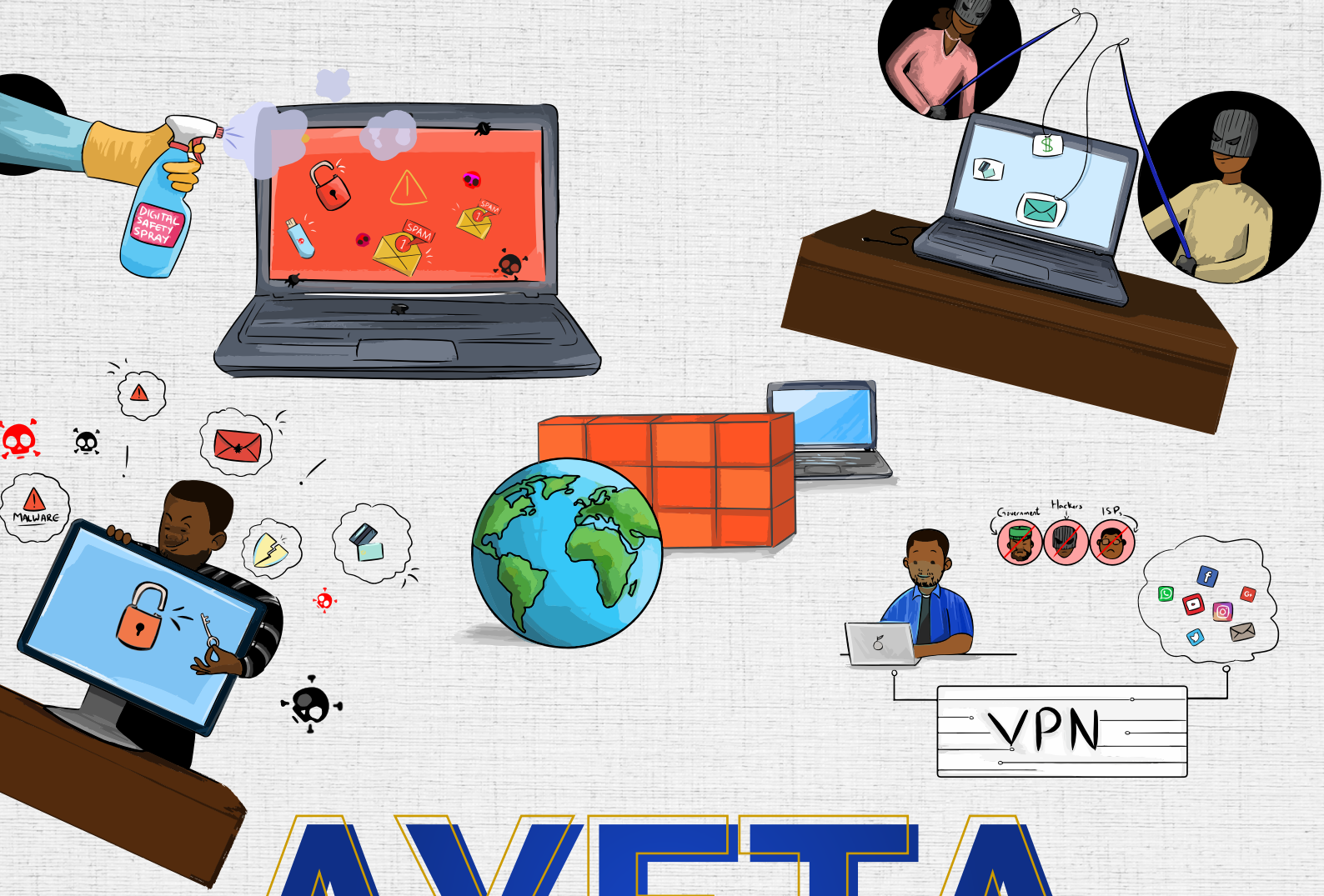
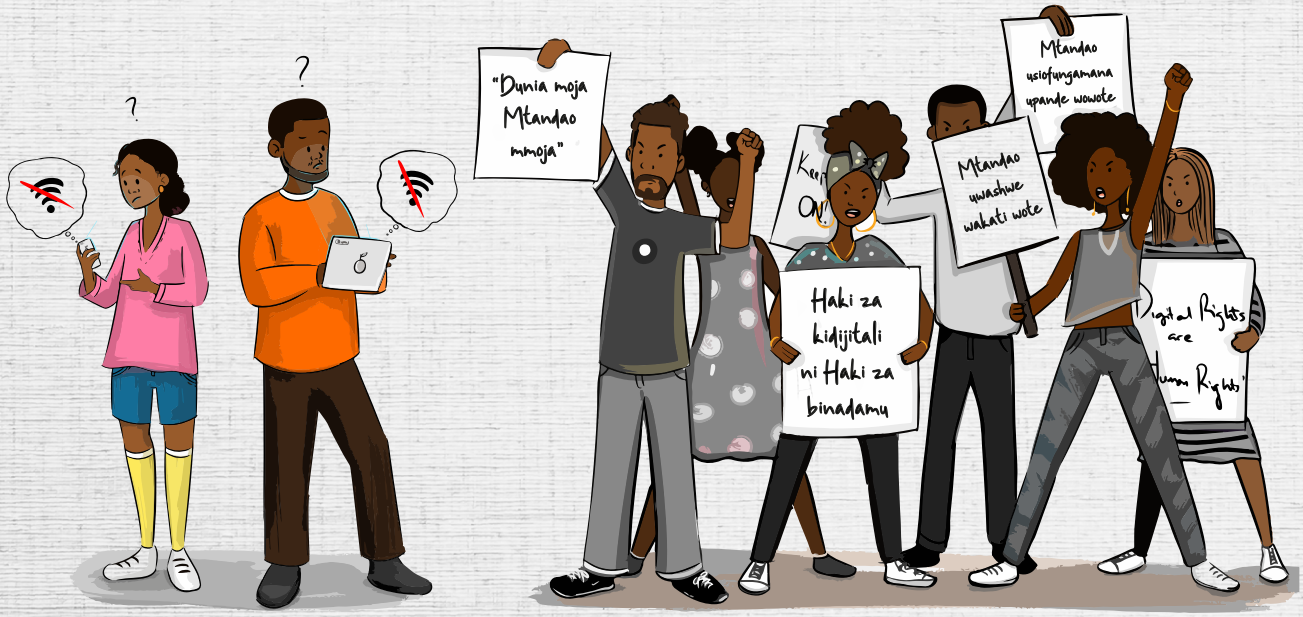


AYETA

Kifaa cha Zana cha Haki za Kidijitali



Kingdom of the Netherlands

PARADIGM INITIATIVE

Stanford PACS
Center on Philanthropy and Civil Society
Digital Civil Society Lab

DIBAJI

Kadri watetezi wa haki za kidijitali wanavyozidi kujali kuhusu haki zao na usalama wao kidijitali, ni muhimu waweze kuchukua hatua mwafaka za kujilinda wanapokuwa kwenye majukumu yao ya kila siku. Kifaa hiki cha zana kinatoa vidokezo vya usalama wa kidijitali na hatua zinazoweza kuchukuliwa dhidi ya vitisho vinavyoweza kujitokeza. Kifaa hiki pia kinajumuisha wasifu wa wanaharakati wanaojihusisha na masuala ya usalama wa kidijitali, ratiba ya matukio mahususi ya kujadiliana kuhusu haki za kidijitali barani Afrika, na mwisho, japo si kwa umuhimu, kimeweka fungo tovuti za kuunganisha wadau na rasilimali elemishi kama vile marejeo ya baadhi ya mafunzo ya kifani ya usalama wa kidijitali kutoka nchi mbalimbali barani Afrika, muhtasari wa sera mbalimbali, na mkusanyiko wa taarifa kwa vyombo vya habari, pamoja na wito wa pamoja wa washirika kwa vyombo vya habari. Kifaa hiki kina sehemu maalum iliyotengewa kuzungumzia adha za uvurugaji ovyo wa mtandao na hatua zinazoweza kuchukuliwa kuepuka uvurugaji huo, namna ya kuhifadhi kumbukumbu za matukio hayo pamoja na jinsi ya kuhifadhi kumbukumbu, na rasilimali za utetezi za matukioa kama hayo.

Kifaa hiki kimetengenezwa kama mradi wa 2020 wa Stanford Digital Civil Society Fellowship na kupata msaada wa nyongeza kutoka Netherlands Human Rights Fund.
‘Gbenga Sesan na Bonface Witaba waliongoza uratibu wa mradi, ukuzaji wa mtaala, uandishi na usahihishaji, huku wakipewa msaada na timu ya watu wa Paradigm Initiative (PIN). Usomaji wa makini na uhariri wa lugha ya kiingereza ulifanywa na Fisayo Alo. Shukrani za pekee ziwaendee Ashnah Kalemera (CIPESA), Berhan Taye (AccessNow), Demba Kandeh (School of Journalism & Digital Media, University of The Gambia) Chuo Kikuu cha The Gambia, na Ephraim Kenyanito (Article19 UK). Wengine ni Koliwe Majama (AfDEC), Liz Orembo (KICTANet), Neema Iyer (Pollicy), Neil Blazevic, Oluwatosin Alagbe (PTCIJ), Oyinkansola Akintola-Bello (Co-creation Hub), Ronald Kekembo (FrontlineDefenders) na Vivian Affoah (Media Foundation for West Africa) kwa kukagua na kutoa maoni katika toleo kielelezo la kifaa hiki. Maoni yenu maridhawa yametusaidia kuboresha toleo hili.

Kifaa hiki cha zana kimebuniwa kwa lengo kuu la kushughulikia hitaji linaloongezeka la watetezi wa haki za kidijitali, waandishi wa habari, wafichuzi, na wengine wanaofanya kazi za habari nyeti dunia ya kusini. Shirika la Paradigm Initiative (PIN) limejitolea kutayarisha kifaa hiki cha zana kinachoeleweka kwa urahisi na kinachovutia kusoma na ambacho kitasalia kuwa rasilimali hai inayoweza kufanyiwa matoleo mapya kila wakati yanapohitajika.
Tunategemea kupata mrejesho, maoni, mawazo, ukosoaji, na simulizi nyingine ili kufanikisha lengo hili.
Tafadhali tuma mrejesho au maoni kwenda: hello@ayeta.africa

YALIYOMO

Sura ya Kwanza

Haki za Kidijitali

1.1 Usuli

Ujio wa mtandao mnamo mwaka wa 1989 na ufunguliwaji wake kwa ulimwengu kumeshuhuhudia watetezi wa haki za binadamu wakiibua mbinu mpya za kimtandao za kuendeleza uhuru wa kusema, uhuru wa kuwasiliana na pia kukuza uwezo wa jamii ya kidijitali kutumia mtandao kwa ufanisi. Leo hii, mtandao unaonekana kuleta faida kubwa kwenye jamii iliyotamalaki zaidi ya nusu ya ulimwengu kwa kuweza kuiunganisha kimawasiliano. Hata hivyo, hali imezidi kuwa tete sasa na ongezeko ya matukio yanayozua changamoto kwa wanaharakati, watetezi wa haki za Binadamu, wanahabari na wakosoaji serikali.
Serikali za kiimla ambazo zimeishia kutumia zana za kidijitali na mbinu kama vile uzimaji mtandao kwa makusudi, kudhibiti na kukagua maudhui mtandaoni na ufuatiliaji wa karibu wa watumiaji wa mtandao ili kubana uhuru wao wa kusema.

Kielelezo 1: Wahusika wa Afrika Wakitetea Haki za Kidijitali

Kama ilivyobainika katika Ripoti ya Haki za Kidijitali ya Afrika (Digital Rights in Africa report)[1], iliyotayarishwa na Paradigm Initiative ya 2019, imenukuliwa hivi, “Katika muongo mmoja uliopita, kumekuwa na ongezeko la athari kwa mashirika ya Kiafrika yanayotetea haki za kidijitali hasa katika kupunguza gharama za matumizi, kuongeza ubora wa maunganisho yasiyoyumba yumba, kulinda faragha za watumiaji na uhuru wao wa maoni, kusema na kuwasiliana bila kikwazo. Kinyume kabisa na ufufuaji huu wa haki za kidijitali, na ukuaji wa matumizi yake kwa bara hili, ujio wa mtandao umekabiliwa na udhibiti mkali ili kudumisha nguvu za kisiasa. Serikali nyingi zimekuwa zikihujumu haki za matumizi ya mtandao ili kuimarisha mamlaka za kisiasa juu ya raia. “.

Ripoti ya CIPESA ya 2019 inafichua kuwa serikali 22 za Afrika ziliamuru kuvurugwa kwa upatikanaji wa mtandao katika miaka minne iliyopita na kwamba tangu kuanza kwa 2019, nchi 6 za Afrika - Algeria, Jamhuri ya Kidemokrasia ya Kongo (DR Congo), Chad, Gabon, Sudan na Zimbabwe zilishinikiza kufungwa kabisa kwa mtandao na wakati huo huo, nchi kadhaa, zimeendelea kuchukua hatua mbalimbali za kuminya haki za upatikanaji wa habari mtandaoni. [2] LVitendo vya nchi hizi vinakiuka moja kwa moja kanuni za Azimio la Afrika juu ya Haki na Uhuru wa Mtandao (African Declaration on Internet Rights and Freedoms (AfDec) Principles),[3] na zile za Azimio la Haki za Binadamu za Ulimwengu (General Assembly Resolution 217 A).[4]

1.2 Haki za Kidijitali ni nini?

Haki za kidijitali kimsingi ni haki za binadamu. Ni haki za faragha binafsi na uhuru wa kusema kwa kutumia mtandao na kwa kweli ni mwendelezo wa haki zisizonyang’anyika kama zilivyoainishwa katika Azimio la Umoja wa Mataifa la Haki za Binadamu.[5] Haki za kidijitali ni pamoja na zile za watu binafsi kuwa na kompyuta na uwezo wa kuzitumia na kuchapisha yaliyomo kwenye vifaa hivi vya kidijitali. Hii inamaanisha kwamba ni haki ya msingi kwa yeyote kutumia vifaa vya kidijitali bila kubugudhiwa kwa kuzingatia haki za faragha za kila mtu. Kulingana na Umoja wa Mataifa, kuzuia au kuvuruga shughuli za mtandao kunakiuka kabisa haki hizi na ni kinyume cha sheria za kimataifa.[6]

1.3 Hati, Matamko na Itifaki za Kimataifa kuhusu Haki za Kidijitali / Haki za Binadamu

Haki za kidijitali na haki za binadamu lazima zioanishwe ili misingi iliyopo ya kanuni za haki za binadamu itafsirike katika mazingira ya mtandao na katika wigo wote wa nyanja za utengenezaji wa sera za matumizi ya mtandao.

1 https://paradigmhq.org/download/dra19/
2 https://cipesa.org/2019/03/despots-and-disruptions-five-dimensions-of-internet-shutdowns-in-africa/
3 https://africaninternetrights.org/articles/
4 http://www.un.org/en/ga/search/view_doc.asp?symbol=A/RES/217%28III%29
5 http://www.un.org/en/ga/search/view_doc.asp?symbol=A/RES/217%28III%29
6 http://www2.ohchr.org/english/bodies/hrcouncil/docs/17session/A.HRC.17.27_en.pdf

1. Azimio la Haki za Binadamu la Umoja wa Mataifa (UN)

Tamko la Ulimwengu la Haki za Binadamu (Universal Declaration of Human Rights - UDHR) ni hati muhimu katika historia ya haki za binadamu.Tamko hili lilitayarishwa na wawakilishi tofauti walio kwenye nyanja za kisheria na kitamaduni kutoka maeneo yote ya ulimwengu, Azimio hilo lilitangazwa na Baraza Kuu la Umoja wa Mataifa huko Paris mnamo tarehe 10 Desemba 1948 (Azimio la Mkutano Mkuu 217 A) Azimio hili ni kielelezo kinachodhihirisha upeo wa pamoja ulioleta mafanikio kwa watu wote wa mataifa yote katika kutetea haki za binadamu. Tamko linaweka wazi, kwa mara ya kwanza, haki za kimsingi za binadamu zinazopaswa kulindwa kote ulimwenguni na limetafsiriwa katika lugha zaidi ya 500.[7]

2. African Charter on Human and People's Rights

Hati ya Mkataba wa Afrika kuhusu Haki za Binadamu na za Watu (pia unajulikana kama Mkataba wa Banjul) ni chombo cha kimataifa cha haki za binadamu ambacho kinatarajiwa kukuza na kulinda haki za binadamu na uhuru wa kawaida katika bara la Afrika.Hati hiyo ilipitishwa mnamo Juni 1, 1981, na ilianza kutumika Oktoba 21, 1986. Hata hivyo, hati inayoanzisha Shirika la Umoja wa Afrika (OAU) haikuweka wazi wajibu wowote kwa nchi wanachama wa kulinda haki za binadamu japo hati hiyo inasisitiza mataifa ya Afrika kuzingatia haki za binadamu kama zilivyoainishwa katika Azimio la Ulimwengu la Haki za Binadamu katika mahusiano yao ya kimataifa.[8]

3. African Declaration on Digital Rights

Azimio la Afrika kuhusu Haki na Uhuru wa Kidijitali ni mpango wa bara lote la Afrika katika kukuza viwango vya haki za binadamu na kanuni za uwazi katika uundaji wa sera za mtandao na utekelezaji wake katika Bara hili. Azimio limekusudia kufafanua kanuni ambazo ni muhimu katika kutetea haki za binadamu na za watu kwenye mtandao na kuumba mazingira ya mtandao ambayo yatasaidia kukidhi kwa ubora zaidi mahitaji na malengo ya maendeleo ya kijamii na kiuchumi ya Afrika. Azimio hilo linaimarika zaidi kutokana na uwepo wa nyaraka zinazotambulika mno za haki za binadamu za Kiafrika zilizohifadhiwa vizuri ikiwa ni pamoja na Hati ya Kiafrika ya Haki za Binadamu na Watu ya 1981, (African Charter on Human and Peoples' Rights of 1981) Azimio la Windhoek juu ya Kukuza Tasnia ya Uandishi ya Kiafrika iliyo Jumlishi na yenye Kujitegemea ya 1991 (Windhoek Declaration on Promoting an Independent and Pluralistic African Press of 1991) Mkataba wa Afrika juu ya Utangazaji wa mwaka 2001 (African Charter on Broadcasting of 2001), Kanuni juu ya Uhuru wa Kusema katika Afrika ya 2002 (Declaration of Principles on Freedom of Expression in Africa of 2002) na Azimio la Jukwaa la Afrika juu ya Upatikanaji wa Taarifa ya 2011 (African Platform on Access to Information Declaration of 2011).[9]

4. African Union Declaration of Principles on Freedom of Expression and Access to Information in Africa

7 https://www.un.org/en/universal-declaration-human-rights/
8 https://au.int/en/treaties/african-charter-human-and-peoples-rights
9 https://africaninternetrights.org/about/

Azimio la kanuni za uhuru wa kusema barani Afrika lilipitishwa mnamo mwaka 2002 na Tume ya Afrika ya Haki za Binadamu na Watu. Hati hiyo inatumika kama kigezo cha kutathmini rekodi za nchi za kiafrika katika kutathmini utekelezaji wa malengo ya Tume hiyo. Pia, Azimio hili limekuwa mahala pazuri pa kupata kumbukumbu za utekelezaji wa matakwa ya kisheria ya Tume kwa serikali mbalimbali za Afrika.[10]

5. African Union Declaration on Internet Governance

Azimio la Umoja wa Afrika kuhusu Utawala wa Mtandao lilitengenezwa kupitia mchakato wa mashauriano ya kuunda mazingira mazuri na wezeshi yaliyolenga kubainisha manufaa ya kiuchumi yatokanayo na matumizi ya dijitali kwa wadau wa Afrika. Mashauriano haya ya pamoja yalijadili maswala muhimu yanayoibuka mtandaoni na hivyo kuchangia maendeleo ya Mtandao na hatimaye kuwezesha utengenezaji wa sera zinazozingatia mahitaji ya Afrika yaliyopo.

