vorkommt.

Suchmaschinen-Phishing: Viele Bankkunden loggen sich ins E-Banking ein, indem sie zuerst die Login-Seite ihrer Bank im Internet suchen – also etwa bei Google, Bing oder Yahoo. Sie unterschätzen dabei, wie gefährlich das ist. Denn Kriminelle bewerben ihre betrügerischen E-Banking-Webseiten auch über die meistgenutzten Suchmaschinen:

- Bei einer Suchanfrage wird die gefälschte Login-Seite der Bank prominent angezeigt – im Browser erscheint sie erfahrungsgemäss an erster Stelle der Trefferliste und ist oft mit «Gesponsert», «Werbung» oder «Anzeige» gekennzeichnet.
- Wer in der Trefferliste auf einen solchen Link klickt, landet auf einer gefälschten E-Banking-Seite, die praktisch so aussieht wie die echte Bankseite.
- Wer dort seine persönlichen Zugangsdaten für das E-Banking eintippt, ist sich darum nicht bewusst, dass diese Daten direkt bei den Betrügern landen.
- Mit den Login-Daten können sich die Betrüger dann in das echte E-Banking einloggen und auf Kosten der Kontoinhaber Geldbeträge entwenden.

SMS-Phishing (Smishing): Häufig werden auch Kurznachrichten-Dienste wie SMS und WhatsApp für Angriffe genutzt. Diese Angriffe sind besonders gefährlich, weil viele Kriterien zur Erkennung von Phishing-E-Mails nicht greifen:

- Betrüger verschicken gefälschte Nachrichten und geben sich als Bankmitarbeitende oder technischen Dienst einer Bank aus.
- Den Empfängern der Kurznachricht wird zum Beispiel vorgetäuscht, dass ihre Zugangsdaten und Kontoinformationen nicht mehr sicher seien.
- Unter diesem Vorwand werden die Kunden dazu verleitet, ihr Login und Passwort über einen Link in der Kurznachricht zu aktualisieren.
- Dieser Link führt aber zu einer gefälschten Webseite, die genauso aussieht wie der gewohnte Login-Bereich der Bank.
- Auf dieser Fake-Seite «fischen» die Betrüger dann nach den Login-Daten der Bankkunden.

Voice-Phishing (Vishing): Betrüger schrecken nicht davor zurück, Bankkunden telefonisch zu kontaktieren. Solche Angriffe werden «Vishing» genannt und nehmen immer mehr zu:

- Die Betrüger rufen Kundinnen und Kunden an und täuschen dabei eine falsche Identität vor. Sie geben sich beispielsweise als Beamte einer Behörde wie etwa der Polizei oder als Bankangestellte aus – oder als Mitarbeitende eines grossen Unternehmens wie etwa Microsoft oder Swisscom.
- Im Gespräch setzen die Betrüger ihre Opfer unter Zeitdruck, wenden verschiedene Manipulationstechniken an und drohen mit schwerwiegenden Konsequenzen – dies mit dem Ziel, die Bankkunden zu unüberlegten Handlungen zu verleiten.
- Eine Aufforderung kann beispielsweise sein, dass der Bankkunde ein angeblich neues Sicherheitsprogramm installieren soll, weil sein PC von einem Computervirus befallen sei.
- In den meisten Fällen handelt es sich aber um Schadsoftware. Sind solche Programme einmal installiert, können die Betrüger auf Logins und Passwörter der Bankkunden zurückgreifen – und so auch auf ihre Konten und Ersparnisse.

Tipps: So schützen Sie sich vor Phishing-Angriffen

Betrüger und Internetkriminelle entwickeln ihre Methoden laufend weiter und versuchen, das ganze Potenzial der jeweiligen Technologie auszuschöpfen. Oft nutzen sie dabei eine Kombination aus Phishing, Vishing und Smishing. Achten Sie darum auf die folgenden Punkte.

