

# Sim Card Swapping
# Betrugsmasche

**Quelle: Zusammengestellt vom Autor**



**SIM-Card Swapping**, auch bekannt als SIM-Swapping oder SIM-Hijacking, ist eine Betrugsmethode, **bei der Angreifer die Kontrolle über die Telefonnummer eines Opfers erlangen, indem sie die SIM-Karte des Opfers auf eine neue SIM-Karte übertragen.** Dadurch erhalten die Betrüger Zugang zu allen Diensten und Konten, die mit der Telefonnummer verknüpft sind, wie z.B. Bankkonten, E-Mail-Konten und soziale Netzwerke. Hier ist eine Auflistung wie SIM-Swapping funktioniert:

## *Ablauf des SIM-Swappings*:

1. **Zielauswahl und Informationsbeschaffung**:
   - Der Angreifer identifiziert ein Ziel, oft jemanden mit einem hohen finanziellen Status oder jemand, der Zugang zu wertvollen Konten hat.
   - Der Angreifer sammelt persönliche Informationen über das Opfer, wie Name, Adresse, Geburtsdatum, Telefonnummer, und möglicherweise auch Informationen zu Bank- und Online-Konten. Diese Informationen können durch Phishing, Social Engineering, Datenlecks oder das Dark Web beschafft werden.

2. **Kontaktaufnahme mit dem Mobilfunkanbieter**:
   - Der Angreifer kontaktiert den Mobilfunkanbieter des Opfers und gibt sich als das Opfer aus.
   - Der Angreifer behauptet, die SIM-Karte sei verloren gegangen oder gestohlen worden und bittet den Anbieter, die Telefonnummer auf eine neue SIM-Karte zu übertragen, die sich in ihrem Besitz befindet.
   - Oft nutzt der Angreifer die gesammelten persönlichen Informationen, um sich gegenüber dem Anbieter als das Opfer zu authentifizieren.

3. **SIM-Kartenwechsel**:
   - Wenn der Mobilfunkanbieter die Anfrage akzeptiert, wird die Telefonnummer des Opfers auf die neue SIM-Karte des Angreifers übertragen.
   - Die alte SIM-Karte des Opfers wird deaktiviert, und das Opfer verliert die Kontrolle über seine Telefonnummer.

4. **Kontozugriff und Ausnutzung**:
   - Mit der übernommenen Telefonnummer kann der Angreifer nun die Zwei-Faktor-Authentifizierung (2FA) umgehen, da viele Online-Dienste Einmal-Passwörter (OTP) per SMS versenden.
   - Der Angreifer kann sich bei den Konten des Opfers anmelden, Passwörter zurücksetzen und vollen Zugriff auf deren E-Mail, soziale Netzwerke, Bankkonten und andere Dienste erhalten.
   - Der Angreifer kann finanziellen Schaden anrichten, Identitätsdiebstahl begehen oder vertrauliche Informationen stehlen.

# Schutzmaßnahmen gegen SIM-Swapping:

1. **Starke Authentifizierung**:
   - Nutze nach Möglichkeit Authentifizierungs-Apps oder physische Sicherheits-Keys anstelle von SMS-basierten 2FA, da diese sicherer sind.

2. **PIN/Passwort bei Mobilfunkanbietern**:
   - Viele Mobilfunkanbieter bieten die Möglichkeit, ein zusätzliches PIN oder Passwort für den Support einzurichten, das bei Änderungen an der SIM-Karte abgefragt wird.

3. **Vorsicht bei der Preisgabe persönlicher Informationen**:
   - Sei vorsichtig bei der Weitergabe persönlicher Informationen und achte darauf, dass du nicht auf Phishing-Angriffe hereinfällst.

4. **Überwachung von Konten**:
   - Überwache deine Konten auf verdächtige Aktivitäten und reagiere sofort, wenn du ungewöhnliche Nachrichten oder Benachrichtigungen erhältst.

5. **Kundenservice-Optionen**:
   - Erkundige dich bei deinem Mobilfunkanbieter, welche Schutzmaßnahmen sie gegen SIM-Swapping anbieten und nutze diese Optionen.

*SIM-Swapping ist eine ernstzunehmende Bedrohung, aber mit den richtigen Schutzmaßnahmen kannst du das Risiko erheblich reduzieren.*