Vilevile, Azimio hilo linatoa kanuni elekezi kwa wadau, linabeba mtazamo wa pamoja na ni msingi imara wa muendelezo wa mazungumzo na mijadala hapo baadaye yenye lengo la kuwa na uelewa wa pamoja kuhusu mustakabali wa Mtandao kama waafrika na kwa mtazamo wa kiafrika.[11]

6. ECOWAS Protocol on Democracy and Good Governance

Itifaki ya ECOWAS kuhusu Demokrasia na Utawala Bora ilipitishwa na Wakuu wa Nchi na Serikali wanachama wa ECOWAS Afrika Magharibi mnamo Desemba 2001. Itifaki hii ni kama nyongeza ya itifaki inayohusiana na utaratibu wa kuzuia kutokea kwa migogoro, usimamizi wake, utatuzi na ulinzi wa amani na usalama (1999) yaani (Protocol relating to the Mechanism for Conflict Prevention, Management, Resolution, Peacekeeping and Security (1999).[12]

1.4 Watendaji wa Usalama wa Kidijitali

Kielelezo 2: Wanaharakati wa usalama wa kidijitali

10 https://www.achpr.org/public/Document/file/English/draft_declaration_of_principles_on_freedom_of_expression_in_africa_eng.pdf
11 https://au.int/sites/default/files/newseventsworkingdocuments/33025-wd- african_declaration_on_internet_governance_en_0.pdf
12 https://www.ohchr.org/EN/Issues/RuleOfLaw/CompilationDemocracy/Pages/ECOWASProtocol.aspx

Watendaji wengi wa usalama wa kidijitali wana mbinu anuwai za kupunguza madhara na hatari wanazoweza kupata waandishi wa habari na watetezi wa haki za binadamu wanapotumia mtandao. Zaidi ya hivyo, mashirika haya yafuatayo ambayo unaweza kuwasiliana nayo yanaweza kukupa ushauri au msaada mwingine kwa maswala yanayohusiana na ukiukwaji wa matumizi ya takwimu, kuripoti matukio, na maswala ya sera n.k.

1. **AccessNow - https://www.accessnow.org/**
   AccessNow hutoa msaada wa masaa ishirini na nne kwa siku kwa kutumia namba ya simu maalum kuhusu usalama wa kidijitali, hufanya uchambuzi na utetezi wa sera zitokanazo na misingi ya ushahidi waukiukwaji wa haki za kidijitali na kutoa misaada kwa mashirika ya ngazi za mashina vijijini na vikundi vya wanaharakati vinavyofanya kazi na watu au jamii zilizo katika hatari zaidi ya kunyimwa haki za kidijitali.

2. **AfricanDefenders - https://africandefenders.org/**
   Huu ni Mtandao wa watetezi wa haki za binadamu wa mashirika matano katika baadhi ya nchi za Afrika yaliyojitolea kukuza na kulinda watetezi wa haki za binadamu (HRDs) kote katika bara la Afrika.

3. **Africtivists - https://www.africtivistes.org/**
   Africtivists ni mtandao wa wanaharakati wa mtandaoni na wanablogu wa demokrasia, unaojumuisha jamii ya wanaharakati 200 kutoka nchi 35 tofauti za Afrika..

4. **Association for Progressive Communication (APC) - https://www.apc.org/**
   APC wanafanya kazi kujenga ulimwengu ambao watu wote wanafikiwa kimawasiliano kirahisi, kwa usawa na kwa gharama nafuu. Uwezo huo unatokana na kutumia mbinu za kibunifu wa matumizi ya teknolojia ya habari (ICTs) katika kuboresha maisha ya watu na hivyo kuunda jamii za kidemokrasia na usawa zaidi.

5. **Association of Media Women in Kenya (AMWIK) - http://amwik.org/**
   AMWIK ni Chama cha Wanawake cha Vyombo vya Habari kinacholenga kuongeza taswira chanya ya wanawake katika jamii na kukuza ushiriki wao katika nafasi za uongozi na zile za maamuzi.

6. **Article 19 - https://www.article19.org/**
   Article 19 ni Kikundi kinachofanya kazi kuunganisha uhuru wa kusema na uhuru wa kujua kinachokusudia kuwawezesha watu wote kila mahali wawe na uwezo wa kusema kwa uhuru na waweze kushiriki kikamilifu katika shughuli za umma kama wanajamii bila hofu au kubaguliwa.

7. **Cc-Hub - https://cchubnigeria.com/**

Kwa watu wengi inajulikana kama Cc-HUB au HUB. Hili ni jukwaa ambalo watu wanaozingatia teknolojia wanashiriki kuchangia maoni juu ya kutatua shida za kijamii nchini Nigeria..

8. Central Africa Human Rights Defenders Network (Réseau des Défenseurs des Droits Humains en Afrique Centrale – REDHAC) - https://defenddefenders.org/africandefenders/

Mtandao huu wa watetezi wa haki za binadamu wa Afrika ya Kati unashirikiana na kuimarisha kazi ya watetezi wa haki za binadamu (HRDs) wengine kwa lengo la kupunguza unyonge na hatari zinazowakabili na vilevile kuongeza uelewa wao juu ya hali ya haki za binadamu katika Afrika ya Kati.

9. Collaboration on International ICT Policy in East and Southern Africa (CIPESA) - https://cipesa.org/

Ushirikiano juu ya Sera ya Kimataifa ya Teknolojia Mashariki na Kusini mwa Afrika (CIPESA) ni shirika lenye makao yake makuu Kampala Uganda linalojishughulisha na ushauri wa sera za teknolojia (ICT) zenye kuleta ufanisi katika eneo la Mashariki na Kusini mwa Afrika.

10. Committee to Protect Journalists (CPJ) - https://cpj.org/

Kamati ya Kulinda Wanahabari (Committee to Protect Journalists) ni shirika huru la Marekani lisilo la kiserikali wala faida, lililoko jiji la New York na lenye uwakilishi katika nchi nyingi duniani. Jukumu la CPJ ni kukuza uhuru wa vyombo vya habari na kutetea haki za waandishi wa habari ulimwenguni kote.

11. Cyber Security Africa - https://www.cybersecurityafrica.com/

Cyber security Africa wanatoa huduma iliyo kamili ya ushauri bobezi na mbinu anuwai kusaidia mashirika kulinda mali zao muhimu za kidijitali dhidi ya hatari za usalama za kimtandao.

12. Defend Defenders - https://defenddefenders.org/

Defend Defenders ni watetea watetezi ambao wapo kwa makusudi ya kulinda na kuimarisha watetezi na utetezi wa haki za binadamu katika maeneo ya mashariki na Pembe ya Kaskazini mwa Afrika.

13. Digital Security Alliance (DSA) – https://defendersprotection.org/the-digital-security-alliance/

Huu ni muungano wa mashirika na wataalam binafsi wanaojihusisha na usalama wa kidijitali wanaofanya kazi ya kulinda mali na vifaa vya kidijitali vya asasi za kiraia, utetezi wa haki za binadamu, utetezi wa waandishi wa habari na wanaharakati wengine dhidi

ya vitisho vinavyo fanywa na mashirika yenye nguvu, wahalifu walio hatari, serikali na watendaji wengine wasio wa serikali.

14. Freedom House - https://freedomhouse.org/

Hili ni shirika la Kimarekani lisilo la kiserikali na lisilo la faida ambalo hufanya utafiti na utetezi wa demokrasia, uhuru wa kisiasa, na haki za binadamu.

15. Frontline Defenders - https://www.frontlinedefenders.org/

Hili ni shirika la haki za binadamu la Kiairishi lililoanzishwa huko Dublin, Ireland mnamo mwaka 2001. Lengo kuu la shirika hili ni kulinda wale wanaofanya kazi kwa utulivu bila vurugu kupambania haki za binadamu kama ilivyoainishwa katika Azimio la Haki za Binadamu la Umoja wa Mataifa.

16. Gambia Cyber Security Alliance - http://gamcybersecurityalliance.com/

Muungano huu wa Gambia unalenga kujenga na kuongeza uelewa wa Wagambia juu ya usalama katika matumizi ya mtandao, vitisho vya mtandao, ujasusi na kuwawezesha kwa kuwapa mbinu za matumizi ya kiusalama na kiulinzi mtandaoni.

17. Gambia Press Union - http://www.gambiapressunion.org/our-work/

Gambia Press Union ni chama cha wafanyikazi ambao ni waandishi wa habari huko Gambia, kilichoanzishwa mnamo 1978 na kundi la waandishi wa habari. Dhamira ya Chama hiki ni kukuza uhuru na umahiri wa uandishi na vyombo vya habari.

18. Human Rights Defenders Network - Sierra Leone (HRDN-SL) https://namati.org/network/organization/pan-african-human-rights-defenders-network/

HRDN-SL ni muungano wa asasi, mashirika ya kiraia na watu binafsi wanaofanya kazi ya kulinda na kukuza haki za binadamu nchini Sierra Leone. Muungano huu uliundwa Siera Leone kama tawi la Mtandao wa Watetezi wa Haki za Binadamu wa Afrika yote (Pan African Human Rights Defenders Network (PAHRDN) wenye makao makuu nchini Uganda na vilevile mtandao mwingine wa aina hiyo wa Afrika Magharibi yaani (West Africa Human Rights Defenders Network (WAHRDN) wenye makazi yake nchini Togo. Ushauri wa kitaalaam wa kuanzisha mtandao huu ulipatikana kutoka Shirika la Huduma za Kimataifa za Haki za Binadamu yaani International Service for Human Rights (ISHR) lenye makao makuu Geneva Uswisi.

19. Kenya ICT Action Network (KICTANET) - https://www.kictanet.or.ke

 Mtandao huu unahusisha jopo la wadau mbalimbali wachemsha bongo wenye utashi na kuvutiwa katika kubuni sera na kanuni za matumizi sahihi na salama ya teknolojia (ICT)

Kazi ya KICTANET inaongozwa kwa kuzingatia nguzo nne ambazo ni utetezi wa sera,

kujenga uwezo, kufanya utafiti, na ushirikishwaji wa wadau. Pamoja na majukumu yaliyoainishwa, KICTANET imejiongeza na kuchukua nafasi ya kutafsiri maoni yanayowakilishwa na wadau wake kwa vitendo katika utatuzi wa changamoto zinazoikabili tasnia ya ya teknolojia.

20. Media Foundation for West Africa (MfWA) - https://www.mfwa.org/

Jukwaa hili la uandishi la Afrika Magharibi lilianzishwa mwaka 1997 mjini Accra, Ghana, MfWA ni shirika lisilo la kiserikali la kukuza na kutetea haki ya uhuru wa kusema kwa watu wote hasa vyombo vya habari na watetezi wa haki za binadamu Afrika Magharibi.

21. Media Legal Defense Initiative (MLDI) - https://www.mediadefence.org/

MLDI ni shirika lisilo la kiserikali lililoanzishwa mnamo mwaka 2008 kwa mintarafu ya kutoa msaada wa kisheria kwa waandishi wa habari na vyombo huru vya habari. Shirika hili linasaidia pia kutoa mafunzo ya kisheria kwa vyombo vya habari, kuhamasisha ubadilishanaji wa habari, kusaidia mbinu za kisheria na mikakati ya utetezi kwa wanasheria wanaofanya kazi kwenye kesi zinazohusu uhuru wa vyombo vya habari.

22. National Coalition of Human Rights Defenders – Kenya (NCHRD-K) - https://defenderscoalition.org/

Huu ni muungano wa kitaifa wa watetezi wa haki za binadamu ulioandikishwa kisheria katika Jamhuri ya Kenya kama shirika la kujitolea. Dhamira ya muungano huu ni kuimarisha uwezo wa watetezi wa haki za binadamu (Human Rights Defenders - HRDs) ili waweze kufanya kazi kwa ufanisi nchini na kupunguza hofu yao kwa hatari ya kuteswa.

23. Paradigm Initiative (PIN) - https://paradigmhq.org/

Paradigm Initiative ni wito wa kijamii ambao unasaidia kuunda mfumo unaowezeshwa na Tekinolojia (ICT) ili kutetea haki za kidijitali na kuboresha maisha kwa vijana wanaokosa huduma muhimu za kimaisha kwa kutumia mtandao. Programu ya utetezi wa haki za kidijitali ya PIN imejikita katika uendelezaji wa sera za umma zinazotetea uhuru wa mtandao barani Afrika..

24. Pollicy - https://pollicy.org/

Pollicy ni kampuni ya ushauri bobezi wa teknolojia inayolenga kuboresha utoaji wa huduma za kiserikali kupitia ushirikishwaji na ushiriki wenye tija wa raia.

25. Safe Sisters - https://safesisters.net/

Safe Sisters ni ushirika wa kidugu wa wanawake watetezi wa haki za binadamu, waandishi wa habari au wafanyikazi wa vyombo vya habari na wanaharakati. Ushirika unawafundisha wana kikundi kuelewa na kuzifanyia kazi changamoto za usalama wa kidijitali wanazokabiliana nazo katika kazi zao na maisha ya kila siku.

26. Women Human Rights Defenders (WHRD) - https://www.peacewomen.org/

HRD ni watetezi wa haki za binadamu za wanawake na pia ni watetezi wa haki za binadamu kwa watu wengine wowote lakini ambao hufanya kazi zaidi katika kutetea haki za wanawake au maswala ya kijinsia.

27. Women of Uganda Network (WOUGNET) - https://wougnet.org/

WOUGNET ni mtandao ulioanzishwa mnamo Mei 2000 kwa nia ya kujitolea kusaidia Mashirika ya Wanawake na wanawake wenyewe katika matumizi ya teknolojia ya habari na mawasiliano, utumiaji wa simu za mkononi, barua pepe na tovuti, na pia utumiaji wa "njia za jadi" kama vile redio, video na machapisho kwa namna inayowezesha ufikiaji mpana wa walengwa.

1.5 Hafla muhimu za Haki za Kidijitali

Kila mwaka, kote Afrika, hafla kadhaa za haki za kidijitali na usalama hufanyika. Hafla hizo huleta pamoja wadau kutoka asili za kiujuzi tofauti kujadili maswala ya sera, kinachojiri kuhusu mwelekeo wa haki za kidijitali na kutoa mafunzo ya vitendo.

