Sparkasse Oberlausitz-Niederschlesien

FALLBEISPIEL ANLAGEBETRUG

Anlagebetrug mit angeblich hohen Renditen

Ein verlockendes Angebot

Frau K. stößt beim Surfen im Internet auf eine auffällige Anzeige: „Verdoppeln Sie Ihr Geld in nur wenigen Wochen! – Sicher investieren mit Kryptowährungen." Neugierig klickt sie auf den Link zu einem vermeintlich seriösen Anbieter. Die Webseite beeindruckt mit professionell gestalteten Grafiken, angeblichen Zertifikaten und Kundenbewertungen.

Der Betrug

Nach Eingabe ihrer Kontaktdaten wird Frau K. von einem „Finanzberater" kontaktiert, der sie überzeugt, 2.000 Euro in eine „sichere Anlage" einzuzahlen. Auf einer Online-Plattform kann sie scheinbar den rasanten Anstieg ihres Guthabens beobachten. Wenige Tage später steht dort ein Betrag von angeblich 3.800 Euro.
Motiviert investiert Frau K. weiter, bis ihre Einlagen 25.000 Euro betragen. Als sie eine Auszahlung fordert, wird ihr erklärt, dass zunächst „Steuern und Bearbeitungsgebühren" zu zahlen seien. Dieser Moment weckt ihr Misstrauen, doch ihr gesamtes investiertes Geld ist bereits verloren.

Wie Sie sich schützen können

- **Hohe Gewinne ohne Risiko gibt es nicht.** Seien Sie skeptisch bei Online-Werbung.
- **Keine Vorkasse für Steuern oder Gebühren leisten.** Seriöse Anbieter behalten Abgaben automatisch ein.
- **Anbieter sorgfältig prüfen.** Betrügerische Plattformen sitzen oft im Ausland und haben keine BaFin-Erlaubnis.
- **Rücksprache mit der Sparkasse halten.** Ihre Berater informieren Sie über sichere Anlagen.
- **Vertrauen Sie nicht nur auf schöne Internetseiten oder Telefonate.** Betrüger geben sich professionell, die Seriosität ist oft nur Fassade.
- **Offizielle Register nutzen.** Prüfen Sie Anbieter in Registern wie der BaFin-Warnliste; seien Sie bei Auslandssitzen besonders skeptisch.

Fazit: Schein-Gewinne sollen Vertrauen schaffen. Eine sorgfältige Prüfung des Anbieters und das Ablehnen von Vorab-Gebühren hätten den Verlust verhindert.

Tipp: Unter **www.spk-on.de/sicherheit** finden Sie Sicherheitshinweise und Warnmeldungen.

Sparkasse Oberlausitz-Niederschlesien

FALLBEISPIEL SMISHING

Smishing – Vorsicht vor angeblichen pushTAN-Verlängerungen per SMS

Herr K. erhält eine unerwartete SMS: Seine pushTAN-App laufe bald ab, und er solle den Link zur „Erneuerung“ nutzen. Die Webseite, die sich hinter dem Link verbirgt, sieht aus wie eine Sparkassen-Seite, verlangt jedoch umfangreiche persönliche Angaben wie Name, Adresse, Wohnort, Telefonnummer und Zugangsdaten – Informationen, die die Sparkasse bereits besitzt und online nicht erneut abfragt.
Noch am selben Abend ruft ein vermeintlicher Sparkassen-Mitarbeiter an. Auf dem Telefon wird die Sparkassen-Rufnummer angezeigt. Dieser führt Herrn K. durch mehrere Schritte, bei denen Herr K. in seiner pushTAN-App Freigaben bestätigt, die als Teil der Einrichtung dargestellt werden. In Wahrheit handelt es sich jedoch um Überweisungen an die Täter. Am nächsten Morgen fehlen mehrere tausend Euro auf Herrn K.s Konto.

Wie Sie sich schützen können

- **Keine Links in SMS von vermeintlichen Banken nutzen:** Sparkassen versenden keine SMS mit Links zu Anmeldeseiten. Geben Sie keine Daten über SMS-Links preis.
- **Achten Sie auf pushTAN-Texte:** Freigaben gelten immer nur für eigene Aufträge (z. B. Überweisungen), niemals für ein App-„Update“.
- **Vorsicht bei Formularen auf Bankseiten:** Formulare, die umfangreiche persönliche Daten anfordern, sind ein Alarmzeichen.
- **Seien Sie skeptisch bei Anrufen:** Nennen Sie niemals Zugangsdaten oder TANs am Telefon. Rufen Sie im Zweifel selbst über die offizielle Nummer der Bank zurück.

Fazit: Der Mix aus SMS-Link und Fake-Anruf ist klassisches Social Engineering. Eine genaue Prüfung der pushTAN-Auftragsdaten und ein eigener Rückruf bei der Sparkasse hätten den Schaden verhindern können.

Tipp: Unter **www.spk-on.de/sicherheit** finden Sie Sicherheitshinweise und Warnmeldungen.

