15.01.2025

Aktuelle Betrugsmaschen und wie Sie diese erkennen

Guten Tag,

aktuell versuchen Kriminelle wieder durch diverse Maschen, Sie um Ihr Geld zu bringen. Uns liegt es daher sehr am Herzen, Sie über aktuelle Betrugsmaschen aufzuklären und Sie zu schützen.

#Masche Nr. 1
Anrufe von angeblichen ING-Mitarbeitenden

Sie haben vielleicht schon davon gehört: Kriminelle rufen Sie an und geben sich als Bankmitarbeiterin oder Bankmitarbeiter aus, um an Ihre Zugangs- oder Kreditkartendaten und damit an Ihr Geld zu kommen.

Ein angeblicher Bankmitarbeiter ruft Sie an und bittet darum, aus Sicherheitsgründen oder wegen notwendiger Aktualisierung Daten abzugleichen. Unter Umständen bittet man Sie auch, Zugriff auf den PC zu gewähren. Auch wenn Ihr Gegenüber einige Daten von Ihnen kennt, wie z.B. Ihre Adresse oder Ihr Geburtsdatum, gehen Sie auf keinen Fall darauf ein. Bestätigen Sie nichts und geben Sie auf keinen Fall Daten preis.

Woran Sie erkennen, dass es sich um Betrüger und nicht um uns handelt? Sollten wir den Verdacht haben, dass Ihr Geld gefährdet ist, melden wir uns bei Ihnen oder sperren ggf. die Konten sofort und informieren Sie natürlich darüber. Wir kontaktieren Sie, um Sachverhalte zu klären. Wir fragen dafür aber weder Zugangsdaten ab noch brauchen wir eine Freigabe oder drohen mit Gebühren.

Im Zweifel legen Sie auf. Rufen Sie uns an und erkundigen Sie sich nach dem Sachverhalt. Unsere Mitarbeiterinnen und Mitarbeiter sind Montag bis Samstag von 8 bis 19 Uhr für Sie da – telefonisch unter 069 / 34 22 24.

#Masche Nr. 2
Phishing per E-Mail

In E-Mails, die angeblich von Ihrer Bank kommen, werden Sie plötzlich zu einer dringenden Aktion, wie z.B. einer Daten- oder App-Aktualisierung, aufgefordert. Hierzu sollen Sie auf einen Link klicken und Ihre persönlichen Daten eingeben. Tun Sie dies nicht, wird Ihnen mit Konsequenzen, wie beispielsweise einer Kontosperrung oder einer Gebührenzahlung, gedroht.

Mit Phishing-Mails versuchen Betrüger an Ihre Passwörter und vertrauliche Daten zu kommen. Sie können sicher sein, dass wir solche Informationen immer in Ihre Post-Box stellen und natürlich auch nicht darum bitten würden, Ihre Daten in einer verlinkten Seite einzugeben.
Phishing-Mails sind schwer zu erkennen, weil sie meist täuschend echt aussehen und sich immer weiterentwickeln. Woran Sie den Betrugsversuch trotzdem gut erkennen:

- Die E-Mail enthält oft keine persönliche Anrede
- Sie werden aufgefordert, einen Link anzuklicken: Nutzen Sie den „Mouse-over-Effekt“ – fahren Sie mit der Maus über den mitgelieferten Link in einer Mail. Dann sehen Sie sehr schnell, ob der Link tatsächlich zur Website Ihrer Bank führt oder ganz woanders hin.
- Geben Sie den Betreff der E-Mail in einer Suchmaschine ein. Oft wurde die Phishing-Mail bereits gemeldet und Sie finden entsprechende Informationen im Netz.
- Fragen Sie nach: Kontaktieren Sie das Unternehmen, das Sie angeblich angeschrieben hat – und zwar **über die offizielle Website oder Telefonnummer.** So gehen Sie ganz sicher und wissen direkt, ob die erhaltene Mail gefälscht ist.

