EFF'S SURVEILLANCE SELF-DEFENSE

UWEZESHAJI WA UHALALISHAJI WA VIGEZO VIWILI

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

ELECTRONIC FRONTIER FOUNDATION

LOCALIZATION LAB

Uhalalishaji wa vigezo viwili(au “2FA”) ni njia ya kufanya akaunti zako za mtandaoni kuwa salama zaidi kwa kuongeza hitaji la uyakinifu wa ziada ("vigezo") pamoja na nenosiri lako unapoingia. Hili linaweza kuwa jambo unalojua (kama vile nenosiri au PIN), kitu ulicho nacho (kama vile ufunguo wa usalama au simu ya rununu), au kitu ambacho kimeambatishwa au kisichoweza kutenganishwa na wewe (kama vile alama ya kidole au uso).

Pengine tayari unatumia 2FA katika baadhi ya shughuli za maisha yako. Unapotumia ATM kutoa pesa taslimu, lazima uwe na kadi yako ya benki halisi (kitu ulichonacho) na PIN yako (jambo unalojua). 2FA kwa huduma za mtandaoni hutumia mantiki sawa ya msingi.

Je, 2FA Hufanyaje Kazi Mtandaoni?

Huduma nyingi za mtandaoni—ikiwa ni pamoja na Facebook (pamoja na Instagram na WhatsApp), Apple, Google, X, Reddit, WeChat, Telegram, na TikTok—zinatoa 2FA kama njia mbadala ya uhalalishaji wa nenosiri pekee. Ukishaiwezesha, utaulizwa nenosiri na njia mbadala ya uhalalishaji.

Mbinu hii ya pili inaweza kuwa mojawapo ya mambo kadhaa: ujumbe wa SMS, msimbo unaobadilika unaotolewa na programu ya uhalalishaji, arifa msukumo, au kifaa cha USB (kinachoitwa ufunguo wa usalama).

Programu ya uhalalishaji hutoa misimbo inayobadilika yenye herufi sita ambayo ni mahususi kwa kila tovuti ambayo umejisajili nayo. Kampuni nyingi hutengeneza programu za kihalalishaji cha simu za rununu bila malipo, kama vile Kithibitishaji cha Google na Authy. Baadhi ya vidhibiti vya nenosiri hutumika kama programu ya kihalalishaji pia, kwa hivyo hakuna sababu yoyote ya kulipia. Programu za 2FA kwa kawaida hutumia manenosiri ya mara moja yanayotegemea muda (TOTP), manenosiri ya kipekee ya nambari yanayotolewa na kanuni. Hii inamaanisha kuwa zinatumika mara moja, na ni halali kwa muda mfupi tu. Kwa kweli, programu nyingi za 2FA huonyesha saa ya kuhesabu kurudi nyuma, kwa kawaida kwa sekunde 30, ikibainisha wakati msimbo utabadilika. Katika hali hizi, kigezo mbadala ni simu yako ya mkononi, kitu ambacho wewe (kwa kawaida) unamiliki.

Huenda pia ukakumbana na "taarifa msukumo inayoambatana na 2FA," ambayo ni kawaida kwa waajiri na huduma kama vile Duo au Okta, lakini unaweza kuwa tayari umeitumia kwenye akaunti ya Google, Apple au Microsoft. Pia ni maarufu kwa huduma

za michezo ya kamari, kama vile Steam na Blizzard. Kwa kutumia 2FA inayotokana na msukumo, huduma inaweza kutuma kidokezo kwa mojawapo ya vifaa vyako wakati wa kuingia. Kidokezo hiki kitaonyesha kuwa mtu (labda wewe) anajaribu kuingia, na eneo linalokadiriwa la jaribio la kuingia. Kisha unaweza kuidhinisha au kukataa jaribio hilo.

