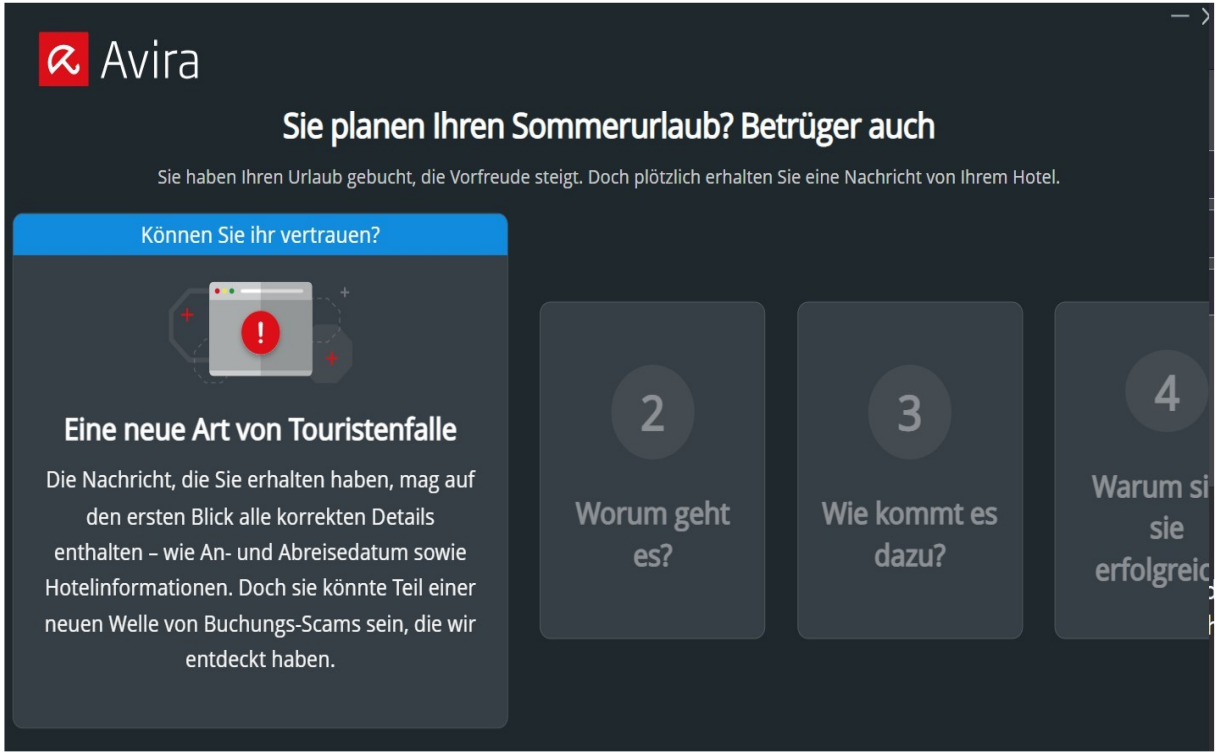
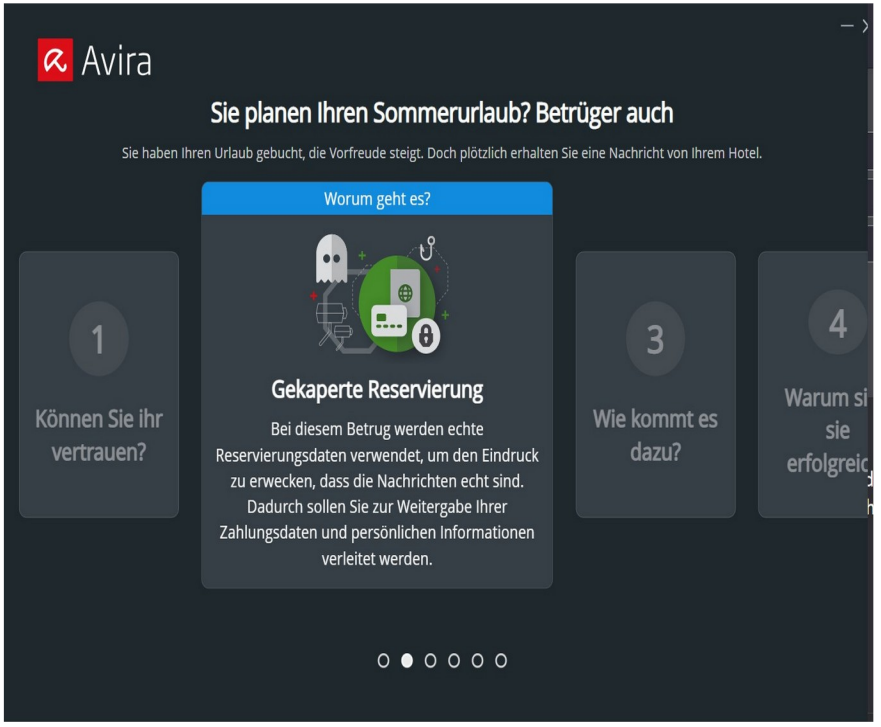
Cyberkriminalität (Cybercrime)

