

Falsche Sicherheitswarnung

Wenn angeblicher Microsoft- oder IT-Support aus einer Warnmeldung einen Notfall macht.

WAS IST PASSIERT?

- Auf dem Computer erscheint plötzlich eine beunruhigende Sicherheitswarnung - oft mit Telefonnummer.
- Angeblicher Microsoft-, IT- oder Sicherheits-Support erzeugt Angst und Zeitdruck.
- Sie sollen anrufen, Fernzugriff erlauben oder sogar Online-Banking öffnen und eine Zahlung bestätigen.

SO LÄUFT DIE MASCHKE AB



1 KONTAKT

Warnmeldung erscheint.
Sie sollen die dort angezeigte Telefonnummer anrufen.



2 TÄUSCHUNG

Angebliche Experten helfen.
Die Täter geben sich als Support aus und erzeugen Angst und Zeitdruck.



3 HANDLUNG

Sie sollen Anweisungen folgen.
Fernzugriff, Online-Banking oder eine Zahlungsfreigabe werden verlangt.



4 SCHADEN

Echte Zahlung möglich.
Die Täuschung kann zu Zahlungen oder zum Verlust sensibler Daten führen.

HIER SOLLTEN SIE MISSTRAUISCH WERDEN

- ⚠ Eine Warnmeldung fordert Sie zum Anruf auf.
- ⚠ Angeblicher Support setzt Sie unter starken Zeitdruck.
- ⚠ Fernzugriff auf Ihren Computer wird verlangt.
- ⚠ Banking, Zahlung oder Freigabe wird als Sicherheitsmaßnahme dargestellt.

SO SCHÜTZEN SIE SICH

- ✓ Rufen Sie keine Nummer aus einer unerwarteten Warnmeldung an.
- ✓ Gewähren Sie unbekannten Personen keinen Fernzugriff.
- ✓ Öffnen Sie auf Anweisung kein Online-Banking.
- ✓ Bestätigen Sie keine Zahlung, um angeblich einen Angriff oder Schaden zu stoppen.

MERKEN SIE SICH:



Eine Zahlung oder Freigabe stoppt keinen angeblichen Angriff. Prüfen Sie immer, was Sie tatsächlich bestätigen.

WENN ES PASSIERT IST: SCHNELL HANDELN

- 1 Gespräch und Fernzugriff sofort beenden.**
- 2 Sparkasse bzw. Bank unverzüglich informieren.**
- 3 Zugänge/Karten ggf. sperren und Computer prüfen lassen.**
- 4 Beweise sichern und Polizei informieren.**



Kleinanzeigen- Betrug

Wenn aus einem Verkauf eine gefälschte Zahlungs- oder Versandabwicklung wird.

WAS IST PASSIERT?

- Ein angeblicher Käufer meldet sich zu Ihrem Inserat.
- Das Gespräch wechselt oft unbemerkt auf Messenger, E-Mail oder SMS.
- Ein Link führt zu einer falschen Zahlungs- oder Versandseite. Dort sollen Sie Daten eingeben oder etwas freigeben.



SO LÄUFT DIE MASCHKE AB



1 KONTAKT

Käufer zeigt Interesse.
Die Anfrage wirkt zunächst normal.



2 VERLAGERUNG

Chat wechselt den Kanal.
Messenger, E-Mail oder SMS wirken wie eine Fortsetzung des Verkaufs.



3 TÄUSCHUNG

Link zur „Zahlung“.
Eine professionell wirkende Seite verlangt Karten-, Banking- oder Zugangsdaten.



4 SCHADEN

Daten oder Freigabe.
Daten oder eine Freigabe werden für echte Zahlungen missbraucht.

HIER SOLLTEN SIE MISSTRAUISCH WERDEN

- ❌ Der Chat wechselt auf Messenger, E-Mail oder SMS.
- ❌ Sie erhalten einen Zahlungslink oder QR-Code.
- ❌ Zum Geldempfang werden Karten- oder Zugangsdaten verlangt.
- ❌ Eine Freigabe passt nicht zu Ihrem Verkauf.

SO SCHÜTZEN SIE SICH

- ✅ Bleiben Sie möglichst in der Plattform.
- ✅ Öffnen Sie keine Zahlungslinks aus Nachrichten.
- ✅ Geben Sie keine Kartendaten ein, um Geld zu erhalten.
- ✅ Prüfen Sie Freigaben gegen den von Ihnen gestarteten Vorgang.

MERKEN SIE SICH:



Um Geld für einen Verkauf zu erhalten, müssen Sie keine Kartenzahlung oder unbekannte Freigabe bestätigen.

WENN ES PASSIERT IST: SCHNELL HANDELN

1 Kontakt sofort beenden.

2 Sparkasse bzw. Bank informieren.

3 Zugänge/Kartensperren und Beweise sichern.

4 Polizei informieren bzw. Anzeige erstatten.

Schockanruf

Wenn Betrüger am Telefon Angst machen - und Geld oder Wertsachen fordern.

WAS IST PASSIERT?

