

Wi-Fi ya Umma

Washirika watajifunza kuhusu mitandao ya umma ya Wi-Fi na manufaa na hatari zake. Kwa ubainifu zaidi, watajifunza kutambua Wi-Fi isiyo salama inapopatikana kwao, kuelewa ujanja halisi katika kutumia Wi-Fi isiyo salama, na kufanya maamuzi ya busara kuhusu wakati wa kuunganishwa kwenye na kutumia Wi-Fi isiyo salama.

Rasilimali

Taswira ya Modemu Pasiwaya
Kitini cha Usalama wa Muunganisho

Je, Wi-Fi ni nini?

Sehemu ya Kwanza

Uliza Wanafunzi Wako

Ni vifaa vipi unavyotumia kufikia Intaneti?

Je, vifaa hivyo vinaunganishwa vipi kwenye Intaneti?

Mwingiliano wa Darasa la Taswira

Wi-Fi ni njia ya kawaida ya kuunganisha vifaa kwenye Intaneti. Wi-Fi hutumia ishara za redio kuunganisha vifaa bila muunganisho halisi au wa waya.

Fikiria kuwa una kompyuta ndogo tatu nyumbani kwako ambazo ungependa kutumia ili kuunganishwa kwenye Intaneti. Ili kufanya hivyo, utahitaji vitu vifuatavyo:

1. Eneo la ufikiaji: Eneo la ufikiaji ni kitu chochote kinachosambaza (matangazo?) ishara ya Wi-Fi na kutoa ufikiaji kwenye Intaneti. Vifaa vyako vinahitaji kuchukua ishara hizi ili kuunganisha kwenye Intaneti. Wakati mwingine unaweza kuhitaji kibali maalum (km. jina la mtumiaji na nenosiri) ili kuingia na kutumia ishara pasiwaya ambayo AP hutangaza.
2. Kipanga njia: Kipanga njia ni kifaa kinachounda mtandao baina ya vifaa vyote (km. kompyuta, kompyuta ndogo, simu za mkononi) katika eneo fulani (kama shule, maktaba, au nyumbani kwako). Kwa kawaida, vipanga njia vinafikia eneo lilojengewa ndani yake (tazama mchoro ulio hapo juu).

Vipanga njia vinawekewa mipaka kwenye masafa (kwa mafupi). Hiyo ndiyo sababu iwapo kifaa chako kipo mbali sana kutoka kwenye kipanga njia, utapata ishara dhaifu ya Wi-Fi au ukose kupata yoyote hata kidogo. Pia, iwapo kuna kitu katikati yako na kipanga njia (kama jengo au ukuta wa matofali), hicho kitapunguza ishara yako.

Ingawaje kuunganisha kwenye kipanga njia hutoa ufikiaji kwenye mtandao, hii haimaanishi utafikia Intaneti. Ili vifaa mbalimbali kwenye mtandao viweze kuunganishwa kwenye Intaneti, kipanga njia kinafaa kuunganishwa kwenye modemu.

3. Modemu: Modemu ni kifaa ambacho kinaunda na kudumisha muunganisho kwenye Mtoa Huduma Wako wa Intaneti (ISP) ili kukupa ufikiaji kwenye Intaneti. Kinageuza ishara kutoka nje ya eneo lako lililotolewa hadi kwenye ishara ambazo zinaweza kusomwa na kompyuta yako na vifaa vingine vya kidijitali.

Katika usanidi wa kawaida, AP na kipanga njia ni kifaa kimoja ambacho kinaunganishwa kihalisi kwenye modemu, kwa kutumia kebo maalum inayoitwa kebo ya Ethernet. Watu humaanisha hiyo wanapozungumzia kuhusu muunganisho wa Internet wa "waya".

