



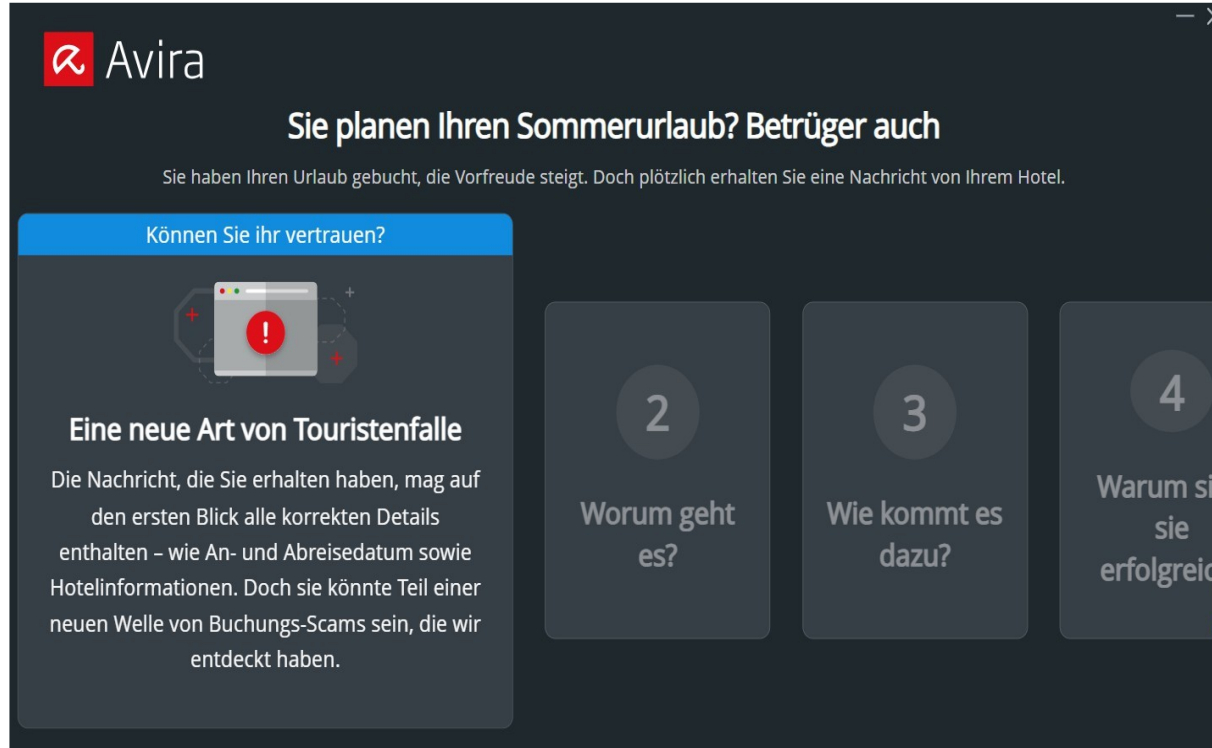
Cyberkriminalität (Cybercrime)



1. Beispiel von AVIRA (Urlaubsbuchung)
2. Schutzmechanismen



1.



The image shows a screenshot of an Avira security alert. At the top left is the Avira logo. The main heading reads 'Sie planen Ihren Sommerurlaub? Betrüger auch'. Below this is a sub-heading 'Können Sie ihr vertrauen?' and a warning icon of a computer window with a red exclamation mark. The main text describes a new type of tourist scam. To the right, there are three numbered steps: 2 'Worum geht es?', 3 'Wie kommt es dazu?', and 4 'Warum sind sie erfolgreich?'.

Avira

Sie planen Ihren Sommerurlaub? Betrüger auch

Sie haben Ihren Urlaub gebucht, die Vorfreude steigt. Doch plötzlich erhalten Sie eine Nachricht von Ihrem Hotel.

Können Sie ihr vertrauen?

Eine neue Art von Touristenfalle

Die Nachricht, die Sie erhalten haben, mag auf den ersten Blick alle korrekten Details enthalten – wie An- und Abreisedatum sowie Hotelinformationen. Doch sie könnte Teil einer neuen Welle von Buchungs-Scams sein, die wir entdeckt haben.