Kielelezo 3: Hafla muhimu za haki za kidijitali

1. **African School on Internet Governance (AfriSIG):**
   Shule ya Kiafrika ya Utawala wa Mtandao hutoa mafunzo mbalimbali yanayo wapatia Waafrika fursa ya kupata maarifa na ujasiri wa kushiriki vyema katika michakato, mijadala ya kitaifa, kikanda na ulimwenguni inayohusu utawala wa mtandao
   https://www.apc.org/en/project/african-school-internet-governance-afrisig

2. **Cc-HUB Digital Security Demo Day:**
   Siku ya Maonyesho ya Usalama wa kidijitali huleta pamoja makampuni ya biashara, asasi za kiraia, wanafunzi na mashabiki wa usalama wa habari kutoka ndani na nje ya Lagos kushuhudia mubashara maonyesho ya mashambulio ya mtandaoni na hatua za kuyakabili kimtandao pia.
   https://cchubnigeria.com/cchub-hosts-first-cybersecurity-conference

3. **Digital Rights and Inclusion Forum (DRIF):**
   DRIF ni jukwaa la lugha mbili linalofanyika kila mwezi Aprili linalotayarishwa na Paradigm Initiative ambapo maswala magumu ya ulimwengu kuhusu haki za mtandao, haswa barani Afrika, yanajadiliwa na wadau kutoka asasi za kiraia, kampuni za teknolojia, serikali, wasomi na wadau wengine.
   https://drif.paradigmhq.org/

4. **East Africa Cyber Security Convention:**
   Huu ni Mkutano wa Usalama wa Mtandao wa Afrika Mashariki unaowapatia washiriki maarifa ya jinsi ya kujihami au kupunguza vitisho vya Usalama wa Mtandaoni.
   https://cloudsecurityalliance.org/csa_events/east-africa-cyber-security-convention/

5. **Forum on Internet Freedom in Africa (FIFAfrica):**
   Baraza la Uhuru wa Mtandao wa Afrika hutayarishwa na CIPESA na hufanyika mwezi Septemba kila mwaka kwa lengo la kukuza matumizi huru ya mtandao bila malipo kwa wote barani Afrika.
   https://cipesa.org/fifafrica/

6. **Mipango ya Kikanda / Shule za Utawala wa Mtandao**
   Shule ya Utawala wa Mtandao ya Afrika Mashariki
   East Africa School of Internet Governance (EASIG)
   Shule ya Utawala wa Mtandao ya Afrika Magharibi
   West Africa School of Internet Governance (WASIG)

7. **Mipango ya Kitaifa / Shule za Utawala wa Mtandao (National Initiatives/ Schools of Internet Governance)**
   Shule ya Kenya ya Utawala wa Mtandao (Kenya School of Internet Governance KeSIG)

Shule ya Utawala wa Mtandao ya Nigeria (Nigeria School of Internet Governance NSIG)
Shule ya Utawala wa Mtandao ya Sudan Kusini (South Sudan School of Internet Governance - SSSIG)
Shule ya Utawala wa Mtandao ya Tanzania (Tanzania School of Internet Governance (TzSIG)
Shule ya Wanawake ya Arusha ya Utawala wa Mtandao (Arusha Women School of Internet Governance (AruWSIG)

1.6 Mafunzo Zoefu ya Haki za Kidijitali

Yapo majaribio mengi ya serikali kukiuka haki za waandishi wa habari na watetezi wa haki za kidijitali kwa kutumia sheria, kufunga mtandao, na hatua za kimahakama kati ya njia nyingi nyingine. Hapa chini utaona baadhi ya funzo zilizochaguliwa (tazama fungo tovuti) nchini Nigeria, Cameroon, Tanzania na Zimbabwe.

https://tinyurl.com/y5p57qkw
https://tinyurl.com/y3fedl7f
https://tinyurl.com/y324dmeu
https://tinyurl.com/y63gbr3m

1.7 Mifano ya Sera Muhtasari (Model Policy Briefs)

Kazi za watetezi wa haki za kidijitali, waandishi wa habari na wanaharakati wengine katika jamii zinathaminiwa zaidi zinapoonekana kuchangia kutoa suluhisho kwa changamoto nyingi zinazoikabili jamii. Fungo tovuti zifuatazo zinaonyesha sera muhtasari chache zenye mwelekeo wa kutatua changamoto hizo.

https://tinyurl.com/y2ynk6oc
https://tinyurl.com/y3r9t974
https://tinyurl.com/y2v9ucfl

1.8 Mifano ya Kauli Muunganiko

Kuongezeka kwa duru za serikali za Kiafrika kudhibiti matumizi ya mitandao ya kijamii kupitia rasimu za sheria zisizokuwa wazi hupunguza matumizi huria ya mtandao, huficha ukiukaji wa serikali wa haki za binadamu na kusababisha vikwazo katika kuendelea kwa utulivu uliodumu kwa muda mrefu na majadiliano ya kuendeleza amani. Namna ya kukabiliana na tabia hizi za serikali nyingi zitapata nguvu na uhalali kama wadau wote wanakutana na kuzungumza kwa sauti moja. Mifano michache ya kauli muunganiko zilizotolewa kupambana na adha hii zinabainishwa katika fungo tovuti zifuatazo.

https://tinyurl.com/yyt8kkhp
https://tinyurl.com/y5eku8et
https://tinyurl.com/y4l6lwkg
https://tinyurl.com/y38k8mut

Sura ya Pili

2.1 Ulinzi na Usalama wa Kidijita

Ulinzi wa kidijitali au ulinzi wa mtandao, ulinzi wa mkondoni au ulinzi mtandao anga unamaanisha tabia anuwai na tahadhari za kujilinda anazofuata mtu wakati anatumia mtandao katika kuhakikisha kuwa habari nyeti za kibinafsi na za vifaa anavyotumia mtandaoni vinabaki kuwa salama.

a. Jinsi ya Kujilinda Mtandaoni

Kutokana na takwimu za 2020 zilizotayarishwa na Infographic zinazozungumzia "Kinachotokea katika dakika moja ya Matandaoni" wameona kuna barua pepe milioni 190, twiti 194,444 na meseji za WhatsApp milioni 19 zinazotumwa na kupokelewa katika kila sekunde 60.
Kwa upande wa takwimu za shirika la Umoja wa Mawasiliano duniani (ITU) inaonyesha kuwa zaidi ya watu bilioni 4.5 au nusu ya idadi ya watu wote ulimwenguni wameunganishwa mkondoni. Hii inaweza kumaanisha kitu kimoja kwamba wahalifu wa mtandao, wadukuzi, vitendo vya ulaghai na vitisho mkondoni vitazidi kuongezeka na kufanyika mashambulio kuliko hapo awali. Ili kuhakikisha ulinzi wa kidijitali kwa waandishi wa habari, watetezi wa haki za kidijitali na watumiaji wengine wa mtandao, anuwai ya mazingatio ya unadhifu wa kidijitali yanahitaji kutiliwa maanani ili kusaidia katika kudhibiti matukio na vitisho vya usalama wa kidijitali.

Kielelezo 4: Kinachojiri mtandaoni ndani ya dakika moja

b. Unadhifu wa Kidijitali

Unadhifu wa kidijitali ni hitaji la wakati wote na ni kama mazoea au tabia zinazopaswa kuendelezwa ili kudumisha unadhifu katika ulimwengu wetu wa kidijitali. Hii inajumuisha kila kitu kutoka kuandaa mafaili kwenye kompyuta yako, kusitisha akaunti zako za mitandao ya jamii, kuanzisha programu mpya au teknolojia ili kufanya maisha yako ya kidijitali yawe rahisi au salama zaidi. Tunaweza kusikia hii ikiitwa unadhifu wa mtandao au usafi wa mtandao anga. Hizi zote zinamaanisha kitu kile kile.

Kielelezo 5: Usalama wa kidijitali na unadhifu

c. Faida za Unadhifu wa Kidijitali

Kwa kulinda habari unayosafirisha mkondoni na au kulinda vifaa vya dijitali unavyotumia, unapunguza uwezekano wa kushambuliwa au kupunguza madhara ya shambulio lililofanikiwa. Ni budi kufahamu kwamba chochote unachotuma mkondoni kinaweza kuwa chanzo au habari inayotumiwa na maharamia wa mtandao kuzindua kashfa au shambulio la mtandao dhidi yako. Hivyo kama mdau wa haki za kidijitali, kuzingatia tabia zinazohakikisha unadhifu wa matumizi ya mtandao ni muhimu sana katika kujipa ulinzi mtandaoni.

2.2 Desturi za Unadhifu wa Kidijitali

Kielelezo 6: Kuza mienendo salama mtandaoni

a. Endeleza Tabia Salama Mtandaoni

Kuna mambo kadhaa rahisi unayoweza kufanya bila kununua teknolojia ya gharama kubwa au kuwekeza muda mwingi katika kusanidi upya mtandao wako wa nyumbani kwa lengo la kufanya kompyuta yako unayotumia mtandaoni ipate ulinzi bora zaidi. Orodha hii hapa chini ni mahala pazuri pa kuanzia na inakuunganisha na maeneo mengine ya tovuti yetu kupata habari zaidi juu ya kila hatua ya usalama na kujilinda kimtandao.

1. Weka mifumo yako na programu yako hai wakati wote.[13]
2. Daima kuwa na programu ya kupambana na virusi iliyo hai wakati wote.[14]
3. Epuka wizi wa hadaa au utapeli wa taarifa zako.[15]
4. Tumia nywila ngumu au meneja wa nywila.[16]
5. Kuwa mwangalifu unabofya nini; tovuti isiyo salama inaweza kukuunganisha na maharamia wa mtandao.
6. Kamwe usiache kompyuta au vifaa vyako vya dijitali wazi. Funga komyuta yako unapoelekea hata uani. Kuacha kompyuta wazi ni mwaliko wa wazi wa kushambuliwa kwa mafaili yako.
7. Weka namba ya siri kwa kifaa chako cha rununu, na usijaribu kamwe kukiacha wazi ukiwa ndani ya ndege[17]
8. Linda taarifa zako.
9. Kwa faili zote za kibinafsi, chelezo taarifa zako! Huwezi kujua ni lini kihifadhio (hard disk) chako cha kompyuta kitaharibika na pengine usipate taarifa zako tena. Chelezo kutumia huduma za mtandao wingu (cloud) au kihifadhio huru.[18]
10. Unaponunua mtandaoni, au kutuma taarifa nyeti, hakikisha unatuma habari iliyosimbwa na utume kwenye tovuti zenye anuani zinazoanzia na “https” au ikoni ya kufuli kwenye mwambaa wa anuani yako.
11. Kuwa mwerevu juu ya kile unachowasilisha (au acha kuwasilisha) kwenye mitandao ya kijamii.[19]
12. Katika ulimwengu wa muingiliano mkubwa wa watu, kuwa mwangalifu kwa ‘uhandisi wa kijamii’. Hii inaweza kuwa jaribio la mtu usiyemjua kukuvuta kijanja na kumpa habari kama siku yako ya kuzaliwa, wapi unapenda kwenda likizo, jina la mnyama unayemfuga nyumbani, Ukiulizwa na mtu jiulize je ni kweli anahitaji taarifa hizo? Ukimpatia majibu ya maswali kama haya yanaweza kusababisha akaunti yako kuibiwa na ushindwe kuwepo mtandaoni.
13. Hakikisha unafuatilia matukio yanayotia shaka yanayogusa akaunti zako za kifedha na za mitandao ya kijamii bila kuchoka ili ubakie salama siku zote.[20]

13 https://cybersecurity.osu.edu/cybersecurity-you/avoid-threats/updates-patching
14 https://cybersecurity.osu.edu/cybersecurity-you/use-right-tools/anti-virus
15 https://cybersecurity.osu.edu/cybersecurity-you/avoid-threats/phishing
16 https://cybersecurity.osu.edu/cybersecurity-you/passwords-authentication/passwords
17 https://cybersecurity.osu.edu/cybersecurity-you/protect-personal-devices/mobile-devices
18 https://cybersecurity.osu.edu/cybersecurity-you/develop-safe-habits/file-backups
19 https://cybersecurity.osu.edu/cybersecurity-you/develop-safe-habits/file-backups
20 https://cybersecurity.osu.edu/about/teams/identity-access-management

b. Nywila & Uthibitishaji

Ikiwa unatafuta njia ya kuboresha ulinzi wako wa mtandao, usalama wa nywila ndio unapaswa kuanza. Kwa kawaida, nywila ni ulinzi wa kimsingi wa usalama ambao una nishani ya siri iliyoundwa kwa kutumia herufi za alfabeti, nambari, ishara au mchanganyiko wa hivyo vyote. Utaratibu huu wa ulinzi hutumiwa kuruhusu kuingia kwenye mfumo au huduma kwa wale watumiaji ambao wameidhinishwa kwa kutumia nywila. Mazoezi ya kawaida ya usalama wa kidijitali yanajumuisha kuunda nywila zenye uimara, kuto tumia nywila hiyohiyo zaidi ya mara moja, kutumia kaulisiri ikiambatana na uthibitisho wa pili, mchanganyiko wa herufi, nambari, alama na kuzingatia kwa uangalifu maswali gani ya kuweka ili kurudisha upya nywila iliyosahaulika na mwisho japo si kwa umuhimu kutumia program ya meneja nywila. Haitakiwi kuiandika nywila popote ni hatari.

c. Jenereta za Nywila

Jenereta ya nywila ni zana ya programu ambayo hutengeneza nywila zisizo za kawaida au zisizotabirika kwa watumiaji. Hivyo inasaidia watumiaji kuunda nywila imara ambazo hutoa ulinzi zaidi kwa ufikiaji wa mfumo au akaunti zinazohitaji ulinzi maalum.

d. Umuhimu wa Jenereta za Nywila

Jenereta za nenosiri husaidia wale ambao wanapaswa kuja na nywila mpya kila wakati ili kuruhusiwa kuingia kwenye mfumo au akaunti kama ilivyoidhinishwa na programu na kuwezesha kufanya usimamiaji wa idadi kubwa ya nywila na kuweza kuingia kwenye akaunti au mfumo kwa urahisi. Aina nyingine za zana ni pamoja na stoo ya nywila, inayowezesha watumiaji kusimamia nywila lukuki katika eneo salama.

e. Programu za Usimamizi wa Nywila

Meneja wa nywila ni programu au zana ambayo huunda na kuhifadhi nywila ili nywila nyingi tofauti zitumike kuingia kwenye tovuti na huduma nyingine bila ya haja ya kuzikumbuka.

Meneja wa Nywila:

- **Inatengeneza nywila imara ambazo mwanadamu hawezi kuzikisia.**
- **Inahifadhi nywila kadhaa (na majibu ya maswali ya usalama) salama.**
- **Inakinga nywila zako zote kwa kutumia nywilakuu moja (au kaulisiri).**[21]

KeePassXC ni mfano wa programu ya meneja wa nywila ambayo ni ya chanzo wazi na bure. Programu hii inaweza kuwekwa kwenye kompyuta ya mezani au kuunganishwa kwenye kivinjari cha tovuti. KeePassXC[22] Khaihifadhi data kwa kujiendesha yenyewe kiotomatiki hivyo mabadiliko, kama ya kuongeza nywila zingine, yaliyofanywa wakati wa kuitumia, yanaweza kupotea ikiwa itasambaratika. Hata hivyo unaweza kuzuia haya yasitokee kama kwenye maelekezo ya matumizi ya programu umeamuru kwa usahihi. Tafadhali kumbuka kuwa kutumia mameneja wa nywila ni kama kuweka mayai yako yote kwenye kikapu kimoja

21 https://ssd.eff.org/en/glossary/passphrase
22 https://ssd.eff.org/en/glossary/web-browser

na unapaswa kuyalinda kama uhai wako. Hatari ya kutumia programu ya meneja wa nywila ni kwamba ikisambaratika ina maanisha ndio mwisho wa nywila zote zilizomo ndani yake pia.

2.3 Mashambulizi ya Nywila zilizo zoeleka

Kielelezo 7: Nywila salama

a. Kujaribu Nywila zilizo zoeleka

Moja ya njia rahisi na ya kawaida ya kuingia kwenye akaunti ya mtu mwingine ni kujaribu [23] nywila zilizo zoeleka au kufanya utafiti kidogo juu ya yule aliyekusudiwa kwa shambulio na kujaribu kwa kubahatisha nywila zinazohusiana na mtu huyo. Ripoti ya CNN ya 2019 ilibainisha kwamba nywila 10 zinazotumiwa sana na kudukuliwa ni:

1. 123456
2. 123456789
3. qwerty
4. password
5. 111111
6. 12345678
7. abc123
8. 1234567
9. password1
10. 12345

Hizi ni nywila zisizo salama KABISA. Ni rahisi kuzibashiri na wahalifu wa mtandao wanapenda kujaribu kuingilia akaunti za walengwa wao wenye nywila zinazoonekana kuwa dhaifu kama hizi. Tunapendekeza kuwa KAMWE usitumie nywila zilizo na habari zifuatazo:

- **Jina lako au majina ya mwanafamilia wako au marafiki,**
- **Siku yako ya kuzaliwa au ya mwanafamilia wako au marafiki,**
- **Majina ya mnyama unayefuga nyumbani kwako**

23 https://edition.cnn.com/2019/04/22/uk/most-common-passwords-scli-gbr-intl/index.html

- **Maeneo unayoishi au umewahi kuishi pamoja na miji au majina ya barabara.**

Inashangaza ni habari ngapi juu ya mtu iko wazi kwenye tovuti. Kwa hivyo ikiwa nywila yako ina habari ambayo inakuhusu kwa njia ambayo inaweza kutambuliwa kutoka kwenye tovuti au kwa kuzungumza na marafiki zako, inaweza kubashiriwa haraka na kwa urahisi.

b. Shambulio la Kikatili

Shambulio la kikatili hutokea pale mhalifu wa mtandao anapoanza kwa kubahatisha tu kila mchanganyiko unaowezekana wa herufi, alama au nambari zinazoruhusiwa hadi nywila kupatikana. Shambulio aina hii linafanikiwa zaidi kwa nywila fupi na hata kama nywila hizo ni za herufi zilizochanganywa nyuma mbele au mbele nyuma. Hivyo urefu wa nyilwa ni jambo muhimu sana.

Shambulio la Kikatili halikamiliki kirahisi ikiwa nywila yako ni ndefu vya kutosha. Inakuwa vigumu kuinyakua kimtandao. Hapa chini utaona jedwali linaloonyesha muda gani itachukua kuweza kunyakua nywila zilizo tofauti kwa uimara kwa urefu na ugumu. Kumbuka kwamba jedwali hili lina tanabahi kwamba kompyuta inaweza kuchapa zaidi ya nywila 1000 kwa sekunde.

Urefu wa Nywila yenye herufi, namba, alama	Mchanganyiko wa herufi, namba, alama	Herufi ndogo pekee
***	sekunde 0.86	sekunde 0.02
****	dakika 1.36	sekunde 0.46
*****	saa 2.15	sekunde 11.9
******	siku 8.51	dakika 5.15
*******	miaka 2.21	saa 2.23
********	karne 2.10	siku 2.42
*********	milenia 20	miezi 2.07
**********	milenia 1.899	miaka 4.48
**********	milenia 180,365	karne 1.16
**********	milenia17,184,705	milenia 3.03
**********	Milenia1,627,797,068	milenia 78.7
**********	milenia154,640,721,434	milenia 2,046

Kielelezo 8: Jedwali la urefu/ ugumu wa nywila

Unaweza kuona kuwa muda unaotumika kudukua nywila huongezeka sana kila mchanganyiko wa namba, herufi au alama unapoongezwa kwenye nywila yako. Kwa nenosiri ambalo lina mchanganyiko wa nasibu za kila aina, tofauti kati ya nasibu 6, 7, 8 na 9 huchukua siku, miaka, karne na milenia kudukua!!! Pia utaona ni muda gani unachukua kudukua nywila ambayo ina herufi, namba na alama ikilinganishwa na nywila ya urefu sawa ambayo hutumia herufi ndogo tu.

c. Kuunda na Kudumisha Nywila Imara na Salama.

Kutumia nywila ileile zaidi ya sehemu moja ni tabia mbaya kiulinzi na usalama mtandaoni. Ikiwa maharamia wa mtandao watashika nywila ambayo umetumia tena na tena kwenye huduma nyingi, wanaweza kupata akaunti zako zote kwa mpigo. Hii ndio sababu unapokuwa na nywila nyingi, zenye nguvu na za kipekee ni salama zaidi. Kwa bahati nzuri, programu ya meneja wa nenosiri inaweza kusaidia.[24]

d. Kuunda Nenosiri Imara kwa Kutumia Kete

Kuna manenosiri machache ambayo unapaswa kukariri na ambayo yanatakiwa yawe imara hasa kama haya yafuatayo:

- **Nywila za kifaa chako unachotumia mtandaoni kama simu yako**
- **Nywila za usimbuaji (kama usimbuaji wa diski nzima)** [25]
- **Nywila kuu,** [26] **au neno la siri** [27] **kwa ajili program yako ya meneja nywila**
- **Nywila yako ya barua pepe**[28]

Moja ya shida nyingi wakati watu wanachagua nywila wenyewe ni kwamba watu sio wazuri sana katika kufanya uchaguzi huria na usiotabirika.[29] Moja ya njia bora ya kuunda nywila imara na iliyo rahisi kukumbuka[30] ni kutumia kete[31] ikiambatana na orodha ya maneno[32] na kuyachagua maneno hayo kiholela kwa makusudi. Utaratibu huu huunda “kaulisiri” yako. “Kaulisiri” ni aina ya nenosiri ambalo ni refu na lenye usalama mkubwa zaidi. Kwa usimbuaji wa diski na programu ya meneja wa nywila, tunapendekeza uchague angalau maneno sita ili upate kaulisiri imara.

