EUROPEAN-NEWS-AGENCY.COM

EUROPEAN NEWS AGENCY

International Press Service

Ressort: Internet und Technik

WhatsApp-Kontoübernahme durch gefälschte Online-Votings

Ingolstadt, 21.01.2026 [ENA]

Kaspersky-Experten haben Ende des vergangenen Jahres eine neue Phishing-Kampagne entdeckt, die WhatsApp-Nutzer über fingierte Online-Votings ins Visier nimmt. Hierfür dienen angebliche Abstimmungen, beispielsweise über junge Sporttalente, als Köder. Das Schema lässt sich jedoch mit minimalen Anpassungen auf andere Themen übertragen. Ziel ist die Übernahme von WhatsApp-Konten.

Betroffene landen auf einer scheinbar seriösen Voting-Seite mit Fotos, „Vote"-Buttons sowie angeblichen Live-Zählern für Stimmen und Teilnehmende. Die Seite verspricht Teilnahme nach einer „Autorisierung" und suggeriert auch Preise durch „Sponsoren". Ein Klick auf „Vote" oder „Authorize" führt die Nutzer jedoch auf eine Betrugs-Website, die zur „schnellen, einfachen" Autorisierung über deren bei WhatsApp-hinterlegten Rufnummer auffordert. Parallel stoßen die Angreifer einen Login bei WhatsApp Web an: Sie geben die Rufnummer ein, erhalten einen sechsstelligen Verifizierungscode – und spiegeln diesen Code auf der Betrugs-Website. Gibt die betroffene Person den Code in ihrer App ein, wird die von den Angreifern initiierte Web-Sitzung aktiv.

So können sie Nachrichten mitlesen und sogar senden; das Konto wird schrittweise übernommen. Tatyana Shcherbakova, Web Content Analyst bei Kaspersky, ordnet ein: „Online-Wettbewerbe mit Abstimmungen sind derzeit sehr beliebt – und genau dieses Vertrauen in scheinbar harmlose Interaktionen machen sich Angreifer zunutze. Durch Social Engineering in Kombination mit überzeugend gefälschten Oberflächen wird Nutzerinteraktion zur Waffe, um sensible Daten zu stehlen. Aufmerksamkeit und Wachsamkeit sind entscheidend, um sicher zu bleiben."

Kaspersky-Tipps zum Schutz vor Konto-Übernahmen in WhatsApp:

• Die Zwei-Schritt-Verifizierung in WhatsApp sollte aktiviert werden, damit das Konto durch einen zusätzlichen PIN geschützt ist und Angreifer keinen einfachen Zugriff erhalten.

• Vor der Eingabe persönlicher Daten ist stets die Echtheit einer Webseite zu prüfen – besonders bei Links aus unverlangten Nachrichten; die URL sollte dabei genau kontrolliert werden.

• Der Verifizierungscode darf niemals weitergegeben oder von anderen angenommen werden, da WhatsApp ihn nicht aktiv anfordert; andernfalls könnten Angreifer sofort auf das Konto zugreifen.

Redaktioneller Programmdienst:
European News Agency

Annette-Kolb-Str. 16
D-85055 Ingolstadt
Telefon: +49 (0) 841-951. 99.660
Telefax: +49 (0) 841-951. 99.661
Email: contact@european-news-agency.com
Internet: european-news-agency.com

Haftungsausschluss:

Der Herausgeber übernimmt keine Haftung für die Richtigkeit oder Vollständigkeit der veröffentlichten Meldung, sondern stellt lediglich den Speicherplatz für die Bereitstellung und den Zugriff auf Inhalte Dritter zur Verfügung. Für den Inhalt der Meldung ist der allein jeweilige Autor verantwortlich.



• Eine vertrauenswürdige Sicherheitslösung, wie Kaspersky Premium, nutzen, die vor betrügerischen Webseiten und Links warnt und diese blockiert.

Bericht online lesen:
https://schulz.en-a.de/internet_und_technik/whatsapp_kontouebernahme_durch_gefaelschte_online_votings-92873/

Redaktion und Verantwortlichkeit:
V.i.S.d.P. und gem. § 6 MDStV: Heiko Schulz

Redaktioneller Programmdienst:
European News Agency

Annette-Kolb-Str. 16
D-85055 Ingolstadt
Telefon: +49 (0) 841-951. 99.660
Telefax: +49 (0) 841-951. 99.661
Email: contact@european-news-agency.com
Internet: european-news-agency.com

Haftungsausschluss:

Der Herausgeber übernimmt keine Haftung für die Richtigkeit oder Vollständigkeit der veröffentlichten Meldung, sondern stellt lediglich den Speicherplatz für die Bereitstellung und den Zugriff auf Inhalte Dritter zur Verfügung. Für den Inhalt der Meldung ist der allein jeweilige Autor verantwortlich.