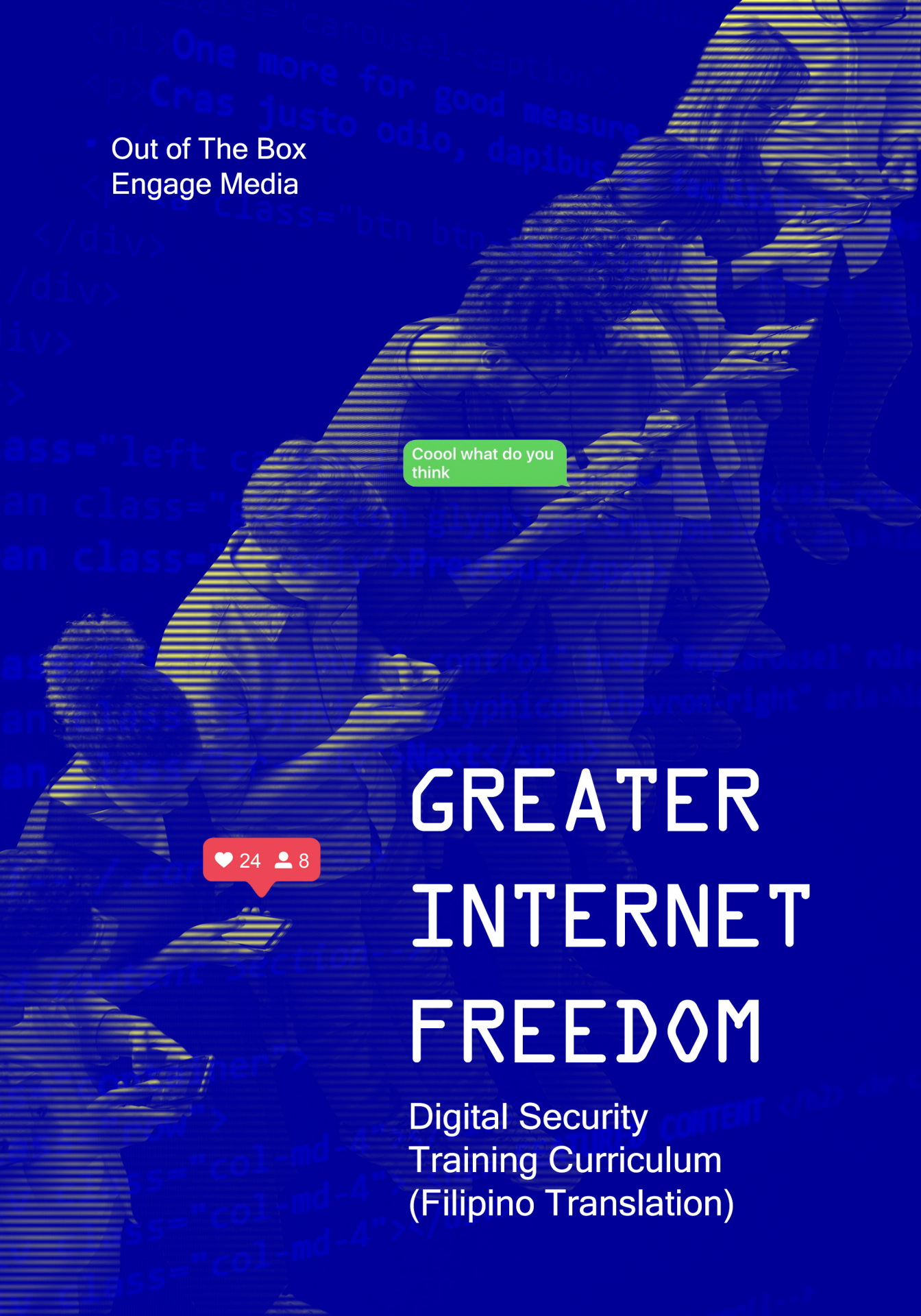
Out of The Box
Engage Media



GREATER INTERNET FREEDOM

Digital Security Training Curriculum (Filipino Translation)

Greater Internet Freedom:
Digital Security Training Curriculum

Published by

Out of The Box
MEDIA LITERACY INITIATIVE

Out of The Box Media Literacy Initiative
www.ootbmedialiteracy.org

EngageMedia

This publication has been produced in partnership with EngageMedia. The contents of this publication are the sole responsibility of Out of The Box Media Literacy, and can under no circumstances be regarded as reflecting the position of the aforementioned partner.

