Raiffeisen
Mehr Nähe. Mehr Bank.

Cybersecurity

Schütze deine Daten.
Schütze dein Geld.

Warum ist Cybersecurity wichtig?

Cybersecurity bedeutet, sich im Internet und am Computer gegen Cyber-Angriffe zu schützen.

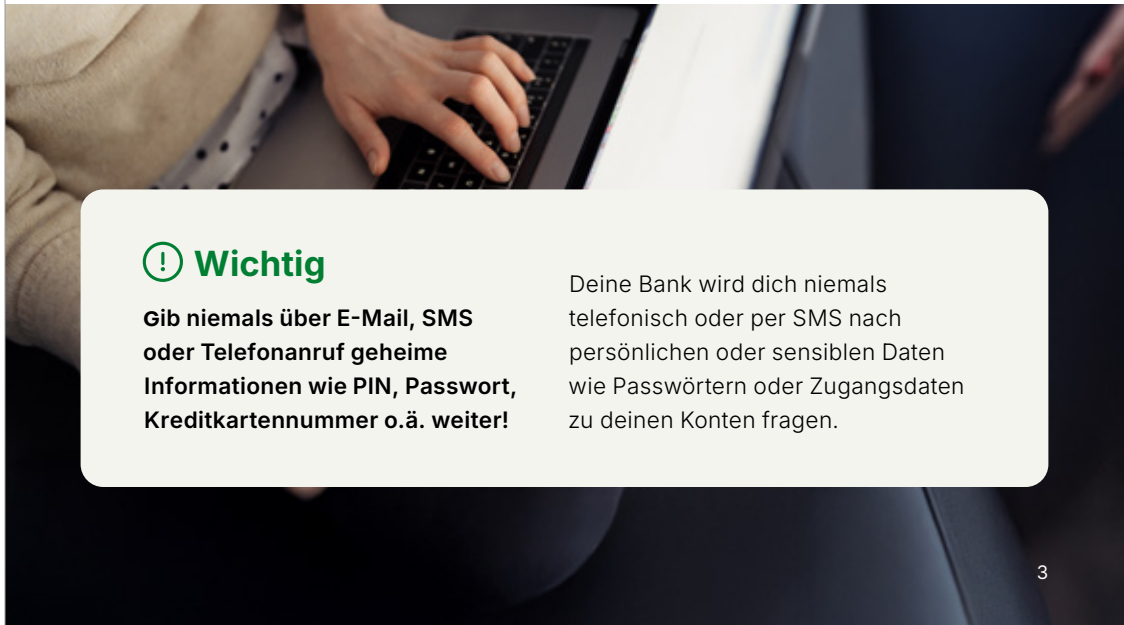
In einer zunehmend vernetzten Welt, in der Bankgeschäfte, Kommunikation und Einkäufe online stattfinden, ist dieser Schutz von zentraler Bedeutung. Cyberkriminelle nutzen gezielt Schwachstellen aus, um an vertrauliche Informationen wie **Passwörter, Kreditkarten- oder Bankdaten** zu gelangen, Betrugsversuche gegen Bankkund*innen nehmen dabei weiter zu. Besonders gefährlich sind **gefälschte E-Mails, SMS, Telefonate oder Webseiten,** die von einem scheinbar vertrauten Absender stammen.

UNBEDACHTE **KLICKS**, DAS PREISGEBEN VON **PERSÖNLICHEN ZUGANGSDATEN** ODER DIE WEITERGABE EINES **PINS** KÖNNEN GROSSE SCHÄDEN VERURSACHEN.

Deshalb ist es wichtig, Gefahren zu erkennen, keine unüberlegten Handlungen vorzunehmen und im Zweifel eine zweite Meinung bei der eigenen Bank einzuholen.

Die häufigsten Betrugsmaschen im Alltag

- **Phishing**
  E-Mail-Betrug
- **Betrug über Social Media**
- **Smishing**
  Betrug per SMS
- **Gefälschte Online-Shops**
- **Vishing**
  Telefonbetrug
- **Unbefugter Zugang über Fernwartungsoftware**
- **Anlage- und Investmentbetrug**
- **Gefälschte Gewinnspiele**



Wichtig

Gib niemals über E-Mail, SMS oder Telefonanruf geheime Informationen wie PIN, Passwort, Kreditkartennummer o.ä. weiter!

Deine Bank wird dich niemals telefonisch oder per SMS nach persönlichen oder sensiblen Daten wie Passwörtern oder Zugangsdaten zu deinen Konten fragen.

