OUCH! 2026. június

Az Ön Havi Biztonsági Tudatosságról Szóló hírlevele

Világkupa láz: ne hagyd, hogy a csalók gólt rúgjanak

Egy életre szóló lehetőség – Ellopva

Diego éveken át várt erre a pillanatra. Végre elérkezett a 2026-os világbajnokság, és most először volt meg hozzá egyszerre az ideje és a pénze is, hogy személyesen részt vegyen rajta. Amikor meglátott egy bejegyzést a közösségi médiában, amely „last minute jegyeket” kínált egy, már teltházas mérkőzésre, szerencsésnek érezte magát. Az eladó azt állította, hogy egy hivatalos forgalmazóval dolgozik együtt, és még egy, a bajnokság szervezőitől származónak tűnő visszaigazoló e-mailt is megosztott.

Az ár magas volt, de nem kirívóan. Az eladó figyelmeztette, hogy a jegyek szinte már elfogytak, és hogy több érdeklődő is van rájuk. Nem akarta elszalasztani a lehetőséget, ezért Diego egy azonnali fizetési alkalmazáson keresztül átutalta a pénzt.

A jegyek sosem érkeztek meg. Az eladó felhasználói fiókja eltűnt. Az üzenetben hivatkozott weboldalt néhány napon belül eltávolították. Diego nem csak a pénzét veszítette el; elszalasztotta az esélyét annak is, hogy részt vegyen egy olyan eseményen, amelyre csak egyszer adódik lehetőség az életben.

Miért vonzóak a nagy sportesemények a csalók számára

Az olyan globális események, mint a világbajnokság, tökéletes táptalajt teremtenek a csalások számára. Óriási a kereslet a jegyek, az utazás, a rajongói termékek és a közvetítésekhez való hozzáférés iránt. Az emberek izgatottak, érzelmileg érintettek, és gyakran gyorsan cselekszenek. A sürgetettség érzete és az érzelmek együttes hatása megkönnyíti a támadók számára az áldozatok manipulálását.

A bűnözők értik az emberi viselkedést. Tisztában vannak azzal, hogy amikor valami szűkösen elérhető, az emberek nyomást éreznek arra, hogy gyorsan cselekedjenek. Azt is tudják, hogy amikor emberek milliói ugyanazt keresik az interneten, a hamis weboldalak és adathalász üzenetek könnyedén beleolvadnak a tömegbe. A támadók következetesen kihasználják a sürgetettséget, a félelmet és az izgatottságot, hogy az embereket gyors döntések meghozatalára késztessék, amelyek pénzügyi és személyes veszteségekhez vezetnek.

Hogyan néznek ki ezek a támadások

Hamis jegyértékesítés: A bűnözők professzionális megjelenésű weboldalakat vagy közösségi média bejegyzéseket hoznak létre, amelyek hitelesnek tűnnek. Egyesek hivatalos arculati elemeket és logókat másolnak, míg mások online hirdetéseket vásárolnak, hogy hamis oldalaik a keresési találatok élén jelenjenek meg. Az áldozatok olyan jegyekért fizetnek, amelyeket soha nem kapnak meg, vagy olyan digitális jegyeket kapnak, amelyek nem működnek a stadion bejáratánál. Gyakran banki átutalással, kriptovalutával vagy peer-to-peer alkalmazásokon keresztül kérik a fizetést, amelyeket nehéz visszakeresni.

Sürgős üzenetek: Olyan e-maileket vagy szöveges üzeneteket kapunk, amelyek a rendezvény szervezőitől, légitársaságoktól, szállodáktól vagy streaming szolgáltatóktól származónak tűnnek. Ezek az üzenetek gyakran arra figyelmeztetnek, hogy a jegyvásárlás sikertelen volt, vagy hogy a foglalást törlik, ha nem erősítjük meg azonnal a fizetést. Úgy készítik el őket, hogy sürgősnek és hivatalosnak tűnjenek, ezért a vásárlók gyorsan anélkül döntenek , hogy logikusan átgondolnák mi történik. A linkek leggyakrabban egy hamis bejelentkezési weboldalra irányítanak, amit úgy terveztek, hogy ellopja a bejelentkezési adatainkat. Ahogyan más csalási kampányok esetében is, a támadók nagymértékben támaszkodnak a sürgetésre és a hozzáférés elvesztésétől való félelemre.