Project Managers: Marlon Julian Nombrado and Sarah Isabelle Torres
Design and Layout: Christian Ralf Dugan
Translations by: Chad Errol Booc, John Reczon Calay, and Michael Vincent Mercado

February 2022

Greater Internet Freedom

Kurikulum Para sa Pagsasanay sa Digital Security

Talaan ng Nilalaman

1.1 *Pinagmulan at Saklaw*

Umiiral ang kasalukuyan nating lipunan sa isang kaligirang ang digital technology ay lumalaganap at bahagi na ng ating mga paraan ng pamumuhay. Pinadadali ng mga teknolohiyang ito ang ating buhay sa pamamagitan ng mabilis na komunikasyon, madaling pag-iimbak at pagbabahagi ng impormasyon, bukod sa iba pa. Dinidigitalisa na ang lahat ngunit may kaakibat na mas malalaking security risk ang mga teknolohiyang ito. Hindi na lamang umaasa ang mga tao sa mga karaniwang security solution katulad ng mga antivirus software at firewall. Gumagaling nang lalo ang mga cybercriminal at ang kanilang mga taktika ay nananaig na sa nakasanayang mga cyber defense. Marapat din nating imulat ang ating mga sarili tungkol sa mga simpleng social engineering scam tulad ng phishing pati na rin ang mas sopistikadong mga banta sa cybersecurity tulad ng mga atakeng ransomware upang ingatan ang ating mga sarili sa malisyosong mga pagtatangkang agawin ang ating intelektwal na ari-arian o personal na datos.

Mahalaga ang digital security at privacy. Para sa mga nagsusulong ng karapatang pantao, peryodista, aktibista, at kahit na mga ordinaryong mamamayan, ang posibilidad na ma-monitor ang iyong mga komunikasyon o kahit na ang pagkalalantad ng iyong pagkakakilanlan o lokasyon ay maaaring magdala ng malaking panganib, lalo na kung ikaw ay nagtatrabaho nang may sensitibong impormasyon. Lubhang kailangan ang ganap na estratehiyang pandigital na seguridad, bilang ang kalakasan nito ay katulad din nang sa kahinaan nito.

Lumalago sa kabuuan ang mga digital na panganib na kinahaharap ng mga aktibista, peryodista, tagapagtanggol ng karapatang pandigital, akademiko, at mga grupong nasa laylayan ng lipunan sa paglipas ng mga taon. Nanggagaling ang mga panganib na ito sa mga awtoritaryang rehimen na nagtutulak ng mga polisiyang pandigital na lumalabag at nagkikriminalisa sa mga batayang karapatan sa pagtitipon, pagkakapisanan, at pamamahayag online. Sa parehong antas pampolisiya at implementasyon, maraming mga pamahalaan ang nakikibahagi sa panlilinlang ng encryption at namumuhunan sa teknolohiya ng pangmalawakang pangmamatiyag habang sinesensura ang boses ng mamamayan sa online. Ang ganitong karaniwang mga banta laban sa kalayaan sa internet na humigit na sa mga hangganan ng bansa ang dahilan ng pagyabong ng Greater Internet Freedom (GIF) project.

Kritikal na bahagi ng GIF project ang pagsasanay at matutulungan nito ang kapasidad ng mga civil society organization (CSO), mga media outlet, at mga indibidwal sa parehong pang-iwas at pantugong mga lapit ng pangkaligtasang digital. Madaragdagan din nito ang bilang ng lokal na mga eksperto sa pangkaligtasang digital na kayang magsulong ng mga naturang kakayahan ng sambayanan, mga organisasyong pangmidya, at mga indibidwal.

Sa pamamagitan ng training program na ito, mapahuhusay ng mga kalahok ang kanilang kaalaman sa mga sumusunod na konsepto ng digital security:

- Pagtatasa ng panganib
- Kalinisang pandigital

- Malware at mga proteksiyon
- Free and open source software (FOSS)
- Seguridad at privacy ng browser
- Pangangasiwa ng password
- Proteksyon sa mga file at folder
- Mga backup
- Pag-encrypt sa data at komunikasyon
- PGP and email encryption
- Paanong gumagana ang internet at network encryption gamit ang mga virtual private network (VPN) at Tor
- Seguridad at privacy sa social media
- Mga panganib na may kaugnayan sa mga mobile phone at paggamit ng mga seguradong kasangkapang pangkomunikasyon
- Pagpaplano at paghahanda ng mga pagsasanay

1.2 *Puntos ng Pakikipag-ugnayan*

Nakabatay ang nilalaman ng kurikulum na ito sa mga nakaraang karanasan sa pagsasanay at maaaring kailanganin ang pag-aangkop nito sa mga tiniyak na konteksto at mga kahingian. Makipag-ugnayan lamang sa mga nakasaad na personalidad sa baba kung kailangan ng tulong sa inyong kurikulum ng pagsasanay.

Vino Lucero
Tagapamuno ng Proyekto
vino@engagemedia.org

Md. Ashraful Haque
Tagapaglinang ng Kurikulum
ashraf@engagemedia.org

1.3 *Organisasyon ng Dokumento*

Nilikha ng EngageMedia ang dokumentong ito para sa mga kapartner na bansa ng GIF sa pagdidisenyo ng sari-sariling kurikulum para sa digital security.

