Sicher im digitalen Alltag – Schutz vor Betrug und Abzocke

Digitale Betrugsmaschen

- Phishing (E-Mail)
- Smishing (SMS)
- Quishing (QR-Codes)
- Online-Shopping-Betrug
- Technischer Support-Betrug

Klassische Betrugsmaschen

- Telefonbetrug (Enkeltrick, falsche Polizei)
- Haustürbetrug (falsche Handwerker, Vertragsfallen)
- Gewinnversprechen

Weitere digitale Fallstricke

- Fake-Updates und gefälschte Sicherheitswarnungen
- Versteckte Abos in Apps oder Webseiten
- Fake-Support über Fernwartung
- Verwirrende Webseiten und gefälschte Login-Seiten

Phishing (E-Mail-Betrug)

- **Was ist das?**

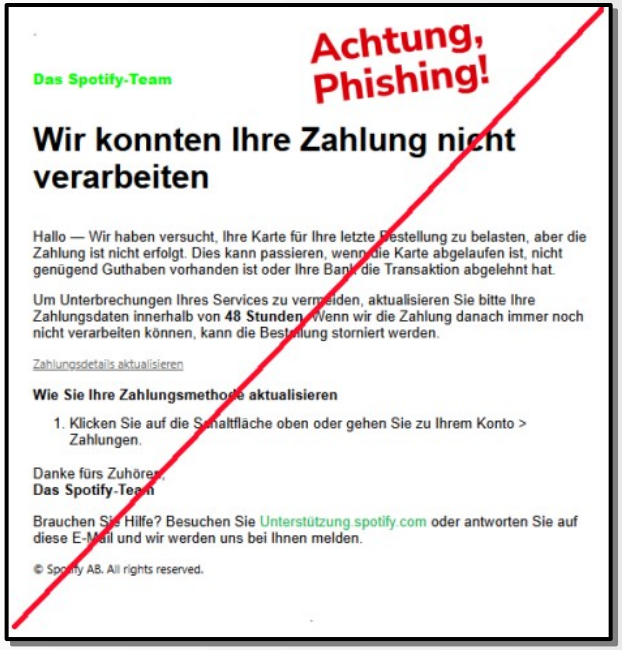
  Betrüger versenden täuschend echte E-Mails im Namen von Banken, Behörden oder bekannten Firmen (z. B. Telekom, Amazon), um an Passwörter oder Kontodaten zu gelangen.

- **Wie erkennt man das?**
  - Ungewöhnliche Absenderadresse (z. B. „support@amaz**0**n.de“)
  - Dringender Handlungsbedarf („Ihr Konto wird gesperrt!“)
  - Rechtschreibfehler oder unpersönliche Anrede („Sehr geehrter Kunde“)

- **Wie schützt man sich?**
  - Niemals auf Links in verdächtigen E-Mails klicken
  - Keine persönlichen Daten per E-Mail weitergeben
  - Im Zweifel direkt bei der Firma anrufen

Phishing (E-Mail-Betrug)

Beispiele von der Verbraucherzentrale:



https://www.verbraucherzentrale-rlp.de/wissen/digitale-welt/phishingradar/phishingradar-aktuelle-warnungen-6059

Smishing (SMS-Phishing)

- **Was ist das?**
  Ähnlich wie Phishing, aber per SMS. Oft mit Paketbenachrichtigungen oder Bankwarnungen.
- **Wie erkennt man das?**
  - Unbekannte Nummern
  - Links zu fremden Webseiten
  - Aufforderung zur Eingabe von Daten
- **Wie schützt man sich?**
  - Keine Links in SMS anklicken
  - Nummer blockieren
  - Offizielle App der Post oder Bank nutzen

Smishing (SMS-Phishing)

Beispiele:

