Sicherheit? Einfacher, als man denkt.

Nehmen Sie Ihre Sicherheit selbst in die Hand! So haben Betrüger keine Chance.

Weil technische Sicherheitsbarrieren immer besser werden, konzentrieren sich Betrüger auf die „Schwachstelle Mensch“. Dabei setzen sie auf Gutgläubigkeit und psychologische Tricks, um so an Ihre sensiblen Daten zu kommen.

Doch ihre Maschen zu entlarven, ist zum Glück einfacher, als man denkt. Mit einer gesunden Skepsis und unseren Infos über typische Warnsignale, wirksame Verhaltensregeln und technische Maßnahmen können Sie Ihre Sicherheit selbst in die Hand nehmen.

Der wichtigste Tipp vorweg: Seriöse Institutionen wie die Sparkasse fragen Sie niemals nach vertraulichen Informationen wie PIN, TAN oder Passwort!

Sie müssen kein Experte sein, um Betrug zu erkennen und zu verhindern. Mit ein paar einfachen Tipps können Sie Ihre Sicherheit selbst in die Hand nehmen – ob online oder im Alltag.

Sparkasse

Der beste Schutz vor Betrug: Ruhe bewahren und die Tricks der Betrüger durchschauen.

Für Betrüger eine klassische PIN-win-Situation.

Phishing ist eine Betrugsmethode, bei der Kriminelle gefälschte E-Mails, SMS oder Websites verwenden, um an persönliche Informationen wie Passwörter oder Bankdaten zu gelangen. Sie geben sich als vertrauenswürdige Institutionen aus, um Menschen dazu zu bringen, auf Links zu klicken, Anhänge herunterzuladen oder vertrauliche Informationen preiszugeben.

So verhalten Sie sich richtig:

- → Prüfen Sie die Absenderadresse und die URL.
- → Achten Sie auf ungewöhnliche Aufforderungen und Rechtschreibfehler.
- → Öffnen Sie keine verdächtigen Links oder Anhänge.
- → Nutzen Sie technische Maßnahmen wie die Zwei-Faktor-Authentifizierung.

Ein typisches Beispiel für Phishing: Diese Nachricht erzeugt Druck und enthält einen Link, der zu einer gefälschten Website führt. Dort sollen potenzielle Opfer ihre persönlichen Daten eingeben. Mit unseren Tipps fallen Sie nicht darauf herein.

War Ihr Enkelkind schon immer so nett?

Beim **Social Engineering** wird das Vertrauen der potenziellen Opfer ausgenutzt, um sie geschickt zu manipulieren. Betrüger kommen so an ihr Geld bzw. an vertrauliche Informationen oder installieren Schadsoftware. Social Engineering kann online, per Telefon, WhatsApp, SMS oder sogar persönlich stattfinden.

So verhalten Sie sich richtig:

- → Seien Sie vorsichtig, wenn Mails von scheinbar vertrauenswürdigen Quellen kommen, und prüfen Sie die Absenderadresse.
- → Verifizieren Sie die Identität der Kontaktperson, besonders wenn sie behauptet, von einer Bank oder Behörde zu sein.
- → Lassen Sie sich nicht unter Druck setzen – nehmen Sie sich Zeit, die Situation zu prüfen.
- → Geben Sie niemals vertrauliche Daten preis, wenn Sie dazu in einer Mail aufgefordert werden.
- → Nutzen Sie technische Maßnahmen wie die Zwei-Faktor-Authentifizierung.

Schnäppchen gesucht, Betrüger gefunden.

Beim **Marktplatzbetrug** auf Kleinanzeigenplattformen täuschen Betrüger Käufer und Verkäufer gleichermaßen. Sie bieten Waren an, die nie versendet werden, oder behaupten als Käufer, gezahlt zu haben, ohne tatsächlich zu zahlen. Ziel der Betrüger ist es, Geld zu stehlen, sensible Daten zu erlangen oder die Ware ohne Bezahlung zu erhalten.