Kigezo mbadala kinaweza pia kuwa kifaa kingine halisi ambacho unanunua kivyake, kinachoitwa ufunguo wa usalama. Funguo za usalama huchomekwa kwenye kompyuta au simu yako kupitia USB, au kuunganishwa kwenye simu bila waya kwa kutumia NFC. Kama programu zilizotajwa hapo juu, unazisajili kwenye wavuti, na huwezi kuingia kwenye wavuti hiyo bila kuweka ufunguo huo. Funguo za usalama ni aina ya 2FA thabiti zaidi, lakini hazitumiki sana kwenye wavuti kama chaguo zingine.

Mara tu unapojijumuisha kutumia 2FA, utahitaji kuweka nenosiri lako kisha kigezo mbadala—msimbo uliotumwa kwa SMS au kutolewa na programu yako ya 2FA, au ufunguo wa usalama—ili uingie katika akaunti yako.

Kwa nini Niwezeshe 2FA?

2FA hukupa usalama zaidi wa akaunti. Hata kama mtu angepata nenosiri lako, hangeweza kufikia akaunti yako isipokuwa pia awe na simu yako ya rununu au njia nyingine mbadala ya uhalalishaji. Hili ni muhimu hasa kwa vile uvamizi wa data unaojumuisha manenosiri ya mtumiaji ni jambo la kawaida. Wavuti huvamiwa kila wakati na kufichua nenosiri na jina la mtumiaji la mtu. 2FA si njia mbadala ya kutumia manenosiri thabiti na ya kipekee, lakini inaweza kutoa safu ndogo ya ziada ya usalama iwapo mtu ataweka jina la mtumiaji na nenosiri lako kwenye wavuti tofauti.

Zaidi ya hayo, uthibitishaji wa ufunguo wa usalama wa 2FA na ufunguo nywila ni ufanisi wa kuzuia utapeli data, kwa sababu ufunguo hauwezi kutumika kwenye wavuti ambayo haujasajiliwa. Lakini sivyo ilivyo kwa aina nyingine za 2FA, kama vile misimbo inayotolewa katika programu au na SMS. Katika miaka ya hivi karibuni, mashambulizi ya utapeli data yamekua ya kisasa kiasi cha kuomba misimbo ya 2FA, ambayo SMS na programu za kithibitishaji hazina ulinzi dhidi yake.

Je, Kuna Mapungufu ya Kutumia 2FA?

Ijapokuwa 2FA inatoa njia salama zaidi za uhalalishaji, kuna ongezeko la hatari ya kunyimwa ufikiaji wa akaunti yako. Kwa mfano, ukipoteza simu yako, ukibadilisha nambari yako ya simu, au ukisafiri kwenda nchi bila kuwasha ulandaji unaweza kupoteza idhini ya kufikia akaunti zako. Hii ni kweli pia kwa funguo za usalama, ambayo inaweza kuwa rahisi kupoteza kuliko simu.

Huduma nyingi za 2FA hutoa orodha fupi ya misimbo ya "chelezo" au "rejeshi" inayotumiwa mara moja tu. Kila msimbo hutumika mara moja haswa ili kuingia kwenye akaunti yako, na haiwezi kutumika tena baada ya hapo. Ikiwa una wasiwasi kuhusu kupoteza ufikiaji wa simu yako au kifaa kingine cha uthibitishaji, chapisha na ubebe misimbo. Bado itatumika kama "kitu ulicho nacho," mradi tu utengeneze nakala moja, na kuiweka karibu. Kumbuka kuweka misimbo salama na uhakikishe kuwa hakuna mtu mwingine anayeiona au anayeweza kuifikia wakati wowote. Ukitumia au kupoteza misimbo yako ya hifadhi rudufu, unaweza kutengeneza orodha mpya utakapoweza kuingia katika akaunti yako wakati mwingine.

