WHATSAPP PODVOD

„HLASUJTE ZA TANEČNICU“ KEĎ SA DÔVERA STÁVA ZBRAŇOU ÚTOČNÍKOV

Útok typu „Hlasujte za tanečnicu“ je zameraný na naše dobré vlastnosti a prirodzenú ochotu pomáhať. Ľudia radi podporia svojich známych, priateľov či dokonca neznámych, najmä ak ide o talentové súťaže, deti alebo mladých ľudí snažiacich sa presadiť. Práve túto empatiu a spolupatričnosť však útočníci zneužívajú. Ich cieľom nie je podpora umenia ani pomoc tanečnici, ale získanie kontroly nad WhatsApp účtom obete. Po jeho prevzatí podvodníci vystupujú pod menom obete, šíria podvodné správy ďalej, žiadajú peniaze od jej kontaktov alebo rozposielajú odkazy na škodlivý softvér. Dôvera, ktorú majú ľudia k známym kontaktom, sa tak mení na nástroj útoku. Tento útok sa nemusí zameriavať len na podporu tanečníc, ale môže smerovať aj na podporu športu alebo pomoc pri hľadaní domáceho zvieratka.
My si špecifikáciu podvodu vysvetlíme na príklade podpory tanečníc.

Spolufinancovaný Európskou úniou

Financované Európskou úniou. Vyjadrené názory a postoje sú názormi a vyhláseniami autora(-ov) a nemusia nevyhnutne odrážať názory a stanoviská Európskej únie. Európska únia za ne nepreberá žiadnu zodpovednosť.

NCC-SK SLOVAKIA CYBERSECURITY COORDINATION CENTRE

ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

Kompetenčné a certifikačné centrum kybernetickej bezpečnosti

Mechanizmus podvodu

Podvod zvyčajne začína rozoslaním správy cez WhatsApp, ktorá vyzýva na rýchle hlasovanie v údajnej tanečnej súťaži. Správa pôsobí nevinne, často je krátka a emotívna, napríklad s prosbou o podporu „kamarátkinej dcéry" alebo „známej tanečnice". Súčasťou správy je odkaz alebo inštrukcie, ktoré majú používateľa presvedčiť k vykonaniu jediného kroku – kliknutiu na link, potvrdeniu prihlásenia alebo zadaniu overovacieho kódu.

V momente, keď obeť zadá overovací kód alebo potvrdí prihlásenie, ktoré sama neiniciovala, poskytne útočníkom prístup k svojmu WhatsApp účtu. Tí následne prevezmú nad účtom plnú kontrolu. Z kompromitovaného účtu rozposielajú rovnaké „hlasovacie" správy všetkým kontaktom obete, čím sa podvod rýchlo šíri. Okrem toho môžu od kontaktov žiadať peniaze, vylákať ďalšie citlivé údaje alebo šíriť odkazy na podvodné stránky a malware. Keďže správy prichádzajú „od známej osoby", príjemcovia im často bez váhania dôverujú.

Indikátory WhatsApp podvodu

Medzi najčastejšie varovné signály patrí **neočakávaná správa** s výzvou na hlasovanie, ktorá prichádza od známeho kontaktu, no nezodpovedá jeho bežnému štýlu komunikácie. Podozrivé je, ak obsah správy vyzýva k **zdieľaniu odkazu** ďalej alebo k **zadaniu overovacieho kódu**. Rizikovým znakom sú aj odkazy vedúce na **neznáme alebo podozrivé webové stránky**.

Ďalším indikátorom je, ak kontakt po odoslaní hlasovacej správy začne postupne zasielať neobvyklé žiadosti, napríklad prosby o rýchle požičanie peňazí. Mimoriadne nebezpečné sú **požiadavky na zdieľanie jednorazového kódu** alebo **potvrdenia prihlásenia**, ktoré obeť sama nevyvolala. Takéto správanie by malo okamžite vzbudiť podozrenie.

Ako sa chrániť pred WhatsApp podvodom

Základnou ochranou je obozretnosť aj pri správach od známych kontaktov. Ak dostanete výzvu na hlasovanie, je vhodné si ju overiť iným komunikačným kanálom, napríklad telefonátom. Nikdy nezdieľajte jednorazové overovacie kódy ani nepotvrdzujte prihlásenie, ktoré ste sami neiniciovali.

Dôležité je neklikať na podozrivé odkazy a nešíriť správy, ktorých pravosť si nie ste istí. Odporúča sa zapnúť dvojstupňové overenie účtu WhatsApp, ktoré výrazne sťažuje jeho prevzatie. V prípade kompromitácie účtu je potrebné konať okamžite, informovať kontakty a kontaktovať podporu aplikácie.

WhatsApp podvod „Hlasujte za tanečnicu" je nebezpečný, pretože cieli na dôveru a ochotu pomáhať. Útočníci dokážu rýchlo prevziať kontrolu nad účtom a šíriť podvod ďalej. Následkom môžu byť finančné straty aj poškodenie dobrého mena obete. Ochrana si vyžaduje zvýšenú opatrnosť a overovanie správ, aj keď prichádzajú od známych. Prevencia a informovanosť sú kľúčom k zastaveniu šírenia tohto typu útoku.

Spolufinancovaný Európskou úniou

Financované Európskou úniou. Vyjadrené názory a postoje sú názormi a vyhláseniami autora(-ov) a nemusia nevyhnutne odrážať názory a stanoviská Európskej únie. Európska únia za ne nepreberá žiadnu zodpovednosť.

NCC-SK SLOVAKIA CYBERSECURITY COORDINATION CENTRE

ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

Kompetenčné a certifikačné centrum kybernetickej bezpečnosti