- Keine seriöse Bank oder Organisation wird Sie per E-Mail, SMS, WhatsApp oder per Telefon kontaktieren und nach Login und Passwörtern fragen.
- Geben Sie darum niemals vertrauliche Daten und Informationen per Telefon, E-Mail oder auf unbekannten Webseiten an.
- Löschen Sie verdächtige Nachrichten und leeren Sie sofort den Papierkorb - auch wenn Sie nicht ganz sicher sind, ob eine Nachricht echt oder betrügerisch ist.
- Seien Sie sehr misstrauisch, wenn Sie unerwartete E-Mails bekommen.
- Lassen Sie sich nicht unter Druck setzen, wenn jemand Ihre persönlichen Daten verlangt und mit Folgen wie Geldverlust, Strafanzeige oder Kartensperrung droht.
- Verwenden Sie sichere Passwörter, und halten Sie Betriebssystem, Internet-Browser und Mail-Client immer aktuell. Aktualisieren Sie Ihr Antivirenprogramm regelmässig.
- Auch ein Spam-Filter oder eine Anti-Phishing-Software helfen, Phishing-Webseiten und Phishing-E-Mails zu entdecken. Laden Sie die Software nur aus offiziellen App-Stores herunter.
- Prüfen Sie regelmässig Ihre Bankauszüge und Kreditkartenabrechnungen, und melden Sie Unstimmigkeiten sofort bei der Bank.

Quellen: Schweiz. Kriminalprävention, Stiftung für Konsumentenschutz, www.ebas.ch/phishing, www.cybercrimepolice.ch

Geldanlagen und Immobilien – Vorsicht vor fiesen Maschen

Internetkriminelle ziehen alle Register und setzen modernste Technologien ein, um Bankkunden, Konsumenten und Internetnutzer zu täuschen. Gemäss dem Schweizerischen Bankenombudsman ist grösste Vorsicht geboten. Dies auch, weil Personen, die etwa freiwillig Zahlungen tätigen, ohne zu wissen, dass sie Opfer eines Betrugs geworden sind, die Konsequenzen meistens selber tragen müssen. Denn die Banken haften in solchen Fällen meist nicht. Diese Betrugsmaschen kommen sehr häufig vor.

Online-Anlagebetrug: Mit aggressiven Inseraten per E-Mail und auf Social Media werben Kriminelle für angebliche Anlageplattformen, die schnelles Geld oder ein Millionenvermögen versprechen. Um das Vertrauen der Opfer zu gewinnen, fälschen sie Webseiten von seriösen Medien wie SRF oder «Blick». Dort publizieren sie Artikel mit bekannten Persönlichkeiten – diese wissen aber nichts davon (siehe Bild). Wer sich auf einer solchen betrügerischen Plattform anmeldet, wird laut Kantonspolizei

Screenshot eines gefälschten Promi-Artikels (Quelle: Mit freundlicher Genehmigung der Kantonspolizei Zürich. Weitere Informationen zu solchen Betrugsfällen finden Sie unter: www.cybercrimepolice.ch)

Zürich meist innert kurzer Zeit per E-Mail oder Telefon kontaktiert. Ziel der Betrüger ist es, dass die Opfer raschmöglichst Geld einzahlen. Dieses Geld soll dann angeblich in Anlageprodukte oder Kryptowährungen investiert werden. Allerdings: Ein Handel findet nie statt. Stattdessen landet das Geld direkt bei den Betrügern. Dahinter stecken international agierende Kriminelle, die technisch auf dem neuesten Stand sind und sogar mit eigenen Callcentern operieren. Vorsicht: Lassen Sie sich nicht von unrealistischen Versprechen blenden. Kein seriöser Finanzdienstleister stellt überdurchschnittliche Gewinne in kurzer Zeit in Aussicht. Befolgen Sie die Empfehlungen der Behörden und der Polizei. Die Schweizer Finanzmarktaufsicht Finma führt zum Beispiel eine Warnliste (Link: www.finma.ch/de/finma-public/warnliste). Melden Sie zweifelhafte Angebote der Finma.