Vifaa vya mkononi pia vinaweza kutumia muunganisho wa mtandao wa simu ili kuunganisha kwenye Internet, hususan iwapo hawapo kwenye mtandao wa shuleni, mkataba, au nyumbani. Miunganisho ya mtandao wa simu ni aina ya ishara pasivaya ya radio inayotumika katika eneo kubwa ambalo kipanga njia kipo. Miunganisho ya mtandao wa simu hutumia vipokezi na visambazaji maalum vya mawasiliano, vinavyoitwa minara ya seli, ili kuunganisha vifaa vyako kwenye Internet.

Sehemu ya Pili

Uliza Wanafunzi Wako

Je, manufaa ya Wi-Fi ni yapi?

Je, baadhi ya changamoto za Wi-Fi ni zipi?

Je, baadhi ya matatizo ya usalama wakati wa kutumia Wi-Fi dhidi ya muunganisho wa Internet kupitia waya yanaweza kuwa yapi?

Mbona unapoteza ufikiaji wa Wi-Fi kwenye simu yako unapoondoka kwenye jengo?

Kuchagua Mtandao wa Wi-Fi

Sehemu ya Kwanza

Uliza Wanafunzi Wako

Je, mitandao yote ya Wi-Fi ni salama? Mbona/kwa nini siyo?

Ambia Wanafunzi Wako

Wakati mwingine, unapewa chaguo kuhusu mtandao wa Wi-Fi ambao ungependa kutumia. Ni muhimu kukumbuka kuwa kuna hatari kubwa iwapo utaunganishwa kwenye mtandao mbaya. Kwa mfano, mitandao ya Wi-Fi isiyo salama ni ile ambayo haihitaji nenosiri ili kuingia. Iwapo upo kwenye mtandao usio salama, inawezekana watu wengine kwenye mtandao kama huo kuona maelezo yako. Wanaweza kuiba maelezo unayoyatuma kupitia mtandao au kufuatilia unachofanya.

Upande mwingine, mitandao ya wi-Fi salama na inayoaminika ni ile ambayo inahitaji nenosiri, limewezeshwa usimbajifiche, na ile ambayo una uhakika kuhusu mtandao unaoingia ni ile ambayo jina la mtandao linawakilisha. Kwa mfano, kuingia kwenye mtandao unaoiga jina la mtandao wa shule yako kunaweza kusababisha ufichuzi wa maelezo ya akaunti. Kwa hivyo, mitandao ambayo ni salama na inaaminika ni ile ambayo hutoa ulinzi zaidi.

Jambo moja la kuzingatia ni muktadha au eneo la mtandao wa Wi-Fi. Kwa mfano, iwapo upo katika ukumbi wa filamu na unatumia jina la mtandao wako wa shuleni kwenye simu yako unapotafuta muunganisho wa Wi-Fi, huenda ukazingatia kuwa mtandao unajaribu kuiga au "iga" mtandao wako wa shule ili kukusanya manenosiri kutoka kwa wanafunzi wasio na ufahamu.

Unaposanidi mtandao wa Wi-Fi uliolindwa kwa nenosiri, mmiliki anafaa kuchagua kuwasha itifaki ya usimbaji fiche wa kipanga jina. Itifaki za kawaida za usimbaji fiche ni Faragha Sawa ya Waya (WEP), Ufikiaji Uliolindwa wa Wi-Fi (WAP), au WPA2. Itifaki hizi zinasaidia ili maelezo yaliyotumwa kwa njia pasiwaya kupitia mtandao yanasimbwa fiche (au "yanaharakishwa").

Usimbaji fiche uliundwa ili kufanya iwe vigumu kwa wadakuzi kuona unachotuma. Itifaki hizi zote (WEP, WPA, na WPA2), hata hivyo, zimeonyeshwa kuwa katika hatari ya kulaghaiwa. Kwa hivyo, ni muhimu pia kutegemea miunganisho salama ya wavuti unaposambaza maelezo mtandaoni.

