

# Digitaler Betrug: Wie kann ich mich schützen?

**Eine SMS von der Bank, eine WhatsApp-Nachricht von einem Familienmitglied, eine E-Mail vom Paketdienst oder ein QR-Code auf einem Schreiben: Betrüger versuchen auf vielen Wegen, an unser Geld oder unsere persönlichen Daten zu kommen. Die VSZ sagt Ihnen, worauf Sie achten müssen.**

Betrugsmaschen werden immer professioneller. Vieles ist klassisches Phishing, wird aber technisch und auch psychologisch immer raffinierter. Eine Nachricht kann täuschend echt aussehen. Logos, Namen und Internetseiten lassen sich kopieren und selbst die angezeigte Telefonnummer oder der Absender einer Nachricht können manipuliert werden.

Deshalb gilt vor allem eine Regel: **Nicht unter Druck setzen lassen. Erst prüfen, dann handeln.**

## Was ist digitaler Betrug?

Beim digitalen Betrug versuchen Kriminelle, über E-Mail, SMS, Messenger-Dienste, soziale Netzwerke, Telefonanrufe, QR-Codes oder gefälschte Internetseiten an Geld, Passwörter, Bankdaten oder andere persönliche Informationen zu gelangen.

Oft geben sich die Betrüger als jemand aus, dem wir vertrauen: als Bank, Behörde, Paketdienst, Energieanbieter, Polizei oder sogar als Familienmitglied.

## Welche Betrugsformen gibt es?

Die Namen klingen kompliziert, das Prinzip dahinter ist meistens ähnlich.

**Phishing:** Betrüger verschicken gefälschte E-Mails oder locken Sie auf gefälschte Internetseiten. Dort sollen Sie zum Beispiel Passwörter, persönliche Daten oder Bankdaten eingeben.

**Smishing:** Das ist Phishing per SMS. Die Nachricht enthält häufig einen Link oder fordert Sie auf, dringend zu reagieren oder eine Telefonnummer anzurufen.

**Vishing:** Hier findet der Betrugsversuch am Telefon statt. Der Anrufer gibt sich zum Beispiel als Mitarbeiter einer Bank, eines Unternehmens oder einer Behörde aus und versucht, an persönliche Daten oder Geld zu gelangen.

**Messenger-Betrug:** Über WhatsApp oder andere Messenger geben sich Betrüger zum Beispiel als Sohn, Tochter oder Bekannter aus. Typisch ist die Nachricht: „Hallo Mama, das ist meine neue Nummer.“ Kurz danach folgt häufig die Bitte, dringend Geld zu überweisen.

**Quishing:** Hier verwenden Betrüger gefälschte QR-Codes. Wer einen solchen Code scannt, kann auf einer gefälschten Internetseite landen. Dort sollen dann beispielsweise persönliche Daten oder Bankdaten eingegeben werden.

**Betrug über soziale Netzwerke:** Gefälschte Profile, Werbeanzeigen oder Nachrichten auf Facebook, Instagram und anderen sozialen Netzwerken können zu Fake-Shops, falschen Gewinnspielen oder unseriösen Geldanlagen führen.

**Paketbetrug:** Sie erhalten eine SMS oder E-Mail, die scheinbar von einem Paketdienst stammt. Angeblich konnte ein Paket nicht zugestellt werden oder es fehlen noch Angaben. Über einen Link sollen Sie persönliche Daten oder Zahlungsinformationen eingeben.

**Betrügerische Anlagetipps:** Über Werbung in sozialen Netzwerken werden Verbraucher zum Beispiel in WhatsApp-Gruppen gelockt. Dort versprechen angebliche Experten hohe Gewinne und geben vermeintlich exklusive Börsen- oder Anlagetipps. Ziel ist es, Sie zu einer Geldanlage zu bewegen.

**Gefälschte Trading- und Krypto-Plattformen:** Betrüger locken Verbraucher auf gefälschte Internetseiten für Geldanlagen oder Kryptowährungen. Dort werden hohe Gewinne versprochen. Das eingezahlte Geld landet jedoch bei den Betrügern.

**Gefälschte Rechnungen:** Betrüger verschicken oder verändern Rechnungen und ersetzen die richtige Kontonummer durch ihre eigene. Wer die Rechnung bezahlt, überweist das Geld direkt an die Betrüger.

Die Methoden ändern sich ständig. Deshalb ist es wichtiger, die typischen Warnzeichen zu kennen als sich jeden Namen einer Betrugsmasche zu merken.

