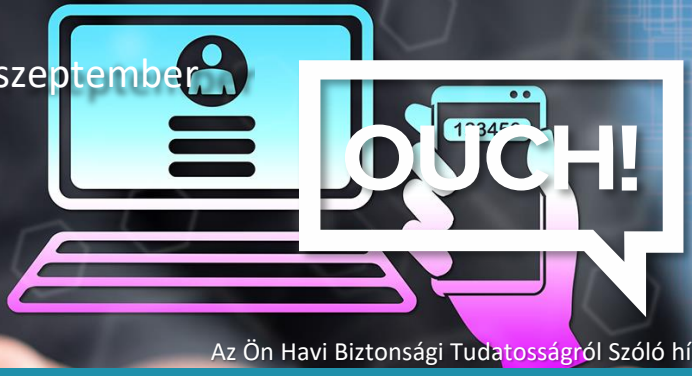

Az Ön Havi Biztonsági Tudatosságról Szóló hírlevele

Hogyan tegyük tönkre egy támadó napját? Többfaktoros hitelesítéssel!

Ami neked könnyű, az egy támadónak is az

James éppen otthon pihent, amikor a telefonját hirtelen elárasztották az értesítések. A személyes e-mail fiókjának jelszava megváltozott, pedig nem emlékezett rá, hogy bármit is módosított volna. Nem sokkal később közösségimédia-fiókjai is sorra jelezték, hogy azok jelszavai is megváltoztak, majd a bankja gyanús vásárlásokra figyelmeztette. James pánikba esve próbált bejelentkezni e-mail fiókjába, de a jelszava már nem működött. Valaki kizárta őt onnan! A következő néhány nap során James hosszú órákat töltött felhasználói helyreállításával, a jogosulatlan terhelések vitatásával és jelszavai megváltoztatásával. Ami a leginkább összezavarta az az, hogy tudomása szerint mindent megtett a biztonsága érdekében. Erős jelszót használt, és nem osztotta meg senkivel!

Azonban nem a jelszavával volt a probléma: inkább azzal, hogy csak a jelszavára támaszkodott. James nem tudta, hogy a múlt héten kapott sürgős szöveges üzenetet, amelyről azt hitte, hogy az e-mail-szolgáltatójától érkezett, valójában egy kiberbűnöző küldte, aki megtévesztéssel kicsalta tőle a jelszavát. Amint a kiberbűnöző megszerezte James jelszavát, teljesen átvette az irányítást az e-mail fiókja felett. Így a kiberbűnöző nemcsak James e-mailjeihez fért hozzá, hanem az e-mail fiókját felhasználva számos más fiókjának jelszavát is át tudta állítani.

James testvére, Ariel ugyanazt a szöveges üzenetet kapta, és a bátyjához hasonlóan őt is rávették arra, hogy rákattintson a rosszindulatú hivatkozásra, és megadja a jelszavát. Azonban James-szel ellentétben Ariel többfaktoros hitelesítést (MFA) használt e-mail fiókja védelme érdekében. Ez azt jelentette, hogy a támadónak hiányzott a bejelentkezéshez szükséges második hitelesítési tényező, amely a jelszótól független volt, így egy frusztráló napot töltött sikertelen bejelentkezési kísérletekkel. Ariel letiltotta a támadót, biztonságossá tette a felhasználóját, és sokkal jobb napja volt, mint Jamesnek. Nem sokkal később segített a testvérének is beállítani a többfaktoros hitelesítést (MFA), hogy ő is megkeseríthesse egy támadó napját.

Mi az a többfaktoros hitelesítés (MFA)?

A többtényezős hitelesítés, vagy MFA, egy ingyenes és egyszerű módja annak, hogy extra biztonsági réteget adjunk a fiókjainkhoz. Ahelyett, hogy kizárólag a jelszóra támaszkodnánk, az MFA egy második lépést (vagy hitelesítési tényezőt) is hozzáad, amellyel igazoljuk, hogy valóban mi próbálunk bejelentkezni. Az MFA használata esetén a bejelentkezéshez általában az alábbiak közül legalább kettőre van szükség:

- **Valami, amit tudsz**: a jelszavunk.
- **Valami, amit birtoklunk**: egy egyszer használatos kód, amelyet a telefonunkra küldenek, vagy amelyet egy alkalmazás generál.
- **Valami, ami mi vagyunk**: egy ujjlenyomat vagy arcfelismerés.