2
Worum geht es?

3
Wie kommt es dazu?

4
Warum sind sie erfolgreich?

Quelle:  Avira





Sie planen Ihren Sommerurlaub? Betrüger auch

Sie haben Ihren Urlaub gebucht, die Vorfreude steigt. Doch plötzlich erhalten Sie eine Nachricht von Ihrem Hotel.

Worum geht es?

1 Können Sie ihr vertrauen?

Gekaperte Reservierung

Bei diesem Betrug werden echte Reservierungsdaten verwendet, um den Eindruck zu erwecken, dass die Nachrichten echt sind. Dadurch sollen Sie zur Weitergabe Ihrer Zahlungsdaten und persönlichen Informationen verleitet werden.

3 Wie kommt es dazu?

4 Warum sind sie erfolgreich?

○ ● ○ ○ ○ ○

Quelle:  Avira



Sie planen Ihren Sommerurlaub? Betrüger auch

Sie haben Ihren Urlaub gebucht, die Vorfreude steigt. Doch plötzlich erhalten Sie eine Nachricht von Ihrem Hotel.

Wie kommt es dazu?



Ihre Daten wurden gehackt

Betrüger stehlen Ihre Buchungsdaten durch Phishing-E-Mails, schwache oder mehrmals verwendete Passwörter oder indem sie die Systeme von Hotels und Reisepartnern angreifen.

2

Worum geht es?

4

Warum sind sie erfolgreich?



Quelle:  Avira





Sie planen Ihren Sommerurlaub? Betrüger auch

Sie haben Ihren Urlaub gebucht, die Vorfreude steigt. Doch plötzlich erhalten Sie eine Nachricht von Ihrem Hotel.

Warum sind sie erfolgreich?



3

Wie kommt es dazu?

Täuschend echte Nachrichten

In Gedanken sind Sie schon bei Ihrer Reise. Eine Nachricht zu Ihrer Buchung erscheint da völlig normal. Wenn sie dann auch noch dringlich klingt, handelt man leicht unüberlegt, ohne genauer hinzusehen.

5

Wie sieht ein Beispiel aus?



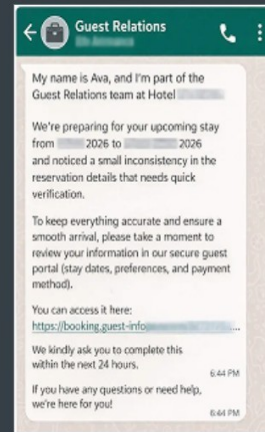
Quelle:  Avira



Sie planen Ihren Sommerurlaub? Betrüger auch

Sie haben Ihren Urlaub gebucht, die Vorfreude steigt. Doch plötzlich erhalten Sie eine Nachricht von Ihrem Hotel.

Wie sieht ein Beispiel aus?



✓ SMS, E-Mail oder Sofortnachricht

✓ Reservierungsdetails stimmen exakt mit Ihrer Buchung überein

✓ Angebliches Problem

✓ Phishing-Link zu einer Zahlungsseite

✓ Dringender Ton, um Sie unter Druck zu setzen

4

Warum sind sie erfolgreich?

6

Wie können Sie geschützt bleiben?

Alle Beispiele aus dem Internet, keine von uns erfundenen Fälle. Alle dargestellten Logos oder Marken sind eingetragene Marken ihrer jeweiligen Unternehmen.

Quelle:





Sie planen Ihren Sommerurlaub? Betrüger auch

Sie haben Ihren Urlaub gebucht, die Vorfreude steigt. Doch plötzlich erhalten Sie eine Nachricht von Ihrem Hotel.

3

Wie kommt es dazu?

4

Warum sind sie erfolgreich?

5

Wie sieht ein Beispiel aus?

Wie können Sie geschützt bleiben?