2.0 *Instruktibong Pagsusuri*

2.1 Pagsusuri sa Mga Pangangailangan at Kakayahan

Bago isagawa ang bawat sesyon ng pagsasanay, inirerekomendang kumuha ng isang needs and skills analysis. Iba't iba ang bawat kalahok at may iba't iba rin silang mga work area na nagpapakita ng pagkakaiba sa kani-kanilang mga pangangailangan at ang mga kinahaharap nilang mga security risk. Mainam ding malaman ang kasalukuyang mga antas ng kaalaman ng mga kalahok upang mapili ang pinakaangkop na mga paksa at kapamaraanan sa pagsasanay.

Padron ng Pagtatasa ng Kakayahan

Sagutan ang sumusunod na mga tanong upang matiyak ang iyong mga kakayahan at mga pangangailangan. Makatutulong ang mga resulta ng pagtatasang ito sa pagdisenyo naming ng mas mahusay na training program para sa iyo. Tandaang may mga tanong na mayroong dalawa o higit pang posibleng tamang mga sagot; piliin kung ano ang pinakatama para sa iyo.

1. Ano ang pinakaimportanteng alituntunin ng digital security?
- I-update ang antivirus program
- I-update ang operating system
- Huwag magtiwala sa kahit sino
- Huwag magbukas ng mga email attachment

2. Sa pinakakaunti, ilang characters na mayroon dapat ang iyong password?
- May habang 8 characters
- May habang 14 characters
- May habang 20 characters
- May habang 25 characters

3. Bakit mahalagang komplikado ang mga password?
- Mas pinahihirapan nito ang pag-crack ng password sa pamamagitan ng isang software tulad ng brute force
- Pinahahaba nito ang password encryption
- Pinahihirapan nito ang panghuhula ng password
- Mas pinahihirapan nito ang pagpapaunawa sa password

4. Paano mo poprotektahan ang iyong computer mula sa pisikal na paninira?
- Ifo-format ang aking hard disk
- Ie-encrypt ang aking buong hard disk
- Ie-encrypt ang aking mga document
- Ila-lock ang aking computer

5. Saan mo itinatago ang iyong mga backup file?
- Sa hiwalay na drive sa parehong computer
- Sa isang hidden folder sa parehong computer

- Hindi ako nagtatago ng kahit anong mga backup
- Sa hiwalay na device at lokasiyon

6. Paano ko masisiyasat kung tama ang https sa isang website?
- Hinahanap ko ang https sa header
- Hinahanap ko ang key lock kung ito ba ay nasa URL
- Tinitingnan ko ang digital certificate
- Tinitingnan ko ang pangalan sa URL

7. Ano ang isang ligtas na paraan sa pagpapadala at pagtanggap ng mga email?
- Secure mail
- SMTP
- FTP
- PGP

8. Ano ang dapat kong hingiin mula sa iyo upang makapagpadala ng isang encrypted na email?
- Ang aking private key
- Ang aking public key
- Ang pareho kong mga key
- Wala

9. Ano ang gagawin mo sa iyong mga open account (email, Twitter, Facebook...) bago mo isara ang iyong computer?
- Basta lamang isara ang takip ng laptop
- Isara ang browser saka patayin ang computer
- Mag-log out sa lahat ng mga account, isara ang browser, at saka patayin ang computer
- Pindutin ang power button hanggang sa magsara ang computer

10. Dapat mo bang i-save ang mga password mo sa iyong browser upang mapadali ang pag-access sa iyong mga account?
- Oo
- Hindi

11. Dapat ka bang gumamit ng magkakaibang password sa bawat account? O isang password na lang para sa lahat ng iyong mga account para hindi mo malimutan ito at para hindi mawala ang iyong account?
- Isa para sa lahat ng mga account
- Iba't ibang password para sa bawat account

12. Paano mo malalaman kung ano ang operating system na nasa computer mo?
- Sa pakikipag-ugnayan sa manufacturing company
- Nakasulat ito sa bandang likuran ng computer
- Mag-right click sa aking computer at piliin ang Properties
- Dadalhin ko ang computer sa repair shop at saka sila na ang magsasabi sa akin

13. Makapagbibigay ng karagdagang proteksiyon ang paggamit ng higit sa isang antivirus program.
- Oo
- Hindi

14. Ano ang ginagawa ng mga rootkit?
- Itago ang mga virus at mga Trojan sa detection
- Itago ang mga file
- Pigilan ang mga antivirus program
- Mag-install ng malware

15. Sapat na ba ang pagfo-format ng hard drive upang burahin ang iyong mga data?
- Oo
- Hindi

16. Upang maprotektahan ang aking computer mula sa mga virus na galing sa mga USB at CD...
- Hindi ako dapat gumamit ng kahit anong USB
- Hindi ko dapat paganahin ang auto run sa Windows
- Dapat kong i-scan ang aking computer
- Wala akong dapat gawin