Sparkasse Oberlausitz-Niederschlesien

FALLBEISPIEL
MICROSOFT BETRUG

Microsoft-Support-Betrug – Gefälschte Warnfenster

Der Vorfall

Frau L. stößt beim Surfen im Internet auf ein vollflächiges „Windows-Warnfenster“. Dieses blockiert ihren PC und fordert sie auf, sofort eine eingeblendete Telefonnummer anzurufen. Am anderen Ende der Leitung gibt sich ein angeblicher Techniker aus, der die Installation einer Fernwartungssoftware verlangt, um angebliche Schäden zu beheben.

Frau L. folgt den Anweisungen, wodurch die Täter Vollzugriff auf ihren PC erhalten. Sie kopieren Dateien und behaupten, betrügerische Zahlungen im Online-Banking verhindern zu wollen. Dafür fordern sie die pushTAN- oder chipTAN-Freigaben von Frau L. an. Ohne es zu wissen, unterstützt Frau L. damit die Täter bei Überweisungen. Erst das Trennen der Internetverbindung beendet den unberechtigten Zugriff.

Schutzmaßnahmen

- **Keine eingeblendeten Hotlines anrufen**: Microsoft und ähnliche Unternehmen zeigen keine Telefonnummern in Systemwarnungen an.
- **Browser oder PC über den Task-Manager schließen oder neu starten**: Führen Sie anschließend einen Virenscan durch, um mögliche Schadsoftware zu entfernen.
- **Keinen Fremdzugriff erlauben**: Installieren Sie keine „Reparatursoftware“ auf Aufforderung unbekannter Personen.
- **pushTAN / chipTAN sorgfältig prüfen**: Achten Sie genau auf Betrag und Empfänger-IBAN. Diese Daten betreffen Überweisungen, keine Stornierungen. +
- **Passwörter ändern und Sparkasse kontaktieren**: Bei Betrugsverdacht Passwörter sofort ändern, Sparkasse informieren und Geräte auf Sicherheitsprobleme prüfen.

Fazit: Diese Masche nutzt Angst: Nutzer sollen glauben, ihr PC sei beschädigt und nur ein Anruf helfe. Ein Neustart, kein Fernzugriff und das Ignorieren solcher Nummern schützen zuverlässig.

Tipp: Unter **www.spk-on.de/sicherheit** finden Sie Sicherheitshinweise und Warnmeldungen.

Sparkasse Oberlausitz-Niederschlesien

FALLBEISPIEL HANDYVERKAUF

Kleinanzeigen – „Sicher bezahlen"-Betrug beim Handyverkauf

Beim Verkauf ihres gebrauchten Handys über Kleinanzeigen.de wurde Frau M. Opfer eines Betrugs. Ein vermeintlicher Käufer schlug die Funktion „Sicher bezahlen" vor und sendete einen täuschend echten Link. Die nachfolgende Kommunikation schien über die Plattform von Kleinanzeigen zu erfolgen. Frau M., vertraut mit dem Zwei-Faktor-Login ihrer Sparkasse, hielt die geforderte „Bestätigung" für normal und gab auf der gefälschten Seite ihre Bankdaten ein. Kurz darauf erschien in ihrer Sparkassen-pushTAN-App eine Freigabe zur Überweisung von fast 1.000 € an eine fremde IBAN. In der Annahme, den Zahlungseingang für den Verkauf freizuschalten, bestätigte sie die Überweisung und autorisierte damit den Betrug. Der Käufer verschwand, und das Geld war weg.

Wie Sie sich schützen können

- **pushTAN genau prüfen:** Prüfen Sie Betrag, IBAN und Verwendungszweck – ein Geldeingang wird nie per pushTAN bestätigt.
- **Geräteregistrierung/Zwei-Faktor:** Diese erfolgt ausschließlich über das echte Sparkassen-Login. Klicken Sie niemals auf Links von Plattformen.
- **Funktion „Sicher bezahlen" kennen:** Informieren Sie sich vorab darüber, wie diese wirklich funktioniert. Kleinanzeigen verlangt keine Bankdaten oder TAN-Freigaben für einen Geldeingang.
- **Echte Funktionen nutzen:** Verwenden Sie nur die Funktionen der Kleinanzeigen-App oder -Website. Klicken Sie keine Links aus Chats an.
- **Keine PIN/Zugangsdaten eingeben:** Geben Sie niemals PINs oder Zugangsdaten auf fremden (unbekannten) Seiten ein.

Fazit: Ein entscheidender Schutz gegen Betrug ist der Blick in die pushTAN-Details: Eine Freigabe bedeutet immer, dass *Sie* einen Auftrag erteilen. Hätte Frau M. die Empfänger-IBAN und den Betrag geprüft, wäre der Betrug aufgefallen.

Tipp: Unter **www.spk-on.de/sicherheit** finden Sie Sicherheitshinweise und Warnmeldungen.