1. Beispiel von AVIRA (Urlaubsbuchung)
2. Schutzmechanismen

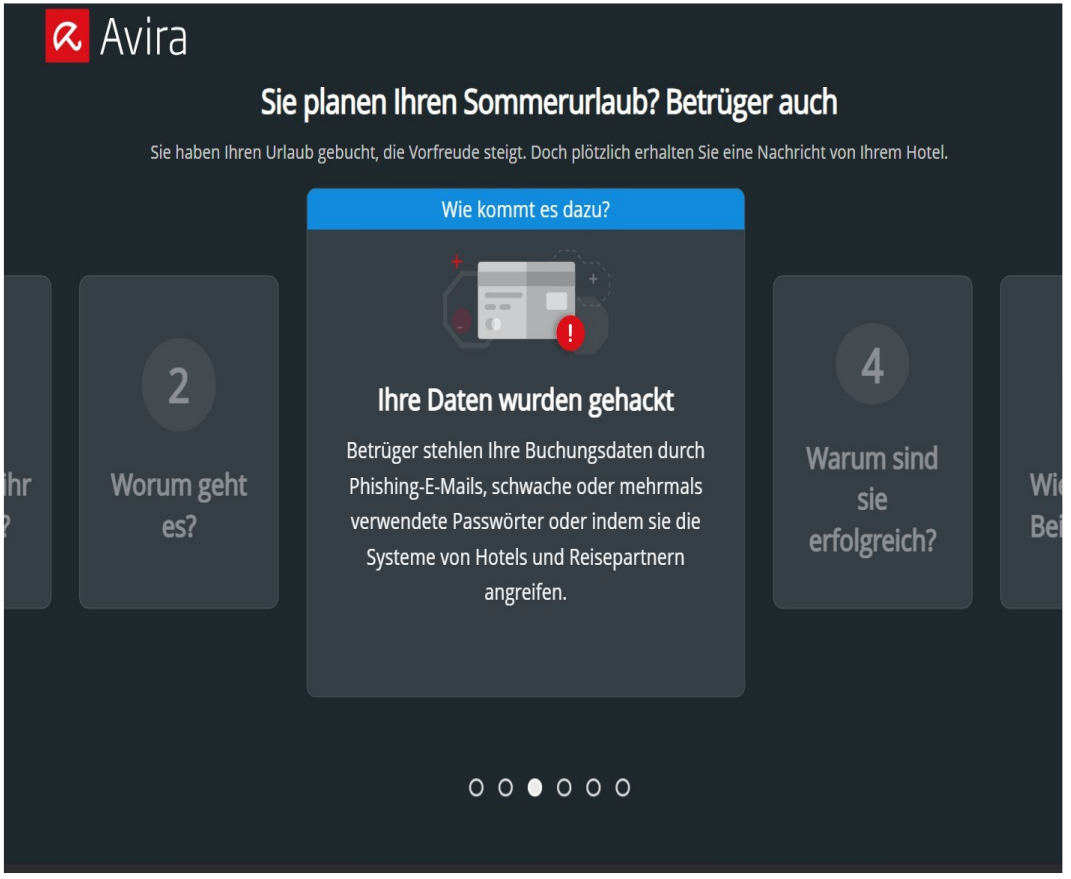
1.