17. Kung makatatanggap ka ng isang link o attachment sa isang hindi inaasahang email mula sa iyong kaibigan, ano ang gagawin mo?
- Check it and decide whether to open it or not
- Open it because you have a good antivirus that protects your computer
- Contact the sender and check if he sent it, then check and open it
- Open it because the firewall is activated, nothing can harm your computer

18. Bago mo i-install ang isang app sa iyong mobile phone, ano ang dapat mong siyasatin?
- Kung anong mga permiso ang hinihingi nito
- Kung sino ba ang gumawa nito
- Kung ibinubunyag ba nito ang aking lokasiyon
- Kung kumokonsumo ba ito ng maraming bandwith

19. Kung mayroon kang mahalagang pagpupulong at ayaw mong ipabatid sa iyong mobile company ang iyong lokasiyon, ano ang gagawin mo?
- Isara ang GPS sa iyong mobile phone
- Hindi nila malalaman ang aking lokasiyon dahil luma na ang aking mobile phone at wala itong GPS
- Bago magsimula ang pagpupulong, patayin ang mobile phone at tanggalin ang SIM card
- Patayin ang mobile phone at tanggalin ang battery bago ako umalis ng bahay

20. Upang protektahan ang iyong mobile phone laban sa sinumang magtatangkang magbukas nito:
- Gumamit ng passcode
- Gumamit ng full device encryption
- Gumamit ng passcode para sa SIM card
- Gumamit ng pattern upang i-unlock at mabuksan ang phone

2.2 Lapit sa Paglilinang

Maaaring may pangangailangan sa muling paglilinang o muling pagdidisenyo ng kurikulum na ito. Maaaring kumpletuhin ang mga kahingian at mga sarbey ng kakayahan at suriin ito bago makipag-ugnayan sa EngageMedia para sa tulong sa pagpapaunlad ng kurikulum at para talakayin ang pagsasaayos nito at posibleng susunod na mga hakbang.

2.3 Mga Isyu at Mungkahi

Iminumungkahi ang pagsasagawa ng pagtatasa ng mga panganib bago ang mismong pagsasanay. Batay sa pagtatasa, maghanda at asahan ang hindi inaasahan. Laging maghanda ng backup plan. Habang nagpaplano para sa isang sesyon ng pagsasanay, isaalang-alang ang mga sumusunod:

- Anong uri ng pagsasanay ang dapat ibigay – at para kanino? Nakabatay dapat sa survey data ng target na mga kalahok ang pagpaplano ng sesyon. Pumili ng mga kalahok at mga paksa na may kaugnayan dito.

- Sino ang mamamahala sa pagsasanay? Halos lahat ng magiging kahihinatnan ng isang pagsasanay ay nakadepende sa taong magpapadaloy ng programa ng pagsasanay. Dapat na isaalang-alang ang bihasa at may karanasang mga tagapagsanay na marunong at mamamando ang mga paksa.

- Sino ang maglilinang ng mga materyales sa pagsasanay at kaligiran nito? Habang nililinang ng EngageMedia ang template ng kurikulum na ito, kailangang iniaangkop dapat sa lokal na mga konteksto ang bawat training program.

- Paano mapagsisilbihan ng training program na ito ang isang grupong ang mga kalahok ay may iba't ibang paniniwala o katayuan sa buhay? Magmumula ang mga kalahok sa iba't ibang mga pamayanan at organisasyon. Mayroon silang iba't ibang mga edad, kasarian, paniniwala, sakop ng paggawa, atbp. Mayroon din silang iba't ibang mga gawi at estilo ng pampagkatuto. Dapat mapangasiwaan ang programa ng pagsasanay habang isinasaisip ang pagkakaiba-iba ng mga kalahok.

- Ano kaya ang lokal na kapaligiran sa kapanahunan ng pagsasanay? Alamin ang tungkol sa lokal na politikal at panlipunang kaligiran bago ang pag-oorganisa ng isang pagsasanay upang maseguro ang isang ligtas at naaangkop na kapaligirang pampagkatuto para sa mga kalahok

3.0 *Mga Paraan ng Pagtuturo*

3.1 Metodolohiya ng Pagsasanay

Habang kontekstuwal at iba-iba ang metodolohiya ng pagsasanay sa bawat programa ng pagsasanay, iminumungkahi naming sundin ang Activity-Discussion-Inputs-Deepening-Synthesis o ADIDS (o Gawain-Talakayan-Input-Pagpapalalim-Sintesis) na metodolohiya ng pagsasanay. Mabisang ginagamit ang ADIDS sa mga pagsasanay na pang-adbokasiya at pangkasanayan tungkol sa mga isyu sa karapatang pantao, at napag-alaman naming kapaki-pakinabang ito upang tulungan ang mga kalahok sa minimal na kaalamang teknikal upang maunawaan nang maayos ang komplehidad ng pandigital na seguridad at kaligtasan online. Para sa mga tagapagsanay, makapaglalaan din ito ng kapaki-pakinabang na balangkas sa paglikha ng mga lesson plan. Higit pang alamin dito: https://level-up.cc/before-an-event/preparing-sessions-using-adids/

3.2 Mga Pagsusulit at Pagtatasa

Iminumungkahing magsagawa ng maramihang mga pagsusulit at ebalwasyon habang isinasagawa ang programa ng pagsasanay.

