**Utangulizi**

Mapinduzi ya teknolojia ya mtandao yamezidi kubadilika na kukua kwa kasi na kusababisha matukio ya uhalifu mtandao kuongezeka, hivyo kupelekea kukua kwa uhalifu mtandaoni. Katika jitihada za kuwalinda watumiaji wa huduma za mtandaoni dhidi ya uhalifu wa mtandao, Wizara ya Habari, Mawasiliano na Teknolojia ya Habari (WHMTH) inaungana na ulimwengu kuadhimisha Mwezi wa Uelimishaji wa Usalama Mtandao ambao hufanyika mwezi Oktoba kila mwaka.

Lengo la kuelimisha matumizi salama ya mtandao kwa watu binafsi na taasisi ni kupunguza matukio ya uhalifu mtandaoni kwa kujenga uelewa kuhusu mbinu zinazotumika kufanya uhalifu mtandaoni, namna wanavyoweza kubaini mashambulizi ya mtandao na masuala gani wanayoweza kufanya ili kujikinga dhidi ya uhalifu wa mtandao.

Kwa mujibu wa tafiti mbalimbali imebainika kuwa sababu inayopelekea matukio ya uhalifu mtandao ni udhaifu wa kibinadamu ikiwemo ulaghai kimtandao, makosa na matumizi mabaya ya taarifa za kuingia kwenye mifumo kwa wasiohusika. Kwa mujibu wa utafiti uliofanywa na Kampuni ya Verizon mwaka 2022, ilibainika kuwa zaidi ya asilimia 80 ya uhalifu wa mtandao uliofanyika ulihusisha udhaifu wa mwanadamu. Kwa msingi huo, suala la uelimishaji wa usalama mtandao ni muhimu ili kuzuia uhalifu kwa njia ya udhaifu wa mwanadamu.

**Umuhimu wa Elimu ya Usalama Mtandao**

Elimu ya usalama mtandao inasaidia kupunguza athari za uhalifu mtandao ambazo husababishwa na udhaifu wa mwanadamu. Hivyo, programu ya elimu kwa umma ya matumizi salama ya mtandao ni dhana muhimu inayoongeza ujuzi na maarifa kwa watendaji na kuwawezesha kubaini viashiria vya mashambulizi kabla ya kusababisha madhara kwa mwananchi, taasisi na nchi kwa ujumla.

Elimu kwa umma ya usalama mtandao ya mara kwa mara ni muhimu kwa biashara na taasisi hususan kwa kuwa inazuia changamoto kadhaa kama vile kupigwa faini kwa mujibu wa sheria, upotevu wa fedha, upotevu wa haki miliki, uharibifu wa taswira ya taasisi/biashara, upotevu wa wateja, n.k.

**Kauli Mbiu ya Mwezi wa Elimu kwa Umma ya Usalama Mtandao**

Kauli mbiu ya mwezi wa elimu kwa umma ya usalama mtandao ya mwaka huu ni "**Usalama wa Mtandao Huanza na Mtu Binafsi".** Kwa upande wa Jamhuri ya Muungano wa Tanzania tunajikita katika kipengele cha udhaifu wa mwanadamu kwenye usalama mtandao, ambapo tutahabarisha na kuelimisha umma ili kuhakikisha kila mtu binafsi na taasisi zinatumia mitandao kwa usalama popote walipo.

WHMTH inatoa hamasa kwa watu binafsi, taasisi na wadau wengine kutoa ushirikiano katika jitihada hii muhimu ya kujenga uelewa, ujuzi na maarifa ya matumizi salama ya mtandao, kulinda miundombinu muhimu ya Taifa na kukabiliana na uhalifu wa mtandao nchini. Hivyo, kuwezesha kufanya anga ya mtandao ya Tanzania kuwa salama na ya kuaminika.

**Mambo Kumi (10) Unayoweza Kufanya**

1. Jiridhishe kabla ya kufungua au kupakua chochote mtandaoni

Ikitokea umepokea barua pepe inayoonekana imetoka kwa mtu unayemfahamu, kuwa makini kabla ya kufungua viambatisho vyake. Ni vema ukiwa na mashaka uchukue tahadhari au kutojibu barua pepe husika kwa sababu utambulisho wa mhusika unaweza kuwa umedukuliwa.