Kwa nini utumie angalau maneno sita? Kwa nini utumie kete kuchukua maneno kiholela ili kupata kaulisiri? Ni kwamba jinsi kaulisiri au nenosiri linavyozidi kuwa refu au limechanganywa bila mpangilio, ndio jinsi inavyozidi kuwa vigumu kwa kompyuta na wanadamu kugundua nenosiri hilo. Ili kujua ni kwanini unahitaji nenosiri refu na gumu kukisia, hapa kuna maelezo ya video.[33]

24 https://ssd.eff.org/en/glossary/password-manager
25 https://ssd.eff.org/en/glossary/encryption
26 https://ssd.eff.org/en/glossary/master-password
27 https://ssd.eff.org/en/glossary/passphrase
28 https://ssd.eff.org/en/glossary/password
29 http://people.ischool.berkeley.edu/~nick/aaronson-oracle/
30 https://www.eff.org/deeplinks/2016/07/new-wordlists-random-passphrases
31 https://www.eff.org/dice
32 https://www.eff.org/files/2016/07/18/eff_large_wordlist.txt
33 https://ssd.eff.org/en/module/animated-overview-how-make-super-secure-password-using-dice

Ikiwa kompyuta yako au kifaa unachotumia mtandaoni hakina ulinzi imara kinaweza kuwekwa programu ya ujasusi bila ya mwenyewe kujua ambayo ina uwezo wa kukuangalia ukiandika nywila yako kuu na pia hivyo inaweza kuiba programu yako ya meneja nywila na kwa maana hiyo nywila zako zote ulizohifadhi humo. Kwa hivyo bado ni muhimu sana kuweka kompyuta yako na vifaa vingine salama zisiweze kushambuliwa na programu hasidi wakati wa kutumia meneja wa nywila.

e. Kulinganisha Nywila Katika Vifaa Vingi

Programu za Meneja Nywila nyingi huruhusu ufikiaji wa nywila kwenye vifaa vyote kupitia huduma ya ulinganishaji wa nywila inayopatikana kwenye programu yenyewe. Hii inamaanisha kwamba wakati unalinganisha faili la nenosiri kwenye kifaa kimoja, itakuwa hivyo kiotomatiki kwenye vifaa vingine vyote. Programu za Meneja Nywila zina uwezo wa kuhifadhi nywila "winguni," kwa maana kwamba nywila imesimbwa na kuhifadhiwa kwenye seva iliyo mbali. Nywila zinapohitajika, programu ya menejanywila husimbua[34] nywila hizo na kuzirejesha moja kwa moja kwako. Programu za meneja nywila zinazotumia seva zao na zile zenye uwezo wa kuhifadhi au kusaidia kulinganisha (sync) nywila ni rahisi zaidi kutumia, lakini ziko hatarini zaidi kushambuliwa kimtandao. Ikiwa nywila zimehifadhiwa kwenye kompyuta na winguni, mshambuliaji hahitaji kuchukua kompyuta ili kunyakua nywila. (Hata hivyo watahitaji kunyakua nywila kuu kufungua programu ya Menejanywila) Ikiwa una mashaka na hili la winguni, usiweke nywila zako huko badala yake chagua kuzihifadhi kwenye vifaa unavyotumia mtandaoni tu inaweza kuwa salama zaidi.

- **Kumbuka!**

Weka chelezo ya hifadhidata ya nenosiri kwa tahadhari maana huwezi jua kinachoweza kutokea. Kuwa na chelezo ni muhimu ikiwa hifadhidata ya nenosiri itadhurika na kukoma kufanya kazi katika ajali ya mfumo, au kwa kifaa chenyewe kusombwa. Kwa kawaida Meneja nywila zina mfumo wa ndani wa kutengeneza mafaili chelezo zenyewe vinginevyo unaweza pia kutumia njia za kawaida za kutengeneza nakala za mafaili chelezo na kuyahifadhi pembeni vizuri.

2.4 Uthibitishaji Kwa Kutumia Vipengele Mtambuka Na Nywila za Mara Moja

Nywila imara na za kipekee hufanya iwe vigumu zaidi kwa maharamia mtandao kunyakua akaunti za watu za kidijitali. Ili kulinda zaidi akaunti zako, unapaswa kuwezesha uthibitishaji wa vipengele viwili vya ulinzi.[35] Zipo huduma zingine ambazo hutoa uthibitishaji wa vipengele

34 https://ssd.eff.org/en/glossary/decrypt
35 https://ssd.eff.org/en/glossary/two-factor-authentication

viwili (pia huitwa 2FA, uthibitishaji wa vipengele vingi, au uthibitishaji wa hatua mbili), utaratibu huu unahitaji watumiaji kumiliki vitu viwili (nywila na kipengele kingine) ili kufungua akaunti yao. Kipengele kingine kilichotajwa hapo juu kinaweza kuwa nambari ya siri itumikayo mara moja tu au nambari iliyozuka kwenye skrini kutokana na programu inayoendesha kifaa cha rununu.

Uthibitishaji wa vipengele viwili kwa kutumia simu ya rununu unaweza kufanyika kwa namna mojawapo ya hizi mbili:

- **simu inaweza kuwa na programu ya uthibitishaji ambayo huzalisha nambari za usalama (kama Google Authenticator [36] au Authy[37]) au kwa kutumia kifaa kinachosimama pekee (kama vile YubiKey); au**
- **huduma ya meseji inaweza kutuma ujumbe mfupi wa maandishi na nambari ya usalama ya ziada ambayo hutumiwa wakati wowote ili kukamilisha uthibitisho kabla ya kuingia mtandaoni.**

Kwa ushauri wako, chagua programu ya uthibitishaji au kifaa cha kusimama pekee bila kuwa mtandaoni badala ya kupokea nambari za uthibitisho kwa ujumbe wa maandishi kwasababu ni rahisi kwa mshambuliaji mtandao kuelekeza nambari hizi kwenye simu yake kuliko kupenya kwenye programu za uthibitisho. Huduma nyingine kama vile Google zinaruhusu. Pia kuzalishwa kwa orodha ya nywila za kutumia mara moja tu. Upatapo hizi nywila, unatakiwa uziandike kwenye karatasi au kuzichapisha na kuzibeba popote uendako. Kila moja ya nywila hizi hufanya kazi mara moja tu kwa hivyo ikiwa moja imeibiwa na programu ya ujasusi mwizi hataweza kuitumia kwa popote mbeleni.

a. Uthibitishaji wa Vipengele vingi (“MFA”)

Uthibitishaji wa Vipengele vingi (MFA) ni huduma ya usalama inayopatikana kwenye tovuti nyingi, programu mbalimbali na vifaa mtandao vingi. Huduma ya MFA huboresha sana ulinzi wa akaunti. Kitaalamu, MFA inaweza kuelezewa kama mfumo ambao una lazimu aina zaidi ya mbili za uthibitishaji kabla ya kuingia kwenye akaunti.

b. Uthibitishaji wa Vipengele vingi (“MFA”) hufanyaje kazi

Ikiwa una usanidi wa MFA kwa akaunti uliyopewa (tovuti, programu tumizi au kifaa), unapoingia na jina lako kama mtumiaji na halafu nywila yako, seva ya akaunti unayojaribu kuingia itauliza kipengele cha pili huru ili kukamilisha uthibitishaji kabla ya kukuruhusu uingie. Ni sawa na wakati unapofungua akaunti ya benki wanauliza kuona kitambulisho chenye picha na aina nyingine ya utambulisho, kama kadi ya uanachama wa mifuko ya kijamii au pasipoti ya kimataifa. Ni vigumu sana kudanganya kwamba wewe ni nani wakati unapaswa kuthibitisha kwa njia mbili tofauti kama hizi za MFA!

c. Njia za Uthibitishaji kwa Vipengele Vingi (MFA)

36 https://support.google.com/accounts/answer/1066447?hl=en
37 https://authy.com/

Kwa sababu ya usalama zaidi, tunapendekeza kusajili angalau vifaa viwili kwa uthibitishaji wa vipengele vingi, kwa hivyo ukipoteza kifaa kimoja, unaweza kujilinda kwa kufuta data kwa mbali mkondoni na kisha utumie kifaa kingine kuthibitisha. Kwa kutumia MFA, uthibitishaji wa pili unaweza kufanywa kwa kutumia njia nyingi tofauti lakini baadhi ya zile zinazojulikana zaidi ni hizi zifuatazo:

i. i. Njia ya Matumizi ya Kifaa cha Rununu “Push”

Njia maarufu zaidi ya kukamilisha uthibitishaji wa vipengele viwili ni kupitia “kishinikiza” ili kukamilisha uthibitishaji kwenye kifaa chako cha rununu. Kuna programu anuwai ambazo ni za bure na rahisi kuweka kwenye kifaa chako na ni rahisi kutumia kwa uthibitishaji! Kishinikiza hiki ni arifa ambayo itajitokeza ghafla kwenye kifaa cha rununu na kusema kitu kama, “Hei, mtu anajaribu kuingia kwenye tovuti hii, ni wewe? Je, tumruhusu kuingia?

Kwa kawaida swali hili huja na kitufe kikubwa cha kijani na chekundu na ili uweze kujibu “Ndio” au “Hapana” huna budi kugusa kimojawapo. Ukigonga “Ndio”, umeingia. Lakini ikiwa haukufanya ombi la asili la kuingia, unajua kuwa kuna haramia mtandao ameiba tayari nenosiri lako na anajaribu kuingia kwenye akaunti yako. Kama ndivyo unapaswa kugonga kitufe cha “Hapana” na hivyo hataweza kuingia. Baadae utaingia kwenye akaunti mwenyewe na ubadilishe nywila yako ili kukomesha mshambuliaji asiweze kujaribu mara nyingine.

Ni njia rahisi, lakini ni njia ya kujilinda bora sana. Faida ya msingi ya njia hii ni kwamba haitoshi kwa mshambuliaji kunyakua nywila yako tu, lakini pia anapaswa kuiba kifaa chako cha rununu yaani simu ili aweze kujibu kipengele cha pili cha uthibitishaji ndipo akamilishe zoezi lake. Ni wazi kwamba uwezekano wa mshambuliaji kufanikiwa ni mdogo mno. Ki ukweli ni karibu na sifuri ikiwa unatumia nywila imara na unalinda vizuri simu yako. Faida nyingine ya njia hii ni kwamba unapata arifa katika wakati halisi yaani wakati mtu anajaribu kuingia kinyume cha sheria kwenye akaunti yako. Kama ilivyoelezwa hapo juu, unaweza kutumia maarifa haya kujibu haraka kwa kubadilisha nywila yako.

ii. Njia ya Kuthibitisha kwa Nambari kupitia Kifaa cha rununu

Wakati mwingine seva ya akaunti haitakutumia meseji ya kishinikiza lakini inaweza kukuhitaji uandike nambari ya kipekee ambayo hutolewa na programu ya uthibitishaji kwenye kifaa chako cha rununu. Tarakimu hizi ni fupi, labda 6, kwa hivyo inaweza kuonekana kama sio salama sana.

Jambo la kupendeza ni kwamba nambari hutengenezwa kila dakika au karibu na hapo na zinategemea hesabu ambayo inajulikana tu kwa programu yako ya uthibitishaji na seva ya akaunti unayojaribu kuungana nayo. Itakuwa vigumu sana kwa mhalifu wa

mtandao kubashiri kwa usahihi nambari ya tarakimu 6 katika mazingira hayo kwa kuwa muda ni mfupi sana. Tena, faida kuu hapa ni kwamba mshambuliaji anapaswa kuwa na kifaa chako cha rununu na awe na uwezo wa kukifungua na kukitumia. Shida moja ni kwamba haupati arifa yoyote ya wakati ule ule ikiwa mtu anajaribu kuingia kwenye akaunti yako. Kawaida njia hii ni chaguo kama chelezo ya ile mbinu nyingine iliyo bora zaidi ya kutumia kishinikiza. Hata hivyo, programu nyingi za uthibitishaji zina uwezo wa kutumika kwa njia zote mbili

iii. Njia ya Msimbo wa Ujumbe Mfupi (SMS)

Hii ni mbinu nyingine ambayo hutumia kifaa chako cha rununu pia lakini haitumii programu tumizi. Kwa hivyo, si lazima kuwa na simu janja inayotumia programu za uthibitishaji kupata huduma hii. Ikiwa utaanzisha njia hii ya MFA, unapoingia na jina lako la mtumiaji na nywila, seva ya akaunti unayoingia itatuma kwenye simu yako ya mkononi ujumbe wa maandishi na nambari ya kutumika kwa wakati mmoja tu. Ukishaipata utaandika nambari hiyo kwenye tovuti ambapo uliingiza nywila yako. Hii kimsingi ina faida zote za njia ya “kishinikiza”, lakini sio rahisi sana kwa sababu lazima uandike nambari badala ya kujibu ndio au hapana. Ni kweli utapata arifa ya wakati ule ule ya jaribio la kuingia kwa sababu utapata ujumbe wa maandishi kwa kila jaribio. Ubaya mmoja ni kwamba mshambuliaji sio lazima afungue na kuingia kwenye simu yako kwa vile ujumbe wa maandishi mara nyingi hujitokeza kwenye skrini ya simu hata wakati simu imefungwa. Akiwa karibu na simu yako pengine itatosha kukamilisha zoezi.

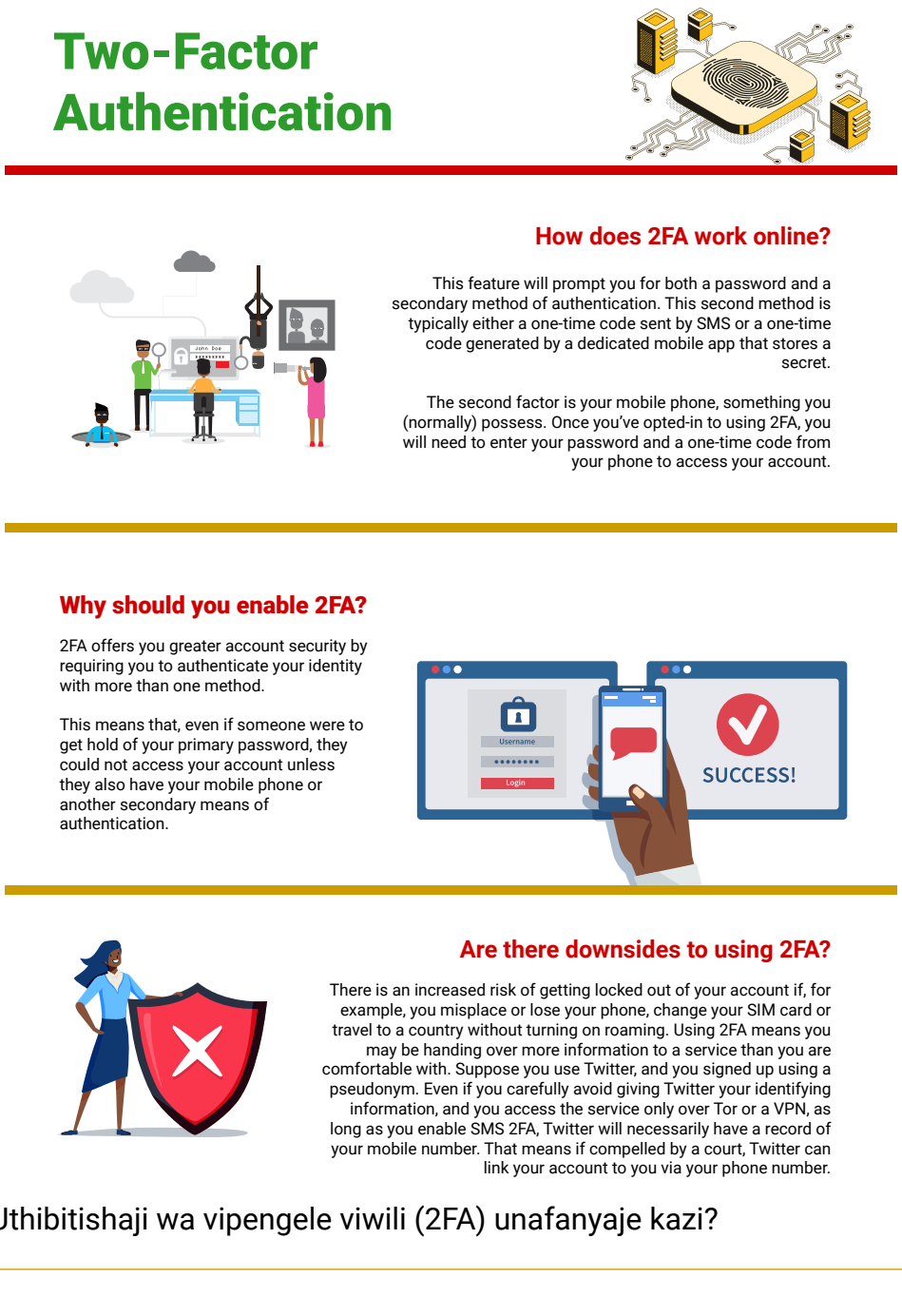
iv. Njia ya Msimbo wa Barua pepe

Njia hii inafanya kazi vizuri kama njia ya nambari ya ujumbe mfupi (SMS) isipokuwa kwamba nambari hiyo inatumwa kwenye akaunti yako ya barua pepe ambayo uliiwasilisha mapema kwenye seva ya akaunti unayojaribu kufikia. Mara nyingi utaweka akaunti yako wakati unasajili kupata huduma ya uthibitishaji wa vipengele vingi (MFA). Ikiwa utatumia aina hii ya MFA, utahitaji kuhakikisha kuwa akaunti yako ya barua pepe yenyewe ni salama, na hii huenda ikamaanisha kuwa unapaswa kuwezesha huduma ya MFA ili kuweza kuifikia akaunti yako ya barua pepe. Sababu ni kwamba barua pepe inaweza kuchunguzwa kutoka mahali popote, pamoja na kituo hicho cha kompyuta ambapo haramia mtandao anajaribu kuingia kwenye akaunti yako. Kwa maneno mengine, njia hii haihitaji uwepo wa vifaa viwili tofauti kukamilisha uhalifu. Ndio sababu unapaswa kuwa na nywila imara ya barua pepe yako ambayo haitumiki mahali pengine popote. Ikiwa utafanya hivyo, basi njia hii itahitaji mshambuliaji kujua nywila zako mbili ili afanikiwe. Hivyo utaona kwamba kumlazimisha mshambuliaji kupata kifaa kingine zaidi ya kile anachotumia ni chaguo imara na salama zaidi kulinganisha na hii ya barua pepe. Hivyo ni sawa ikiwa tovuti inaruhusu tu aina hii ya MFA. Unachohitaji ili uwe salama salimini ni kukamilisha usanidi wa MFA kwa kufanya taratibu ya uthibitishaji unaohusisha kifaa chako cha rununu ili ufikie barua pepe yako.

v. Kidude nambari

Njia hii ilikuwa maarufu zaidi kabla ya ujio wa simu janja. Kidude nambari ni kifaa kidogo cha mfukoni ambacho huzalisha tarakimu kila wakati kwa njia ile ile ambayo programu ya uthibitishaji kwenye kifaa chako cha rununu ingefanya. Kidude nambari kinafanya kazi vizuri tu lakini kina mapungufu yake kwavile inabidi uwe nacho muda wote. Siku hizi maisha yetu yamefungwa na simu zetu za rununu kidude hiki pamoja na umuhimu wake wa kujilinda kimtandao, ni rahisi kukipoteza na hata usijue kimetoweka muda gani. Ikiwa unatumia kidude nambari kama hiki kihifadhi mahali salama. Lakini kama ni lazima kukibeba muda wote, labda itabidi kukifunga na mnyororo wa funguo zako na kujifunga kibindoni ili kisipotee.