HTTPS ni kiwango kinachotumiwa na tovuti ili kusimba fiche data iliyopitishwa kupitia Intaneti. Usimbaji fiche unaweza kuzuia mhusika yeyote mwingine kutazama rahisi data kutoka kwenye muunganisho wako. Inatoa safu ya ziada ya usalama na inaweza kutumiwa kwenye kivinjari chochote kwa kuongeza "https://" mbele ya URL unayotumia (km., <https://www.mysite.com>). Hata hivyo, sio tovuti zote zinaauni

HTTPS.

1. Unafaa kuingiza tu maelezo nyeti (km., manenosiri, maelezo ya kadi ya mkopo) kwenye kurasa za wavuti kwa kiambishi awali cha HTTPS://.
2. Vivinjari zaidi vikuu vina viashirio vya usalama vinavyoonekana kama kufuli karibu na mwambaa wa anwani ili kuashiria miunganisho ya HTTPS.
3. Kwa bahati mbaya, HTTPS haihakikishi kuwa uko salama kwa kuwa baadhi ya tovuti hasidi pia zinaweza kuauni HTTPS. HTTPS hulinda muunganisho lakini haihakikishi kuwa tovuti ni nzuri.

Ambia Wanafunzi Wako

Safu ya Soketi Salama (SSL)/Usalama wa Safu ya Usafiri (TLS) ni majina ya teknolojia inayolinda HTTPS. SSL/TLS hutumia vitufe vya usimbaji wa kidijitali, vinavyofanya kazi zaidi kama vitufe halisi. Iwapo uliandika siri kwenye sehemu ya karatasi la rafiki yako, yeyote aliyepata karatasi anaweza kuona siri yako. Badala yake, fikiria kuwa ulimpa nakala ya kitufe mwenyewe, na kisha kutuma siri zako kwenye vikasha vilivyofungwa vinavyofanana. Iwapo mtu atasitisha kikasha, atakumbana na wakati mgumu kuona siri yako bila kitufe. Iwapo mtu alijaribu kubadilisha kikasha na kile kinachofanana, utagundua kuwa kitufe chako hakitafanya kazi. SSL/TLS hufanya kazi kwa njia sawa, lakini kwa tovuti.

Viashirio vya usalama wa kivinjari pia vitawasilisha maelezo ya cheti cha Uhalali Uliorefushwa (EV). Vyeti vya EV vinatolewa kwa tovuti inayobainisha utambulisho wake kwa mamlaka ya cheti. Kwenye vivinjari, wakati mwingine kiashirio cha EV kinachukua aina ya jina la tovuti ama shirika linalosajiliwa karibu na mwambaa wa anwani. Iwapo unashuku maudhui kwenye tovuti fulani, unaweza kuangalia ili kuona iwapo cheti kinafanana na URL kwenye kivinjari kwa kubofya kwenye "Tazama Cheti." [inaweza kuwa na umuhimu, kwenye kiwambo, kuonyesha washiriki jinsi ya kutafuta "tazama Cheti." Jinsi ya kuabiri kwenye hii hutofautiana na kivinjari. Kwa mfano, kwenye Chrome, chini ya "Tazama," bofya "Msanidi programu" na kisha "Zana za Msanidi programu." Kutoka kwenye "Zana za Msanidi programu" bofya kichopo cha "Usalama", kisha "Tazama Cheti."

Uliza Wanafunzi Wako

Unafaa kufikiria nini kuhusu wakati wa kuunganisha kwenye mtandao mpya?

1. Majibu yanayotarajiwa yanajumuisha: eneo (au anayemiliki mtandao), kufikia (au mtu mwingine aliyeunganishwa kwenye mtandao), na shughuli (au unachofanya kwenye mtandao).

Ni nani anamiliki mtandao wako wa Wi-Fi nyumbani? Shuleni? Katika duka la

kahawa?

1. wazazi/walezi wako wanamiliki mtandao wako wa Wi-Fi wa nyumbani, wasimamizi na/au wilaya inamiliki mtandao shuleni, na mmiliki anamiliki mtandao wa duka la kahawa.