Baadhi ya programu za simu za 2FA hutatua tatizo hili kwa kutoa chaguo la kuhifadhi nakala za taarifa zinazotoa misimbo ya mara moja. Kwa hivyo, ukipoteza simu yako, unaweza kupata hifadhi rudufu. Kwa watu wengi, kuhifadhi nakala za misimbo yao ya kithibitishaji ni wazo zuri. Lakini unaweza kupendelea kutohifadhi nakala za misimbo ya kithibitishaji ikiwa una wasiwasi kuhusu usalama wa huduma unapozihifadhi, na una uhakika hutapoteza au kuvunja simu yako. Ukiziwasha, angalia hati za programu ili kuhakikisha kuwa inatumia usimbaji fiche kutoka kwa mtuma ujumbe hadi mpokeaji kwa hifadhi rudufu hizo.

SMS 2FA ni bora kuliko kutokuwa na chochote, lakini inaweza kuwa na matatizo kwa sababu ujumbe wa SMS si salama sana. Inawezekana kwa mshambuliaji ambaye ana ujuzi wa hali ya juu na ana uwezo wa kufikia mtandao wa simu (kama vile shirika la kijasusi au operesheni ya uhalifu uliopangwa) kuchukua na kutumia misimbo inayotumwa kwa SMS. Pia kumekuwa na matukio ambapo mshambuliaji asiye na ujuzi wa hali ya juu (kama vile mtu binafsi) ameweza kusambaza simu zilizopigwa au ujumbe mfupi uliokusudiwa kwa nambari moja hadi kwa nambari yake, au kufikia huduma za kampuni za simu zinazoonyesha ujumbe mfupi wa maandishi uliotumwa kwa nambari ya simu bila kuhitaji kuwa na simu. Ubadilishaji wa SIM pia ni tatizo linaloweza kutokea, ambalo hutokea mtu anapohamisha nambari yako ya simu hadi kwa kifaa anachodhibiti, kwa kudanganya mtoa huduma wako wa simu (au kwa kuwa mtu wa ndani). Baada ya kufanya hivyo, wanaweza kufikia misimbo yoyote ya SMS 2FA, au mbaya zaidi, kuweka upya nenosiri kupitia SMS. Tume ya Biashara ya Shirikisho imejaribu kuelekeza kampuni kuepuka 2FA inayotumia SMS.

Inapowezekana, chagua kutumia programu ya kihalalishi, ufunguo nywila au ufunguo wa usalama badala ya SMS. Unapaswa pia kuwasiliana na mtoa huduma wako wa simu ili kuona kama wanatoa baadhi ya zana za kulinda dhidi ya ubadilishaji wa SIM. Hii inaweza kuwa PIN au nenosiri la maneno unalopaswa kutoa unapopigia usaidizi kwa wateja kufanya mabadiliko.

Zaidi ya hayo, kutumia 2FA inayotegemea SMS inamaanisha kuwa unaweza kuwa unakabidhi maelezo zaidi kwa huduma kuliko vile unavyoridhika nayo. Tuseme unatumia TikTok, na umejisajili kwa kutumia jina bandia. Hata ukiepuka kwa uangalifu kuipa TikTok maelezo yako ya utambulisho, na hata ikiwa unapata huduma kupitia Tor au VPN pekee, ikiwa utawasha SMS 2FA, TikTok lazima iwe na rekodi ya nambari yako ya simu. Hiyo inamaanisha kwamba, ikiwa italazimishwa na mahakama, TikTok inaweza kukuunganisha na akaunti yako kupitia nambari yako ya simu. Hili huenda lisiwe tatizo kwako, hasa ikiwa tayari unatumia jina lako halali kwenye huduma fulani, lakini ikiwa kudumisha kutokujulikana kwako ni muhimu, fikiria kwa uangalifu kuhusu kutumia SMS 2FA.

Hata baada ya kuwezesha 2FA, hakikisha bado unatumia kidhibiti cha nenosiri kuunda manenosiri thabiti na ya kipekee. Tazama mwongozo wetu wa kuunda manenosiri thabiti kwa vidokezo.