Die gängigsten Cyber-Angriffs-methoden

Woran erkenne ich sie, was sind die Folgen und wie kann ich mich schützen?

Phishing

Was ist Phishing?

PHISHING IST EINE DER HÄUFIGSTEN BETRUGSMETHODEN IM INTERNET.

Dabei versenden Betrüger*innen **E-Mails**, die wie offizielle Nachrichten von Banken oder bekannten Unternehmen aussehen. Meist enthalten diese E-Mails einen Link, der auf eine **gefälschte Webseite** führt, welche der echten Bankseite und Unternehmensseite sehr ähnlich ist.

Was sind die Folgen?

Gibt man auf dieser Webseite seine **Zugangsdaten** ein, gelangen diese direkt in die **Hände der Betrüger*innen.** Diese können sich anschließend in das Online Banking einloggen und Überweisungen vorbereiten. Die Überweisungen werden erst ausgeführt, sobald die betroffene Person sie auf ihrem Gerät genehmigt.

Woran lässt sich Phishing erkennen?

Typische Anzeichen sind **Rechtschreib- oder Formatierungsfehler,** ungewöhnliche Absenderadressen oder leicht falsch geschriebene Internetlinks. Häufig versuchen Betrüger*innen Druck aufzubauen - zum Beispiel durch Drohungen mit einer Kontosperre.

Wie kann ich mich schützen?

- Öffne **keine Links** aus **verdächtigen E-Mails.**
- Gib niemals **Zugangsdaten** wie Benutzername, Passwort, PIN oder TAN ein.
- Prüfe **Absender** und **Internetadresse** genau.
- Kontaktiere bei Zweifeln sofort deine Raiffeisenkasse.

Smishing

Was ist Smishing?

SMISHING IST EINE BETRUGSFORM, BEI DER KRIMINELLE VERSUCHEN, ÜBER **SMS** AN PERSÖNLICHE ODER SENSIBLE DATEN ZU GELANGEN.

Die Nachrichten wirken, als kämen sie direkt von der Bank oder vom Kreditkartenanbieter. Sie enthalten entweder einen **Link** zu einer gefälschten Webseite oder eine **Telefonnummer** mit der Aufforderung zur Kontaktaufnahme.

Was sind die Folgen?

Nach Eingabe der Zugangsdaten können Betrüger*innen das **Online Banking nutzen** und Überweisungen vorbereiten.

Die Überweisungen werden ausgeführt, sobald die betroffene Person sie auf ihrem Gerät genehmigt.

Woran lässt sich Smishing erkennen?

Die SMS erzeugt **Stress oder Angst,** zum Beispiel durch Hinweise auf eine verdächtige Zahlung oder fremde Gerätezugriffe. Der Link sieht echt aus, ist aber oft falsch geschrieben. Achte auf **Rechtschreib- oder Grammatikfehler** im Text – sie sind ein deutliches Warnsignal.

Häufige Absender sind z.B. Nexi, Raiffeisen, Booking, Lugano, Lissabon und unbekannte Nummern.

Wie kann ich mich schützen?

- Öffne **keine Links** aus einer SMS.
- Rufe niemals die angegebene **Telefonnummer** an.
- Gib niemals persönliche oder vertrauliche **Daten** ein.
- Prüfe dringende oder beängstigende **Nachrichten kritisch**.
- Kontaktiere bei Verdacht sofort deine Raiffeisenkasse.

Vishing

Was ist Vishing?

BEIM VISHING KONTAKTIEREN BETRÜGER*INNEN IHRE OPFER **TELEFONISCH.**

Sie geben sich als Bankmitarbeiter*innen oder als Angestellte anderer vertrauenswürdiger Stellen aus und berichten von angeblichen Problemen mit dem Konto.

Was sind die Folgen?

Gibt man Zugangsdaten oder Freigabepasswörter weiter, können Betrüger*innen **Überweisungen durchführen oder bestätigen lassen.**

Woran lässt sich Vishing erkennen?

Am Telefon werden **vertrauliche Online Banking-Daten** abgefragt – echte Banken tun dies niemals! Zudem wird großer **Zeitdruck** erzeugt, besonders bei Aufforderungen zur Freigabe von Transaktionen, die angeblich der **Sperrung von Überweisungen** dienen.

Wie kann ich mich schützen?

- Nenne am Telefon niemals **Passwörter** oder **PINs.**
- **Beende** bei Zweifeln sofort das **Gespräch.**
- Melde den Vorfall umgehend deiner Raiffeisenkasse.

