

## Neue Betrugsmasche auf WhatsApp:

Mi, 28.01.2026 - 10:44

### Was hinter dem GhostPairing steckt und wie Verbraucher sich schützen können

**Eine neue digitale Bedrohung gefährdet die Privatsphäre von Millionen WhatsApp-Nutzerinnen und -Nutzern. Sicherheitsexperten des IT-Sicherheitsunternehmens „Gen Digital“ haben eine besonders raffinierte Social-Engineering-Methode identifiziert, die unter dem Namen GhostPairing bekannt ist. Sie ermöglicht es Kriminellen, WhatsApp-Konten auszuspähen, ohne die Ende-zu-Ende-Verschlüsselung der Plattform zu umgehen.**

Im Mittelpunkt des Angriffs steht eine eigentlich legitime Funktion von WhatsApp: die **„Verknüpften Geräte“**. Durch gezielte Täuschung bringen Betrüger ihre Opfer dazu, ein zusätzliches Gerät zu autorisieren, das in Wirklichkeit vom Angreifer kontrolliert wird. Der Zugriff bleibt für die Betroffenen unbemerkt, während die **Täter Nachrichten mitlesen, Sprachnachrichten abhören, Fotos und Videos herunterladen und sogar Nachrichten im Namen des Kontoinhabers versenden können**. Auf diese Weise wird das kompromittierte Profil selbst zum Einfallstor für weitere Betrugsversuche im persönlichen Kontaktumfeld.

Der Betrug beginnt in der Regel mit einer harmlos wirkenden Nachricht von einem bekannten Kontakt aus dem eigenen Adressbuch, dessen Konto bereits kompromittiert wurde. Kurze, vertraulich formulierte Texte wie „Ich habe gerade ein Foto von dir gefunden“ in Kombination mit einem Link senken die Hemmschwelle zum Anklicken. Der Link führt jedoch nicht zu einem echten sozialen Netzwerk, sondern zu einer täuschend echt gestalteten Webseite, die Facebook imitiert und eine angebliche „Identitätsprüfung“ verlangt. Tatsächlich dient dieser Schritt dazu, die Kopplung eines neuen WhatsApp-Geräts über einen numerischen Code einzuleiten, den das Opfer in der Annahme eingibt, einen legitimen Sicherheitsvorgang abzuschließen.

Zum Schutz vor GhostPairing sollten Verbraucher:innen grundsätzlich **misstrauisch gegenüber externen Webseiten sein, die dazu auffordern, WhatsApp-Codes einzugeben oder Geräte zu verknüpfen**, um Fotos oder Videos ansehen zu können. Das Hinzufügen neuer Geräte sollte ausschließlich direkt innerhalb der App und auf eigene Initiative erfolgen. Zusätzlich **empfiehlt sich die Aktivierung der Zwei-Schritt-Verifizierung**, da sie den Handlungsspielraum von Angreifern im Falle eines unbefugten Zugriffs deutlich einschränkt.

Abschließend ist es ratsam, regelmäßig den Menüpunkt **„Einstellungen > Verknüpfte Geräte“ in WhatsApp zu überprüfen und verdächtige Geräte umgehend zu entfernen**. Aufmerksamkeit und Prävention bleiben die wirksamsten Mittel, um die eigene digitale Sicherheit und Verbraucherrechte zu schützen.