Vipi Kuhusu Funguo Nywila?

Funguo nywila ni chaguo jipya zaidi la kuingia ambalo hutoa usalama kamili wa 2FA, ulio na masumbuko machache sana. Ufunguo nywila ni takriban baiti 100-1400 za data nasibu, inayotolewa kwenye kifaa chako (kama vile simu, kipakatalishi, au ufunguo wa usalama) kwa madhumuni ya kuingia kwenye tovuti mahususi. Sio nenosiri wala 2FA, lakini inaweza kuchukua nafasi ya zote mbili kiutendaji.

Badala ya kuhitajika kuweka nenosiri lako na msimbo, funguo nywila huunda kigezo mbadala. Kila wakati unapotumia ufunguo nywila kuingia, kivinjari au mfumo wako wa uendeshaji unaweza kukuuliza uweke tena PIN ya kufungua kifaa. Ikiwa unatumia alama ya kidole au utambuzi wa uso ili kufungua kifaa chako, kivinjari chako badala yake kinaweza kukuomba uweke alama ya kidole upya au uonyeshe uso wako, ili kuyakinisha kuwa ni wewe unayeomba kuingia. Hiyo inatoa vigezo viwili vya uthibitishaji: kifaa ambacho huhifadhi ufunguo nywila wako ni kitu ulicho nacho, na kinaambatana na kitu unachokijua (PIN) au kitu ulicho (alama ya vidole au uso).

Ikiwa tayari unatumia 2FA kwenye wavuti fulani, ufunguo nywila utakuwa wa kufaa zaidi, na unaweza kuwa salama zaidi. SMS au mbinu za programu za kihalalishi cha 2FA zinaweza kushambuliwa na utapeli data, kwa kuwa tovuti bandia inaweza kukuuliza msimbo wa mara moja na kuupitisha kwenye tovuti halisi pamoja na nenosiri lako lililotapeliwa. Funguo nywila ni salama zaidi kuliko SMS au programu ya kihalalishi 2FA kwa sababu si rahisi kutapeliwa. Kivinjari chako kinatambua ni tovuti gani haswa inatumia ufunguo nywila fulani, na hakidanganyiki na wavuti bandia.

Je, Ninawezaje Kuwezesha 2FA?

Kumbuka: ikiwa bado hujaweka kidhibiti cha nenosiri na kuanza kutumia manenosiri ya kipekee kwa kila wavuti, fanya hivyo kwanza. Kutumia manenosiri ya kipekee kwa kila tovuti husaidia kwa kiasi kikubwa yenyewe.

Kuwasha 2FA hutofautiana katika jukwaa mbalimbali, kama vile istilahi inayotumika. Orodha pana ya tovuti zinazotumia 2FA inapatikana katikahttps://2fa.directory/. Mpango wa usalama wa kila mtu una mahitaji tofauti, na sio kila wavuti itakupa chaguo za aina tofauti za 2FA, lakini unapokuwa na chaguo nyingi, fikiria kila aina ya 2FA kwa mpangilio huu:

- **Funguo nywila** ni thabiti na ni rahisi kutumia (zinapotumika kwa usahihi), lakini bado ni teknolojia mpya ambayo haitolewi kila mara, na ambayo inaweza kusababisha matatizo katika mchakato wa kuingia wakati haijatekelezwa kwa usahihi na ambayo hufadhaisha kutatua.
- **Funguo za usalama** ni thabiti sana lakini zinaweza kuudhi kutumia kwa kuwa unahitaji kuwa na ufunguo huo halisi kila wakati.
- **Uhalalishaji unaotegemea taarifa msukumo** hutoa usalama wa wastani na ni rahisi kutumia, lakini unapatikana tu kwa idadi ndogo ya huduma za wavuti, na kwa kuwa haujasawazishwa, inaweza kumaanisha kwamba utaishia kuwa na kundi la programu tofauti za kihalalishaji kwenye simu yako.
- **Uhalalishaji wa programu/TOTP ya kihalalishaji** ni wa kawaida sana siku hizi, na hutoa usalama wa kiwango cha wastani lakini unaweza kuudhi kunakili/kubandika misimbo kati ya programu, hasa kwenye vifaa vya mkononi.
- **SMS** hutoa kiwango cha chini zaidi cha usalama, inaweza kuwa ya kuudhi kutumia katika hali fulani (au haiwezekani ikiwa huna huduma ya simu), lakini bado ni bora kuliko kutokuwa na chochote ikiwa ndilo chaguo pekee linalotolewa.