Anlage- und Investmentbetrug

Worum handelt es sich dabei?

BETRÜGEREIEN MIT FALSCHEN INVESTITIONEN TRETEN AUF, WENN KRIMINELLE VERLOCKENDE **INVESTITIONSANGEBOTE** MACHEN, DIE HOHE RENDITEN BEI GERINGEM RISIKO VERSPRECHEN.

Diese Offerte können über Websites, E-Mails, Telefonanrufe oder Anzeigen in sozialen Medien verbreitet werden und zielen auf Investitionen in **Aktien, Kryptowährungen, Immobilien oder andere Finanzprodukte** ab.

Was sind die Folgen?

Opfer solcher Betrügereien riskieren **erhebliche finanzielle Verluste**. Die an Betrüger*innen überwiesenen Gelder sind in der Regel unwiederbringlich verloren, und die versprochenen Gewinne treten niemals ein.

Woran lassen sich diese Betrügereien erkennen?

Häufig werden **unrealistisch hohe Renditen** in kurzer Zeit und **ohne Risiko** versprochen. Gleichzeitig wird **Druck** ausgeübt, sofort zu investieren, um ein vermeintlich einmaliges oder zeitlich begrenztes Angebot nicht zu verpassen.

Zudem verlangen die Betrüger*innen **persönliche oder finanzielle Daten.** Auch das Fehlen von **klaren Unternehmensinformationen** oder **offiziellen Dokumenten** sind ein klares Warnsignal.

Wie kann ich mich schützen?

- Sei **skeptisch** bei **Angeboten**, die zu gut erscheinen, um wahr zu sein.
- Prüfe immer die **Seriosität** des Unternehmens oder der Person, die das Investment anbietet, anhand verlässlicher Quellen oder Bewertungen.
- Gib niemals deine persönlichen oder finanziellen Informationen preis, ohne die **Echtheit des Angebots** bestätigt zu haben.

Betrug auf Social Media

Worum handelt es sich dabei?

BETRÜGER*INNEN NUTZEN **SOZIALE NETZWERKE** WIE FACEBOOK, INSTAGRAM ODER LINKEDIN, UM **KONTAKT** AUFZUNEHMEN.

Sie geben sich häufig als Service-Mitarbeitende oder bekannte Personen aus und kontaktieren ihre Opfer über private Nachrichten.

Was sind die Folgen?

Über gefälschte Links oder Nachrichten gelangen Betrüger*innen an **Zugangsdaten** und können das **Konto missbräuchlich verwenden.**

Woran lassen sich diese Betrügereien erkennen?

Unbekannte Profile fragen nach **persönlichen oder finanziellen Daten** oder fordern zum Klicken auf Links auf.

Wie kann ich mich schützen?

- Gib keine **sensiblen Daten** über soziale Netzwerke weiter.
- Ignoriere **unbekannte Kontakte.**
- Melde verdächtige Nachrichten und nimm Kontakt mit deiner Bank auf.

Betrug im E-Commerce

Worum handelt es sich dabei?

BEIM E-COMMERCE-BETRUG BETREIBEN KRIMINELLE **GEFÄLSCHTE ONLINE-SHOPS** MIT **GÜNSTIGEN ANGEBOTEN**.

Beim Kauf werden Zahlungs- oder Kreditkartendaten abgefragt.

Was sind die Folgen?

Die Ware wird **nicht geliefert** oder die Zahlungsdaten werden für weitere **betrügerische Abbuchungen** verwendet.

Woran lassen sich diese Betrügereien erkennen?

Fehlendes Impressum, keine klare Firmenadresse, **nur Vorauszahlung** möglich oder **sehr auffällige Preisnachlässe.**

Wie kann ich mich schützen?

- Prüfe **Anbieter** und **Impressum**.
- Kaufe nur auf **bekannten und vertrauenswürdigen Webseiten** ein.
- Achte auf **„https“** in der Internetadresse. Das „s“ steht für „secure“.
- Prüfe **Bewertungen.**
- Sperre bei Betrug sofort deine Karte und informiere deine Bank.

So kannst du dich gegen Cyberangriffe schützen:

Die Sicherheit der eigenen Daten wird immer wichtiger.