2.5 Uthibitishaji wa Vipengele Viwili ("2FA")



Kielelezo 9: Uthibitishaji wa vipengele viwili (2FA) unafanyaje kazi?

Uthibitishaji wa Vipengele Viwili (au "2FA") ni aina, au sehemu ndogo, ya uthibitishaji wa vitu anuwai, na ni njia ya kumruhusu mtumiaji ajitambulishe kwa mtoa huduma mtandaoni kwa kuhitaji mchanganyiko wa njia mbili tofauti za uthibitishaji. Njia hizi zinaweza kuwa kitu ambacho mtumiaji anajua (kama nenosiri au pini), kitu ambacho mtumiaji anacho (kama kidude nambari, vifaa au simu ya rununu), au kitu ambacho kimeambatanishwa au kisichoweza kutenganishwa na mtumiaji (kama alama za vidole).

a. Je! 2FA inafanyaje kazi mtandaoni?

Huduma kadhaa mtandaoni – pamoja na Facebook, Google, na Twitter - hutoa 2FA kama njia ya ziada ya uthibitishaji badala ya nenosiri pekee. Ukiwezesha kipengele hiki kwanza utaombwa nywila na halafu utaombwa njia ya pili ya uthibitishaji. Njia hii ya pili kawaida ni nambari fupi ya wakati huo huo inayotumwa kwa ujumbe mfupi wa simu au nambari ya wakati mmoja inayotokana na programu ya uthibitishaji ya rununu ambayo ni maalum kwa kuhifadhi siri (kama kithibitishaji cha Google, Duo mobile, programu ya Facebook, au Clef). Kwa hali yoyote, kipengele cha pili utakachoamua kutumia kitahitaji simu yako ya rununu ambayo kwa kawaida utakuwa nayo. Tovuti zingine (pamoja na Google) pia zina uwezo wa kutumia namba fupi (codes) za kutumika kwa mara moja ambazo zinaweza kupakuliwa kutoka mtandaoni, kuchapishwa kwenye karatasi, na kuhifadhiwa mahali salama kwa matumizi baadae na kama chelezo ya ziada. Kwahiyo kama umeamua kutumia mbinu ya 2FA, utahitaji kuweka nenosiri lako na pia nambari fupi ya wakati huo huo utakayopokea kwenye simu yako ili kufungua akaunti yako.

b. Kwa nini unapaswa kuwezesha matumizi ya 2FA

2FA inakupa ulinzi imara zaidi wa akaunti kwa kukuhitaji uthibitishe utambulisho wako kwa njia zaidi ya moja. Hii inamaanisha kuwa, hata ikiwa mtu angeshikilia nywila yako ya msingi, hataweza kufikia akaunti yako isipokuwa kama ana simu yako ya rununu au njia nyingine ya kumwezesha kufanya uthibitisho wa pili.

c. Je! Kuna Changamoto gani kutumia 2FA?

Ingawa 2FA inatoa njia salama zaidi ya uthibitishaji, kuna hatari kubwa ya kufungiwa nje ya akaunti yako ikiwa, kwa mfano, ukibadilisha au kupoteza simu yako, ukibadilisha kadiwia[38] yako au kusafiri kwenda nchi za nje bila kuwasha kuvinjari. Vivyo hivyo, kutumia 2FA inaweza kumaanisha kuwa huenda unatoa habari zako nyingi zaidi kwa mtoa huduma wako ili kupata huduma ya 2FA kuliko vile ambavyo ungependa. Tuseme unatumia Twitter, na umejiandikisha ukitumia jina bandia.[39] Hata ukiepuka kwa uangalifu kuwapa Twitter habari zako za utambulisho, na unapata huduma hiyo tu kupitia Tor au VPN[40], tau maadamu umewezesha matumizi ya huduma ya ujumbe mfupi (SMS) kupata huduma ya 2FA, Twitter itakuwa na rekodi ya nambari yako ya rununu. Hiyo inamaanisha kwamba kama mahakama itaamrisha Twitter kutoa taarifa zako, inaweza kupata namba yako ya simu kupitia akaunti yako ya twitter hata kama ina

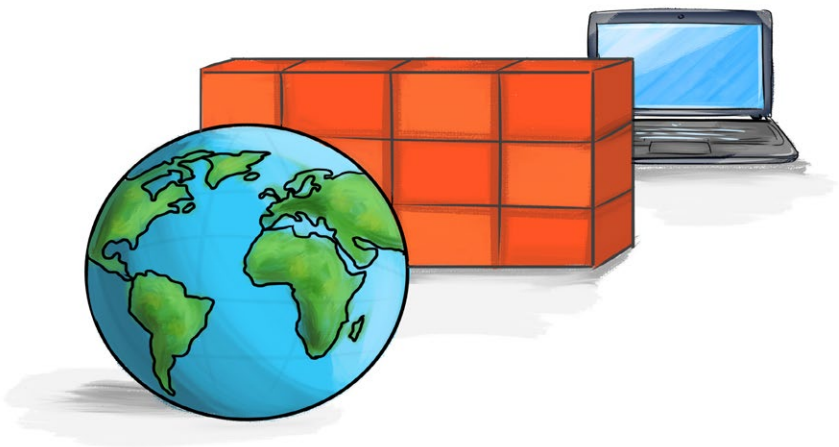
38 https://ssd.eff.org/en/glossary/sim-card
39 https://ssd.eff.org/en/glossary/pseudonym
40 https://ssd.eff.org/en/glossary/vpn

jina bandia. Hii itakuwa sio shida kwako, haswa ikiwa tayari unatumia jina lako la kisheria kwenye huduma uliyopewa, lakini ikiwa unataka kuendelea kutojulikana, fikiria mara mbili juu ya kutumia huduma ya ujumbe mfupi unapotumia huduma ya 2FA.

d. Uthibitishaji wa Vipengele vya Jumla

Uthibitishaji wa jumla, pia unajulikana kama “saini moja” (SSO), ni njia ya uthibitishaji wa utambulisho wa mtandao ambayo inaruhusu mtumiaji kuvinjari kutoka tovuti moja kwenda nyingine kwa salama bila kuwa na haja ya kuingiza uthibitisho mara kadhaa. Kwa uthibitishaji wa jumla, mteja huingiza seti moja ya uthibitisho (kama jina la mtumiaji na nywila) mwanzoni mwa kila kipindi aingiacho kwenye mtandao. Taaarifa za uthibitishaji kwa kila tovuti uliyotembelea baadaye hutengenezwa kiotomatiki kuonyesha muda uliotumia kwa kila kipindi ulipokuwa mtandaoni. Moja ya changamoto kubwa kuhusu usalama wa mtandao ni kuwa kila tovuti ina mfumo wake wa uthibitishaji. Mtumiaji wa kawaida wa Mtandaoni, ambaye ana anuani mbili za barua pepe mbili au tatu za tovutini na anayefanya mauzo au manunuzi kwenye maduka mtandao tuseme kama dazani moja hivi lazima akariri majina kadhaa ya yeye mwenyewe kama mtumiaji na nywila. Hii inaweza kuwa ngumu kukariri na hivyo inabidi data ya uthibitishaji iandikwe au kuhifadhiwa kama faili ya maandishi, kitu ambacho si sahihi kiusalama. Hata hivyo, uthibitishaji wa jumla unaweza kuondoa tatizo hili bila kuathiri usalama au faragha.

2.6 Ngomemoto



Kielelezo 10: Ngomemoto

Huu ni mfumo wa usalama wa mtandao ambao unalinda kompyuta dhidi ya unganisho usilohitaji kwenda au kuingia kutoka kwenye mitandao ya nje au ndani haswa mitandao iliyo ndani ya mtandao wako (intranets). Ngomemoto zinaweza kutekelezwa kama vifaa au

programu, au mchanganyiko wa vyote viwili. Ngomemoto[41] inaweza kuwa na sheria ambazo zinakataza barua pepe kutoka au kukataza unganisho kwa tovuti zingine. Ngomemoto zinaweza kutumika kama safu ya kwanza ya ulinzi ya kulinda kifaa kutokana na uvamizi wa kimtandao usiyotarajiwa. Zianaweza pia kutumiwa kuzuia watumiaji kuingia mtandaoni bila utaratibu unaokubalika.

a. Vifaa vya Kompyuta na Programu

Ngomemoto zinaweza kuwa vifaa vya dijitali au programu lakini usanidi ulio bora ni ule wa kujumuisha zote mbili. Mbali na kupunguza ufikiaji wa kompyuta yako na mtandao wako, ngomemoto pia ni muhimu kwa kuruhusu ufikiaji wa mbali ili kuingia kwenye mtandao wa faragha kwa kutumia njia salama zaidi za uthibitishaji. Ngomemoto ya vifaa inaweza kununuliwa kama bidhaa ya kusimama peke yake lakini kwakuwa ni chombo kinachounganishwa mkondoni muda wote ili kifanye kazi yake, inapaswa kuchukuliwa kama kama sehemu muhimu sana ya usalama wa mfumo wako na usanidi wa mtandao. Ngomemoto nyingi za vifaa au ruta zinakuwa na vipenyo vinne ili kuunganisha mtandao na kompyuta zingine, lakini kwa mitandao mikubwa ya kibiashara ngomemoto kubwa zaidi zinazokidhi mahitaji zinapatikana. Ngomemoto ya programu inawekwa kwenye kompyuta yako, kama programu yoyote ile na unaweza kuiratibu na kuweza kudhibiti inavyofanya kazi na huduma zake za ulinzi. Ngomemoto ya programu italinda kompyuta yako dhidi ya majaribio ya nje yanayokusudia kuteka na kudhibiti kompyuta yako. Ngomemoto pia inaweza kuwa sehemu ya programu vinjari au mfumo endeshi wa kompyuta yako. Kwa mfano, Ngomemoto inaweza kuwa ndani ya program vinjari kama ile iliyomo ndani ya programu ya windows ambayo ina uwezo wa kutoa tahadhari kwa mtumiaji kama kuna dalili ya shambulio au shaka nyingine. Programu hii inaweza pia kugundua na kuzuia virusi, minyoo mtandao, na wadukuzi wasiweze kusababisha madhara yoyote.

b. Ngomemoto Inavyochuja habari zinazoingia

Ngomemoto hutumiwa kulinda mitandao ya nyumbani na ya mashirika. Programu ya kawaida ya ngomemoto au kifaa cha ngomemoto huchuja habari zote zinazoingia kwenye mtandao wako au mfumo wa kompyuta. Ngomemoto hutumia mbinu ambazo za kuchuja habari zinazoweza kudhuru kupitia:

- **Kichuja Pakiti :** Kinaangalia kila pakiti[42] inayoingia au inayoondoka kwenye mtandao wako na kinaikubali au kukikataa kwa kuzingatia sheria zilizoainishwa na mtumiaji wakati wa kusanidi. Kichuja pakiti kinaleta ufanisi kwa kiasi fulani na uwazi kwa watumiaji, lakini ni ngumu kusanidi. Na kwa kuongezea, ni kwamba kinadhurika kirahisi kupitia hadaa ya anuani ya mtandaoni (IP). [43]
- **Programu ya Lango Tumizi :** Programu hii inachangia kuleta usalama wa mtandao kupitia programu maalum, kama vile FTP[44] na seva za Telnet[45] kukamilisha unganisho. Hii ni mbinu yenye kuleta ufanisi kiusalama, lakini inaweza kusababisha kudorora kwa

41 https://ssd.eff.org/en/glossary/firewall
42 https://www.webopedia.com/TERM/P/packet.html
43 https://www.webopedia.com/TERM/I/IP_spoofing.html
44 https://www.webopedia.com/TERM/F/ftp.html
45 https://www.webopedia.com/TERM/T/Telnet.html

ukamilishaji wa unganisho lenyewe

- **Lango Tumizi la Sakiti:** Lango Sakiti huanzisha taratibu za kuhakikisha usalama kwa kiingiacho mtandaoni au kwenye kompyuta yako ikiwa unganisho la TCP[46] au UDP[47] limekamilika. Mara tu unganisho linapokuwa limefanywa, pakiti zinaweza kutiririka kwa usalama kufikia ngazi tofauti za mtandao wako au kompyuta yako bila kuwa na haja ya kufuatilia tena.
- **Seva Wakala:** Seva hii ndio kama dalali au wakala wako unapotumia mtandao. Ina kazi ya kudaka na kusambaza kwa aliye tumiwa kila ujumbe unaoingia na kuondoka kwenye mtandao wako. Seva wakala[48] inaficha anuani halisi ya mtandao ya mpeleka ujumbe aliyepo kwenye mtandao unaotumia seva wakala.

Kiuhalisia, ngomemoto nyingi hutumia mbili au zaidi ya mbinu hizo hapo juu kwa pamoja. Ngomemoto inachukuliwa kama safu ya kwanza ya ulinzi katika kulinda taarifa za kibinafsi. Hata hivyo, na kwa usalama mkubwa zaidi, kinachotumwa mtandaoni ni vizuri kusimbwa kwa njia fiche.

2.7 Usimbu Fiche (Encryption)

Usimbu fiche ni mbinu ya kukoroga taarifa au ujumbe kihisbati (kusimbu fiche), ili isafirishwe kama fumbo au ionekane haina maana, lakini bado inaweza kurejeshwa katika hali yake ya asili na mtu au kupitia kifaacha kidijitali ambacho kina kipande cha data kinachoweza kusimbua fiche (funguo ya kusimbua fiche). Hii inadhibitisha ni nani anayeweza kupata habari au ujumbe ule kwa sababu bila ufunguo sahihi, ni vigumu kubadili usimbu fiche na kupata habari ya asili. Usimbu fiche na usimbua fiche ni moja ya teknolojia kadhaa ambazo zinaunda uwanja unaoitwa usimbuaji.

Usimbu fiche wa mwisho kwa mwisho unahakikisha kuwa ujumbe umegeuzwa kuwa ujumbe wa siri na mtumaji wake wa asili, na utaweza kusimbuliwa fiche tu na mpokeaji wake wa mwisho. Aina zingine za usimbu fiche nje ya zile anazofanya mtumaji mwenyewe, zinaweza kufanywa na mtu wa tatu anayepaswa kuaminiwa kwanza na kupatiwa ujumbe au maandishi ya asili na mtumaji. Usimbu fiche wa mwisho hadi mwisho kwa ujumla huonekana kuwa salama zaidi, kwa sababu hupunguza idadi ya watu wa katikati ambao wanaweza kuingilia au kuvunja usimbu fiche uliofanywa.

2.8 Mtandao wa kibinafsi (VPNs)

Mtandao wa kibinafsi (au VPN) ni njia salama ya kuunganisha kompyuta kwenda kwenye mtandao mwingine wa shirika uliopo upande wa pili. Unapo unganishwa na VPN, data zote za

46 https://www.webopedia.com/TERM/T/Telnet.html
47 https://www.webopedia.com/TERM/U/User_Datagram_Protocol.html
48 https://www.w ebopedia.com/TERM/P/proxy_server.html

kuvinjari kwenye tovuti zinaonekana kutoka kwa VPN yenyewe, badala ya Mtoa Huduma wako wa Mtandao (au ISP).[49] Habari nyeti inaweza kujumuisha fomu za mawasiliano zilizojazwa au taarifa ya kadi za malipo za benki. Kwa kutumia VPN, anuani yako ya kimtandao uliyopewa na mtoa huduma wako anaye kuunganisha na mtandao (ISP) itafichika na haitaonekana kwenye tovuti ambazo utavinjari hivyo kuongeza tabaka jingine la faragha. Pamoja na kuficha anuani yako ya asili[50] aya (IP), pia VPN inasimbu fiche data yako hata ukiwa unavinjari na upo kati ya tovuti moja na nyingine.

a. VPN za Kibiashara

Mtandao binafsi wa kibiashara (VPN) ni huduma ya kibinafsi ambayo hupokea na kusafirisha mawasiliano yako mtandaoni kwa usalama mkubwa kupitia mtandao wao huo. Faida ya huduma hii ni kwamba data zote unazotuma na kupokea zimefichwa zisionekane kwenye mitandao yako ya kawaida unayotumia, kwa hivyo ni salama zaidi dhidi ya wahalifu wa mtandaoni, watoa huduma wa mtandao wasioaminika (ISPs) au mtu mwingine yeyote anayetaka kupeleleza mawasiliano yako kwenye mtandao. VPN inaweza kuwa imesimikwa katika nchi ya kigeni, kitu ambacho kinakuwezesha kufanya mawasiliano bila kuwa na wasiwasi na serikali yako, na hivyo kukwepa udhibiti unaominya uhuru wa kuwasiliana wa kitaifa unaoweza kuwepo. Ubaya ni kwamba mawasiliano yote yanasimbuliwa fiche yafikapo mwisho kwenye mtandao wa kibinafsi wa kibiashara yaani VPN[51]. Hiyo inamaanisha unahitaji kuijua na kuiamini VPN unayotumia (na nchi ambayo iko) wasije kuwa wapelelezi wa mawasiliano yako. Wakati VPN ya kibiashara inaweza kukupa “usalama”, sio lazima ikuhakikishie ulinzi.

b. VPN za Bure

VPN ya bure ni huduma ambayo inakupa programu muhimu ya kukuwezesha kuingia kwenye seva ya VPN bila ya kulipa chochote. Wakati VPN ya bure inaweza “kuokoa” pesa yako, lakini pia inaweza kusababisha hatari kubwa ya usalama wako na kupoteza udhibiti wa data yako. Mifano ya Mitandao ya Binafsi (VPNs) ni pamoja na; NordVPN,[52] Private Access VPN,[53] Windscribe VPN,[54] CyberGhost VPN,[55] TunnelBear[56] etc.

nk. Kumbuka! Kabla ya kuchagua huduma ya VPN, soma kila wakati hakiki za watumiaji ili kubaini watumiaji wao walikuwa na malalamiko gani. Pia, kila wakati chunguza sifa ya mtoa huduma wa VPN, na uone mahali alipo na hapo labda utajua kwamba kuna sababu ya kutumia au kutotumia huduma yoyote ya VPN ambayo pengine ipo katika nchi iliyo na historia yenye mashaka kiusalama.

