

19.12.2023

Vorsicht – Perfide Betrugsversuche im Umlauf

Behörden und Banken schlagen Alarm: Zurzeit versuchen Kriminelle vermehrt, sich Zugang zum E-Banking von Konsumenten zu verschaffen. Mit professionellen Mitteln, und nicht selten mit Erfolg.

Gleich mehrere sehr gut aufgemachte Betrugsmaschinen beschäftigen zurzeit diverse Finanzinstitute sowie deren Kunden.

Zum einen grassieren aktuell authentische Kopien von Bankseiten (Phishing-Websites), welche in Phishing-Mails oder über Suchmaschinenresultate verlinkt werden. Geben Bankkunden ihre Zugangsdaten dort ein, werden diese von den Angreifern in Echtzeit zur richtigen Anmeldeseite der jeweiligen Bank übertragen. Im nächsten Schritt wird der zweite Sicherheitsfaktor aus der echten Bankseite – z.B. ein QR-Code, eine Zahlenkombination oder ein Mosaikbild – ebenfalls in Echtzeit in die gefälschte Seite übernommen und vom nichtsahnenden Opfer bestätigt, wonach die Betrüger Zugang zum E-Banking haben. Nachfolgende missbräuchliche Geldüberweisungen werden nach dem gleichen Muster dem Opfer zur Freigabe weitergeleitet.

Ein ähnliches Betrugsmuster betrifft Verkäufer auf Kleinanzeige- und Auktionsplattformen. In diesem Fall meldet sich ein Betrüger als Kaufinteressent und verlangt die Kontaktdaten des Opfers für die Bezahlung des verkauften Artikels mittels Zahlungsdienstleister wie Paypal. Die so ergatterten Daten werden nachfolgend für weitere Angriffsschritte verwendet, die letztlich wiederum zur Übernahme des E-Banking des Verkäufers führen können.

In einem weiteren Betrugsfall geben sich Kriminelle telefonisch als Mitarbeitende oder Sicherheitsbeauftragte eines Finanzinstitutes aus, um auf diese Weise an sensible Informationen wie Zugangsdaten zum E-Banking des Bankkunden zu gelangen. Oft wird in diesen Fällen sogar die Telefonnummer gefälscht, um beim Opfer Vertrauen zu schaffen. Auch hier kommt oft das oben beschriebene Echtzeit-Phishing zum Einsatz, um die Zwei-Faktor-Authentifizierung des E-Bankings auszuheben.

Auch Anlagebetrug (engl. «Investment Fraud») ist derzeit hoch im Kurs. Häufig beginnen die Betrugsversuche mit lukrativen Job-Angeboten via Messenger-Dienste wie WhatsApp oder mit vermeintlich aufgedeckten Skandalen von prominenten Personen in den Sozialen Medien. Nach einer Phase des Vertrauensaufbaus werden Opfer oft zur Einzahlung einer kleinen Summe auf ein angeblich profitträchtiges Anlage-Portal animiert, wonach Gewinne vorgegaukelt werden, um höhere Einlagen zu erschleichen. In Wahrheit landet das Geld jedoch auf dem Bankkonto der Kriminellen.

Schützen Sie sich vor Phishing, indem Sie...

- nie einen Link verwenden, der per E-Mail, SMS oder Messenger-Dienst zugeschickt oder per QR-Code eingescannt wurde, um sich bei einem Finanzinstitut anzumelden.
- Anhänge von E-Mails und Kurznachrichtendiensten mit grosser Vorsicht behandeln.
- in Telefongesprächen nie vertrauliche Informationen, wie z.B. Passwörter, preisgeben.
- die Adresse zur Anmeldeseite Ihres Online-Dienstleisters oder Finanzinstituts immer manuell in die Adresszeile Ihres Browsers eingeben.

- sich bei Unsicherheit oder Unklarheit an das Finanzinstitut wenden.

Beachten Sie die folgenden Verhaltensregeln zum Schutz vor Anlagebetrug:

- Lassen Sie sich von unrealistischen Versprechen nicht blenden. Kein seriöser Finanzdienstleister verspricht überdurchschnittliche Gewinne in kurzer Zeit.
- Recherchieren Sie über den Anbieter, etwa auf Google, Internetforen und Konsumentenseiten. Überprüfen Sie, ob der Anbieter eine [Bewilligung der FINMA](https://www.finma.ch/de/finma-public/bewilligte-institute-personen-und-produkte/) (<https://www.finma.ch/de/finma-public/bewilligte-institute-personen-und-produkte/>) hat oder in der [FINMA-Warnliste](https://www.finma.ch/de/finma-public/warnliste/) (<https://www.finma.ch/de/finma-public/warnliste/>) oder im [IOSCO Investor Alerts Portal](https://www.iosco.org/investor_protection/?subsection=investor_alerts_portal) (https://www.iosco.org/investor_protection/?subsection=investor_alerts_portal) aufgeführt ist. Überprüfen Sie zudem den Handelsregisterauszug von Schweizer Anbietern unter www.zefix.ch (<https://www.zefix.ch/de/search/entity/welcome>).
- Wenden Sie sich an Ihren Kundenberater Ihrer Bank, wenn Sie unsicher sind.