EFF'S SURVEILLANCE SELF-DEFENSE

JINSI YA: KUWEZESHA UTHIBITISHAJI WA PILI

https://ssd.eff.org/en/about-surveillance-self-defense

LOCALIZATION LAB

https://ssd.eff.org/en/module/how-enable-two-factor-authentication
Uharirishaji wa mwisho 9-7-2017

Uthibitishaji wa mara ya pili (au "2FA") ni njia ya kuruhusu mtumiaji kujitambulisha kwa mtoa huduma kwa kuhitaji mchanganyiko wa mbinu mbili za kuthibitisha. Hizi zinaweza kuwa mbinu ambazo mtumiaji anajua (kama nenosiri au PIN), kitu ambacho mtumiaji anacho (kama token ya vifaa au simu ya mkononi), au kitu ambacho kinaunganishwa au kisichotenganishwa kutoka kwa mtumiaji (kama alama za kidole).

Labda tayari unatumia 2FA katika sehemu nyingine za maisha yako. Unapotumia ATM ili kutoa fedha, lazima uwe na kadi ya benki yako kimwili (kitu ambacho unacho) na PIN yako (kitu unachojua). Hivi sasa, hata hivyo huduma nyingi za mtandao zinatumia tu thibitisho moja kutambua watumiaji wao kwa kipaumbele-nenosili.

Jinsi 2FA inavyofanya kazi mtandaoni?

Huduma kadhaa mtandaoni-ikiwa ni pamoja na Facebook, Google, na Twitter-hupeana 2FA kama njia mbadala ya kuthibitisha nenosiri.Ukiwezesha kipengele hiki utatakiwa kuhamishwa kwa nenosiri na njia ya pili ya uthibitishaji.
Njia hii ya pili huwa ni msimbo wa wakati mmoja uliotumwa kwa SMS au msimbo wa wakati mmoja unaozalishwa na programu ya simu ya kujitolea inayoweka siri (kama Google Authenticator, Duo Mobile, programu ya Facebook, au Clef). Katika hali yoyote, sababu ya pili ni simu yako ya mkononi, kitu ambacho wewe (kawaida) unacho. Nje za tovuti (ikiwa ni pamoja na Google) pia husaidia nambari za kuhifadhi nakala moja, ambayo inaweza kupakuliwa, kuchapishwa kwenye karatasi, na kuhifadhiwa mahali salama kama ziada ya ziada. Mara baada ya kuingia katika kutumia 2FA, utahitaji kuingia nenosiri lako na msimbo wa wakati mmoja kutoka simu yako ili upate akaunti yako.

Kwa nini uwezeshe 2FA?

2FA inakupa usalama zaidi wa akaunti kwa kukuhitaji kuthibitisha utambulisho wako kwa njia zaidi ya moja. Hii ina maana kwamba, hata kama mtu angeweza kupata nywila lako la msingi, hawawezi kufikia akaunti yako isipokuwa pia alikuwa na simu yako ya mkononi au njia nyingine ya uthibitishaji.

Je! Kuna tatizo la kutumia 2FA?

Ijapokuwa 2FA inatoa njia salama zaidi ya kuthibitisha, kuna hatari kubwa ya kupata imefungwa nje ya akaunti yako ikiw a, kwa mfano, ukipoteza simu yako, kubadilisha kadi yako ya SIM, au kusafiri kwenda nchi nyingine bila kugeuka.

Huduma nyingi za 2FA hutoa orodha fupi ya nambari za kutumia "salama" au "kupona". Kila msimbo hutumika mara moja kuingia kwenye akaunti yako, na haitumiwi tena baadae. Ikiwa una wasiwasi juu ya kupoteza upatikanaji wa simu yako au kifaa kingine cha kuthibitisha, chapisha na ubebe msimbo hizi na wewe. Bado zitafanya kazi kama "kitu ambacho unacho," kwa muda tu unapofanya

nakala moja, na uiweke karibu nawe. Kumbuka kuweka msimbo salama na kuhakikisha kuwa hakuna mtu mwingine anayeiona au kuifikia wakati wowote. Ikiwa utatumia au kupoteza msimbo wako wa kuhifadhi, unaweza kuzalisha orodha mpya wakati unapoweza kuingia kwenye akaunti yako.

Tatizo lingine la mifumo ya 2FA ambayo hutumia ujumbe wa SMS ni kwamba ujumbe wa SMS hauko salama. Inawezekana kwa mshambulizi wa hali ya juu ambaye ana uwezo wa kufikia mtandao wa simu (kama vile shirika la majasusi au operesheni ya uhalifu iliyoandaliwa) ili kuepuka na kutumia nambari zinazotumwa na SMS. Pia kuna matukio ambapo mshambulizi asiye wa hali ya juu (kama vile mtu binafsi) ameweza kujitumia wito au ujumbe wa maandishi unaotengwa kwa namba moja kwa huduma zake, au huduma za kampuni za simu zinazoonyesha ujumbe uliotumwa kwa nambari ya simu bila kuhitaji kuwa na simu.

Kama una wasiwasi juu ya ngazi hii ya ushambulizi, toa uthibitishaji wa SMS, na uendelee kutumia programu za kuthibitisha kama Google Authenticator au Authy. Kwa bahati mbaya chaguo hili halipatikani kwa kila huduma ya 2FA iliyowezeshwa.

Kwa kuongeza, kutumia 2FA inamaanisha kuwa unaweza kuwapa taarifa zaidi kwa huduma kuliko wewe unavyotaka. Tuseme unatumia Twitter, na umejiunguka kwa kutumia pseudonym. Hata kama unakataa kwa uangalifu kutoa maelezo yako ya kujitambua kwenye Twitter, na hata ikiwa unapata huduma tu juu ya Tor au VPN, ikiwa utawezesha SMS 2FA, Twitter itakuwa na rekodi ya nambari yako ya simu ya mkononi. Hiyo ina maana kwamba, ikiwa inakabiliwa na mahakama, Twitter inaweza kuunganisha akaunti yako kwako kupitia namba yako ya simu. Hii inaweza kuwa si shida kwako, hasa ikiwa tayari unatumia jina lako la kisheria kwenye huduma iliyotolewa, lakini ikiwa kudumisha kutokujulikana kwako ni muhimu, fikiria mara mbili kuhusu kutumia SMS 2FA.

Hatimaye, utafiti umeonyesha kuwa watumiaji wengine watachagua nywila dhaifu baada ya kuwezesha 2FA, kuhisi kwamba thibitisho la pili ni linawaweka salama. Hakikisha bado kuchagua nywila ya nguvu hata baada ya kuwezesha 2FA. Tazama uundaji wetu wa nywila wenye nguvu kwa vidokezo.

Ninawezaje kuwawezesha 2FA?

Jihadharini na "maswali ya usalama" ambayo tovuti hutumia kuthibitisha utambulisho wako. Majibu ya uaminifu kwa maswali haya mara nyingi hupatikana kwa urahisi na adui huwa anaurahisi wa kuingia bila rusa na kujali kama una nywili au la.

Badala yake, kutoa majibu ya uongo ambayo hakuna mtu anayejua ila wewe tu. Kwa mfano, ikiwa swali la usalama linauliza:

"Jina la mfugo wa nyumbani kwako wa kwanza ulikuwa gani?"