Még ha egy kiberbűnöző meg is szerzi a jelszavunkat, a második hitelesítési tényező nélkül akkor sem tud hozzáférni a fiókunkhoz. Ezért tartják az MFA engedélyezését gyakran **a legfontosabb lépésnek, amelyet megtehetünk fiókjaink védelme érdekében**.

Hogyan használjuk helyesen az MFA-t

A jó hír az, hogy az MFA egyszerűen használható és széles körben elérhető. A legtöbb nagy szolgáltató - beleértve az e-mail, a banki, a közösségi média és az online vásárlási szolgáltatásokat - ingyenesen biztosítja ezt a lehetőséget. Sőt, ami még ennél is jobb, hogy az MFA használatával sok esetben webhelyenként csak egyszer kell ilyen módon bejelentkeznünk. Ezt követően a webhely felismeri és megjegyzi a böngészőnket, így a hitelesítés nemcsak biztonságosabbá, hanem egyszerűbbé is válik. Így kezdhetünk bele:

1. Kapcsoljuk be az MFA-t fontos fiókjainkhoz: Kezdjük a legfontosabbakkal: az e-mail, a banki és befektetési-, valamint minden egyéb fontos felhasználóval. Ne feledjük: ha valaki hozzáfér az e-mail fiókunkhoz, gyakran a többi felhasználóhoz való hozzáférést is módosítani tudja.

2. Amikor csak lehetséges, használjunk hitelesítő alkalmazást: A második hitelesítési tényező egyik leggyakoribb formája egy egyedi kód, amelyet szöveges üzenetben küldenek a telefonunkra. Ugyanakkor egy erre a célra szolgáló hitelesítő alkalmazás használata még biztonságosabb és megbízhatóbb megoldást jelenthet. A hitelesítő alkalmazás olyan mobilalkalmazás, amelyet a telefonunkra telepítünk, és amely egyszer használatos kódokat generál ahelyett, hogy ezeket SMS-ben kapnánk meg.

3. Kombináljuk az MFA-t erős jelszavakkal: Az MFA hatékony védelmet nyújt, de a legjobb eredményt akkor érhetjük el, ha erős, egyedi jelszavakkal együtt használjuk. Az MFA mellé minden fiókunkhoz használjunk erős és egyedi jelszót! Ha olyan weboldallal találkozunk, ami felajánlja, hogy engedélyezzük a hozzáférési kulcsok (passkeys) használatát a fiókunkhoz, érdemes tudnunk, hogy a passkey lényegében az MFA egy még biztonságosabb változata.

4. Védjük mobileszközeinket: Mobiljaink mára kulcsszerepet töltenek be az MFA használatában, és gyakran a jelszókezelőnket is ezen tároljuk, így sok szempontból ez őrzi digitális életünk összes kulcsát. Gondoskodjunk eszközeink biztonságáról: kapcsoljuk be a képernyőzárat, és engedélyezzük az automatikus frissítéseket.

Vegyük kézbe saját biztonságunkat

Az MFA engedélyezése az egyik leghatékonyabb módja annak, hogy megvédjük magunkat az online térben. Ne várjuk meg, amíg fiókjainkat feltörik, ahogyan az James esetében is történt. Legyünk inkább olyanok, mint Ariel, és gondoskodjunk róla, hogy a támadónak legyen rossz napja.

Vendégszerkesztő

Betta Lyon Delsordo, az AWS pentestere alkalmazás-, felhő- és mesterséges intelligencia biztonságra szakosodott. A Georgia Tech intézményben szerzett kiberbiztonsági mesterdiplomával, valamint GPEN minősítéssel rendelkezik. Betta előadóként szerepelt többek között a DEF CON rendezvényen, a Világbanknál (World Bank), a WiCyS konferencián, valamint számos egyéb konferencián az Egyesült Államokban és az Európai Unióban.

Források

Hogyan használják ki a kiberbűnözők érzelmeinket: https://www.sans.org/newsletters/ouch/cybercriminals-exploit-your-emotions
A jelmondatok ereje: miért jobb a hosszabb, mint az okosabb?: https://www.sans.org/newsletters/ouch/power-passphrase-why-longer-beats-smarter
Tegyük könnyebbé a jelszókezelést: használjunk megbízható jelszószéfet: https://www.sans.org/newsletters/ouch/stop-password-pain-reliable-password-manager

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