- Sie erhalten einen überraschenden Anruf über einen angeblichen Notfall eines Angehörigen.
- Die Täter geben sich z. B. als Polizei, Staatsanwaltschaft oder Arzt aus und erzeugen starken Druck.
- Sie sollen sofort Geld oder Wertsachen übergeben und möglichst mit niemandem darüber sprechen.

SO LÄUFT DIE MASCHKE AB



1 ANRUF

Ein Notfall wird behauptet.

Eine unterdrückte oder unbekannte Nummer ist möglich - entscheidend ist die dramatische Geschichte.



2 SCHOCK & DRUCK

Angst verhindert ruhiges Prüfen.

Die Täter fordern sofortiges Handeln und oft Geheimhaltung.



3 FORDERUNG

Geld oder Wertsachen.

Bargeld, Schmuck oder andere Werte sollen bereitgestellt werden.



4 ÜBERGABE

Ein „Abholer“ erscheint.

Die Täter organisieren die Übergabe und halten den telefonischen Druck aufrecht.

HIER SOLLTEN SIE MISSTRAUISCH WERDEN

- ⚠ Ein angeblicher Notfall verlangt sofort Geld.
- ⚠ Polizei oder andere Amtspersonen fordern Wertsachen.
- ⚠ Sie sollen mit Angehörigen nicht sprechen.
- ⚠ Ein unbekannter „Abholer“ soll Geld oder Schmuck übernehmen.

SO SCHÜTZEN SIE SICH

- ✓ Legen Sie auf und beenden Sie den Druck.
- ✓ Rufen Sie Angehörige selbst unter einer bekannten Nummer an.
- ✓ Sprechen Sie mit einer Vertrauensperson.
- ✓ Übergeben Sie kein Geld oder Wertsachen an Unbekannte.

MERKEN SIE SICH:



Polizei, Staatsanwaltschaft und Ärzte fordern am Telefon keine Übergabe von Bargeld oder Wertsachen.

WENN ES PASSIERT IST: SCHNELL HANDELN

1 Übergabe sofort stoppen.

2 Polizei unter 110 informieren.

3 Bei bereits erfolgter Zahlung auch Bank/Sparkasse informieren.

4 Beweise sichern und Angehörige einbeziehen.

Anlagebetrug im Internet

Wenn hohe Renditen versprochen werden - aber Ihr Geld am Ende weg ist.

WAS IST PASSIERT?

- Werbung, soziale Medien oder Messenger führen zu einer vermeintlichen Anlageplattform.
- Ein persönlicher „Berater“ baut Vertrauen auf; erste kleine Einzahlungen scheinen Gewinne zu erzielen.
- Für eine Auszahlung werden weitere Zahlungen verlangt - etwa für Steuern, Gebühren oder Versicherungen.

SO LÄUFT DIE MASCHKE AB



1 KONTAKT

Werbung oder Nachricht.
Sie werden auf eine professionell wirkende Trading- oder Anlageplattform gelockt.



2 VERTRAUEN

Persönliche Betreuung.
Ein angeblicher Berater begleitet Sie und zeigt vermeintliche Gewinne.



3 EINZAHLUNGEN

Erst klein, dann mehr.
Nach der ersten Zahlung folgen immer neue Forderungen und höhere Beträge.



4 KEINE AUSZAHLUNG

Geld wird zurückgehalten.
Für die Auszahlung werden weitere Gebühren verlangt oder der Kontakt bricht ab.



HIER SOLLTEN SIE MISSTRAUISCH WERDEN

- ⚠ Unrealistisch hohe oder „sichere“ Renditen.
- ⚠ Starker Druck, schnell zu investieren.
- ⚠ Kontakt fast ausschließlich online oder per Messenger.
- ⚠ Für eine Auszahlung sollen Sie nochmals Geld zahlen.

SO SCHÜTZEN SIE SICH

- ✓ Prüfen Sie Anbieter und Plattform vor jeder Zahlung.
- ✓ Lassen Sie sich nicht unter Zeitdruck setzen.
- ✓ Überweisen Sie kein weiteres Geld, um eine Auszahlung zu erhalten.
- ✓ Fragen Sie im Zweifel Ihre Sparkasse oder eine Verbraucherberatung.

MERKEN SIE SICH:



Wenn Sie erst weiteres Geld zahlen sollen, um an Ihr angebliches Guthaben zu kommen, ist das ein starkes Warnsignal.

WENN ES PASSIERT IST: SCHNELL HANDELN

1 Keine weiteren Zahlungen leisten.

2 Bank/Sparkasse informieren und Möglichkeiten prüfen.

3 Polizei informieren und Anzeige erstatten.

4 Chats, Belege und Plattformdaten sichern.



Falscher Bankmitarbeiter

Wenn sich Betrüger als Mitarbeiter Ihrer Bank ausgeben, um an Daten oder Geld zu gelangen.

WAS IST PASSIERT?