- Bago ang pagsasanay – Upang malaman ang tungkol sa umiiral na kaalaman ng mga kalahok at makapagplano ng mga kaugnay na mga sesyon, iminumungkahi ang isang online na sarbey. Magtanong nang may kinalaman sa gawa ng mga kalahok at adyenda ng pagsasanay.

- Habang nagsasanay – Habang nagsasanay, maaaring kunin ang mga feedback ng mga kalahok pagkatapos ng bawat sesyon upang mapabuti ang mga susunod.

- Pagkatapos ng pagsasanay – Sa pagwawakas ng programa ng pagsasanay, inirerekomendang magsagawa ng isa pang pagsusulit upang tasahin ang mga pagbabago sa kaalaman at kakayahan ng mga kalahok.

4.0 *Kurikulum ng Pagsasanay*

SESYON 01
Pagpapakilala at Pagsusulit Bago Magsanay

Uri ng sesyon: Panimula at gawain

INAASAHANG MGA KAHINATNAN NG LEKSIYON
- Kilalanin ng mga kalahok at tagapagsanay ang isa't isa
- Masukat ang batayang kaalaman at kasanayan ng mga kalahok

MGA LAYUNING PAMPAGKATUTO
- Maunawaan ang mga konsepto ng pagsasanay na ito.
- Makipagkilala sa iba.
- Matuto kung paanong mag-organisa ng isang pre-training test.
- Matuto kung paanong ilalapat ang mga konseptong mula sa panimulang sesyon sa mga pagsasanay sa hinaharap.

KARAGDAGANG MGA SANGGUNIAN
https://internews.org/
https://engagemedia.org/

GABAY NG SESYON
1. Magbibigay ng pambungad na pananalita ang tagapagsanay tungkol sa pagsasanay at magpapakilala
2. Pasisimulan ng tagapagsanay ang pagpapakilala ng mga kalahok.
3. Magtatakda ang tagapagsanay ng mga panuntunan sa kaligiran ng pagsasanay.
4. Magsasagawa ng pagsusulit bago magsanay ang tagapagsanay gamit ang isang online survey form. Dapat may kinalaman sa pagsasanay at sakop ng paggawa ang mga tanong dito.

SESYON 02
Panimula sa Digital Security

Uri ng sesyon: Gawain-Talakayan-Input-Pagpapalalim-Sintesis

INAASAHANG MGA KAHINATNAN NG LEKSIYON
- Matututunan ng mga kalahok kung ano ang digital security at bakit ito mahalaga
- Malalaman din nila ang tungkol sa free and open source software (FOSS)

MGA LAYUNING PAMPAGKATUTO
- Maintindihan kung ano ang holistikong seguridad.
- Maunawaan ang kahalagahan ng pangangalaga sa sarili sa kaligtasang pandigital.
- Maunawaan ang kaugnayan ng holistikong seguridad sa ating mga buhay at ating mga paggawa.
- Matutunan ang tungkol sa free and open source software (FOSS).

KARAGDAGANG MGA SANGGUNIAN
https://holistic-security.tacticaltech.org/

GABAY NG SESYON
1. Magpapalabas ng maigsing video ang tagapagsanay tungkol sa mga insidenteng may kinalaman sa digital security
2. Tatalakayin ng tagapagsanay kung ano ang holistic security at kung bakit mahalaga para sa atin ang self-care.
3. Ibabahagi ng mga kalahok ang kani-kanilang mga naiisip tungkol sa paksa.
4. Ipakikilala ng tagapagsanay ang FOSS

BUOD NG SESYON

Isang kolektibong termino ang pandigital na seguridad (digital security) na naglalarawan sa mga mapagkukunang ginagamit upang protektahan ang iyong identidad sa online, data, at iba pang mga ari-arian. Kasama sa mga kasangkapang ito ang mga serbisyo sa web, antivirus na software, mga SIM card ng smartphone, biometrics, at seguradong personal na mga device.

Sa madaling sabi, ang ibig sabihin ng pandigital na seguridad ay ang pagprotekta sa iyong computer, mga mobile device, mga table, at iba pang mga device na kumokonekta sa internet mula sa mga nanghihimasok dito, na maaaring nasa porma ng pangha-hack, phishing, at iba pa. Ang pagsasapraktika ng pandigital na seguridad ay pumoprotekta sa iyong personal na datos laban sa mga kompanya na gumagamit at nagbebenta nito. Mahalaga ang cybersecurity dahil pinoprotektahan nito ang lahat ng uri ng datos mula sa pagnanakaw at pagkasira. Kasama rito ang mga sensitibong datos, personally identifiable information (PII),

protected health information (PHI), personal na impormasyon, pagmamay-aring intelektwal, at mga information system ng pamahalaan at industriya. Kung lundo ang anumang aspekto ng iyong pandigital na seguridad, ang lahat ng iyong personal na impormasyon – iyong mga credit card, bank account, email account, ang iyong buong pagkakakilalan – ay maaring nasa panganib.