#### **Aktuelle Betrugsmaschen in Belgien – Stand Oktober 2026**

- Falsche Bankmitarbeiter am Telefon (Vishing)
- Paket-SMS und Paket-E-Mails (Smishing/Phishing)
- “Hallo Mama/Papa, das ist meine neue Nummer” (Messenger-Betrug)
- Falsche Anlagetipps und Trading-Gruppen über WhatsApp
- Betrügerische Trading/Krypto-Plattformen
- Falsche Zahlungsaufforderungen bzw. Bestätigungen über itsme

**Egal ob SMS, WhatsApp, Telefon, QR-Code oder E-Mail: Sobald jemand Druck macht, sollten Sie vorsichtig werden. Überweisen Sie nicht vorschnell Geld, geben Sie keine Bankdaten ein und bestätigen Sie keine unbekannten Vorgänge über itsme oder Ihre Bank-App. Prüfen Sie zuerst über einen offiziellen Kontakt, ob die Nachricht wirklich echt ist.**

## **Woran erkenne ich einen möglichen Betrugsversuch?**

Misstrauisch sollten Sie vor allem werden, wenn eine Nachricht unerwartet kommt und Sie zu einer schnellen Handlung auffordert.

Typische Warnzeichen sind:

- Sie sollen sofort reagieren.
- Ihnen wird mit einer Kontosperrung, Mahnung oder anderen Folgen gedroht.
- Sie sollen auf einen Link klicken oder einen QR-Code scannen.
- Sie sollen ein Passwort, einen PIN-Code oder Bankdaten eingeben.
- Sie sollen eine Zahlung oder Überweisung durchführen.
- Sie sollen eine Anmeldung oder Zahlung über itsme oder Ihre Banking-App bestätigen.
- Sie sollen eine Datei oder App herunterladen.
- Eine bekannte Person meldet sich plötzlich unter einer neuen Telefonnummer und bittet um Geld.
- Ein Angebot oder Gewinn klingt zu gut, um wahr zu sein.

Ein einzelnes Merkmal beweist noch keinen Betrug. Treffen mehrere Punkte zusammen, ist besondere Vorsicht angesagt.

## **Sind Rechtschreibfehler noch ein gutes Erkennungszeichen?**

Nicht unbedingt. Früher waren betrügerische Nachrichten häufig an schlechtem Deutsch, merkwürdigen Formulierungen oder Rechtschreibfehlern zu erkennen. Darauf sollte man sich heute nicht mehr verlassen.

Betrügerische Nachrichten können professionell formuliert sein und Logos, Namen und Gestaltung bekannter Unternehmen täuschend echt nachahmen.

## **Kann ich dem Namen des Absenders vertrauen?**

Nein. Nur weil auf Ihrem Smartphone beispielsweise der Name einer Bank oder eines Paketdienstes angezeigt wird, bedeutet das nicht automatisch, dass die Nachricht tatsächlich von diesem Unternehmen stammt.

Auch Telefonnummern und Absenderangaben können manipuliert werden.

## **Was mache ich, wenn ich eine verdächtige Nachricht erhalte?**

Klicken Sie zunächst auf nichts. Öffnen Sie keine Anhänge, scannen Sie keinen QR-Code und geben Sie keine persönlichen Daten ein.

Möchten Sie überprüfen, ob eine Nachricht tatsächlich von Ihrer Bank, einem Unternehmen oder einer Behörde stammt, suchen Sie selbst deren offizielle Internetseite oder App auf. Benutzen Sie nicht den Link oder die Telefonnummer aus der verdächtigen Nachricht.

Im Zweifelsfall kontaktieren Sie das Unternehmen über die Ihnen bekannte Telefonnummer.

### **Darf ich QR-Codes bedenkenlos scannen?**

Nein. Ein QR-Code ist im Grunde nur ein anderer Weg zu einem Link. Betrüger können beispielsweise gefälschte QR-Codes in E-Mails und Briefen verwenden oder echte QR-Codes an öffentlichen Orten überkleben.

Prüfen Sie deshalb nach dem Scannen die angezeigte Internetadresse, bevor Sie die Seite öffnen oder dort Daten eingeben.

Besondere Vorsicht ist geboten, wenn Sie über einen QR-Code zu einer Zahlung oder zur Eingabe von Bankdaten aufgefordert werden.

### **Was mache ich bei einer WhatsApp-Nachricht von einer „neuen Nummer“?**

Werden Sie misstrauisch, sobald Geld ins Spiel kommt. Rufen Sie Ihren Sohn, Ihre Tochter oder die betreffende Person unter der alten, Ihnen bekannten Telefonnummer an. Stellen Sie eine Frage, die nur die betreffende Person beantworten kann.

Überweisen Sie kein Geld, solange Sie nicht sicher sind, mit wem Sie tatsächlich kommunizieren.

### **Darf ich eine Anmeldung über itsme bestätigen?**

Bestätigen Sie über itsme oder Ihre Banking-App nur Vorgänge, **die Sie selbst begonnen haben.**

Werden Sie während eines Telefongesprächs oder nach einer unerwarteten Nachricht aufgefordert, etwas über itsme oder Ihre Banking-App zu bestätigen, brechen Sie den Vorgang ab.

### **Was ist mit Kettenbriefen und weitergeleiteten Nachrichten?**

Auch hier ist Vorsicht angebracht. Kettenbriefe und weitergeleitete Nachrichten können Falschmeldungen, gefälschte Spendenaufrufe, Links zu betrügerischen Internetseiten oder Schadsoftware enthalten.