Mara tu unapokagua mipangilio ya akaunti na kupata chaguo la kuweasha 2FA, mara nyingi utahitaji kuchukua hatua moja zaidi ili kukamilisha mchakato. Jinsi hii inavyofanya kazi pia inategemea aina ya 2FA unayotumia na wavuti yenyewe, lakini kawaida hufanyika hivi:

- **Ukichagua kutumia ufunguo nywila**, wavuti utaunda na kuhifadhi ufunguo nywila kwenye kifaa unachotumia (kama vile simu au kipakatalishi chako). Utahitaji kuwa na kifaa hicho maalum ili kuingia ukitumia ufunguo nywila huo, ingawa baadhi ya vidhibiti vya nenosiri vitalandanisha ufunguo nywila kwenye vifaa vyote. Huduma nyingi *pia* bado zitahitaji uwe na jina la mtumiaji na nenosiri, kwa hivyo bado unaweza kuhitaji kutumia aina nyingine ya 2FA kwa sasa.

- **Ukichagua ufunguo wa usalama**, utahitaji kuingiza ufunguo, hakikisha kuwa unataka kuunda kitambulisho (jambo hili hutegemea ufunguo wenyewe, lakini kwa kawaida inamaanisha kugonga ufunguo, au kubonyeza kitufe kilicho juu yake) na kisha ufuate maelekezo ya kukamilisha kuunganisha kwenye akaunti yako. Kumbuka kuwa baadhi ya tovuti zinahitaji aina mbadala ya 2FA kama hifadhi rudufu unapotumia ufunguo wa usalama, kwa hivyo huenda ukahitaji kusanidi hiyo kwanza.
- **Ikiwa unatumia programu ya kihalalishaji cha simu ya rununu**, utahitaji kuchanganua msimbo wa QR kwenye skrini ya kompyuta yako ukitumia simu yako. Baada ya hapo simu yako itaanza kutoa misimbo inayobadilika, na itabidi uweke mojawapo ya misimbo hiyo ili kuthibitisha kuwa umekamilisha mchakato huu kwa mafanikio.
- **Ukiwasha SMS**, utapokea msimbo ambao utahitaji kuandika ili kukamilisha mchakato wa kuwasha 2FA.

Mchakato wa kuwasha 2FA unaweza kuogepesha unapoanza, lakini unaweza kuurahisisha kwa kuugawanya katika miradi midogo.

Anza na akaunti zako za baruapepe. Kwa sababu huduma nyingi huruhusu uwekaji upya nenosiri kupitia baruapepe, mtu yeyote anayechukua anwani yako anaweza kuweka upya nenosiri ili kuingia katika huduma nyingine, kwa hivyo ndiyo huduma muhimu zaidi kulinda kwanza. Kisha, isanidi kwa ajili ya huduma zozote zinazohifadhi nakala za faili zako—kama vile akaunti ya Apple, Google au Microsoft. Baada ya hapo, mitandao ya kijamii na programu za mawasiliano zinapaswa kuwa zinafuata kuzipa kipaumbele kuziwekea usalama. Kisha, unaweza kuweka alama kwenye orodha kwenye wavuti ya saraka ya 2FA ili kutafuta wavuti unazotumia.