Unawafahamu hawa watu kibinafsi? Je, unawaamini hawa watu?

1. Wahusishe washiriki katika majadiliano kuhusu jinsi wanavyofaa kuwaamini watu hawa tofauti.

Ambia Wanafunzi Wako

Unafaa kufahamu na kuamini mtu anayepangisha mtandao wa Wi-Fi. Wakati mwingine, unaweza kuthibitisha mmiliki ni nani kwa kutumia SSID ya mtandao.

Kitambulishi cha Seti ya Huduma (SSID) ni jina lililotolewa la mtandao wa Wi-Fi unaloweza kuona unapotaribu kuunganisha. Mara kwa mara SSID inatumika kuwasiliana na anayemiliki mtandao na maelezo mengine kuhusu mtandao. Hata hivyo tahadhari kwa kuwa karibu kila mtu (anayefahamu jinsi ya kufanya hivyo) anaweza kuunda SSID. Kwa mfano, mtu anaweza kuunda SSID inayofanana na ile unayoitumia shuleni. Huu ni mfano wa uigaji wa mtandao unaojulikana na kuaminika, ili kuweza kupata majina ya mtumiaji na manenosiri.

Kufahamu anayepangisha mtandao kunaweza kukusaidia kuthibitisha iwapo mtandao ni salama. Iwapo ni wa mtu au shirika unaloamini, basi utajihisi vizuri kuunganishwa. Hata hivyo, iwapo ni mtandao usiojulikana, hufai kuunganishwa kwa kuwa hufahamu anayemiliki kipanga njia ambacho unaunganishwa. Kwa sababu trafiki yote kwenye mtandao hupitia kwenye kipanga njia, mmiliki anafaa kufuatilia au kurekodi trafiki ya wavuti wako.

Unapounganishwa kwenye Wi-Fi, kifaa chako kinaunganishwa kwenye mtandao wa ndani wa vifaa, na mtandao huo huunganishwa kwenye Intaneti pana. Kwa sababu kifaa chako kinabadilishana maelezo kwa mtandao huu, ni muhimu kuamini vifaa vingine ulivyounganishwa — ana hilo linamaanisha kifaa chochote kwenye mtandao. Ni kama tu kazi ya kikundi unayofanya shuleni — unataka kuweza kuwaamini watu unaofanya kazi nao!

Kwa kutumia nenosiri kwenye mtandao kunaweza kuweka mipaka kwa anayeweza kuutumia. Hii inamaanisha kuwa utakuwa na wazo bora kuhusu aliye kwenye mtandao — iwapo ni familia yako, marafiki zako, au wateja wengine katika duka la kahawa — kuliko iwapo mtandao ulikuwa huru kikamilifu.

Iwapo utaamua kujiunga kwenye mtandao ambao huenda ukanonekana kushukiwa unafaa kufanya kwa upande wa usalama wa mtandaoni au la. Huenda ukazingatia,

Nitapimaje uwezekano wa akaunti yangu kukiukwa dhidi ya urahisi wa kujiunga kwenye mtandao uliopo?

Uliza Wanafunzi Wako

Je, unafaa kusoma habari za mtandaoni/blogu kwa kutumia mtandao wako wa Wi-Fi nyumbani? Shuleni? Katika duka la kahawa?

1. Fafanua kuwa maudhui ya ukurasa wa wavuti kwa kawaida sio maelezo nyeti. Huwezi kufanya hilo kwenye mtandao wowote.

Je, unafaa kutuma nambari ya kadi ya mkopo kwa kutumia mtandao wako wa Wi-Fi nyumbani? Shuleni? Katika duka la kahawa? Kwa nini?