- "Sie haben eine neue Mitteilung von Ihrem Dienstanbieter erhalten"
- "Sie haben einen verpassten Anruf. Der Anrufer hat Ihnen eine Nachricht hinterlassen"
- "Verpasster Anruf. Die aufgezeichnete Nachricht ist verfuegbar unter"
- "Am 08.02. um 20:10 Uhr wurde eine Voicemail-Nachricht fur Sie hinterlassen. Bitte besuchen Sie"
- "Neue Nachricht des Mobilfunkbetreibers"
- "Sie . - haben zwei neue . Sprachnachrichten erhalten"
- "Ich mochte dir eine Sprachnachricht uber HeyTell . senden. Link: {yi2}"
- "Free Msg: <h> Neue Nachricht! Klicekn Sie auf den Link, um sie zu lesen:"
- "Sie . haben eine MMS-Nachricht_ erhalten. Lesen Sie . hier:"
- "Sie haben eine MMS-Nachricht - erhalten. Lesen (p2a) Sie hier: "
- "Uberprufen Sie Ihre Voicemail - Sie haben eine neue Nachrich t"
- "<Betreff: Voicemail> Sie haben zwei neue Sprachnachrichten erhalten: [Link] jn"

Quishing (QR-Code-Betrug)

- **Was ist das?**
  Gefälschte QR-Codes, z. B. auf Parkautomaten oder Flyern, führen auf betrügerische Webseiten.
- **Wie erkennt man das?**
  - QR-Code überklebt ein Original
  - QR-Code an ungewöhnlichen Orten (z. B. Laternenpfahl)
- **Wie schützt man sich?**
  - QR-Codes nur von vertrauenswürdigen Quellen scannen
  - Vorschau-Link prüfen, bevor man ihn öffnet
  - QR-Scanner mit Sicherheitsfunktion verwenden

Quishing (QR-Code-Betrug)

Beispiele

Wo tauchen falsche QR-Codes auf?

- QR-Codes in Phishing-Mails
- Briefe von angeblichen Banken
- QR-Codes an Ladesäulen für E-Autos
- QR-Codes auf Parkscheinautomaten
- Strafzettel für Falschparker
- Plakate in Bussen und Bahnen
- im öffentlichen Raum, z.B. auf Laternenpfählen

https://www.verbraucherzentrale-rlp.de/wissen/digitale-welt/phishingradar/quishing-falsche-qrcodes-in-mails-briefen-oepnv-und-strassenverkehr-98612

Online-Shopping-Betrug

- **Was ist das?**
  Gefälschte Online-Shops locken mit günstigen Preisen, liefern aber nie die Ware.
- **Wie erkennt man das?**
  - Kein Impressum oder nur E-Mail-Adresse
  - Nur Vorkasse möglich
  - Schlechte Bewertungen oder keine Rückgabemöglichkeit
- **Wie schützt man sich?**
  - Nur bei bekannten Shops kaufen
  - Auf Gütesiegel wie „Trusted Shops“ achten
  - Mit PayPal oder Kreditkarte zahlen (Rückbuchung möglich)

Technischer Support-Betrug

- **Was ist das?**

  Betrüger geben sich am Telefon oder per Pop-up als Microsoft- oder Telekom-Mitarbeiter aus.

- **Wie erkennt man das?**
  - Anrufe oder Warnmeldungen am Bildschirm
  - Aufforderung, Fernzugriffssoftware zu installieren

- **Wie schützt man sich?**
  - Niemals Fremden Zugriff auf den PC geben
  - Sofort auflegen oder Browser schließen
  - Polizei oder Verbraucherzentrale informieren

Telefonbetrug: Die häufigsten Maschen

Falsche Polizisten

- **Was passiert?**
  Betrüger geben sich als Polizei aus und behaupten, das Geld auf dem Konto sei in Gefahr.
- **Wie erkennt man das?**
  - Dringlichkeit, angebliche Geheimhaltung
  - Aufforderung zur Geldübergabe oder Überweisung.
- **Wie schützt man sich?**
  - Niemals persönliche Daten oder Kontoinformationen am Telefon preisgeben.
  - Polizei ruft niemals mit solchen Forderungen an.
  - Auflegen und Polizei mit allg. Rufnummer aus Telefonbuch anrufen und rückfragen

Telefonbetrug: Die häufigsten Maschen

Schockanruf / Enkeltrick

- **Was passiert?**
  Ein angeblicher Verwandter oder Anwalt meldet sich und behauptet, ein Angehöriger sei in Not (Unfall, Gefängnis).
- **Wie erkennt man das?**
  - Emotionale Drucksituation, Geldforderung für Kaution oder Hilfe
- **Wie schützt man sich?**
  - Sofort auflegen!
  - Lassen Sie sich nicht unter Druck setzen.
  - Rückruf bei echten Angehörigen, niemals Geld übergeben oder überweisen.
  - Achtung: mit KI können Stimmern von echten Personen erzeugt werden.

