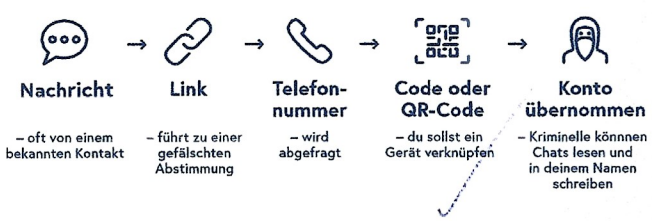
Bundesministerium
Inneres
Bundeskriminalamt

KRIMINAL
PRÄVENTION

Ghost Pairing – WhatsApp-Kontoübernahme durch Geräteverknüpfung

Beim Ghost Pairing bringen Kriminelle Nutzerinnen und Nutzer dazu, ein fremdes Gerät mit dem eigenen WhatsApp-Konto zu verknüpfen. Häufig kommt die Nachricht von einem bereits übernommenen Kontakt. Aktuell wird etwa zu einer angeblichen Abstimmung aufgefordert.



Typische Warnsignale

- Eine bekannte Person bittet plötzlich um eine Abstimmung oder ähnliche Unterstützung.
- Ein externer Link führt zu einer Voting-, Gewinnspiel- oder Verifizierungsseite.
- Telefonnummer, WhatsApp-Verknüpfungscode oder QR-Code werden verlangt.
- WhatsApp meldet die Verknüpfung eines neuen oder unbekannten Gerätes.

Präventionsempfehlungen der Polizei

☑ Ungewöhnliche Nachrichten auch bei bekannten Kontakten hinterfragen und im Zweifel telefonisch rückfragen.

☑ Nur Geräte verknüpfen, deren Verbindung Sie selbst bewusst gestartet haben.

☑ Den Bereich „Verknüpfte Geräte" regelmäßig kontrollieren und WhatsApp-Sicherheitswarnungen beachten.

✕ Keine Verknüpfungscodes oder QR-Codes für Votings, Gewinnspiele oder fremde Websites verwenden.

Maßnahmen im Schadensfall

- Unter „Verknüpfte Geräte" unbekannte Geräte sofort abmelden.
- Kontakte über einen anderen Kommunikationsweg warnen.
- Bei verlorenem Zugriff die Telefonnummer bei WhatsApp erneut registrieren und die offiziellen Wiederherstellungsschritte nutzen.
- Beweise sichern; bei Geldtransfer sofort Bank/Zahlungsdienstleister kontaktieren.
- Bei Kontoübernahme, Betrugsversuch oder Schaden Anzeige bei der nächsten Polizeidienststelle erstatten.

Weiterführende Links

- Polizeiliche Kriminalprävention Österreich: www.kriminalpraevention.gv.at
- Bundeskriminalamt: www.bundeskriminalamt.at
- Watchlist Internet: www.watchlist-internet.at
- WhatsApp Help Center: faq.whatsapp.com