Ghost Pairing – WhatsApp-Kontoübernahme durch Geräteverknüpfung

Beschreibung

Beim Ghost Pairing bringen Kriminelle Nutzerinnen und Nutzer dazu, ein fremdes Gerät mit dem eigenen WhatsApp-Konto zu verknüpfen. Dafür missbrauchen sie eine reguläre WhatsApp-Funktion zur Geräteverknüpfung. Häufig kommt die Nachricht scheinbar von einem bekannten Kontakt, dessen Konto bereits kompromittiert wurde.

Aktuell verbreitet ist die Bitte, bei einer angeblichen Abstimmung für ein Kind oder eine jugendliche Person zu voten. Nach dem Öffnen des Links wird die Telefonnummer abgefragt. Danach soll ein WhatsApp-Verknüpfungscode eingegeben oder ein QR-Code gescannt werden. Damit wird tatsächlich ein Gerät der Täterinnen oder Täter mit dem WhatsApp-Konto verbunden.

Nachricht
– oft von einem bekannten Kontakt

Link
– führt zu einer gefälschten Abstimmung

Telefonnummer
– wird abgefragt

Code oder QR-Code
– du sollst ein Gerät verknüpfen

Konto übernommen
– Kriminelle könnnen Chats lesen und in deinem Namen schreiben

Typische Warnsignale

- Eine bekannte Person schickt plötzlich eine ungewöhnliche Bitte um eine Abstimmung.
- Ein Link führt auf eine externe Voting-, Gewinnspiel- oder Verifizierungsseite.
- Für die angebliche Stimmabgabe soll die eigene Telefonnummer eingegeben werden.
- Danach wird ein WhatsApp-Code verlangt oder ein QR-Code zur Geräteverknüpfung angezeigt.
- WhatsApp meldet die Verknüpfung eines neuen oder unbekannten Gerätes.

Präventionsempfehlungen der Polizei

- ☑ Hinterfragen Sie auch Nachrichten von bekannten Kontakten, wenn die verlangte Handlung ungewöhnlich ist.
- ☑ Kontaktieren Sie die Person im Zweifel telefonisch oder über einen anderen Kommunikationsweg.
- ☑ Kontrollieren Sie regelmäßig in WhatsApp den Bereich „Verknüpfte Geräte".
- ☑ Lesen Sie WhatsApp-Sicherheitswarnungen aufmerksam und lehnen Sie unbekannte Verknüpfungen ab.
- ✕ Geben Sie keinen Verknüpfungscode für ein Voting, Gewinnspiel oder eine fremde Website ein.
- ✕ Scannen Sie keine QR-Codes zur Geräteverknüpfung, die Sie nicht selbst angefordert haben.

Maßnahmen im Schadensfall

- Prüfen Sie sofort in WhatsApp unter „Verknüpfte Geräte", welche Geräte mit Ihrem Konto verbunden sind.
- Melden Sie unbekannte oder nicht eindeutig zuordenbare Geräte unverzüglich ab.
- Warnen Sie wichtige Kontakte über einen anderen Kommunikationsweg, wenn über Ihr Konto Links oder Geldforderungen versendet wurden.
- Sichern Sie Beweise wie Screenshots, Chatverläufe, Telefonnummern, Internetadressen, angezeigte Codes und Zahlungsdaten.
- Wurde bereits Geld überwiesen, kontaktieren Sie unverzüglich Ihre Bank beziehungsweise den verwendeten Zahlungsdienstleister.
- Wenn Sie den Zugriff auf Ihr Konto verloren haben, registrieren Sie Ihre Telefonnummer erneut bei WhatsApp und folgen Sie den offiziellen Wiederherstellungsschritten.
- Erstatten Sie bei einer Kontoübernahme, einem Betrugsversuch oder einem Schaden Anzeige bei der nächsten Polizeidienststelle.

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