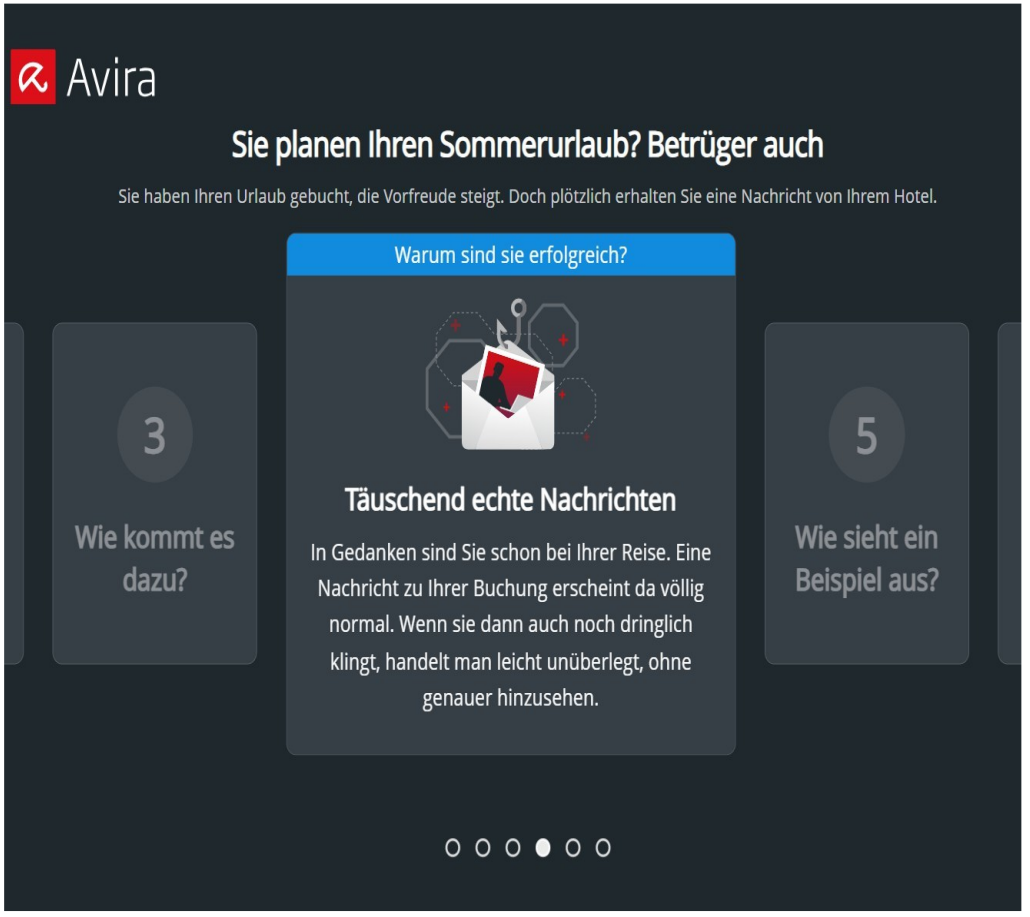
Quelle: Avira



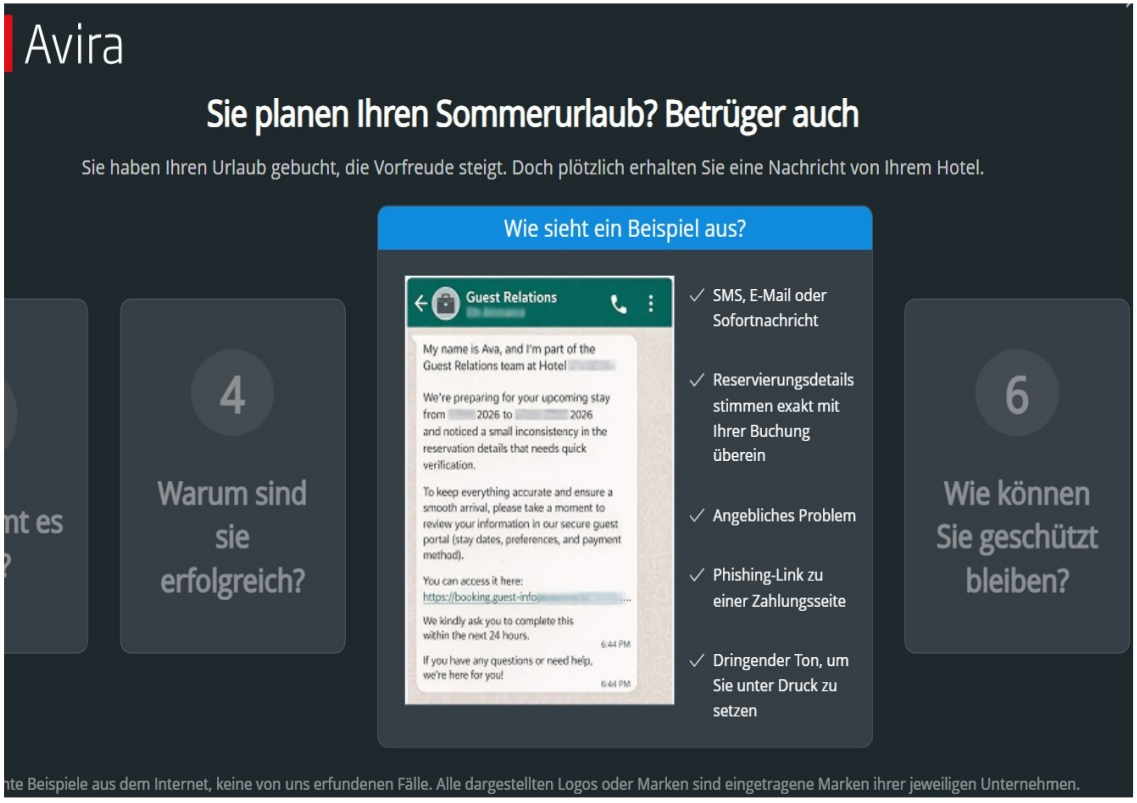
Quelle: Avira