Isang pinagsamang lapit ang holistikong seguridad (holistic security) sa digital, pisikal, at siko-sosyal na seguridad para sa mga indibidwal at organisasyon. Kasama sa mga layon ng isang holistikong lapit sa seguridad at proteksto ng mga aktibista at mga tagapagtanggol ng karapatang pantao (human rights defenders, HRD) ang mga sumusunod:

- Pagpapatibay sa pagpapanatili ng aktibismo sa konteksto ng karahasan (sa malawak at interseksiyonal na pagkakaunawa)
- Pagpapatibay sa mga kapasidad ng mga aktibista na maglimi, matuto, at maglunsad ng mga kontra-hakbang upang mapabuti ang kanilang seguridad at proteksiyon
- Pinagtitibay nito ang katatagan at kapasidad ng mga aktibista sa malikhaing pagtugon sa panahon ng krisis.

FOSS: Iniaalok ng mga open-source na software ang kakayahan nito sa pag-angkop, kolaborasyon, at pinahusay na seguridad. Ang open-source na software ay isinasapubliko sa ilalim ng isang awtorisasyon na kung saan ipinagkakaloob ng may-ari nito ang karapatan sa paggamit, pag-aaral, pagbabago, at pagbabahagi ng software at source code nito sa kahit sino at sa kahit anong dahilan. Maaaring linangin ang isang open-source software sa isang paraang kolaboratibo at pampubliko.

SESYON 03

Pagmomodelo ng Mga Banta (Threat Modeling)

Uri ng sesyon: Gawain-Talakayan-Input-Pagpapalalim

INAASAHANG MGA KAHINATNAN NG LEKSIYON

- Makapagtasa at makapagkilala ng mga panganib ang mga kalahok

MGA LAYUNING PAMPAGKATUTO

- Maunawaan ang pagmomodelo ng mga banta (threat modeling).
- Matutunan ang pagtatasa ng personal at pang-organisasyong mga panganib.

KARAGDAGANG MGA SANGGUNIAN

https://ssd.eff.org/en/module/your-security-plan

GABAY NG SESYON

1. Magpepresenta ang tagapagsanay ng isang threat modeling flowchart at tatalakayin niya ang proseso nito nang bai-baitang.
2. Magpapakita ang tagapagsanay ng mga halimbawa ng pang-organisasyon o pampersonal na mga panganib.
3. Hihikayatin ang mga kalahok na tasahin ang mga nabanggit na panganib na nakapaloob sa modelo.
4. Tatalakayin ng tagapagsanay ang pagtatasa ng panganib ng mga kalahok batay sa tinalakay na modelo at itama ang anumang mga pagkakamali o mga hindi wastong pagpapakahulugan.

BUOD NG SESYON

Isang proseso ang seguridad, at sa pamamagitan ng masusing pagpaplano, makabubuo ka ng isang planong wasto para sa iyo. Hindi lamang tungkol sa mga kasangkapang gagamitin o ida-download na software ang seguridad. Nagsisimula ito sa pag-unawa sa mga kakaibang mga banta na iyong kinahaharap at kung paano mo lalabanan ang mga ito.

- Ano ang gusto kong protektahan?
- Laban kanino ko ito gustong protektahan?
- Gaano kalala ang mga kahihinatnan kung mabibigo ako?
- Gaano kalamang na kailangan kong protektahan ito?
- Gaano ako kahanda sa abalang tatahakin ko sa pagsubok na iwasan ang potensyal na mga kahinatnan nito?

Kapag naitanong na sa sarili, nasa katayuan ka na sa pagtatasa sa kung anong mga hakbang ang isasagawa.

Isipin sa ganitong paraan ang pagtatasa ng panganib: Kung mahalaga ang iyong mga ari-arian, ngunit ang pagkakataonng makapagnakaw ay mababa, maaaring hindi mo nanaising mamuhunan ng masyadong maraming salaping panlagak. Ngunit

kung mataas naman ang pagkakataong makapagnakaw, talagang nanaisin mong makakuha ng pinakamagandang panlagak sa mercado, at ikonsidera ang pagdadagdag ng sistemang panseguridad. Makatutulong ang paggawa mo ng isang security plan upang maunawaan ang mga bantang katangi-tangi sa iyo at ang posibilidad ng mga panganib na kakaharapin mo. Hahayaan ka nitong maayos na suriin ang iyong mga ari-arian, iyong mga katunggali, at ang mga kakayahan nila.