Telefonbetrug: Die häufigsten Maschen

Gewinnversprechen

- **Was passiert?**
  Man habe angeblich einen hohen Geldbetrag gewonnen – aber müsse vorher Gebühren zahlen.
- **Wie erkennt man das?**
  - Vorkasse für „Bearbeitung“, keine echte Gewinnspielteilnahme
- **Wie schützt man sich?**
  - Sofort auflegen!
  - Keine Zahlungen leisten, bei der Verbraucherzentrale nachfragen
  - Werden Sie skeptisch, wenn Sie an keinem Gewinnspiel teilgenommen haben.

Telefonbetrug: Die häufigsten Maschen

Anrufe aus dem Ausland

- Seien Sie skeptisch bei Anrufen aus dem Ausland!
- **Wie erkennt man das?**
  - alle Nummern, die mit **00** oder **+** beginnen und danach **nicht 49** erscheint.
    z.B.: +44… 0044… steht für Groß Britanien
    +48... 0048… steht für Polen
- **Wie schützt man sich?**
  - Anruf nicht annehmen!
  - Sofort auflegen!
  - Auslandsgespräche sperren lassen
  - ruft jemand mit einen Deutschen Handy aus dem Ausland an, erscheint im Display +49 oder 0049

Telefonbetrug: Die häufigsten Maschen

Präventationsmaßnahmen

- **Es ist nicht unhöflich einfach aufzulegen!**
- Lassen Sie Ihren Eintrag im Telefonbuch löschen.
- Wenn, dann lassen Sie nur den Nachnamen ins Telefonbuch eintragen, kein Beruf oder sonstige Informationen etc..
- Melden Sie sich bei unbekannten Nummern nicht mit Ihrem Namen. Sagen Sie nur: „Hallo, wer spricht dort.“ Oder warten Sie, bis sich der Gesprächspartner meldet.
- Raten Sie nicht, wer anruft, sondern fordern Sie Anrufer grundsätzlich dazu auf, ihren Namen selbst zu nennen

wo gibt es weitere Infos und Tipps?

weitere Informationen und Tipps zu Bertugsmaschen gibt es hier:

- Bei der Polizei
  https://www.polizei-beratung.de/themen-und-tipps/betrug/
- Pflegehilfe-Ratgeber für Senioren
  https://www.pflegehilfe-senioren.de/pflegeratgeber/leben-im-alter/tipps/betrugspraevention-fuer-senioren/
- Präventionsmedien für Senioren (PDF)
  https://lsr-bw.de/wp-content/uploads/2025/01/20241104_Uebersicht-Praeventionsmedien-Senioren.pdf
- Bundesamt für Sicherheit in der Informationstechnik (BSI)
  https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/verbraucherinnen-und-verbraucher_node.html
- Verbraucherzentrale Rheinland-Pfalz
  https://www.verbraucherzentrale-rlp.de/sicher-im-internet-handy-tablet-und-pc-schuetzen-69691

Opfer geworden, was nun?

SOS Was tun, wenn man Opfer geworden ist?

Wenn du auf eine Betrugsmasche hereingefallen bist, solltest du schnell handeln:

1. Ruhe bewahren und Beweise sichern
   - E-Mails, SMS, Chatverläufe, Screenshots speichern
2. Anzeige bei der Polizei erstatten
   - Persönlich oder online über die Internetwache deiner Landespolizei
3. Verbraucherzentrale kontaktieren
   - Hilfe bei Vertragskündigung, Rückforderungen und rechtlicher Einschätzung
     https://www.verbraucherzentrale-rlp.de/
5. Rechtsberatung einholen
   - Bei größeren Schäden oder Unsicherheiten empfiehlt sich ein Fachanwalt für IT- oder Strafrecht
6. Bundesministerium für Justiz – Hilfeportal
   - Merkblatt mit konkreten Schritten nach Betrug oder Diebstahl
     https://www.hilfe-info.de/Webs/hilfeinfo/DE/Merkblaetter/19-merkblatt_diebstahlundbetrug.html

Vielen Dank
für
Ihre Aufmerksamkeit