Online-Banking & Kreditkartenbetrug

Wie Betrüger vorgehen – und wie Du dich schützt

Sebastian Koch

Fachanwalt für Bank- und Kapitalmarktrecht

Deine Sicherheitshinweise von SALEO Rechtsanwälte

1.400+	25+	5.0 ★
geführte Verfahren	Jahre Erfahrung	Bewertung anwalt.de

SALEO
RECHTSANWÄLTE

Alle 39 Sekunden wird jemand Opfer.

2,2 Mrd. €

Schaden durch Zahlungsbetrug
in Deutschland (2024)

Smishing-SMS

Fake-Nachricht von „DHL" – ein Klick, alle Daten weg

Spoofed Anruf

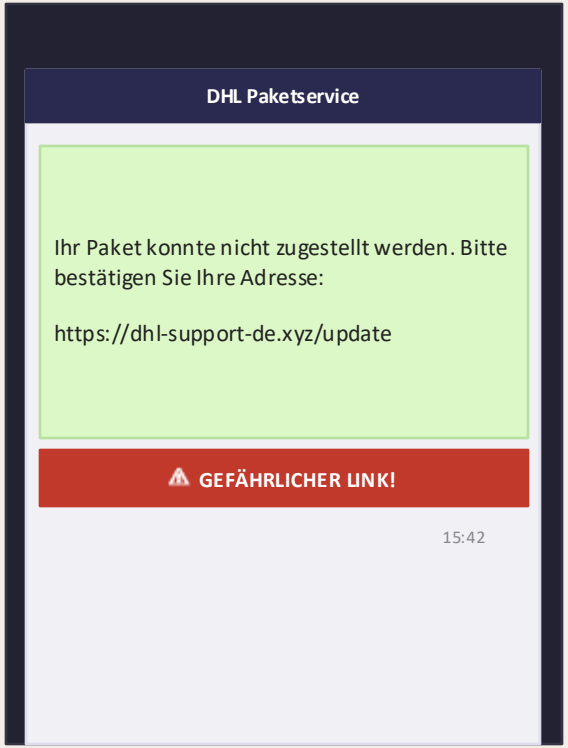
„Sparkasse" ruft an – in Wirklichkeit ein Betrüger

Fake-Käufer

Verkauf auf Kleinanzeigen.de – Zahlung kommt nie an

SALEO
RECHTSANWÄLTE

Smishing – die gefährliche SMS



Was passiert?

Du klickst auf den Link – eine gefälschte Website lädt. Dort gibst du Adresse, Kreditkartendaten oder Passwort ein.

Woran erkennst du es?

Seltsame URL (z. B. dhl-support-de.xyz statt dhl.de), Druck & Dringlichkeit, unerwartete Nachrichten.

Was tun?

Nie auf Links in SMS klicken! Direkt die offizielle Website besuchen oder Paketnummer prüfen.

SALEO
RECHTSANWÄLTE

Call-ID Spoofing – deine Bank ruft an … oder doch nicht?

1 Betrüger manipulieren die angezeigte Rufnummer, sodass z. B. „Sparkasse Frankfurt" erscheint – echt aussehend, komplett gefälscht.

2 Am Telefon: „Ihr Konto wurde gehackt – wir müssen Ihr Geld sofort auf ein Sicherheitskonto überweisen."

3 Schutz: Keine Bank bittet dich per Anruf zur Überweisung! Einfach auflegen und direkt die offizielle Nummer wählen.

SALEO RECHTSANWÄLTE

Kleinanzeigen.de – Verkäufer werden zur Zielscheibe

kleinanzeigen.de – Chat

„Ich möchte das iPhone kaufen! Ich zahle per Sicher-Bezahlen-System."

OK, wie soll das gehen?

„Ich schicke dir einen Link zum Registrieren – du bekommst das Geld sofort!"

https://kleinanzeigen-zahlung.ru/pay

⚠ GEFÄLSCHTER LINK – KEIN OFFIZIELLER LINK!

So läuft die Masche ab

① Kontakt via WhatsApp – emotional, kein Feilschen, wirkt vertrauenswürdig

② Betrüger schlägt „Sicher Bezahlen" vor – sendet gefälschten Link (oft QR-Code = Quishing)

③ Link führt zu täuschend echter Fake-Seite von kleinanzeigen.de oder der Bank

④ Kreditkartendaten + TAN werden eingegeben → vollständiger Kartenzugriff

Neue Masche: Quishing

QR-Codes statt Links – noch schwerer als Fälschung erkennbar.