1. Jihusishe kwenye majadiliano kuhusu ni kwa nini ni salama zaidi kufanya hivyo na Wi-Fi yao ya nyumbani na sio Wi-Fi ya duka la kahawa. Pia jadili jinsi, unapokuwa kwenye mtandao wa shuleni kuna uwezekano wa uaminifu, iwapo inawiana na hatari kwa kuwa maelezo haya maalum ni nyeti zaidi/.

Je, unafaa kuangalia barua pepe yako ya kibinafsi kwa kutumia mtandao wako wa Wi-Fi nyumbani? Shuleni? Katika duka la kahawa?

1. Jadili jinsi ni salama zaidi kufanya hivyo na mtandao wao wa nyumbani, kulingana na maudhui ya akaunti ya barua pepe. Kwa mfano, baadhi ya watu wana akaunti anuwai za barua pepe wanazotumia kwa malengo tofauti (km., uuzaji / barua pepe za matangazo kwa akaunti moja; barua pepe za marafiki na familia kwenye akaunti nyingine).

Ambia Wanafunzi Wako

Maelezo nyeti, yakijumuisha manenosiri na maelezo ya benki, ni bora yatumwe/kutazamwa kwenye mtandao wa kibinafsi na salama, kwenye tovuti zinazotumia SSL/TLS kuliko kwenye mtandao ulioshirikiwa wa umma. Maelezo haya ya kibinafsi yapo hatarini iwapo utawasilisha au kuyafikia unapokuwa kwenye mtandao ulioshirikiwa unaotumika na watu usiowafahamu au kuwaamini.

Huenda isiwe dhahiri jinsi ambavyo maelezo ni nyeti au sio nyeti kwa sababu faragha ni uamuzi wa kibinafsi ambao unafaa kujifanyia. Ni muhimu kuzingatia kila hali kivyake ili kuamua iwapo unafaa kuunganishwa kwenye mtandao. Jiulize iwapo unaamini mmiliki wa mtandao, wengine waliounganishwa, shughuli unayoifanya mtandaoni, na maelezo unayoyashiriki kabla ya kuamua kuunganishwa au la.

Mitandao Salama na Isiyo Salama

Sehemu ya Kwanza

Mwingiliano wa Darasa

Tafadhali kumbuka: Sehemu ya maudhui ya shughuli hii imeshughulikiwa katika “Shughuli #2: Kuchagua Mtandao wa Wi-Fi.” Tunahairisha uamuzi wako kulingana na iwapo ungependa kupitia tena nyenzo hii au kuiruka au la.

Ambia Wanafunzi Wako

Kama ilivyotajwa mapema, mitandao ya Wi-Fi isiyo salama ni ile ambayo haihitaji nenosiri ili kuingia. Matumizi ya mitandao isiyo salama yanahatarisha data unayoisambaza na kuipokea kupitia mtandao.

Mitandao ya Wi-Fi salama ni ile ambayo inahitaji nenosiri na imesimbwa fiche. Mtu aliyesanidi mtandao ndiye huchagua iwapo atawezesha usimbaji fiche au la. Usimbaji fiche hufunga maelezo unayotuma au kupokea kupitia mtandao, kwa hivyo ni vigumu zaidi kwa wadakuji kwenye mtandao huo wa Wi-Fi kuona unachotuma au kupokea.

Kwa sababu mtandao ni salama haimaanishi kuwa data yako ni salama. Kwa hakika ni salama kuliko kutumia mtandao usio salama; hata hivyo, mdakuji aliyejitolea bado anaweza kutafuta njia ya kufikia maelezo yako.

Kuna itifaki tatu za usimbaji fiche wa kawaida kwa mitandao ya Wi-Fi: Faragha Sawa ya Waya (WEP), Ufikiaji Uliolindwa wa Wi-Fi (WAP), au WPA2. WEP na WPA zimepitwa na wakati na mitandao inayotegemea hizi inafaa kuchukuliwa kuwa sio salama. Zaidi ya hayo, pia WPA2 imeonyeshwa kuwa katika hatari ya kulaghaiwa.