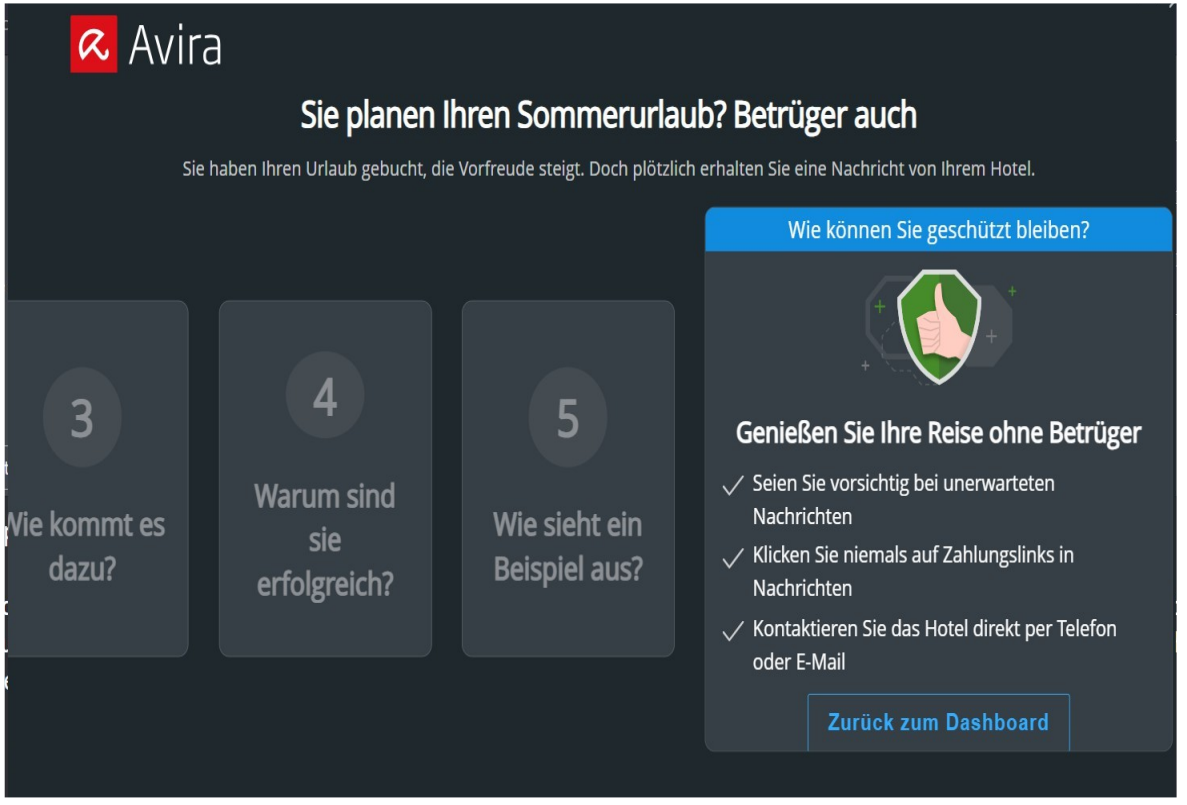
Quelle: Avira



Quelle: Avira



Quelle: Avira



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