Dein Recht (§ 675u BGB)

Bank muss erstatten! Gerichte verneinten grobe Fahrlässigkeit.

So schützt du dich:

Nur über den offiziellen Chat im Portal bezahlen · Niemals externen Links folgen · QR-Codes von Fremden nicht scannen · Telefonat vor Kauf verlangen

SALEO RECHTSANWÄLTE

Phishing & weitere Betrugsmaschen im Überblick

E-Mail Phishing

Gefälschte Bank-E-Mails mit Links zu täuschend echten Login-Seiten. Ziel: Zugangsdaten stehlen.

Skimming

Manipulierte Kartenleser am Geldautomaten lesen deine Karte aus – zusätzlich Kamera für die PIN.

Fake-Banking-App

Gefälschte Banking-Apps im App Store – sie leiten Überweisungen um oder speichern TANs.

Man-in-the-Middle

Betrüger schalten sich zwischen dich und deine Bank – im öffentlichen WLAN besonders gefährlich.

Social Engineering

„Ich bin der IT-Support Ihrer Bank" – Manipulation durch Vertrauen und Druck.

Fake-Investment

Traumrenditen auf Krypto-Plattformen – du zahlst ein, Auszahlung kommt nie.

SALEO
RECHTSANWÄLTE

Sicherheitsmaßnahmen

5 Maßnahmen, die du heute noch umsetzen kannst

01

2-Faktor-Auth aktivieren

Für Banking, E-Mail und alle wichtigen Accounts. Ein Passwort allein reicht nicht!

02

Passwort-Manager nutzen

Einzigartiges Passwort für jeden Dienst. KeePass, Bitwarden & Co. sind kostenlos.

03

Push-Benachrichtigungen an

Sofort informiert bei jeder Kontobewegung – auch über 1-Cent-Testabbuchungen.

04

Banken fordern nie telefonisch oder per SMS zu Freigaben auf

Sofern Druck aufgebaut wird, Ruhe bewahren und selbständig bei der Bank nachfragen / Kein Rückruf

05

Kreditlimit bewusst setzen

Begrenze Online-Transaktionen in deiner Banking-App – weniger Schaden möglich.

SALEO
RECHTSANWÄLTE

Betrogen? So handelst du SOFORT richtig!

1

Karte SOFORT sperren

Sperr-Notruf: 116 116 (kostenlos, 24/7)
Oder direkt in der Banking-App

2

Bank anrufen

Lastschriften widersprechen!
Rückbuchungsantrag stellen (bis 8 Wochen)

3

Beweise sichern

Screenshots von SMS, E-Mails, Chats
Transaktionsübersichten speichern

4

Anzeige erstatten

Online unter: polizei.de oder beim nächsten Polizeirevier – wichtig für Erstattung!

5

Verbraucherzentrale oder Anwalt einschalten

Banken lehnen oft ab – hol dir rechtliche Unterstützung (1.400+ Verfahren bei SALEO)

SALEO
RECHTSANWÄLTE

Dein Recht: Die Bank haftet – meistens!

§ 675u BGB – Erstattungspflicht der Bank

Bei nicht autorisierten Zahlungen hat der Zahlungsdienstleister dem Zahler den Betrag unverzüglich zu erstatten. Die Beweislast liegt bei der Bank!

Du haftest NICHT wenn…	Grobe Fahrlässigkeit vermeiden	Bank lehnt ab? Beratung suchen
→ Du die Zahlung nicht autorisiert hast	→ PIN niemals weitergeben	→ Anwalt oder Verbraucherzentrale
→ Betrüger deine Zugangsdaten gestohlen haben	→ Keine TAN auf Phishing-Seiten eingeben	→ Schlichtungsverfahren
→ Du professionell getäuscht wurdest (Spoofing, Phishing)	→ Sicherheitsupdates installieren	→ SALEO: 1.400+ geführte Verfahren

SALEO
RECHTSANWÄLTE

Awareness schützt!

Danke für Ihr Interesse

- Erkenne die Maschen – Smishing, Spoofing, Handelsplattformen, Fake-Shops
- Handle sofort – Karte sperren, Bank, Anzeige, Anwalt

Empfohlen von Finanztip.de

Kostenloser Erstcheck

06032 / 93 00 – 0
info@saleo-recht.de
www.saleo-recht.de

SALEO
RECHTSANWÄLTE