So verhalten Sie sich richtig:

- → Kommunizieren Sie nur über die Plattform.
- → Prüfen Sie Verkäuferprofile und Bewertungen.
- → Nutzen Sie Plattform-interne Zahlungsmethoden mit Käuferschutz.
- → Lassen Sie sich nicht unter Druck setzen.
- → Nutzen Sie technische Maßnahmen wie 3-D Secure für Online-Kartenzahlungen.

Fake Shop, echte Abzocke.

Fake Shops sind betrügerische Online-Shops, die darauf abzielen, Geld oder Zahlungsinformationen zu stehlen. Sie bieten Produkte zu extrem günstigen Preisen an, aber nach der Zahlung erhalten Kunden weder Ware noch ihr Geld zurück. Fake Shops sehen oft täuschend echt aus, doch mit der richtigen Vorsicht können Sie sie erkennen.

So verhalten Sie sich richtig:

- → Lassen Sie sich nicht von Lockangeboten aufs Glatteis führen.
- → Achten Sie auf Rechtschreibfehler oder unprofessionelles Design.
- → Checken Sie das Impressum – fehlt es oder ist es unvollständig?
- → Sehen Sie nach, ob es glaubwürdige Kundenbewertungen gibt.
- → Prüfen Sie die URL. Vorsicht, wenn die Verbindung nicht verschlüsselt ist.
- → Nutzen Sie technische Maßnahmen wie 3-D Secure für Online-Kartenzahlungen.

Gemeinsam gegen Betrug.

Nutzen Sie auch die technischen Sicherheitsmaßnahmen von Sparkasse, Mastercard und Visa:

- → Aktivieren Sie die Zwei-Faktor-Authentifizierung (2FA), um Ihr Konto noch besser abzusichern.
- → Verwenden Sie 3-D Secure für Online-Kartenzahlungen. Mit Mastercard Identity Check™ oder Visa Secure bestätigen Sie Ihre Zahlungen sicher über die S-ID-Check-App oder S-pushTAN.
- → Nutzen Sie den Chargeback-Service von Mastercard oder Visa, um unautorisierte Kartenzahlungen rückgängig zu machen.
- → Aktivieren Sie Sicherheitsbenachrichtigungen wie den Kontowecker und Kartenwecker der Sparkasse, um verdächtige Aktivitäten sofort zu erkennen.

Schnelle Hilfe

Wenn Sie vermuten, auf einen Betrug hereingefallen zu sein, bewahren Sie Ruhe und ergreifen Sie umgehend folgende Maßnahmen:

1. Ändern Sie Ihre Passwörter für alle Konten, insbesondere fürs Online-Banking, von einem anderen Gerät aus.
2. Informieren Sie sofort Ihre Sparkasse, um unbefugte Zugriffe zu verhindern.
3. Sperren Sie Ihre Konten und Karten, wenn Sie Daten preisgegeben haben. Ihre Sparkasse hilft bei neuen Zugangsdaten und Karten.
4. Erstatten Sie Anzeige bei der Polizei, besonders bei Identitätsdiebstahl oder finanziellem Schaden.
5. Kontaktieren Sie die Verbraucherzentrale für Unterstützung.
6. Überprüfen Sie Ihr Gerät auf Schadsoftware und führen Sie einen umfassenden Sicherheitscheck durch.

Verdacht auf Betrug oder einen Betrugsversuch? Zögern Sie nicht, uns sofort zu kontaktieren:

- → E-Mail: **warnung@sparkasse.de**
- → 24-Stunden-Sperr-Notruf: 116 116

Nehmen Sie Ihre Sicherheit selbst in die Hand.

Weitere ausführliche Informationen, wie Sie einfach und effektiv gegen Betrug vorgehen, finden Sie auf **sparkasse-karlsruhe.de/sicherheit**

Sensibilisieren Sie auch andere für das Thema, beispielsweise indem Sie diesen Flyer teilen.

Mit Ihrer Sparkasse einfach und effektiv gegen Betrug vorgehen.