Genießen Sie Ihre Reise ohne Betrüger

- ✓ Seien Sie vorsichtig bei unerwarteten Nachrichten
- ✓ Klicken Sie niemals auf Zahlungslinks in Nachrichten
- ✓ Kontaktieren Sie das Hotel direkt per Telefon oder E-Mail

[Zurück zum Dashboard](#)

Quelle:  Avira



2.

Online-Schutz: Diese vier Fehler machen Millionen Deutsche



Die Diskrepanz zwischen Wissen und Handeln im Bereich Cybersicherheit ist ein großes Problem. Nicht nur in Deutschland, sondern weltweit.

Warum handeln so viele Menschen nicht, obwohl sie die Risiken kennen?

Das BSI-Digitalbarometer 2026 (oder die aktuellste verfügbare Studie) zeigt ähnliche Muster wie in den Vorjahren:

Viele Nutzer unterschätzen die eigene Betroffenheit („*Mir passiert das schon nicht*“), fühlen sich überfordert von der Komplexität der Maßnahmen oder scheuen den Aufwand. Dazu kommt oft eine gewisse Bequemlichkeit – etwa bei der Verwendung einfacher Passwörter oder dem Ignorieren von Software-Updates.



Typische Schwachstellen, die Cyberkriminelle ausnutzen:

Passwortsicherheit: Wiederverwendung von Passwörtern, einfache Kombinationen.

Phishing: Unvorsichtiges Klicken auf Links oder das Öffnen von Anhängen in verdächtigen E-Mails.

Veraltete Software: Nicht installierte Sicherheitsupdates.

Öffentliche WLANs: Unsichere Verbindungen ohne VPN.

Fake-Shops: Fehlende Überprüfung von Online-Shops (z. B. Impressum, Bewertungen).



Das eigentliche Problem:

1. Bequemlichkeit
2. Unwissenheit

Das zentrale Problem:

Die Menschen kennen die Risiken, handeln aber nicht danach. Und diese Lücke nutzen Angreifer gezielt aus. Ein Blick auf die Zahlen zeigt, wie groß das Problem ist:

- Nur rund 40 Prozent der Menschen nutzen die besonders effektive Zwei-Faktor-Authentifizierung (2FA).
- Nur etwa jeder Vierte führt Updates durch.
- Nicht einmal die Hälfte verwendet konsequent sichere Passwörter.
- Nur 40 Prozent haben überhaupt ein Virenschutzprogramm installiert.



Was kann man konkret tun?

- Zwei-Faktor-Authentifizierung (2FA) aktivieren – wo immer möglich.
- Passwortmanager (z.B. KeePassXC) nutzen und starke, einzigartige Passwörter verwenden.
- Regelmäßige Backups/Datensicherung anlegen, um im Ernstfall Daten wiederherstellen zu können.
- Skeptisch sein bei unerwarteten E-Mails oder Nachrichten – selbst wenn sie vertrauenswürdig aussehen.
- Updates für Betriebssysteme, Programme und Apps zeitnah installieren.



Dass Cybercrime kein theoretisches Problem ist, zeigen die Zahlen deutlich:

Mehr als jede vierte Person in Deutschland war bereits betroffen – jede neunte im Jahr 2025.

Zu den häufigsten Fällen gehören:

Betrug beim Online-Shopping, übernommene Benutzerkonten, Probleme beim Online-Banking und Phishing.

Besonders kritisch:

Viele unterschätzen ihr persönliches Risiko. Mehr als die Hälfte der Befragten glauben, eher nicht betroffen zu sein.



In fünf Minuten sicherer

Diese vier Schritte stoppen viele Angriffe sofort

- **2FA aktivieren:** Richte die Zwei-Faktor-Authentifizierung bei E-Mail, Banking und Social Media ein. Dauert meist nur wenige Minuten.
- **Updates:** Führe empfohlene Updates für Betriebssystem, Programme und Apps durch. Sicherheitslücken werden so automatisch geschlossen.
- **Passwort-Manager nutzen:** Erstelle starke, einzigartige Passwörter – merken muss man sich nur noch eins.
- **Virenschutz nutzen:** Ein Antivirenprogramm kann Malware blockieren, Phishing erkennen und bietet zusätzliche Schutzfunktionen.





ENDE