Q&A

Ich habe bei der Erfassung einer Zahlung, die via InCore Bank erfolgen soll, irrtümlich eine falsche oder gar keine Referenznummer angegeben. Wie gehe ich vor?
Kontaktieren Sie Ihre Bank respektive Ihren Vertragspartner. Gleichzeitig können Sie auch InCore Bank per E-Mail informieren und uns den entsprechenden Zahlungsbeleg mitsenden.

Kann ich ein persönliches Konto bei InCore Bank eröffnen oder mein Geld bei InCore Bank anlegen?
Nein, nicht als Privatperson. Als reine Business-to-Business-Bank pflegt InCore Bank ihre Geschäftskontakte zu Finanzinstituten wie Banken und Wertpapierhäusern sowie Finanzintermediären wie Fintech-Unternehmen. Sie übernimmt in ihrem Auftrag verschiedene Aufgaben. InCore Bank pflegt keine direkte Beziehung zu Endkunden.

Was ist Phishing?
So nennt man den Versuch, über gefälschte Web-Seiten, E-Mails oder SMS (Smishing) an persönliche Daten von Internetnutzern zu gelangen oder diese zu schädlichen Taten zu bewegen. Dabei werden die kontaktierten Personen gebeten, möglichst schnell auf eine Web-Seite zu gehen, Daten einzugeben, Daten zu versenden, Links zu öffnen, Telefonnummern anzurufen oder Anhänge anzusehen/auszufüllen.
Bitte beachten Sie, dass wir unsere Kunden grundsätzlich nie auffordern, aus einer E-Mail oder SMS-Nachricht heraus zwecks Identifizierung/Freischaltung eines Kartenkontos irgendwelche Internetseiten über einen Link zu öffnen und dort sämtliche Kreditkarten- oder persönliche Zugangsdaten einzugeben. Darüber hinaus verlangen wir niemals Zahlungen – weder mit Bitcoin oder anderen digitalen Währungen, noch mit traditionellen Währungen – um ein Konto bei unserer Bank zu eröffnen.

Ich wurde Opfer einer Phishing-Attacke – was kann ich tun?
Kontaktieren Sie Ihre eigene Bank, von der die Zahlungen erfolgten, und die lokalen Behörden. Diese werden InCore Bank kontaktieren. Des Weiteren können Sie uns vorab folgende Informationen zustellen:

- Transaktionsbetrag
- Transaktionsdatum
- Währung
- Bank des Auftragsgebers
- Referenznummer
- Name und Kontonummer des Begünstigten
  Genaue Beschreibung des Betrugsvorganges
- Belege wie Transaktionsbelege, Bestätigung der Betrugsanzeige bei der Strafverfolgungsbehörde, Polizeirapport.

Bitte beachten Sie: Da zwischen Ihnen als Einzelperson und uns als InCore Bank AG keine vertraglich geregelte Kundenbeziehung besteht, ist es aufgrund des Schweizer Bankkundengeheimnisses der InCore Bank AG nicht gestattet, Informationen über allfällige Kundenbeziehungen bekannt zu geben. Bitte stellen Sie zuerst die Anfrage bei Ihrer Bank und/oder Ihrem Vertragspartner.

Ich habe Dokumente von InCore Bank erhalten, kann ich diese verifizieren?
Wenn Sie eine E-Mail oder SMS (angeblich) von InCore Bank erhalten und sich nicht sicher sind, ob es sich um eine Phishing/Smishing-Nachricht handelt, kontaktieren Sie uns bitte, bevor Sie auf die Nachricht antworten, auf einen Link klicken oder wie aufgefordert reagieren.

Wie lange dauert die Bearbeitung einer Anfrage bei InCore Bank?
Anfragen werden so schnell wie möglich, innert maximal zwei Arbeitstagen beantwortet. Bitte senden Sie alle Anfragen via E-Mail an uns.

Wie schütze ich mich vor Anlagebetrug?
Prüfen sie vermeintlich lukrative Finanzanlagen aus dem Netz sorgfältig. Lassen Sie sich niemals drängen und informieren Sie sich über den Anbieter, in dem Sie beispielsweise die FINMA-Warnliste konsultieren. Der Angreifer versucht, Sie zu einer Kontoeröffnung zu bewegen – oft über eine seriös wirkende Webseite. Auf dieses Konto sollen Sie dann einzahlen, per Kreditkarte oder in Kryptowährungen. Nach einem ersten Gewinn werden Sie zu weiteren Investitionen gedrängt. Weigern Sie sich, wird der Kontakt abgebrochen – Ihr Geld ist weg. Tätigen Sie bei einem Verdacht keine weiteren Einzahlungen und erstatten Sie sofort Anzeige.

Unerklärbare E-Banking-Transaktionen – was tun?
Informieren Sie umgehend Ihre Bank, tätigen Sie am betroffenen Gerät keine Transaktionen mehr und lassen Sie Ihren Computer von einer Fachperson untersuchen.

Wie kann ich sonst noch meine digitale Sicherheit erhöhen?
Seien Sie aufmerksam, surfen Sie besonnen im Internet, verwenden Sie sichere Passwörter, geben Sie nicht unvorsichtig persönliche Daten weiter, überprüfen Sie regelmässig Ihre Kontoauszüge, ignorieren oder löschen Sie E-Mails von verdächtigen Absendern, sichern Sie Ihre Daten regelmässig, aktivieren Sie eine Firewall, installieren Sie einen Virenschutz und halten Sie Ihr Betriebssystem sowie Apps und Programme mit Software-Updates immer aktuell. Und: Holen Sie sich bei Unsicherheit oder Verdacht auf einen Betrug sofort Unterstützung.