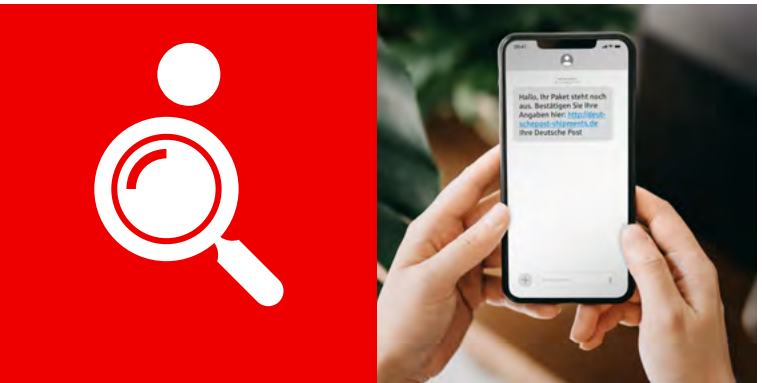
Quiz: Wie gut durchschauen Sie Betrugsmaschen?

In diesem Quiz geht es um typische Betrugsmaschen. Bei jeder Frage sind zwei Antworten richtig und eine ist komplett falsch. Finden Sie die richtigen Antworten und notieren Sie die Buchstaben – am Ende bilden sie ein Lösungswort.

Frage 1: Sie erhalten die abgebildete SMS-Nachricht. Was tun Sie?

> Hallo, Ihr Paket steht noch aus. Bestätigen Sie Ihre Angaben hier: http://deutschepost-shipments.de
> Ihre Deutsche Post

1. Ich wüsste zwar nicht, was ich bestellt habe, aber neugierig, wie ich bin, klicke ich gleich mal auf den Link. **(N)**
2. Netter Versuch, aber ich antworte grundsätzlich nicht auf SMS von unbekannten Absendern und lösche die Nachricht. **(S)**
3. Das könnte meine neue Mini-Wassermelonen-Schneidemaschine sein. Sicherheitshalber nutze ich aber nur die Sendungsverfolgung auf der offiziellen Website meines Paketdienstes. **(I)**



Frage 2: Wie reagieren Sie auf eine WhatsApp-Nachricht mit folgendem Inhalt?
»Hallo Opa, ich stecke in der Klemme und brauche dringend Geld. Ein Freund holt es gleich bei dir ab, okay?«

1. Hat mein Enkel etwa eine neue Handynummer? Das hätte er mir doch gesagt. Ich rufe ihn gleich mal über die Nummer an, die ich kenne, und frage, was da los ist. **(C)**
2. Das klingt so gar nicht nach meinem Enkel. Garantiert ein Trick! Ich mache die Tür nicht auf, höchstens für die Polizei, die ich jetzt umgehend informiere. **(H)**
3. Ach je, der Ärmste! Ich will doch nicht, dass er in Schwierigkeiten gerät. Ein paar Hundert Euro müsste ich noch im Haus haben. **(G)**

Frage 3: Wie reagieren Sie auf folgenden Anruf?
»Hallo, hier ist Ihre Sparkasse. Ihr Konto wurde gesperrt. Sie müssen dringend Ihre Zugangsdaten angeben, um es zu entsperren.«

1. O je, das wäre echt übel, da muss ich wohl sofort handeln. Aber so etwas erledige ich nicht am Telefon. Ich fahre gleich mal bei meiner Sparkasse vorbei. **(E)**
2. Ach du liebe Zeit, wie lautet noch gleich meine Online-Banking-PIN? Die muss ich direkt raussuchen … **(L)**
3. Darauf falle ich doch nicht rein! Natürlich nenne ich keine sensiblen Daten, sondern lege sofort auf. **(R)**

Auflösung:
Haben Sie die zwei richtigen Antworten pro Frage gefunden? Notieren Sie deren Buchstaben. Die sechs Buchstaben der korrekten Antworten ergeben das Lösungswort:

☐ ☐ ☐ ☐ ☐ ☐

Lösungswort: SICHER