Folgende Regeln helfen dir, dich gegen die verschiedenen Betrügereien zu schützen:

- Öffne E-Mails oder SMS nur, wenn du sicher bist, dass der **Absender echt** ist – kontrolliere hierbei die Schreibweise der Adresse.
- Rufe niemals in SMS angegebene **Telefonnummern** an, wenn du den Absender nicht kennst.
- Lade **keine Anhänge** aus verdächtigen E-Mails herunter, bevor du den Absender geprüft hast.
- **Klicke nicht auf Links** in verdächtigen E-Mails. Wenn du schon drauf geklickt hast, melde dich nicht auf der gefälschten Website an und schließe sofort den Browser.
- Benutze stets **starke, unterschiedliche Passwörter** für jeden Dienst.
- **Achtung:** Für das Login ins Raiffeisen Online Banking werden **niemals** Passwort, E-Mail-Adresse oder Telefonnummer abgefragt.
- Halte deine **Zugangsdaten** für dein Online Banking strikt geheim.
- Prüfe die **Auftragsdaten** sorgfältig, bevor du eine Freigabe bestätigst. Lehne verdächtige Push-Nachrichten ab!
- Achte besonders auf Aufträge mit Begriffen wie **‚Echtzeit'** oder **‚sofort überweisen'** und prüfe den Grund genau.

Was kann ich im Betrugsfall tun?

- Bewahre **Ruhe** und **kontaktiere** umgehend deine Bank.
- **Sperre sofort deine Debit- oder Kreditkarte** sowie deinen Zugang zum **Online Banking.**
- Melde **verdächtige Überweisungen** sofort.
- Ändere sofort alle **Zugangsdaten und Passwörter** bei sensiblen Diensten.
- **Sichere Screenshots und andere Beweise** wie E-Mails, SMS oder Telefonnummern zur späteren Nachverfolgung.
- Leite keine **verdächtigen E-Mails** weiter.
- Melde **Phishing-E-Mails** an deine Raiffeisenkasse oder per E-Mail an phishing@raiffeisen.it und lösche die verdächtige Nachricht anschließend sofort.
- Erstatte bei **Identitätsdiebstahl** eine Anzeige bei der Polizei.

- **Überprüfe regelmäßig deine Kontobewegungen.** Unbekannte Abbuchungen sollten sofort gemeldet werden.
- Verwende **kein öffentliches WLAN für Bankgeschäfte.** Offene Netzwerke sind leichter angreifbar.
- Sollte dein Smartphone, Tablet oder deine Bank- oder Kreditkarte **gestohlen werden oder verloren gehen,** sperre sofort den **Zugang** zum Online Banking sowie deine Karten und informiere deine Raiffeisenkasse.
- **Merke:** Öffentliche Behörden verlangen niemals, dass du dein Guthaben in Verdachtsmomenten auf ein sogenanntes **"sicheres Konto"** überweist. Solche Konten gibt es nicht – sie sind **frei erfunden** und Teil der Betrugsmasche, um dich zu einer Überweisung zu drängen.

Betrugsversuch: Erfahrungsbericht eines Raiffeisen-kunden

„Grüße aus San Lugano“

Ein Kunde einer Südtiroler Raiffeisenkasse, beruflich als Techniker tätig und mit umfangreichen EDV-Kenntnissen, erhielt eine SMS, die vermeintlich vom Zahlungsanbieter **Nexi** stammte - sogar mit einer offiziell wirkenden Telefonnummer.
In der Nachricht hieß es, eine Abbuchung von seiner Kreditkarte, lokalisiert in San Lugano, sei eingegangen. Falls er diese nicht autorisiert hatte, sollte er die angegebene Telefonnummer anrufen.

Der Kunde wählte die Nummer. Ein angeblicher Nexi-Mitarbeiter bot seine Hilfe an, die angeblich fälschliche Abbuchung auf seiner Kreditkarte zu verhindern. Um dies durchzuführen, gab er vor, **Benutzernamen und später auch das Passwort zu benötigen.**

Unter Druck – mit der Drohung, die Zahlung sonst sofort freizugeben – gab der Kunde zunächst Teile seines Benutzernamens preis. Als er jedoch zusätzlich zur Eingabe seiner Online Banking-Daten aufgefordert wurde, brach er das Gespräch ab, ignorierte weitere Anrufe und **sperrte umgehend seine Kreditkarte.**

Die Raiffeisenkasse bestätigte den Betrugsversuch und ergriff sofortige Sicherheitsmaßnahmen.

Hier findest du Warnungen zu aktuellen Betrugsfällen.


Klimaneutral
Stand: Mai 2026
Raiffeisen
Mehr Nähe. Mehr Bank.
www.raiffeisen.it/cybersecurity