Finanzagenten-Betrug: Oft suchen Betrüger nach Personen, die sich als «Finanzagenten» missbrauchen lassen. Mit attraktiv tönenden Jobangeboten wenden sie sich an Stellensuchende und Menschen in finanziellen Notlagen – über Online-Portale, soziale Medien und Zeitungsinserate. Oft verfügen die Kriminellen über eine glaubwürdig aussehende Webseite, oder sie missbrauchen den Namen einer seriösen Firma. Vorsicht: Meistens stecken kriminelle Absichten dahinter. Die Betrüger nutzen etwa die Bankkonten der angeworbenen Personen, um Deliktsummen zu verschieben. Immer häufiger wird auch der Transfer von Vermögenswerten in eine Kryptowährung wie etwa Bitcoin verlangt. Als Gegenleistung soll eine finanzielle Entschädigung in Form einer Provision winken. Seien Sie vorsichtig, wenn man Ihnen schnelles Geld für wenig Arbeit verspricht. Wer solche Geschäfte ausführt, macht sich unter Umständen der Geldwäscherei schuldig.

Anzahlungsbetrug: Auch bei der Suche nach einem Eigenheim oder einem interessanten Kaufobjekt ist Vorsicht geboten. Die Behörden melden vermehrt Betrugsfälle mit gefälschten Inseraten. Betrüger kopieren beispielsweise Inserate von bestehenden Mietwohnungen und bieten diese als Eigentumswohnungen zu einem verlockenden Preis an – auf bekannten Immobilienportalen, Social Media oder gefälschten Webseiten, die täuschend echt aussehen. Die Inserate dienen als Köder. Wer darauf antwortet, wird von professionellen Betrügern kontaktiert. Die Täter verlangen zum Beispiel eine Kopie des Reisepasses oder der ID. Um vertrauenswürdig zu wirken, weisen sie sich auch mit einem angeblich eigenen Ausweis aus – oft ist dieser gefälscht oder gehört einem früheren Opfer. Die Betrüger geben vor, die Immobilie für den Interessenten zu reservieren. Bevor die Immobilie besichtigt werden kann, verlangen sie eine Anzahlung. Dieses Geld ist in der Regel weg, und die Täter sind nicht auffindbar. Tipp: Trauen Sie keiner Anzeige, die zu schön tönt, um wahr zu sein. Überweisen Sie nie Geld über einen Geldtransferdienst, wenn Sie keinen rechtsgültigen Vertrag und das Objekt nie besichtigt haben. Und gehen Sie auf Nummer sicher, und zeigen Sie dubiose Inserate immer auch einer erfahrenen Fachperson.

Andere verbreitete Betrugsformen

Daneben gibt es weitere Arten von Betrug. Besonders davon betroffen sind ältere Personen ab 55 Jahren, wie eine Studie von Pro Senectute zeigt. Die Organisation schätzt die Schadensumme auf rund 675 Millionen Franken pro Jahr. Aber auch die Gründer von Start-ups können Opfer von Betrügern werden. Diese Betrugsarten sollten Sie kennen:

Enkeltrick: Der Betrüger gibt sich oft als Verwandter aus, der sich in einer finanziellen Notlage befindet und dringend die Hilfe seiner Familie benötigt. Er ruft das Opfer an, entlockt ihm den Namen und weitere Informationen und lässt sein Wissen wieder ins Gespräch einfliessen. So gaukelt er vor, dieser Verwandte zu sein, der das Geld aus verschiedenen Gründen aber nicht selbst abholen kann. Stattdessen schickt er eine Freundin oder einen Bekannten vor.
Tipp: Seien Sie vorsichtig, wenn Sie einen angeblichen Verwandten am Telefon nicht sofort erkennen. Legen Sie im Zweifel einfach auf. Und übergeben Sie niemals Geld oder Wertsachen an Unbekannte – auch dann nicht, wenn es sich um vermeintliche Autoritätspersonen wie Polizisten, Anwälte oder Gerichtsmitarbeitende handeln soll.