SESYON 04

Kamalayan at Paghahanda sa Digital Hygiene

Uri ng sesyon: Talakayan-Input-Pagpapalalim-Sintesis

INAASAHANG MGA KAHINATNAN NG LEKSIYON

- Magiging malay ang mga kalahok tungkol sa konsepto ng digital hygiene at maihahanda silang isapraktika ito.

MGA LAYUNING PAMPAGKATUTO

- Matutunan ang mga batayang kamalayan sa digital security.
- Matutunan ang tungkol sa mga gawing pang-digital hygiene.

KARAGDAGANG MGA SANGGUNIAN

https://coconet.social/digital-hygiene-safety-security/

GABAY NG SESYON

1. Tatalakayin ng tagapagsanay ang batayang kamalayan sa pandigital na seguridad, kasama na ang mga dapat at hindi dapat gawin, seguridad sa hardware at software, pag-unawa sa pagbabago ng pag-uugali, atbp.
2. Hihikayatin ang mga kalahok na magbahagi ng kani-kanilang kasalukuyang mga gawi sa pandigital na seguridad.
3. Palalawigin ng tagapagsanay ang mga konsepto batay sa input ng mga kalahok.

BUOD NG SESYON

Walang duda, maaaring maging lubhang kapaki-pakinabang na kasangkapan ang internet para sa mga tao. Ngunit nakapagdadala rin ng gulo ang instant messaging, mga chat room, email, at social networking site – mula sa cyberbullying hanggang sa panghihimasok ng privacy at pagnanakaw ng pagkakakilanlan.

Sakop ng digital safety/pandigital na kaligtasan, kadalasang binabansagang internet safety, media safety, o cyber safety, ang napakaraming mga bagay. Sa kaibuturan, tungkol sa pagprotekta sa ating mga sarili, ating mga pamilya, at iba ang pandigital na seguridad sa panahong kumokonekta tayo gamit ang ating mga digital device. Mahalaga ang pandigital na kaligtasan dahil pinoprotektahan nito ang mga tao sa mga panganib tulad ng identity theft at fraud. Kung iyong susundin ang mga sumusunod na hakbangin, mapatitibay nito ang iyong pandigital na seguridad at magiging mas segurado ang iyong impormasyon.

1. Huwag ibahagi ang iyong impormasyong pampinansyal sa kahit na sino.

2. Kapag magbubukas ka ng email, seguraduhing tingnan ang mga detalye ng nagpadala.

3. Huwag mag-click sa anumang mga link bago makumpirma ang pupuntahan nito.

4. Maaaring mapanganib ang mga attachment; i-scan ito gamit ang antivirus bago buksan.

5. Palaging i-download ang software mula sa orihinal (opisyal) na website.

6. Iprayoritisa ang paggamit ng open source na software.

7. Palitan ang iyong mga security habit sa parehong online at offline.

8. Mag-sign out sa lahat ng iyong mga account bago patayin ang computer.

9. Laging mag-ingat. Unawain kung saan ka nagki-click – mag-isip muna bago mag-click.

10. Huwag buksan ang anuman sa iyong mga account sa computer o mobile phone ng ibang tao.

11. Huwag ipahiram sa iba ang iyong device. Kung sakaling kailangan talaga, bantayan kung paanong ginagamit ang iyong device.

12. Panatilihing updated ang iyong device.

13. Huwag gumamit ng mga public network sa mga hotel at cyber café maliban kung magsasagawa ng kinakailangang mga hakbang upang maging secure ang connection (katulad ng pag-connect sa pamamagitan ng VPN o Tor). Kung kailangan talagang gumamit ng ibang mga computer, gumamit ng secure at portable na OS tulad ng Tails.

14. Maging malay sa kung anuman ang iyong ipina-publish online.

15. Dalhin lamang ang mga kinakailangang personal na datos / impormasyon sa iyo.

16. Magpanatili ng isang sagisag-panulat para sa iyong privacy.

17. Gumamit ng encryption kung nagpapalitan ng impormasyon

18. Hindi lamang usapin ng pagpoprotekta sa sarili ang digital security; tulungan ang iba na maprotektahan din ang kanilang impormasyong digital.

SESYON 05

Malware, Antivirus, at mga Kasangkapang Pantanggal ng Malware

---

Uri ng sesyon: Talakayan-Input-Pagpapalalim-Sintesis

INAASAHANG MGA KAHINATNAN NG LEKSIYON

- Matutunan ng mga kalahok ang mga uri ng malware. Maunawaan nila ang kahalagahan ng paggamit ng antivirus software at ang gamit ng mga kasangkapang pantanggal ng malware.

MGA LAYUNING PAMPAGKATUTO

- Maunawaan ang mga panganib na nasa internet at pang-araw-araw na mga device.
- Malaman ang tungkol sa iba't ibang mga uri ng malware.
- Maintindihan ang kahalagahan ng paggamit ng antivirus software.
- Maunawaan ang pagkakaiba ng bayad at libreng antivirus software.
- Malaman ang iba't ibang mga kasangkapan at paraan sa pagtanggal ng malware.