2. Tumia programu za kujilinda mtandaoni

Programu ya kulinda vifaa vya TEHAMA (AV) imekuwa suluhisho zuri la kupambana na mashambulizi ya virusi mtandaoni. Programu ya AV huzuia virusi vya mtandao kuingia kwenye kifaa chako na kuhatarisha usalama wa taarifa. Inashauriwa kutumia programu moja ya kuzuia virusi mtandaoni kutoka kwa wachuuzi wanaoaminika.

3. Jiridhishe maombi ya taarifa binafsi

Unapoombwa kutoa taarifa zako binafsi au za mtu mwingine, hakikisha unajiridhisha na utambulisho wa mwombaji - hata kama inaonekana kuwa ni mtu unayemfahamu. Matapeli wana mbinu nyingi za kukusanya, kuiba taarifa au utambulisho wa mtu ili kuzitumia kufanya uhalifu. Jenga tabia ya kuangalia mara kwa mara taarifa zako za kifedha.

4. Linda nywila zako

Usitoe nywila au nambari ya siri (PIN) kwa mtu yeyote. Hakikisha nywila ni ndefu, imara na ya kipekee. inashauriwa utumie uthibitishaji wa vipengele vingi kadiri ya inavyowezekana (mfano alama za vidole, kadi, jumbe za uthibitisho kwa namba binafsi za simu au barua pepe, n.k.).

* Tumia programu za kulinda nywila kama vile *LastPass* au *RoboForm*;
* Tumia nywila/nambari ya siri tofauti kwa akaunti tofauti;
* Tumia nywila/nambari ya siri tofauti kazini na nyumbani; na
* Usikubali programu na tovuti kukumbuka nywila zako.

5. Matumizi salama ya vifaa vya TEHAMA vya mkononi

Kwa mujibu wa utafiti uliofanywa na Kampuni ya McAfee Labs ya Marekani, matukio mapya milioni 1.5 ya programu hasidi na virusi mtandaoni yanalenga zaidi vifaa vya TEHAMA vya mkononi.

Dondoo muhimu za usalama wa vifaa vya TEHAMA vya mkononi:

* Tengeneza Nambari ya siri (PIN) yakipekee. Inashauriwa kutotumia tarehe ya kuzaliwa au namba ya simu;
* Sakinisha (Install) programu tumizi (Application) kutoka kwenye vyanzo vinavyoaminika;
* Hakikisha kifaa chako kimesasishwa (updated) - Wadukuzi hutumia udhaifu uliopo katika programu au mifumo ambayo haijasasishwa kuingilia vifaa au

mifumo husika;

6. Linda vifaa vyako vya kielektroniki

Kuwa makini na vifaa vyako vya kielektroniki unapokuwa katika maeneo ya umma. Hakikisha unafunga vifaa vyako au uende navyo, hata kama utatoka kwa sekunde chache. Ukiwa kazini, chukua tahadhari ya eneo lako na ufunge skrini ya kompyuta yako kabla ya kutoka kwenye meza yako. Jenga tamaduni ya kuchukua simu yako na vifaa vingine vinavyobebeka.

7. Sasisha vifaa vyako, vivinjari (browsers) na programu

Sasisha vifaa vya TEHAMA, vivinjari na programu mara kwa mara ili kupunguza mianya ya udukuzi na wahalifu wa mtandao kuingilia programu au vifaa husika.

8. Hifadhi nakala za faili muhimu

Hifadhi nakala katika maeneo tofauti (physical location) na uzifungue mara kwa mara. Kwa faili muhimu za kazi, nakala rudufu zihifadhiwe kwenye hifadhi tofauti (mfano wingu kompyuta au USB iliyosimbwa (encrypted)) ili kuihifadhi kwa usalama.

9. Usitumie Wi-Fi ya bure *(Public Wi-Fi)*

Inashauriwa usitumie Wi-Fi ya bure isiyohitaji kuingiza nywila bila kutumia programu ya Mtandao Pepe wa Kibinafsi (VPN). Kwa kutumia programu ya VPN, taarifa kati ya kifaa chako na seva ya VPN imesimbwa kwa njia za kitaalamu. Hii inamaanisha kuwa ni vigumu zaidi kwa mhalifu wa mtandao kuzifikia taarifa zako kwenye kifaa husika. Inashauriwa kutumia mtandao wa mtoa huduma wa simu endapo hauna VPN ili kuwa salama.

10. Ukiwa na mashaka, toa taarifa!

Jifunze jinsi ya kutambua viashiria vya uhalifu kimtandao ambavyo vinaleta mashaka. Ripoti masuala yote ya kihalifu mtandao kwenye Kituo cha Polisi kilicho karibu nawe.