Schockanruf: Bei dieser aggressiven Form des Telefonbetrugs ruft eine vermeintliche Autoritätsperson wie etwa ein Chefarzt, Anwalt oder Polizist an. Er überbringt eine erfundene, aber glaubwürdig klingende Nachricht, die das Opfer in Schock versetzen soll. Oft geht es um ein Familienmitglied, das sich in einer schweren Notlage oder in grosser Gefahr befinden soll. Die Betrüger fordern ihre Opfer auf, Geld und Wertsachen an einen Boten zu übergeben – und so ihrem Angehörigen zu helfen. Durch den Schock können die Opfer oft nicht rational denken und fallen auf den Betrug herein.
Tipp: Schockanrufe können Sie nur an der Nachricht selbst erkennen, die immer mit einer Geldforderung verbunden ist. Seien Sie misstrauisch, wenn Sie eine schockierende Nachricht erhalten, gleichzeitig unter Druck gesetzt werden und Geld zahlen sollen. Auch hier gilt: Hängen Sie einfach auf.

Registereinträge: Nach dem Eintrag der neuen Firma ins Handelsregister erhalten Neugründer oft Post für die Eintragung in diverse Register. Auf den ersten Blick wirken die erhaltenen Formulare wie offizielle Dokumente von Behörden. Meistens geht es aber um kostenpflichtige Verträge für die Eintragung in nutzlose Firmen-, Branchen- oder Markenregister, Telefonverzeichnisse, Ortspläne und Ähnliches. Solche Verträge sollte man auf keinen Fall unterschreiben.
Tipp: Fallen Sie nicht auf einen solchen «Registerschwindel» rein. Zahlen Sie immer nur die offiziellen Rechnungen vom Handelsregister des zuständigen Kantons und von allfälligen Partnern wie beispielsweise von Notaren und Treuhändern.

Wichtige Links

Im Internet gibt es verschiedene Anlaufstellen, bei denen man sich über aktuelle Betrugsmaschen informieren kann. Dort erhält man auch wertvolle Tipps, wie man sich selbst schützen kann.

- Schweizerische Kriminalprävention: **www.skppsc.ch**
- «E-Banking – aber sicher!»: **www.ebas.ch**
- Kantonspolizei Zürich: **www.cybercrimepolice.ch**
- Bundesamt für Cybersicherheit: **www.ncsc.admin.ch**

Hier sind Sie gut beraten

Das VZ VermögensZentrum ist der führende unabhängige Finanzdienstleister der Schweiz. Immer mehr Kundinnen und Kunden profitieren von unserer Expertise: Sie gehen gut vorbereitet in Pension, legen ihr Geld intelligent an, finanzieren Häuser günstig, sind optimal versichert, regeln ihren Nachlass nach ihren Wünschen und zahlen nicht mehr Steuern als nötig. Auch Unternehmen und Pensionskassen sind beim VZ VermögensZentrum an der richtigen Adresse. Sie verbessern die Leistungen von Versicherungen und Vorsorge, erwirtschaften höhere Erträge mit ihren Anlagen und sparen gleichzeitig Prämien, Gebühren und Steuern.
Wenn es um Geld geht, sind Sie beim VZ gut beraten.

VZ VermögensZentrum AG (Hauptsitz)
Gotthardstrasse 6, 8002 Zürich
Telefon 044 207 27 27
vzzuerich@vermoegenszentrum.ch
www.vermoegenszentrum.ch

Aarau I Affoltern am Albis I Baden I Basel I Bellinzona I Bern I Brig
Burgdorf I Chur I Fribourg I Genève I Horgen I Kreuzlingen I Lausanne
Lenzburg I Liestal I Lugano I Luzern I Meilen I Neuchâtel I Nyon I Olten
Rapperswil I Rheinfelden I Schaffhausen I Sion I Solothurn I St. Gallen
Sursee I Thun I Uster I Vevey I Wil SG I Winterthur I Zug I Zürich