49 https://en.wikipedia.org/wiki/Internet_service_provider
50 https://ssd.eff.org/en/glossary/ip-address
51 https://ssd.eff.org/en/glossary/commercial-vpn
52 https://nordvpn.com/
53 https://www.privateinternetaccess.com/pages/techradar
54 https://windscribe.com/upgrade?promo=WS50OFF&afftag=tomsguide-623331950543060900 0&affid=fghzq9e1
55 https://www.cyberghostvpn.com/en_US/?media_source=inhouse_affiliates&lp=pro_homepage&transaction_id=1 020f5087b76582644982b711aa6e1&affiliate=futurenet%2FTechRadar&offer_id=135&coupon=YT2M&conversionpoint=externalCP&channel=External+LPs&affiliate_google_cli
56 https://www.tunnelbear.com

2.9 Programu ya Tor Brower

Tor ni programu ya bure ya chanzo huru kwa kuwezesha mawasiliano yasiyo julikana mwenyewe ni nani. Jina limetokana na kifupi cha jina asili la mradi wa programu iitwayo kwa kiingereza"Onion Router". Tor ina vipengele vilivyojengwa ndani kwa ndani ya programu yenyewe ambavyo vinakulinda kutokana na ufuatiliaji wa tovutini, upelelezi, na uchukuaji wa "alama za vidole" za mtumiaji kimtandao.

2.10 Programu ya DuckDuckGo

Hii ni injini ya utafutaji ya mtandao (search engine) ambayo inasisitiza kulinda faragha ya watumiaji wake kwa kutokubakisha kumbukumbu zozote za matokeo ya utafutaji wao wa kibinafsi. DuckDuckGo inajitofautisha na injini zingine za utafutaji mtandao kwa kutoweka wasifu wa watumiaji wake na kwa kuonyesha watumiaji wote matokeo sawa kwa kila neno au ombi la utafutaji.

2.11 Kufanya kazi Kutoka Nyumbani: Vidokezo vya Usalama wa Mtandaoni

Janga la ugonjwa wa Corona (COVID-19) limelazimisha ulimwengu kutengana kijamii kama moja ya hatua kuu za kuzuia kuenea kwa COVID-19 na kupunguza maambukizi. Hii imelazimisha mashirika mengi kuwaamuru wafanyikazi wao kufanya kazi kutoka nyumbani kwa kutumia mawasiliano ya simu. 'Telecommuting' au kufanya kazi kutoka nyumbani kwa sababu yoyote ile, inakuja na changamoto zake kuhusiana na hatari za usalama wa mtandaoni. Hapa chini kuna orodha iliyoandaliwa ya miongozo ya usalama unapo fanya kazi mtandaoni:

Vidokezo kwa Wafanyakazi Kupitia Mtandao

Tumia wifi unayoweza kuiamini tu. Kwa muunganisho wa wifi usio salama, watu walio karibu na wanaoweza kuiona wifi yako wanaweza kuyachungulia mawasiliano yako.

- Tumia vifaa vilivyoidhinishwa na Kampuni.
- Sasisha programu ya kupambana na virusi.
- Sasisha programu zote na programu vinjari.
- Kumbuka kuchelezo mara kwa mara. Faili muhimu sana zinapaswa kuchelezo mara kwa mara. Katika hali mbaya zaidi, inaweza kutokea kwamba mahasidi mtandao wakatumia, kwa mfano, program ya ransomu kuharibu data zako kama wafanyikazi wako wamekataa kulipa fidia inayotakiwa. Bila chelezo faili zako zote zitapotea.
- Hakikisha unatumia unganisho salama kwa mazingira yako ya kazi. Hii inamaanisha kutumia VPN au njia zingine salama kama program ya teamviewer.

- Jihadharini na barua pepe za hadaa. Mtu anapaswa kuwa na shaka juu ya barua pepe zozote zinazo uliza kuangalia au kusasisha vitambulisho vyako hata ikiwa inaonekana kutoka kwa chanzo kinacho aminika. Tafadhali jaribu kuthibitisha ukweli wa ombi lolote muhimu au la tuhuma kupitia njia zingine, usibofye fungo tovuti za tuhuma au kufungua viambatisho vyovyote vyenye kutiliwa shaka..

Vidokezo kwa Waajiri wa Wafanyakazi Watumia Mtandao

- Zingatia kupata mifumo inayowezesha ufikiaji wa mbali, kama vile VPN. Hakikisha mifumo hii imeimarishwa kikamilifu kiulinzi, ngomemoto inafanya kazi vizuri, na programu ya kuzuia programu hasidi na programu vamizi ipo imara.
- Kamwe usifunue moja kwa moja Remote Desk Protocol (RDP) kwenye mtandao (inahitaji kufanya unganisho la VPN kwanza)
- Tekeleza uthibitishaji wa vipengele vingi kila inapowezekana.
- Ikibidi zuia ufikiaji wa mifumo nyeti ya kompyuta yako na hata kuwasambazia wafanyakazi wako barua pepe ili kuwaongezea ufahamu kuhusu hatari za kuibiwa kimtandao taarifa za ofisi kama watakosa umakini
- Hakikisha wafanyikazi wanajua sera, faragha na majukumu ya kisheria ambayo yanatumika kwa habari ya shirika lao.
- Chekecha taratibu za dharura unazokusudia kutekeleza kama litatokea tukio la kiusalama na ikiwa ni lazima, waelemishe wafanyikazi wanaofanya kazi wakiwa mbali wakitumia mtandao kuhusu taratibu hizo
- Pitia upya mipango yako yote inayolenga kulinda na kuendelea biashara yako kiusalama. Hakikisha mipango hiyo haijapitwa na wakati.

2.12 Zana Zitumikazo katika Mikutano ya Video

Mwaka 2020 umekuja na mabadiliko makubwa katika dhana ya mikutano ya uso kwa uso ya na badala yake imekuja mikutano ya video na iliyo mubasahra mtandaoni na kusababisha jukwaa la Zoom kupata umaarufu mkubwa kati ya majukwaa mengi yanayowezesha mikutano ya kimtandao ya aina hii. Maendeleo haya pia yalishuhudia kuongezeka kwa “Bomu la Zoom”, ambapo mikutano ya mtandaoni iliingiliwa na watu wenye nia mbaya, na kusababisha usumbufu katika kuendesha mikutano hiyo vizuri. Ili kukabiliana na matukio kama haya, vidokezo hivi hapa chini vinaangazia hatua ambazo zinaweza kuchukuliwa.

Vidokezo vya Mikutano ya Video na Vikundi vya Gumzo

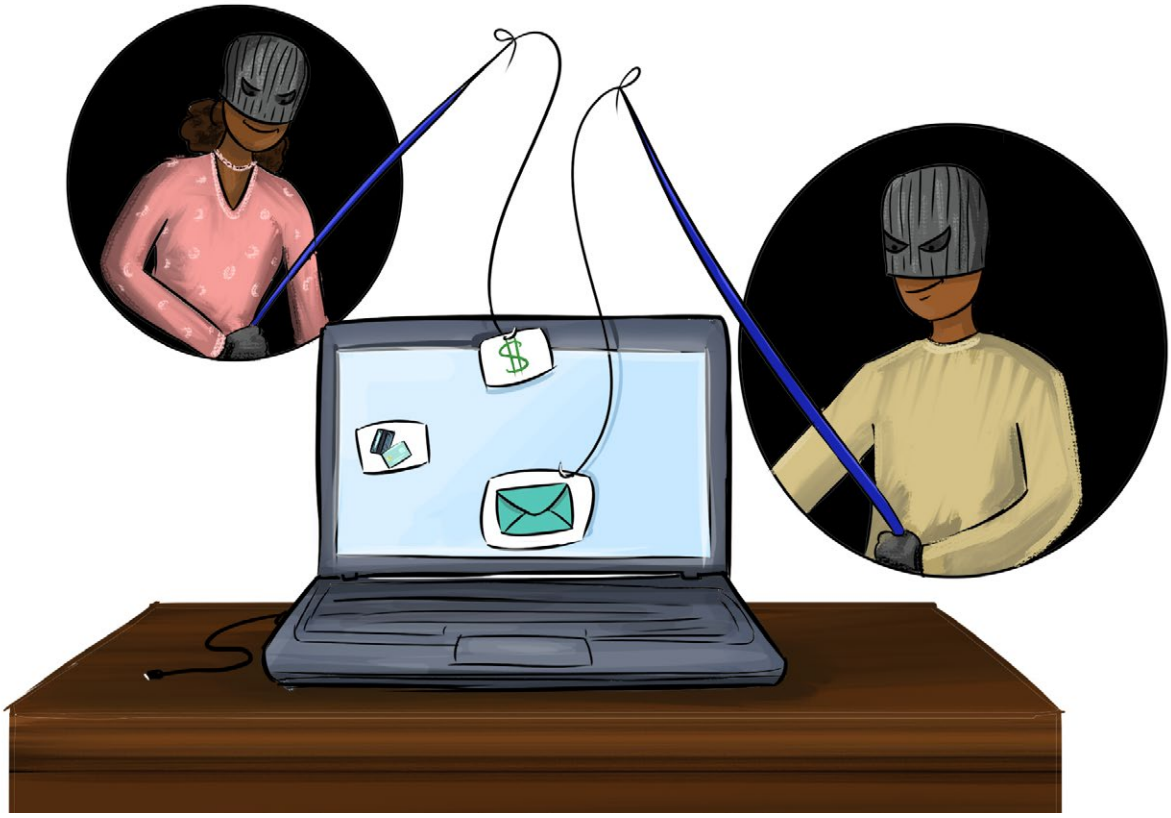
- Hakikisha washiriki wanaweza kujiunga kupitia mwaliko tu.
- Uhitaji wa matumizi ya nywila ili ujiunge na mkutano
- Pale inapowezekana, unahitaji idhini ya msimamizi kabla ya mtu mwingine kujiunga

na mkutano
- Usitume fungo tovuti kuunganisha mkutano kupitia mitandao ya kijamii.
- Hakikisha mkutano wa video na programu ya gumzo iko kila wakati.

Zana zingine za kuendesha mikutano ya video:

- Jitsi – https://jitsi.org/
- Google Meets – https://apps.google.com/meet/
- BlueJeans – https://www.bluejeans.com
- Signal – https://www.signal.org
- Cisco Webex – https://www.webex.com
- Microsoft Teams – https://teams.microsoft.com

2.13 Vitisho vya Usalama Dijitali: Programu Hasidi na Programu Ransomu



Kielelezo 11: Kutambua barua taka, programu hadaa, programu hasidi na virusi

a. Programu hasidi (Malware)

Hii ni programu au faili lililoundwa ili kusumbua, vamizi na linalodhuru mfumo wa kompyuta. Aina za programu hasidi ni pamoja na virusi, programu pelelezi, program ya matangazo ya biashara na minyoo mtandao. Programu hasidi zote mara nyingi husambaa kama viambatisho

vya barua pepe, ujumbe wa papo hapo, vipakuzi, wizi wa taarifa na data, na tovuti wizi. Mlipuko wa virusi husababisha madhara kwa kuharibu data kwenye kompyuta zilizo ambukizwa. Mlipuko unaweza kuchochewa kutokana na usambazaji mkubwa wa barua pepe ambazo hubeba virusi kwenda kwenye anuani zote za barua pepe zilizopo kwenye kitabu cha anuani au mchanganyiko wa anuani. Ikiwa mlipuko hautadhibitiwa haraka, wingi huo wa barua pepe unaweza kuzamisha seva na kuvuruga huduma ya barua pepe kwa wote. Ni rahisi kutambua uwepo wa programu ya virusi kwenye kompyuta yako kutokana na vitendo vyake na zana nyingi zipo zinazoweza kupambana na matishio ya aina hii.

Hatua za Kuzuia Programu hasidi

Haihitaji nguvu nyingi kulinda kompyuta yako dhidi ya program hasidi, unaweza kulinda kompyuta yako na kusaidia kuzuia shida mbali mbali kirahisi. Hatua zifuatazo zitazuia shambulio au kukabiliana na virusi ikiwa kompyuta itaambukizwa.

- Sakinisha[57] programu ya antivirus kwenye kompyuta yako.
- Sasisha[58] programu yako ya virusi hata kama hakuna ripoti ya virusi mpya.
- Usifungue kiambatisho kisichotarajiwa.[59]
- Zima huduma ya hakikisho katika programu zako kwa usalama zaidi.
- Pia zima huduma yoyote ya programu ambayo inaweza kufungua barua pepe moja kwa moja, Ujumbe wa papo hapo, faili ya kiambatisho au kupakua. .

b. Programu ya ransomu

Programu ya ransomu ni aina ya programu hasidi ambayo imeundwa kuzuia ufikiaji wa mfumo wote wa kompyuta au sehemu fulani ya mfumo huo hadi jumla ya pesa ya ransomu iliyoitishwa ilipwe. Kwa sababu washambuliaji wanalenga kupata pesa nyingi huwa, kwa kawaida, wanavizia mashirika makubwa (mashirika, idara, vyuo vikuu, biashara) ambazo sio tu kwamba uwezekano wa kuwa na fedha wanayohitaji upo lakini pia kupotea kwa data zao na kuvurugika kwa mifumo yao ya kompyuta kuna madhara na hasara kubwa. Walakini, watu binafsi bado wanalengwa pia s kwa sababu wanaweza wakawa kama lango la kuingia katika mifumo ya mashirika makubwa. Linapokuja suala la kuzuia mashambulizi ya ransom inaonekana hakuna njia ya mkato. Hata hivyo, mbinu zifuatazo zinaweza kusaidia kuzuia na kugundua programu ya ransom na kupunguza hatari ya kushambuliwa na programu hii hasidi.

Hatua za Kuzuia Programu ya ransomu

- **Punguza usambazaji na upatikanaji wa faili zako mtandaoni :**
  Ruhusu usambazaji wa faili mtandaoni kutegemea mahitaji halisi kwa kazi anazofanya unayemtumia. Kudhibiti usambaaji wa faili kwa kushirikisha watu wachache

57 https://cybersecurity.osu.edu/cybersecurity-you/use-right-tools/anti-virus
58 https://cybersecurity.osu.edu/cybersecurity-you/avoid-threats/updates-patching
59 https://cybersecurity.osu.edu/cybersecurity-you/avoid-threats/phishing

kutapunguza uwezekano wa kompyuta iliyoathiriwa na programu ransomu kuambukiza nyingine zilizomo kwenye mtandao.

- **Sasisha vitu vyako kwenye kompyuta:**
  Hakikisha programu zote zimesasishwa. Programu zilizopitwa na wakati ambazo hazina viraka vya ulinzi vya mara kwa mara husababisha hatari ya kushambuliwa na programu ransomu na programu hasidi zingine.
- **Tumia Programu ya Kupambana na Virusi:**
  Programu ya kupambana na virusi ni chombo kinachosaidia kugundua na kuondoa programu hasidi kutoka kwenye kompyuta yako. Unapaswa kuweka programu hii na kuisaashisha kila wakati kukuwezesha kugundua na kusafisha programu za ransomu ambazo zinaweza kuwekwa kwenye kompyuta yako.

2.14 Ufuatiliaji kawaida na ufuatiliaji wa jumla kwa siri mtandaoni

Ufuatiliaji watu mtandaoni ni pamoja na ufuatiliaji wa mahali alipo mtu, ukaguzi wa pakiti mtandao anazotuma kiundani, utambuzi wa sura, ufuatiliaji wa jumla na udakaji wa mawasiliano yake. Ufuatiliaji una athari mbaya na kuvunja moyo waandishi na wapasha habari kutafiti na kuchapisha habari na inawawia vigumu kulinda vyanzo vyao vya habari

2.15 Mashambulizi ya hadaa

Kampeni za “mashambulizi ya hadaa” mtandaoni au “mashambulizi hadaa mkuki” mara nyingi hutumia fungo tovuti au viambatisho kwenye barua pepe au kwenye mitandao ya kijamii na viambatisho au fungo tovuti hizo hubeba programu hasidi. Mara tu unapobofya fungo tovuti hizi au kufungua viambatisho unaweza kusababisha uharibifu mkubwa. Programu hasidi inaweza kuruhusu washambuliaji kupata habari yoyote wanayotaka kutoka kwa kompyuta iliyoathiriwa, pamoja na habari za kibinafsi za mwandishi wa habari, data na vyanzo husika vya data hiyo.

2.16 Mashambulio ya Domini bandia (Fake domains)

Hizi ni tovuti zenye domini bandia zenye kuiga zile halali kwa malengo mabaya. Vyombo vya habari vinavyojitegemea na tovuti za asasi za kiraia mara nyingi zimekuwa wahanga. Tovuti bandia hutumia programu hasidi au kuchapisha habari za uwongo kwa kujaribu kudhalilisha tovuti halisi ya chombo cha habari au mwandishi fulani wa habari.

2.17 Mashambulio ya Mtu Kati (MitM)

Washambuliaji hujiingiza kati ya mtumiaji na tovuti inayolengwa. Kwa mfano, ruta isiyo na waya imesanidiwa kuwa kama wifi ya 'kituo moto' (hotspot) cha hadharani, ili kudanganya watu wafikiri ni kituo salama. Wakati watu wanajiunganisha na wifi, mshambuliaji ana ufikiaji wa papo hapo kwa data inayopita kwenye ruta.