Streames csalások: A bűnözők hamis platformokat hoznak létre, amelyek „ingyenes élő közvetítést" kínálnak a mérkőzésekről. A megtekintéshez arra kérnek bennünket, hogy hozzunk létre egy fiókot, és adjuk meg a fizetési adatainkat. A mérkőzés megtekintése helyett előfordulhat, hogy anélkül, hogy észrevennénk, rosszindulatú szoftvert telepítünk, vagy ellopják a pénzügyi adatainkat.

Hamis termékek: Még a szuvenírek és ajándéktárgyak is a visszaélések eszközeivé válhatnak. A hamis nyereményjátékok például hivatalos mezeket vagy exkluzív nyereményeket ígérhetnek személyes adatokért cserébe. A hamis online áruházak kedvezményes áron kínálhatnak felszerelést, de végül vagy silány minőségű utánzatokat küldenek, vagy egyáltalán nem szállítanak semmit.

Hogyan védjük meg magunkat

A jó hír az, hogy ezek a csalások megelőzhetőek, ha lelassítunk, és cselekvés előtt ellenőrzünk néhány információt. Jegyeket, utazást és termékeket kizárólag hivatalos partnerektől vagy jól ismert szolgáltatóktól vásároljunk. Ahelyett, hogy e-mailekben, közösségi média bejegyzésekben vagy más, nem ellenőrzött forrásokban található linkekre kattintanánk, gépeljük be közvetlenül a hivatalos weboldal címét a böngészőbe, vagy használjunk megbízható mobilalkalmazást. A hitelesnek bizonyult oldalakat mentsük el könyvjelzőként, hogy minden alkalommal a megfelelő helyre térjünk vissza.

Legyünk különösen óvatosak minden olyan üzenettel, amely azonnali cselekvésre buzdít. A csalók a sebességre támaszkodnak. Ha a foglalás törléséről vagy sikertelen fizetésről szóló figyelmeztetést kapunk, ne kattintsunk a linkre. Ehelyett vegyük fel a kapcsolatot a céggel külön, a hivatalos elérhetőségeiken keresztül.

Végül legyünk óvatosak a szokatlan fizetési módokkal. A kriptovalutával, banki átutalással vagy ajándékkártyákkal történő fizetési kérelmek keltsenek bennünk gyanút! A legitim szolgáltatók ritkán használják ezeket a fizetési formákat. Ezeken felül a bankkártyák és az egyéb népszerű elektronikus fizetési rendszerek, mint például a PayPal, további vásárlóvédelmi lehetőségeket biztosítanak számunkra.

Legyünk óvatosak a vásárlásaink és döntéseink során; a kiberbűnözők arra játszanak, hogy sürgetés érzetével hibázásba hajszolják az embereket.

Vendégszerkesztő

Karyn DiMassa kiberbiztonsági, belső audit-, kontroll- és kockázatkezelési szakértő. Szakterületei közé tartozik az incidenskezelés, a katasztrófa utáni helyreállítás (disaster recovery, DR), valamint az üzletmenet-folytonosság menedzsmentje. Tapasztalattal rendelkezik kiberbiztonsági felmérések, hiányosságelemzések és javító intézkedések kidolgozása terén Mindemellett jártas a belső kockázatok és kontrollok azonosításában, értékelésében és fejlesztésében, a vállalati kockázatkezelésben, valamint a belső ellenőrzési folyamatok támogatásában.

Források

Hogyan használják ki a kiberbűnözők érzelmeinket: https://www.sans.org/newsletters/ouch/cybercriminals-exploit-your-emotions/
Top Három Módszer, Ahogy A (Kiber)támadók Célpontjává Válunk: https://www.sans.org/newsletters/ouch/top-ways-attackers-target-you
A Misztikum Feloldása: Hogyan lopják el a jelszavakat a kiberbűnözők?: https://www.sans.org/newsletters/ouch/unveiling-shadows-how-cyber-criminals-steal-your-passwords

A Közösség számára fordította: Nemzetbiztonsági Szakszolgálat Nemzeti Kiberbiztonsági Intézet (NBSZ NKI)

Többet találhat az Ouch!-ból A következő linken: https://www.sans.org/newsletters/ouch