- Sie erhalten einen Anruf, eine E-Mail oder Nachricht von einem angeblichen Bankmitarbeiter.
- Ein Problem mit Ihrem Konto oder eine verdächtige Zahlung wird behauptet. Das erzeugt Zeitdruck.
- Sie sollen Daten nennen, eine Freigabe bestätigen, eine Überweisung oder Kartenzahlung stornieren.

SO LÄUFT DIE MASCHKE AB



1 KONTAKT

Angebliche Bank meldet sich.

Auch eine bekannte Bankrufnummer kann im Display vorgetäuscht werden.



2 VORWAND

Ein Sicherheitsproblem.

Eine angebliche Buchung oder Sperre soll sofort geklärt werden.



3 DATEN / FREIGABE

Sie sollen handeln.

PIN, TAN, Passwörter, Kartendaten oder eine Freigabe werden verlangt.



4 SCHADEN

Echte Vorgänge folgen.

Mit Daten oder Freigaben können Zahlungen ausgelöst, Karten digitalisiert oder Konten missbraucht werden.



Ihre Bank erkennt man daran:

- ✓ Wir fordern niemals PIN, TAN oder Passwörter.
- ✓ Wir fragen niemals nach Ihrer pushTAN oder Freigabecodes.
- ✓ Wir fordern niemals Überweisungen oder Bargeldübergaben.
- ✓ Im Zweifel kontaktieren Sie uns über die offiziellen Kanäle Ihrer Bank.



Täter geben sich als Bankmitarbeiter aus.
Telefonisch, per E-Mail, SMS oder Messenger.

Druck zur schnellen Entscheidung.
„Wir müssen das jetzt sofort klären.“

Abfrage sensibler Daten.
PIN, TAN, Passwörter, Karten- oder Kontodaten.

Ziel: Zugriff auf Ihr Konto oder unberechtigte Zahlungen.
Überweisungen, Freigaben oder Bargeldübergaben.

HIER SOLLTEN SIE MISSTRAUISCH WERDEN

- ⚠ Unerwarteter Bankkontakt mit starkem Zeitdruck.
- ⚠ PIN, TAN, Passwort oder Kartendaten werden verlangt.
- ⚠ Sie sollen eine Freigabe am Telefon bestätigen.
- ⚠ Überweisung oder Bargeldübergabe wird als „Sicherheitsmaßnahme“ verlangt.

SO SCHÜTZEN SIE SICH

- ✓ Beenden Sie den Kontakt bei ungewöhnlichen Forderungen.
- ✓ Verlassen Sie sich nicht auf die angezeigte Rufnummer.
- ✓ Rufen Sie Ihre Bank selbst über einen bekannten Kontaktweg an.
- ✓ Prüfen Sie jede Freigabe: Betrag, Empfänger/Händler und Vorgang.

MERKEN SIE SICH:



Eine TAN oder Freigabe bestätigt einen konkreten Vorgang - sie stoppt keine verdächtige Zahlung.

WENN ES PASSIERT IST: SCHNELL HANDELN

1 Verbindung sofort beenden.

2 Bank/Sparkasse selbst kontaktieren.

3 Zugänge/Karten ggf. sperren und Konto prüfen.

4 Polizei informieren und Beweise sichern.



Gemeinsam gegen Betrug - für mehr Sicherheit.

Danke für Ihre Aufmerksamkeit und Ihr Interesse!

Informieren. • Austauschen. • Wachsam handeln.

PRÄVENTIONSSONGS

Reinhören. Informieren. Schützen.

Die Songs greifen typische Betrugsmaschen auf -
verständlich, einprägsam und mit wichtigen Tipps.

- ✓ Betrugsmaschen verständlich erklärt
- ✓ Warnsignale leichter wiedererkennen
- ✓ Schutzregeln einprägsam zusammengefasst

Hinweis: Playlist wird von André Thronicker zur Verfügung gestellt.

ZUR PLAYLIST



QR-Code scannen

IHR KONTAKT ZU UNS

SPARKASSE OBERLAUSITZ-NIEDERSCHLESIE DIREKTBANKING

Adresse: Frauenstraße 21 · 02763 Zittau

Telefon: 03583 603-0

E-Mail: info@spk-on.de

Internet: spk-on.de

Bei Fragen zur Sicherheit im Online-Banking und zu
unseren Präventionsangeboten sprechen Sie uns gern an.

WICHTIGE KONTAKTE UND HILFE

Verdächtige E-Mails

warnung@sparkasse.de

Zur Prüfung weiterleiten.

Sperr-Notruf

116 116

Karten und Online-Banking sperren.

Bei akuter Gefahr oder Betrug

Polizei: 110

Im Notfall sofort anrufen.

Aktuelle Sicherheitshinweise

spk-on.de/sicherheit

Warnmeldungen Ihrer Sparkasse.

DAS WICHTIGSTE

MISSTRAUISCH BLEIBEN

Zeitdruck und ungewöhnliche
Forderungen sind Warnsignale.

SELBST ZURÜCKRUFEN

Kontakt abbrechen und einen
bekannten Kontaktweg nutzen.

FREIGABEN PRÜFEN

Betrug, Empfänger oder Händler und Währung
kontrollieren.