2.18 Mashambulio ya Kunyima Huduma (DoS)

Mashambulio haya ni ya kawaida, na yana jumuisha kompyuta moja au zaidi kutuma taarifa nyingi sana kwa makusudi hadi kujaza seva na kufurika na kushindwa kupokea taarifa zaidi kutoka kwa watumiaji wengine halali. Kwa waandishi wa habari, mashambulizi haya yanazuia habari kufikia umma na inaweza ikasababisha gharama kubwa kwa chombo cha habari kwani idadi ya wasomaji inaweza kushuka na kuhitajika msaada wa kiufundi na wa gharama kubwa kutatua tatizo.

2.19 Kuchunguza Watu kwa njia ya Mtandao

Kuchunguza watu kwa njia ya mtandao inahusu utumiaji wa mtandao au njia zingine za kielektroniki ili kumwandama na au kunyanyasa mtu, kikundi, au shirika. Inaweza ikawa shutuma za uwongo, kashfa, na kuaibisha. Inaweza pia kujumuisha ufuatiliaji, wizi wa utambulisho wa mtu, vitisho, uharibifu, au kukusanya habari ambazo zinaweza kutumiwa kutisha, kuadhiri au kunyanyasa.

2.20 Ubabe wa kimtandao

Uonevu wa kibabe wa mtandao ni matumizi ya njia za kielektroniki kama barua pepe, mitandao ya kijamii, ujumbe wa papo hapo, na aina nyingine za mawasiliano mkondoni kwa nia ya kumdhulumu, kumtisha, au kumzidi nguvu mtu au kikundi.

Bofya viungo hivi Kwa habari zaidi

1. https://tinyurl.com/y2kkmckg
2. https://tinyurl.com/y37nrxd7
3. https://tinyurl.com/yyu2y5ub

4. https://tinyurl.com/yxzfprhj
5. https://tinyurl.com/y25p5q3e
6. https://tinyurl.com/y3szuuhz
7. https://tinyurl.com/y692p5yw
8. https://tinyurl.com/yy92uvrc
9. https://tinyurl.com/y28vrj7z
10. https://tinyurl.com/yxpd2vpg

Sura ya Tatu

3.1 Usalama wa Kidijitali na wa Vifaa

a. Usalama wa Kidijitali kwenye Maandamano

Wakati mwingine katika kazi yao, watendaji wa haki za kidijitali huwajibika kushiriki katika maandamano ya kiharakati ili kusikilizwa sauti zao. Kubeba vifaa vya kidijitali katika maandamano kama hayo kunaweza kutumiwa dhidi ya waandamanaji, ikizingatiwa kwamba vikundi vya watekelezaji sheria dhidi ya maandamano wana zana za ufuatiliaji za kidijitali, kama minara bandia ya simu ya rununu na teknolojia ya utambuzi wa sura, ambayo inaweza kutumika kuwatambua waandamanaji na kufuatilia nyendo zao na mawasiliano wanayofanya, na hivyo kuhatarisha usalama na faragha zao. Kabla ya kuelekea kwenye maandamano ya amani, waandamanaji wanapaswa kuzingatia usalama na faragha yao ya kidijitali. Hapa chini ni mambo ambayo wanapaswa kuzingatia.

b. Kufanya matayarisho ya maandamano yawe ya faragha

Kuwa na huduma ya Mtandao wa Kibinafsi (VPN) inayo aminika inaweza kusaidia waandaaji wa maandamano kuyaficha mawasiliano yao ya mtandao. Vinginevyo, waandamanaji wanaweza kutumia zana kama vile Tor browser,[60] ambayo inalinda mawasiliano ya mkondoni ya mtumiaji kwa kudhibiti wafuatiliaji na kusimbu fiche mawasiliano yao ya mtandaoni yasisomeke. Pia, na muhimu sana, ni kuhakikisha upangaji unaohusiana na maandamano unafanywa juu ya Programu zilizosimbwa kwa mwisho hadi mwisho badala ya ujumbe mfupi wa maandishi (ijulikanayo kama SMS)

c. Usimbuaji Kamili wa Diski wa Vifaa vya Kidijitali

Ikiwa kifaa chako kitachukuliwa na maafisa wa kutekeleza sheria, na au kikapotea au kuibiwa, usimbuaji wa diski kamili unaweza kusaidia kulinda data iliyohifadhiwa kwenye kifaa chako. Vifaa vya Android[61] na iOS[62] vina uwezo wa usimbuaji wa diski kamili. Hizi zinapaswa kulindwa kwa kutumia nywila imara ili kuepuka kugundulika taarifa zake kwa kutumia shambulio la kikatili.

d. Sakinisha Programu Ishara

Ishara ni programu inayopatikana kwenye iOS[63] na Android[64] ambayo hutoa usimbuaji wenye nguvu wa mwisho kwa mwisho ili kulinda ujumbe wa maandishi na simu za sauti zisidukuliwe. Mbali na kusimba mawasiliano ya mmoja hadi mmoja, program ya Ishara inawezesha kufanyika mazungumzo ya kikundi yaliyosimbwa. Ni hivi karibuni programu hii iliongeza

60 https://www.torproject.org/
61 https://source.android.com/security/encryption/full-disk.html
62 https://www.apple.com/business/docs/iOS_Security_Guide.pdf
63 https://ssd.eff.org/en/module/how-use-signal-ios
64 https://ssd.eff.org/en/module/how-use-signal-android

utendaji kwa kuwa na ujumbe unapotea kutoka sekunde 10 hadi wiki baada ya kusomwa kwanza. Tofauti na huduma zingine kama SnapChat, ujumbe huu wa muda wa program ya Ishar hauwezi kuhifadhiwa hata kwenye seva yoyote, na huondolewa kwenye kifaa chako baada ya kutoweka.

e. Sasisha data yako

Chukua tahadhari ili kupunguza gharama zinazoweza kutokea za kupoteza ufikiaji wa kifaa chako, au kiwe kimepotea, kimeibiwa au kimechukuliwa na watekelezaji sheria. Hifadhi data yako mara kwa mara na uhifadhi nakala rudufu hiyo mahali salama ili kujiokoa na maumivu ya kichwa baadaye.

f. Simu Moto

Kwa waandamanaji ambao wana wasiwasi juu ya kufuatiliwa kwa simu zao, suluhisho la muda mfupi lakini lililo bora itakuwa kupata simu ya “burner”, au simu moto ambayo ni kifaa kilicho lipiwa salio au kifurushi kwa fedha taslimu ili kutumika kwa kusudi la wazi la kuwasiliana na watu wakati wa maandamano ya amani. Simu Moto huweza kuwapa watumiaji faida ya kuendelea au kuweza kuwasiliana wenyewe au na watu wengine - haswa ikiwa mambo yatageuka kuwa shaghala baghala - bila kufichua data yote kwenye kifaa chao cha kila siku. Vinginevyo, kuweka simu yako katika hali ya ndege kupaa ili kuzuia mawasiliano inaweza kutumika kwa kusudi lile lile. Usomaji zaidi unapatikana katika:
https://ssd.eff.org/en/module/attering-protest.

g. Usalama kwa Wanamtandao

Tishio la wanaharakati wa haki za kidijitali ni halisi kama ilivyo kwa vitisho vya usalama wa kidijitali. Vitisho hivi vina ambatana na kukamatwa, kunyanyaswa, kunyang’anywa vifaa, na kuwekwa kizuizini na watendaji wa serikali. Hali hii inawaweka wanaharakati katika hatari kubwa na inahatarisha usalama wao binafsi. Ili kupunguza vitisho hivi, wanaharakati wa haki za kidijitali wanahimizwa kuwa macho na dalili za tishio kwa usalama wao wa kibinafsi kwa kuzingatia mazingira yao, sheria na aina ya watu katika jamii. Kama ilivyo ada ni kwamba ili mpambanaji wa haki za kidijitali afanikiwe kulinda wengine, usalama wake lazima uhakikishwe kwanza.

3.2 Kupunguza Vitisho vya Usalama wa Wanamtandao

Kwa lengo la kupunguza hatari za wanamtandao, watendaji wa haki za kidijitali wanahimizwa kuzingatia yafuatayo:

a. Kukubali hatari hiyo:

Kukubali hatari hiyo inamaanisha kuwa mwathiriwa mwenyewe anatakiwa ajue na akubali kwamba anaweza kuwa katika hatari wakati wa kutekeleza shughuli zake. Kwa ufahamu kama huo, mtu huyo anatarajiwa kuwa atakuwa tayari kupunguza hatari au uwezekano wa hatari kutokea. Kwa mfano, wakati unakwenda kutoa huduma za kibinadamu katika eneo la vita, unahitaji kujua kwamba usalama wako uko hatarini; kwa hivyo unahitaji kuwa tayari kukimbia kama itakuwa lazima, kuomba msaada na unahitaji kuwasiliana na kuelezea utume wako kwa wapiganaji wanaohusika katika mapigano ili waweze kukupa ushirikiano ili ufike kwenye eneo au watu wanaostahili huduma yako salama. Pia, unapojua kuwa data yako inaweza kuwa katika hatari ya kushambuliwa na shambulio la mtandaoni (cyber attack), unahitaji kuunda nenosiri gumu, chunguza usalama wa majukwaa ya kidijitali ambayo unakusudia kutumia, shirikisha data yako kwa watu unaowaamini na pia uhifadhi data yako katika vifaa tofauti vya kuhifadhi.

b. Kuepuka hatari:

Kujua hatari ni jambo moja na kuiepuka ni jambo lingine. Unapojifunza juu ya hatari, unahitaji kuizuia kwa njia zote isitokee; katika kuizuia, hauhitaji kudai haki kwa yeyote au uhalali wa kufanya hivyo. Katika kuepusha hatari, mawasiliano na matendo yako yanapaswa kuakisi au kubadilika kulingana na hali iliyopo kwa wakati huo. Hivyo ni kwamba unahitaji kuwa makini na lugha yako ya kimwili na utumie maneno yako kwa busara, unahitaji kutathmini mazingira kabla ya kuanza shughuli zozote au kushirikiana na watu. Kadhalika, unahitaji kuelewa ikiwa kuna hatari au la na mwishowe, iwapo imethibitika kwamba unawindwa, huna budi kupinga azma ya mshambuliaji wako kwa ukali.

c. Unapaswa kuwa na kuwasilisha itikadi yako kwa watu sahihi:

Itikadi yako inaweza kukuweka katika hatari wakati wa kuitangaza. Kama mtetezi wa haki za binadamu, unahitaji kuwa na kiwango cha juu cha utambuzi wa yule unaemkabidhi habari yako au unaye mshirikisha mambo yako kwa sababu watu hawalazimiki kukubaliana na maoni yako.

d. Kama mwakilishi wa shirika unahitaji kujua shirika lako vizuri ikiwa ni pamoja na wewe mwenyewe:

Kuepuka hatari kama kiongozi, unahitaji kujua wewe ni nani, unafanya nini na unawakilisha wakina nani. Ni muhimu sana kwako kujua kila mahali uendako; utayari kama huu huwa muhimu sana wakati unashikiliwa mahabusu kama mtuhumiwa. Namna unavyoonekana, msimamo wako na shirika unalowakilisha lina ushawishi mkubwa juu ya jinsi utakavyo tendewa na waliokuweka mahabusu. Katika hali ya kawaida, mtuhumiwa asiye na hatia ataachiliwa baada ya kujieleza vizuri. Lugha ya mwili, uchaguzi wa maneno na utulivu mkubwa unahitajika sana kama uko katika mahojiano kama mtuhumiwa.

e. Mazingira:

Iwe ndani ya eneo lako, nje ya eneo lako au mahali popote ulimwenguni, unahitaji kuzingatia na kujibu maswali yafuatayo; 'Mimi ni nani? mimi niko wapi na wao ni akina nani'? Maswali haya ni muhimu sana kwa sababu shughuli zozote unazofanya zinahitaji kuzingatia maswali haya hapo juu kwa usalama wako. Kwa mfano, mtetezi wa haki za binadamu hawezi kuwa ndani ya kambi ya jeshi na kulaani ukatili unaofanywa na askari; kufanya hivyo ni dalili inayoonyesha kutofaulu kujibu maswali hapo juu kwa usahihi na kwa kutozingatia mazingira uliyopo. Majibu kama hayo yatasababisha kuendelea kuwekwa kizuizini kwa kutoa maoni yako kwa watu na katika eneo lisilo sahihi. Hawatakuachia.

f. Epuka maeneo ya hatari:

Maeneo kama ya mipakani mwa miji, umati wa watu, benki, maeneo yenye misongamano ya magari, mikutano ya hadhara, migogoro au maeneo yenye vita n.k ni maeneo ya hatari na tunahitaji kujifunza ni lini na wakati gani wa kutembelea maeneo kama hayo, kwa kuzingatia nafasi au heshima uliyo nayo kitaaluma na msimamo wako kisiasa au vinginevyo. Kwa mfano mwanaharakati wa haki za binadamu hashauriwi kutembelea maeneo yenye mizozo bila kuhakikishiwa usalama wake kutoka kwa wapiganaji. Mfano hai ni nchi ya Cameroon katika Kanda ya Anglophone ambapo kuna mzozo kati ya wapinzani wa kisiasa na vikosi vya serikali; Kwa ajili ya usalama wao, watoa huduma za kibinadamu hawawezi kuingia katika maeneo ya mapigano bila kupata uhakika wa usalama wao kutoka kwa wapiganaji. Hii ni kwa sababu wanaweza kuumizwa na risasi kwa bahati mbaya, kukamatwa au kutekwa nyara ikiwa watashindwa kuwa na hakikisho la usalama kutoka kwa wapiganaji.

g. Mavazi:

unahitaji kuwa makini na muonekano wako na kuelewa jinsi ya kuvaa wakati unapokuwa unafanya shughuli za kibinadamu katika maeneo hatari kiusalama. Kwa mfano, ikiwa wewe ni mtoa huduma za kibinadamu, wakati wa kwenda kufanya kazi hiyo unahitaji kuvaa viatu vyepesi na mavazi ambayo yanakuwezesha kutoroka kwa urahisi eneo la tukio au kukimbia wakati kuna tafrani iliyojitokeza. Ikiwa eneo lako haliko salama, epuka kuvaa tofauti sana na wengine wanaokuzunguuka au kuvaa nguo za gharama kubwa kwa sababu unaweza kulengwa kulingana na jinsi unavyoonekana tofauti kimavazi.

h. Usithubutu kubisha kama umenyooshewa bunduki au uko kwenye kambi ya kijeshi:

Kama umekamatwa mateka, au umezingirwa na wezi, fanya kila kitu wanacho kuamuru ufanye kunusuru maisha yako. Usipinge kwa sababu wanaweza kukuua; jali uhai wako kwanza

i. Kuwa na mahitaji yako ya kimsingi wakati wote unapokuwa eneo la mizozo ikiwa ni pamoja na sanduku la huduma ya kwanza:

Wakati wote unapokuwa kwenye misheni maeneo ya mizozo, kama kiongozi au mtoa huduma, unapaswa kubeba mahitaji yako ya kimsingi kwa kiasi kinachotosha huku ukizingatia afya yako, ugumu wa safari yenyewe, hali ya hewa ya mahali uendako, hali yako ya kifedha, hisia ulizo nazo nk. Hii itakuwa kwa usalama wako kwa sababu lazima ukubali hatari na uweze kutabiri namna bora ya kukabili hatari hizo kabla ya kwenda kwenye misheni yenyewe.

j. Daima kuwa na mawasiliano ya kuaminiwa na mitandao:

Katika kila taaluma haswa linapokuja suala la kazi hatari kama harakati za haki za binadamu, unahitaji kutabiri hatari ya kukamatwa, kutekwa nyara na au kushambuliwa kwa data ulizokusanya. Kama sababu za kujihami, unahitaji kuwa na watu wa kuaminika ambao unaweza kushirikisha kuhusu taarifa zako. Taarifa hizo ni pamoja na wao kujua eneo unalokwenda, wakati ambao unatarajiwa kuwa huko, wakati ambao unatarajiwa kurudi, kile kinachotarajiwa kufanywa ikiwa watapata wito wa dharura nk.

k. Weka, ujue na kukariri namba za mawasiliano ya dharura:

Unahitaji kuwa na nambari za mawasiliano za dharura kama, polisi, huduma ya wagonjwa, huduma ya moto, hospitali, n.k. Pakua na usakinishe programu ambazo zinaweza kutambua eneo ulilopo katika kifaa chako cha mtandao unapokuwa na shida. Soma zaidi:
https://tinyurl.com/y5wje4zk

Rasilimali nyingine:

1. https://tinyurl.com/y34p99o6
2. https://tinyurl.com/yy4t25hm
3. https://tinyurl.com/y2nn2ot9
4. https://tinyurl.com/y32w6ra
5. https://tinyurl.com/y369rudo
6. https://tinyurl.com/y6arpfw6
7. https://tinyurl.com/y85p49a3
8. https://tinyurl.com/y33cxu2u
9. https://tinyurl.com/y5wje4zk
10. https://tinyurl.com/y6spa5zk
11. https://tinyurl.com/y4tv7srz

Sura ya Nne

4.1 Kufungwa kwa Mitandao

Kielelezo 12: Uzimwaji mtandao

Ibara ya 19 ya Azimio la Ulimwengu la Haki za Binadamu linamhakikishia kila mtu haki ya uhuru wa maoni na na uhuru wa kusema; haki hii ni pamoja na uhuru wa kuwa na maoni binafsi bila kuingiliwa na haki ya kutafuta, kupokea na kutoa habari au maoni kupitia chombo cha habari chochote na bila kipingamizi. Walakini, katika miaka ya hivi karibuni, kumekuwa na tabia iliyojijenga ya mataifa ya Kiafrika kudhibiti mno uhuru wa habari juu ya raia wao. Hii imegeuza mtandao kuwa sehemu tete zaidi, na visa na changamoto zinazotolewa kwa wanaharakati, watetezi wa haki za binadamu, wapinzani, na waandishi wa habari zinaelezwa kuwa zinazidi kuongezeka.