ING-DiBa AG · Theodor-Heuss-Allee 2 · 60486 Frankfurt am Main · Vorsitzende des Aufsichtsrates: Susanne Klöß-Braekler · Vorstand: Lars Stoy (Vorsitzender), Michael Clijdesdale, Eddy Henning, Nikolaus Maximilian Linaric, Dr. Ralph Müller, Nurten Spitzer-Erdogan · Sitz: Frankfurt am Main · AG Frankfurt am Main HRB 7727
Steuernummer: 014 220 28004 · USt-IdNr.: DE 114 103 475 · Internet: www.ing.de · E-Mail: info@ing.de · BIC: INGDDEFFXXX · Mitglied im Einlagensicherungsfonds

86.627/12.24/3430/01

Übrigens: Kein echtes Unternehmen wird Ihnen als einzige Handlungsmöglichkeit einen Link in einer E-Mail zur Verfügung stellen. Ihre Daten aktualisieren, Passwörter ändern, Umsätze prüfen etc. können Sie auch direkt in Ihrem Kundenkonto. Und das erreichen Sie über die offizielle Website.

#Masche Nr. 3
Lukrative Geldanlage entpuppt sich als Betrug

Es klingt zu schön, um wahr zu sein: Betrügerische Anbieterinnen und Anbieter von Finanzprodukten versprechen, angeblich ohne jedes Risiko, lukrative Gewinne oder hervorragende Tagesgeldzinsen. Ein paar Klicks im Internet genügen – und schon locken satte Renditen auf das angelegte Geld. Doch Achtung, lassen Sie sich nicht blenden: Hinter den angeblich seriösen Finanzmaklern stecken oft Kriminelle.

Kaum hat man sich auf der angeblichen Handelsplattform registriert, ruft ein vermeintlicher Anlageberater an. Schnell werden es mehr Anrufe und Sie Ihr Geld los – die Betrüger beherrschen ihr Handwerk.

Es kann auch vorkommen, dass man Sie auffordert, sich erneut zu legitimieren – angebliche Gründe sind zum Beispiel

- um ein zusätzliches Konto für die Steuer zu verifizieren
- um einen Gewinn von der Trading-Plattform zu erhalten
- um angeblich versichertes Handelskapital zu erhalten.
- um Kaufverträge von sogenannten Faksimiles abzuschließen

Dabei werden Ihnen Antworten für das Verfahren bei der Post oder den Videochat vorgegeben. Tatsächlich aber veranlassen Sie mit der erfolgreichen Legitimation etwas ganz anderes. Zum Beispiel wird damit ein Kredit gewährt oder ein neues persönliches Konto eingerichtet. Auf beides können die Betroffenen dann aber nicht verfügen. Denn in den meisten Fällen sorgen die Kriminellen nach erfolgter Authentifizierung dafür, dass die Opfer das Geld schnell auf ein angebliches Konto der Trading-Plattform weiterleiteten. Um sich zu schützen, sollten Sie deshalb die folgenden Punkte befolgen:

- Suchen Sie im Internet nach möglichst umfassenden Informationen über das Unternehmen und das angepriesene Produkt. Hat das Unternehmen z.B. auf seiner Webseite ein Impressum?
- Erkundigen Sie sich beispielsweise bei einer Verbraucherzentrale oder der BaFin, bevor Sie Geld überweisen.
- Schauen Sie auf der Homepage der Bank, ob die Papiere oder Sparanlagen, wie zum Beispiel Tages- oder Festgeld, offiziell angeboten werden. Ein schmeichelhaftes „das Angebot gilt nur für Sie“ bedeutet heute oft Betrug.
- Vorsicht bei vermeintlich Wohltätigen, die geprellte Anlegerinnen und Anleger unterstützen wollen, ihr Geld zurückzuholen. Sie wollen die Abzocke fortsetzen. Kontaktieren Sie bei einem Verdacht die Polizei und Ihre Hausbank.
- Wimmeln Sie am Telefon und an der Haustür Unbekannte ab, die Ihnen unaufgefordert Anlageangebote unterbreiten wollen.
- Achten Sie auf die empfangenden Banken: Sind diese Banken Drittzahlungsdienstleistende oder Börsen für Kryptowährungen, bei denen das Wallet Kriminellen gehören kann, sollten Sie skeptisch sein.
- Seien Sie skeptisch, wenn Personen oder Firmen Sie dazu überreden wollen, ein Legitimationsverfahren mit vorgegebenen Antworten durchzuführen. Es gibt kein Szenario, bei dem Sie dabei von Dritten instruierte Antworten geben sollen.
- Achten Sie außerdem bei der Legitimation auf das Unternehmen, für das Sie sich legitimieren. Sollte dort eine Bank stehen (zum Beispiel die ING), dann handelt es sich höchstwahrscheinlich um die Eröffnung eines Kontos!

