Der falsche Sparkassenmitarbeiter

Der Trick: Ein Anrufer gibt sich als Mitarbeiter der Nospa aus. Möglicherweise nennt er sogar den korrekten Namen Ihres Beraters, kennt Ihre Kontonummer und im Telefondisplay erscheint die Telefonnummer Ihrer Sparkasse.

Die Warnsignale:

- Meist rufen die Betrüger außerhalb der Öffnungszeiten an und geben vor, es besonders eilig zu haben, weil sonst beispielsweise das Konto gesperrt werden müsse.
- Die Betrüger fragen nach PINs, TANs oder Passwörtern. Das würden echte Sparkassenmitarbeiter NIEMALS tun.

Das richtige Verhalten:

- Legen Sie im Zweifel einfach auf und rufen Sie Ihre Sparkasse unter der Ihnen bekannten Rufnummer zurück – so können Sie in Erfahrung bringen, ob wirklich Handlungsbedarf besteht.
  ACHTUNG: keine automatische Wahlwiederholung nutzen, sondern die Telefonnummer der Sparkasse selbst eintippen.
- Ein echter Sparkassen-Mitarbeiter hat mit diesem Vorgehen auch kein Problem.
- Wichtig: Die Betrüger können auch die Rufnummer fälschen, die Ihnen im Display angezeigt wird.
- Wenn Sie jedoch auflegen und selbst noch einmal die Nummer Ihrer Sparkasse **NEU** wählen **(ACHTUNG: keine automatische Wahlwiederholung nutzen)**, landen Sie auch sicher dort. Und: **Lassen Sie sich niemals unter Zeitdruck zu irgendwelchen Handlungen zwingen.**

Betrug an der Haustür.

Der Trick: Ein Fremder bittet um Hilfe, gibt sich als Handwerker oder Behördenmitarbeiter aus oder will etwas verkaufen.

Die Warnsignale:

- Der Besuch kommt unangekündigt.
- Sie sollen etwas bar bezahlen.
- Man macht Ihnen ein Angebot, das „zu schön ist, um wahr zu sein“ und/oder nicht weitererzählt werden darf.

Das richtige Verhalten:

- Verweigern Sie den Zutritt zu Ihrer Wohnung bzw. lehnen Sie das Angebot deutlich ab.
- Bitten Sie Nachbarn um Hilfe.
- Benachrichtigen Sie die Polizei bzw. rufen Sie die Polizei, wenn der Besucher nicht geht.

Immer in Ihrer Nähe.

Wenn Sie einem Trickbetrug zum Opfer gefallen sind oder einen Verdacht haben, zögern Sie nicht, sich Hilfe zu holen. Informieren Sie die Polizei unter 110 und erstatten Sie ggf. Anzeige. Wenn Sie eine Karte sperren möchten, wählen Sie die Notfallnummer 116 116, wenn Sie Ihr Online-Banking sperren lassen möchten oder auffällige Kontobewegungen bemerken, wenden Sie sich an uns:

persönliche Beratung in unseren Regionaldirektionen und Filialen. Montag bis Freitag von 7 bis 19 Uhr.
Bitte vereinbaren Sie einen Termin unter 0461 1500-5555 oder unter nospa.de/termin

telefonisch über unser Kunden Servicecenter:
0461 1500-5555. Montag bis Freitag von 8 bis 19 Uhr.

online und **mobil** über www.nospa.de oder über unsere Sparkassen-App: „rund-um-die-Uhr“

Stand: 04.2022

Gut gewappnet gegen Trickbetrug.

So schützen Sie sich, Ihr Geld und Ihre Wertgegenstände.

Nord-Ostsee Sparkasse

www.nospa.de

POLIZEI
Schleswig-Holstein

Ausgetrickst?! Mit uns passiert Ihnen das nicht.

Gefälschte Gewinnmitteilungen.

Der Trick: Sie erhalten eine Gewinnbenachrichtigung.

Die Warnsignale:

- Sie haben an keinem Gewinnspiel teilgenommen.
- Sie sollen eine 0900-Nummer anrufen oder eine Vorleistung erbringen, um Ihren Gewinn in Anspruch nehmen zu können.
- Die benachrichtigende Firma hat ihren Sitz im Ausland oder gibt nur ein Postfach an.

Das richtige Verhalten:

- Reagieren Sie nicht auf die Mitteilung.
- Leisten Sie keine Vorauszahlungen.
- Prüfen Sie aufmerksam die an den Gewinn geknüpften Bedingungen (z. B. die Buchung einer Unterkunft für eine „geschenkte“ Reise).