Ili kuhakikisha maelezo yako yamelindwa kikamilifu, hakikisha kuwa tovuti unazotumia zimesimbwa fiche kwa kutumia SSL/TLS.

Uliza Wanafunzi Wako

Je, mtu yeyote anaweza kufikiria mfano wa mtandao uliolindwa kwa nenosiri ambao ameutumia?

1. Baadhi ya mifano inajumuisha Wi-Fi yake ya nyumbani, Wi-Fi ya shuleni, na mitandao ya Wi-Fi katika baadhi ya maeneo ya umma kama mikahawa.

Je, mtu yeyote anaweza kufikiria mfano wa mtandao usio salama ambao ameutumia?

Vipi kuhusu mifano ya mtandao salama?

Ambia Wanafunzi Wako

Unaweza kuhakikisha iwapo mtandao wa Wi-Fi umesimbwa fiche kwa kuchunguza mtandao au mipangilio posiwaya kwenye kifaa chako.

Sehemu ya Pili

Mwingiliano wa Darasa

Kabla ya tajiriba hii ya mafunzo, endesha utafutaji wa Intaneti ili kukagua jinsi ya kuangalia aina za usimbaji fiche wa mtandao wa Wi-Fi kwa mifumo tofauti ya uendeshaji. Kisha, onyesha jinsi ya kutafuta aina ya usimbaji fiche ambayo mtandao hutumia. Kwa mfano, kwenye MacOS, bofya kwenye Mapendeleo ya Mfumo -> Mtandao -> Teua Wi-Fi -> teua Jina linalofaa la Mtandao. Unda kichupo cha Wi-Fi, kutakuwa na orodha ya mitandao isiyojulikana na safuwima inayoonyesha aina ya usimbaji fiche inayotumika.

Ambia Wanafunzi Wako

Miunganisho yote sio sawa. Wakati mtandao sio salama, mtu yeyote anaweza kuunganishwa kwenye mtandao, na haijawekwa wazi kuhusu anayedhibiti mtandao. Kujiunga kwenye mtandao usio salama hukuweka hatarini kwa sababu maelezo unayoyatuma na kupokea, kama trafiki ya wavuti wako (kurasa, manenosiri, nk.), yanaweza kutazamwa na mtu yeyote kwenye mtandao iwapo hutumii muunganisho wa SSL/TSL.

Mwingiliano wa Darasa

Kulingana na maarifa ya kiufundi ya mshirika wako, unaweza kutaka kujadili matumizi ya Mitandao Pepe ya Kibinafsi (VPN) kama safu ya ziada ya usalama unapotumia Wi-Fi. Tafadhali rejelea viungo vya VPN kwenye sehemu ya Rasilimali kwa maelezo ya ziada.

Kutambua Usalama wa Muunganisho

Kichwa cha Sehemu

Mwingiliano wa Darasa

Gawanya washirika katika vikundi vya 2-3. Pitisha Usalama wa Muunganisho: Kitini cha Mshiriki na uteue tukio kwa kila kikundi. Wape washirika dakika 5 ili kujadili matukio yao. Baadaye, uliza vikundi kushiriki majibu yao. Majibu yapo katika rangi ya kijani kwenye kitini.

Kazi

Sehemu ya Kwanza

Utoaji

Waulize washiriki:

1. Wachore kalenda ya matukio ya siku ya kawaida, huku wakiweka alama kwenye mitandao ya Wi-Fi wanayounganishwa.
2. Kutoka kwenye mitandao iliyoteuliwa iliyoonyeshwa kwenye kalenda ya matukio, waambie washiriki wachague miwili na katika ya futi kwa kila mmoja, afafanue mtandao — ni nani mwingine amaunganishwa? Je, ni salama vipi?
3. Kwa ziada — kwa mitandao miwili iliyochaguliwa — waruhusu washiriki wafafanue fursa ambazo huja na kuunganishwa kwenye mitandao hii na hatari husika zinazoweza kutokea.