#Masche Nr. 4
Identitätsdiebstahl: Betrugsfälle bei der Wohnungssuche und Jobangeboten

Angesichts zunehmender Wohnungsnot tummeln sich auch vermehrt Kriminelle auf Immobilienportalen. Häufige Betrugsmaschen sind Vorabüberweisungen und Identitätsdiebstahl.

Interessante Anzeigen auf Immobilienportalen, Kleinanzeigen-Portalen, sozialen Medien, oder auch in Zeitungen regen zur Kontaktaufnahme mit der vermeintlich vermietenden Person oder der Hausverwaltung an. Auf ihre Anfrage zur Besichtigung, werden die Wohnungssuchenden aufgefordert, sich vorab über ein Legitimationsverfahren, wie zum Beispiel Postident, zu verifizieren. Besonders glaubwürdig wirken diese Nachrichten vor allem durch eine persönliche Vorgangsnummer und den Verweis auf die Deutsche Post als Partnerunternehmen. Hinzu kommt, dass es sich um eine echte Legitimierung handelt, bei der die Deutsche Post tatsächlich involviert ist. Doch anstatt sich für einen Besichtigungstermin zu verifizieren, eröffnen die Wohnungssuchenden irrtümlich ein Bankkonto, auf das nur die betrügenden Personen Zugriff haben.

Geschädigte erfahren häufig erst viel später von dem Betrug: Wenn ihre Bank sie deswegen kontaktiert, sie angesichts von SCHUFA-Problemen keine weiteren Bankgeschäfte machen können oder auch durch polizeiliche Ermittlungen.

Eine weitere Variante des Betruges dreht sich um Produkttests. Die Betrügenden geben vor, entsprechende Tester oder Testerinnen zu suchen, die dann z.B. eine Banking-App bewerten sollen. Die Anzeigen klingen verlockend: einfacher Nebenjob von zu Hause, keine Vorkenntnisse nötig und schnelle Einarbeitung. Es reichen ein Computer, ein Smartphone und eine stabile Internetverbindung. Die Betrügenden lassen den Testpersonen Zugangsdaten zukommen. Per Videoident-Verfahren stellen die „Testerinnen“ somit ihre Identität zur Verfügung und eröffnen unwissentlich ein echtes Bankkonto auf ihren Namen. Sie gehen aber immer noch von einem Produkttest aus und bemerken nicht, dass das Konto in die Hände von Kriminellen gelangt. Während sie selbst nie Zugriff auf diese Konten haben, nutzen die Täter es zur Geldwäsche – bis im schlimmsten Fall die Polizei eingeschaltet wird.

Egal, wie die Bezeichnung lautet: Finger weg von einem solchen Arbeitsverhältnis! Inzwischen werden auch eigentlich unauffällige Berufsbezeichnungen von Kriminellen gekapert – z.B.: „Aushilfe für Evaluierungen, Mitarbeiter m/w/d im Prozesscontrolling, Produkttester/Produkttesterin (zu Identifikationsverfahren), App-Tester/App-Testerin, Aushilfe im Büro m/w/d, Minijob Bürotätigkeit oder Datenerfasser/Datenerfasserin“.

Weitere Informationen zu allen Betrugsmaschen finden Sie auch auf unserer Webseite unter https://www.ing.de/hilfe/sicherheit-im-banking.

Halten Sie Augen und Ohren offen.

Zusammen sorgen wir dafür, dass Betrügerinnen und Betrüger keine Chance haben.

Ihre ING