Serikali za kimabavu zimeamua kutumia zana na mbinu za kidijitali kama kuzima mtandao, udhibiti wa mkondoni, na ufuatiliaji wa kidijitali ili kubana uhuru wa kujieleza. Ipo pia nukuu iliyotolewa na Uhuru House inayohusu Uhuru wa Mtandao 2018 inayosema “serikali kote ulimwenguni zinaimarisha udhibiti wa data za raia na kutumia madai ya ‘habari bandia’ kukandamiza wapinzani, kupunguza kuaminika kwa habari za mtandaoni na pia kuathiri misingi ya demokrasia.” Ripoti ya CIPESA ya 2019[65] inafichua kuwa serikali 22 za Afrika ziliamuru kuvurugwa kwa upatikanaji mtandao katika miaka minne iliyopita na kwamba tangu kuanza kwa 2019, nchi 6 za Afrika - Algeria, Jamhuri ya Kidemokrasia ya Kongo (DR Congo), Chad, Gabon, Sudan na Zimbabwe zilishinikiza kufungwa kabisa kwa mtandao. Kadhalika, wakati huo huo, nchi kadhaa, zimeendelea kuchukua hatua mbalimbali za kuminya haki za upatikanaji wa habari mtandaoni.

Kwa kuongezea, ripoti ya Mpango wa Paradigm 2019[66] ilibainisha kuwa serikali kadhaa za Kiafrika zimekuwa zikifunga Mtandao kwa sababu za kisiasa, kupitisha kanuni kali juu ya yaliyomo mkondoni, au kutumia mashambulio ya programu za kijasusi dhidi ya watetezi wa haki za binadamu. Ripoti hiyo iliongeza kuwa uhawilishaji huu wa mfano wa Wachina na Warusi za kile kinachoitwa “utawala wa sheria” kwa kudhibiti mtandao umeimarisha udhibiti wa serikali hizo na na hivyo kusababisha kuongezeka kwa ukiukaji wa haki za kidijitali kupitia sheria ambayo imeandikwa kwa kisingizio cha kuimarisha utawala wa sheria na utulivu katika jamii za Kiafrika.

Kielelezo 13: Takwimu za ufungwaji mtandao barani Afrika

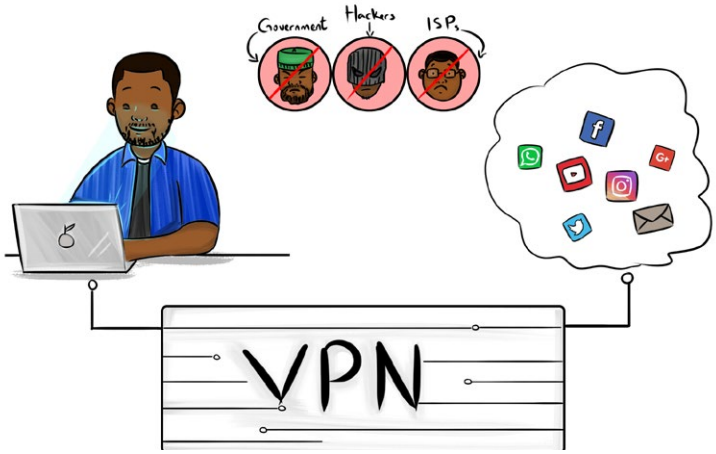
65 https://cipesa.org/2019/03/despots-and-disruptions-five-dimensions-of-internet-shutdowns-in-africa/
66 https://cipesa.org/2019/03/despots-and-disruptions-five-dimensions-of-internet-shutdowns-in-africa/

Zuio hilo limekuwa na athari mbaya za kiuchumi katika nchi zinazohusika. Utafiti wa Deloitte[67] unaonyesha kuwa kwa nchi iliyounganishwa vizuri na mtandao, athari ya kila siku ya kuzimika kwa mtandao kwa muda na huduma zake zote itakuwa wastani wa dola milioni 23.6 kwa kila watu milioni 10. Licha ya hatua hii ya mataifa kadhaa kubana nafasi za kidijitali, na mchakato huo kupunguza kazi ya wale walio mstari wa mbele katika utetezi wa haki za binadamu / kidijitali, sasa zipo ya programu na zana kadhaa za mtandao zinazowezesha kukwepa udhibiti wa serikali kama vile VPN, na nyinginezo kama web proxies ambazo zinatoa tumaini kwa wahudumiaji wa haki za binadamu, watetezi wa haki za kidijitali, waandishi wa habari, makachero na wengineo.

4.2 Kukwepa udhibiti na Kuzimwa kwa Mitandao

Utumiaji wa mtandao kwa kificho unaotumia zana za kukwepa kama vile VPN, Vivinjari vya Tor, na Tovuti wakala (Web proxies) unatoa tumaini kwa wahudumiaji wa haki za binadamu, watetezi wa haki za kidijitali, waandishi wa habari, makacherona wengineo

a. Mtandao wa Kibinafsi wa Virtual (VPN)



Kielelezo 14: Utumiaji wa mtandao wa kibinafsi wa VPN

Kama ilivyojadiliwa tayari katika sura ya pili chini ya usalama wa kidijitali, Mtandao wa Kibinafsi (au VPN) ni njia salama ya kuunganisha kompyuta yako kwenda kwenye mtandao mwingine wa shirika uliopo upande wa pili. Unapotumia VPN, mawasiliano yako yote ya mtandaoni hujumuishwa pamoja katika pakiti, husimbwa kwa njia fiche, na kisha kupelekwa kwa shirika lingine lililohodhi programu ya VPN. Mawasiliano yanapofika hupakuliwa na kutenganishwa au kusimbuliwa fiche, na kisha kupelekwa kwa mlengwa wa mawasiliano hayo. Unapo unganishwa na VPN, data zote za kuvinjari kwenye tovuti zinaonekana kutoka kwa VPN yenyewe, badala ya Mtoa Huduma wako wa Mtandao (au ISP). VPN hutumiwa na watu binafsi kukwepa udhibiti wa mawasiliano wa ndani, au kushinda uchunguzi wa ndani.

67 https://www2.deloitte.com/global/en/pages/technology-media-and-telecommunications/articles/theeconomic-impact-of-disruptions-to-internet-connectivity-report-for-facebook.html

4.3 Mbinu za Kupima Kuzimwa kwa Mtandao na Kiasi cha Udhibiti

a. Open Observatory of Network Interference (OONI):

Shirika la Uchunguzi wa Wazi wa Kuingiliwa kwa Mtandao ni mradi wa programu ya bure ambayo inakusudia kuunga mkono juhudi katika kuongeza uwazi wa udhibiti wa mtandao kote ulimwenguni. OONI hutengeneza programu ya chanzo huru[68] ana wazi inayoitwa OONI Probe ambayo unaweza kuitumia na kupima matukio kama :

- Kuzuia upatikanaji wa tovuti;
- Kuzuia programu za ujumbe wa papo hapo (WhatsApp, Facebook Messenger na Telegram);
- Kuzuia zana za kukwepa udhibiti (kama vile Tor na Psiphon);
- Uwepo wa mifumo (visanduku vya kati) katika mtandao wako ambavyo vinaweza kuwa na jukumu la kudhibiti na / au kufuatilia; na
- Kuvurugwa kwa kasi pamoja na utendaji wa mtandao wako.

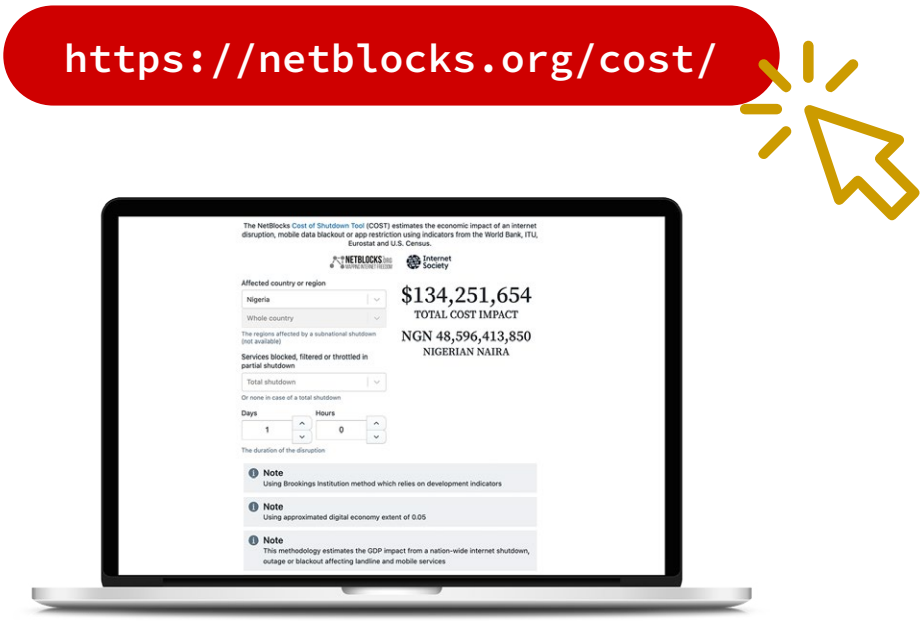
Kwa kuendesha programu ya OONI Probe,[69] unaweza kukusanya data ambazo zinaweza kutumika kama ushahidi wa udhibiti wa mtandao kwani inaonyesha jinsi gani, lini, wapi, na nani ametekeleza udhibiti.

4.4 Utetezi dhidi ya Kuzimwa kwa Mtandao barani Afrika

a. Programu ya Kupima Gharama za Kuzimwa Mtandao (COST)

COST ni jina la programu au zana inayotumiwa kupima gharama za kuzimwa kwa mtandao nakutoa takwimu halisi ili kushawishi serikali zione hasara za kuzimwa mtandao kiuchumi. Chombo hiki huwezesha mtu yeyote - pamoja na waandishi wa habari, watafiti, watetezi, watunga sera, wafanya biashara, na wengine wengi - kukadiria haraka na kwa urahisi gharama za kiuchumi za kuzimwa mtandao. Kwa kutumia na kuboresha misingi ya kitaalamu au kiteknolojia iliyoundwa na Taasisi ya Brookings[70] na CIPESA[71], Programu ya COST inakadiria gharama za kiuchumi zinazotokana na kuzimwa kwa mtandao, kuzimwa kwa data ya rununu na vizuizi vingine vya mitandao ya kijamii kwa kutumia maelfu ya viashiria vya kikanda kutoka Benki ya Dunia, Shirika la Mawasiliano Duniani (ITU), Eurostat na Sensa ya Amerika (US Census).

68 https://github.com/ooni/probe
69 https://ooni.org/install/
70 https://www.brookings.edu/wp-content/uploads/2016/10/intenet-shutdowns-v-3.pdf
71 https://cipesa.org/



Kielelezo 15: Utetezi dhidi ya ufungwaji wa mtandao barani Afrika

b. Kampeni ya #KeepItOn

Hii ni kampeni ya ulimwengu inayoongozwa na AccessNow inayolenga kuzihimiza serikali za ulimwenguni kote kutozima mtandao makusudi ili kuruhusu mtiririko wa habari bila kikwazo chochote.

Rasilimali

1. https://tinyurl.com/y4sul3dd
2. https://tinyurl.com/y5xxucxy
3. https://tinyurl.com/y49ckklq
4. https://tinyurl.com/y669mw6v
5. https://tinyurl.com/y6dhe2o4
6. https://tinyurl.com/y46tnwuk

FAHARASA

Anuwai - Neno linalosimama badala ya neno mbalimbali.

Arifa – Arifa inatokana na neno taarifa au arifu.

Bobezi – Bobezi linatokana na neno bobea au kubuhu hasa kitaaluma.

Chanya – Maana ya hili neno ni tendo au kauli inayoleta matokeo au muonekano bora.

Chelezo - Ni kitendo cha kuhifadhi data katika sehemu mojawapo ndani ya kifaa cha kidijitali kama komyuta au nje ya kifaa kuhakikisha usalama wa data hata kama kifaa hicho kitadhurika na data zilizomo kupotea.

Diski huru - Hifadhidata ni kifaa huru kinachotumiwa kunyonya data katika vifaa vya kidijitali hasa kompyuta ili data zibaki mahali salama hata kama kifaa chenyewe kitapata madhara na kupoteza data zote.

Fungo tovuti – Hii ni anuani unganishi ya kitovuti (web link) anayo bofya mtu kupata habari au taarifa zadi ya kile anachotafuta mtandaoni.

Hifadhidata - Mkusanyiko wa data ulio katika mpangilio maalum kidijitali kurahisisha upatikanaji na matumizi yake.

Kadiwiwa – Kadi ya simu ya mkononi au simu rununu.

Kaulisiri – Kaulisiri ni neno la siri lakini lililo refu zaidi ya neno moja.

Kishinikiza – Kibonyezo cha kuchagua kati ya “ndiyo” au “hapana” au kinachofanana na hicho kukamilisha uthibitishaji wakati wa kuvinjari mtandaoni au unapotumia vifaa vya kidijitali.

Kusimbu fiche – Ni tendo la kubadili maandishi yanayosomeka kawaida kuwa maandishi ya kificho au fiche yasiyosomeka yakiwa yanasafirishwa mkondoni au mtandaoni hadi yafike mwisho wa safari na kusimbuliwa fiche ili yasomeke tena katika hali yake ya asili.

Kusimbua fiche – Ni tendo la kurudisha maandishi kutoka kwenye hali ya simbu fiche yasiyosomeka kwenda kwenye hali ya kusomeka.

Lango tumizi – Lango ni kifaa kinachotumia programu (tumizi) kuunganisha mitandao miwili tofauti hasa maunganisho ya kimtandao.

Meneja Nywila - Meneja wa nywila au nenosiri ni chombo kinacho kutengenezea na kukuhifadhia nywila, kwa hivyo unaweza kutumia nywila nyingi tofauti kwenye tovuti na huduma tofauti bila kuzikumbuka. Ili kuzipata nywila zilizohifadhiwa, unhitaji kuwa nakutumia nywila kuu.

Mintarafu – Makusudi, nia, sababu au lengo.

Mkondoni – Inatokana na neno mkondo au kuwa kwenye mkondo. Mtu anakuwa mkondoni kama ameshaingia kwenye mtandao na kuonekana kwa watu wengine na kuweza kuanzisha mawasiliano.

Msimbo – Mkusanyiko wa namba chache zitumikazo kama nywila au nenosiri la kuwezesha kuingia au kufungua akaunti yako kama ya benki, mtandao au kifaa kama simu rununu.

Nenosiri – Neno la siri ambalo unahitajika kuitumia ili upate ruhusa ya kuingia katika eneo au kufungua kifaa cha kidijitali.

Ngomemoto - Chombo cha ulinzi kinacholinda kompyuta na maunganisho yasiyohitajika au kuaminika kutoka nje. Inaweza kukataza barua pepe zisitoke au kuingia au unganisho kwa tovuti zingine. Ngomemoto zinaweza kutumika kama safu ya kwanza ya ulinzi kulinda kifaa chako au mtandao wako wa ndani ofisini kwako kutokana na usumbufu usiyotarajiwa.

Nywila - Neno la siri au kauli iliyochanganyika au la na nambari au alama ambayo unahitajika kuitumia ili upate ruhusa ya kuingia katika eneo au kufungua kifaa cha kidijitali.

Nywila kuu – Hii ni nywila inayotumika kupata nywila zingine zilizosimbwa na kuhifadhiwa kwenye stoo ya program iitwayo Meneja Nywila. Ni nywila inayolinda nywila zingine.

Programu – Chombo au programu zinazohitajika kupakiwa kwenye kompyuta au kifaa kingine cha kidijitali ili kuweza kufanya kazi mbalimbali kutokana na mahitaji. Kwa kawaida programu za aina hii ni nyingi kwa kila nyanja au taaluma.

Programu Endeshi (OS) - Programu inayoendesha programu zingine zote kwenye kompyuta au kifaa. Windows, Linux, Android ni mifano ya programu vinjari au uendeshaji.

Programu hasidi – Hizi ni programu ambazo zimetengenezwa kutekeleza vitendo visivyohitajika kwenye kifaa au kompyuta yako kama virusi, miyoo mtandao. Virusi vya kompyuta vyote ni aina ya programu hasidi na hata programu zinazoiba nywila, zinazo kurekodi kwa siri, au zinazofuta data yako.

Programu vinjari – Hii ni program ya kompyuta inayomwezesha mwana mtandao kuona kutembelea na kuvinjari kurasa za tovuti mbalimbali.

.

Sasisha – Weka au pakia programu kwenye kifaa au chombo cha kidijitali ili kukiboresha upya kifanye kazi kwa ufanisi unaotakiwa kwa muda uliopo.

Sanisha – Weka au pakia program kwenye chombo au kifaa cha kidijitali tayari kwa matumizi au uendeshaji wa kifaa.

Seva wakala – Hii ni kompyuta inayosimama kama lango linalopitisha maombi ya kuingia au kutoka kwenye kompyuta au mtandao wa nje au kwenda katika mtandao wa ndani wa shirika.

Tasnia – Ni eneo au sekta ya ujuzi wa kitaalamu.

Taswira – Sifa au muonekano wa kifikra wa kitu au mtu mbele ya jamii.

Tovuti – Ni mkusanyiko wa kurasa za habari au taarifa za shughuli za shirika, mtu au watu zinzopatikana kwa kutumia anuani moja ya kimtandao (IP).

Usanidi – Kupanga au kuelekeza mfumo wa programu ya kompyuta au chombo kinachofanana na hicho ili ufanye kazi kutokana na mahitaji ya mtumiaji.

Unadhifu mtandao - Inamaanisha kupanga faili kwenye kompyuta yako, kufunga akaunti zako za mitandao ya kijamii, kuanzisha programu mpya au teknolojia za kufanya maisha yako ya kidijitali yawe rahisi au salama zaidi.

VPN – Mtandao wa kibinafsi ni njia salama ya kuunganisha kompyuta kwenda kwenye mtandao mwingine wa shirika uliopo upande wa pili. Unapounganishwa na VPN, data zote za kuvinjari kwenye tovuti zinaonekana kutoka kwenye jukwaa la VPN yenyewe na sio kwenye anuani inayoweza kukutambulisha wewe mtuma ujumbe na hivyo kukupa faragha kama mtumiaji. Pamoja na kuficha anuani yako ya asili ya (IP), pia VPN inasimbu fiche data yako hata ukiwa unavinjari na upo kati ya tovuti moja na nyingine.

AYETA

Kifaa cha Zana cha Haki za Kidijitali

PARADIGM INITIATIVE

ParadigmHQ.org

@ParadigmHQ

/ParadigmHQ

/ParadigmHQ

Kingdom of the Netherlands

Stanford PACS
Center on Philanthropy and Civil Society
—
Digital Civil Society Lab