Leiten Sie eine Nachricht nicht einfach weiter, nur weil Sie von einem Freund oder Bekannten stammt. Auch dessen Konto könnte gehackt worden sein oder die Person könnte selbst auf eine Falschmeldung hereingefallen sein.

### **Soll ich verdächtige Nachrichten melden?**

Ja. Verdächtige E-Mails und Nachrichten können in Belgien an [verdacht@safeonweb.be](mailto:verdacht@safeonweb.be) weitergeleitet werden. Anschließend können Sie die Nachricht löschen.

### **Ich habe auf einen verdächtigen Link geklickt. Was jetzt?**

Ein Klick allein bedeutet noch nicht automatisch, dass ein Schaden entstanden ist.

Haben Sie anschließend keine Daten eingegeben, keine Datei heruntergeladen und keine App installiert, schließen Sie die Seite.

Haben Sie jedoch persönliche Daten, Passwörter oder Bankdaten eingegeben, sollten Sie sofort handeln.

### **Ich habe mein Passwort eingegeben. Was soll ich tun?**

Ändern Sie das Passwort sofort. Falls Sie dasselbe Passwort auch für andere Konten verwenden, ändern Sie es dort ebenfalls. Verwenden Sie für wichtige Konten unterschiedliche Passwörter.

Aktivieren Sie außerdem, wenn möglich, eine Zwei- oder Multifaktor-Authentifizierung.

### **Ich habe meinen PIN und mein Passwort angegeben. Was muss ich tun?**

**Kontaktieren Sie sofort Ihre Bank.** Wurden Kartendaten gestohlen oder besteht die Gefahr eines Missbrauchs, können Sie Ihre Zahlungsmittel über Card Stop unter **078 170 170** sperren lassen.

Kontrollieren Sie außerdem Ihre Kontobewegungen. Unbekannte Transaktionen sollten Sie möglichst schnell Ihrer Bank melden.

### **Ich habe bereits Geld überwiesen. Ist es zu spät?**

Nicht unbedingt. Aber Sie sollten schnell reagieren. Kontaktieren Sie sofort Ihre Bank und erklären Sie, was passiert ist. Je nach Situation kann möglicherweise noch versucht werden, eine Zahlung zu stoppen oder zurückzuverfolgen.

Bei einem finanziellen Schaden sollten Sie außerdem Anzeige bei der Polizei erstatten.

### **Was sollte ich für die Polizei aufbewahren?**

Löschen Sie nicht sofort alle Beweise. Bewahren Sie beispielsweise Screenshots, E-Mails, SMS, Telefonnummern, Kontonummern, Zahlungsbelege und den Verlauf von WhatsApp- oder anderen Messenger-Nachrichten auf.

Diese Informationen können bei einer Anzeige wichtig sein.

### **Wie kann ich mich grundsätzlich schützen?**

Ein hundertprozentiger Schutz vor digitalem Betrug ist kaum möglich. Einige einfache Gewohnheiten verringern das Risiko aber deutlich:

- Lassen Sie sich nicht unter Zeitdruck setzen.
- Klicken Sie nicht vorschnell auf Links.
- Geben Sie Passwörter, PIN-Codes und Sicherheitscodes niemals weiter.
- Bestätigen Sie keine Vorgänge, die Sie nicht selbst gestartet haben.
- Prüfen Sie ungewöhnliche Geldforderungen über einen zweiten Kontaktweg.
- Verwenden Sie unterschiedliche und sichere Passwörter.
- Aktivieren Sie die Zwei- oder Mehrfaktor-Authentifizierung.
- Halten Sie Smartphone, Computer und Apps aktuell.
- Kontrollieren Sie regelmäßig Ihre Kontobewegungen.

### **Die wichtigste Regel**

- Betrüger versuchen häufig, Angst, Zeitdruck, Hilfsbereitschaft oder Neugier auszunutzen.

Deshalb gilt:

Kommt Ihnen eine Nachricht merkwürdig vor, reagieren Sie nicht sofort. Klicken Sie auf nichts und geben Sie keine Daten weiter. Prüfen Sie die Information über einen zweiten, unabhängigen Weg.

Und wenn Sie doch auf einen Betrugsversuch hereingefallen sind:

- Handeln Sie schnell.
- Kontaktieren Sie bei Bank- oder Kartendaten sofort Ihre Bank beziehungsweise Card Stop und
- erstatten Sie bei einem finanziellen Schaden Anzeige bei der Polizei.

### **Nützliche Anlaufstellen:**

- Safeonweb: Informationen über aktuelle Betrugsmaschinen und Cybersicherheit. Verdächtige Nachrichten: [verdacht@safeonweb.be](mailto:verdacht@safeonweb.be)
- Card Stop: 078 170 170 – rund um die Uhr erreichbar
- Polizei: Bei finanziellem Schaden, Diebstahl von Daten oder anderen Straftaten Anzeige erstatten.