Der Betrugsklassiker: Phishing

Der Trick: Beim Phishing verschicken Betrüger in großem Stil E-Mails oder auch SMS, die so aussehen, als kämen sie von Unternehmen wie beispielsweise Amazon, Ihrem Telefonanbieter oder Ihrer Sparkasse. Die dringend klingende E-Mail lockt Sie über einen Link auf eine täuschend echt aussehende Kopie der originalen Website. Auf der manipulierten Seite sollen Sie dann Ihre Kontodaten samt Passwort oder Geheimzahl eingeben. Vermeintlich, um Ihr Konto wieder freizuschalten. Stattdessen erbeuten die Datendiebe hochsensible Informationen.

Die Warnsignale:

- Der Absender: Häufig wird der Absender bekannter Unternehmen nachgeahmt. Bei genauerer Betrachtung erkennen Sie dann aber den Unterschied hinter dem @-Zeichen: „unternehmensname@betrüger.de“.
- Die Ansprache: Ihre Sparkasse kennt Ihren Namen und spricht Sie nicht mit „Sehr geehrter Kunde,“ an.
- Viele Rechtschreib- und Grammatikfehler.
- Links auf betrügerische Seiten, auf denen Sie Ihre Daten eingeben sollen.

Das richtige Verhalten:

- **Folgen Sie niemals einem Link und öffnen Sie niemals einen Anhang aus solchen „verdächtigen“ Nachrichten.** Geben Sie auf diesen Internetseiten keine sensiblen Kontodaten ein. Tippen Sie die Internet-Adresse Ihrer Sparkasse immer selbst ein.
- Ignorieren Sie grundsätzlich E-Mails, SMS und WhatsApp-Nachrichten von unbekannten Absendern.
- Das Schlosssymbol in Ihrem Browser muss bei Bankgeschäften im Internet immer geschlossen sein. Die Internetzeile muss für eine verschlüsselte Verbindung mit https:// (statt dem normalen http://) beginnen.
- Achten Sie bei der Internetadresse auf die korrekte Rechtschreibung.
- Prüfen Sie das „Zertifikat“ der Internetseite: Banken und viele Internet-Händler bieten Identitätsdaten an. Sie können diese im Symbol neben der Adresszeile abfragen. Ihr Internetschutzprogramm oder der Browserbetreiber bestätigen dann zum Beispiel die Echtheit der Seite mit „Verifiziert von…“.
- Nutzen Sie für Ihre Bankgeschäfte nur private gesicherte WLAN-Verbindungen. Die Startseiten öffentlicher WLANs könnten gefälscht sein.
- Bei Unsicherheiten bezüglich der Echtheit, wenden Sie sich über eine seriöse Kontaktmethode direkt an Ihren Anbieter und fragen Sie lieber einmal mehr nach.

Der falsche Polizist.

Der Trick: Ein Anrufer gibt sich als Polizeibeamter oder sonstiger Behördenvertreter aus.

Die Warnsignale:

- Der Anrufer versucht, Auskünfte über Geld und Wertgegenstände im Haushalt zu erlangen und fordert Sie unter Vorwand zum Abheben höherer Geldbeträge bzw. zum Leeren von Bankschließfächern auf.
- Sie werden mit einer emotional belastenden Situation konfrontiert z. B. Aufforderung zur Zahlung einer Kaution zur Abwendung einer angeblichen Haft oder zur Begleichung angeblicher Behandlungskosten nach Unfall eines Angehörigen (sog. „Schockanrufe“).
- Ein angekündigter Abholer soll Geld und Wertgegenstände übernehmen.
- **Polizeibeamte fordern niemals Bargeld von Ihnen!**

Das richtige Verhalten:

- Lassen Sie sich vom Anrufer nicht ausfragen.
- Ziehen Sie einen „echten“ Verwandten oder eine sonstige Vertrauensperson zu Rate.
- Gehen Sie nicht auf die Geldforderung ein.
- Beenden Sie schnellstmöglich das Telefongespräch.
- Rufen Sie sofort die Polizei über 110 an!

Der Enkeltrick.

Der Trick: Sie erhalten einen Anruf oder eine WhatsApp von einem angeblichen Verwandten. Dieser bittet Sie um Geld.

Die Warnsignale:

- Der Anruf beginnt mit „Rate mal, wer hier ist?“
- Der Anrufer bzw. die angezeigte Telefonnummer der WhatsApp ist Ihnen unbekannt.
- Ihr angeblicher Verwandter behauptet, er habe sein Handy verloren.
- Sie sollen schnell Geld überweisen, möglichst per Echtzeitüberweisung.
- Sie fühlen sich unter Druck gesetzt.

Das richtige Verhalten:

- Lassen Sie sich nur mit abgekürztem Vornamen ins Telefonbuch eintragen.
- Lassen Sie sich vom Anrufer nicht ausfragen.
- Ziehen Sie einen „echten“ Verwandten oder eine sonstige Vertrauensperson zu Rate.
- Gehen Sie nicht auf die Geldforderung ein.
- Reagieren Sie nicht auf die WhatsApp – klicken Sie auf keinen beigefügten Link, beenden Sie schnellstmöglich das Telefongespräch.
- Informieren Sie die Polizei über 110.