KARAGDAGANG MGA SANGGUNIAN

https://www.malwarebytes.com/ Mga kasangkapang pantanggal ng malware
https://www.avira.com/ Libreng/Bayad na antivirus
https://www.avast.com/ Libreng/Bayad na antivirus
https://virustotal.com/ Scanner ng malware sa online
https://level-up.cc/curriculum/malware-protection

GABAY NG SESYON

1. Tatalakayin ng tagapagsanay ang karaniwang mga bantang digital sa online at pang-araw-araw na mga device.
2. Tatalakayin ng tagapagsanay ang mga uri ng malware.
3. Hihikayatin ang mga kalahok na magbahagi ng kani-kanilang karanasan sa pagharap sa malware at kung anong mga aksiyon ang ginawa nila.
4. Tatalakayin ng tagapagsanay ang kahalagahan ng paggamit ng antivirus at ang pangunahing pagkakapareho ng mga libre at bayad na antivirus software.
5. Matututunan ng mga kalahok ang tungkol sa mga kasangkapang pantanggal ng malware at aatasan silang magsagawa ng malware scan habang nagse-sesyon para sa isang hands-on na karanasang pampagkatuto.

BUOD NG SESYON

Ang pagdapo ng isang "malicious software" ang malware. Isang intrusive ding software ang malware na idinisenyo upang maminsala at manira ng mga computer at mga computer system. Ilan lang ang mga virus, worm, Trojan virus, spyware, adware, at ransomware sa mga halimbawa ng karaniwang mga malware. Upang ingatan ang iyong system laban sa malware, sundin ang mga sumusunod na hakbangin:

- Tingnan ang huling bahagi ng file name (extension). Kung hindi ka pamilyar sa file extension, huwag itong buksan.
- Huwag agad buksan o i-run ang file sa pagtingin lamang sa file icon. Mapapalitan ang mga file icon sa gamit ang software.
- Kung nakatago ang file extension, palitawin ito.
- Kadalasan, maaaring ma-infect ang iyong computer sa pagkonekta ng isang external na device. Upang maiwasan ito:
    - o Panatilihing updated ang operating system ng iyong computer
    - o Huwag paganahin ang autorun na mga option sa iyong computer.
    - o Gumamit ng antivirus at mag-scan nang wasto bago magbukas ng isang external na device.
- Huwag gumamit ng software na kinuha mula sa mga hindi katiwa-tiwala at hindi tiyak ang pinagmulan. Maaaring may kasama itong malware mismo.
- Bumili ng antivirus kung kaya o gamitin ang libreng bersiyon nito.
- Panatilihin at palaging i-update ang antivirus database.
- Kayang ayusin ng mga kasangkapang pantanggal ng malware ang infected nang mga file o system. Hindi ito, sa anumang paraan, puwedeng maging alternatibo sa antivirus.
- Maraming antivirus companies ang nag-aalok ng iba't ibang libreng mga kasangkapang pantanggal ng malware.
- Upang maging ligtas mula sa malware o mga link ng phishing, seguraduhing i-scan ang kahit anong file, link, o login page bago ito buksan/puntahan.

SESYON 06
Seguridad ng Browser

Uri ng sesyon: Gawain-Talakayan-Input-Pagpapalalim-Sintesis

INAASAHANG MGA KAHINATNAN NG LEKSIYON
- Matututunan ng mga kalahok ang tungkol sa seguridad at privacy ng web browser.

MGA LAYUNING PAMPAGKATUTO
- Malaman kung paanong pumili ng isang maayos na browser
- Maintindihan ang mga security setting at privacy ng browser sa pamamagitan ng mga tool/extension.
- Malaman ang pinagkaiba ng HTTP at HTTPS.
- Matutunan kung paano makatukoy ng phishing at mga pekeng link.
- Matutunan kung paano gamitin ang DuckDuckGo o Startpage bilang mga search engine sa halip na Google.

KARAGDAGANG MGA SANGGUNIAN
https://brave.com/ Open-source na browser
https://www.mozilla.org/ Open-source na browser
https://www.eff.org/https-everywhere HTTPS redirection extension para sa browser
https://duckduckgo.com/ Alternatibong search engine liban sa Google
https://adblockplus.org/ Extension na nagtatanggal ng advertisement at pang-track sa browser
https://level-up.cc/curriculum/safer-browsing/

GABAY NG SESYON
1. Tatalakayin ng tagapagsanay ang ilang open-source na mga web browser at hikayatin ang paggamit ng mga ito.Hihikayatin ang mga kalahok na magbahagi ng kani-kanilang kasalukuyang mga gawi sa pandigital na seguridad.
2. Tatalakayin ng tagapagsanay ang ilang karaniwang mga security at privacy setting ng mga browser.
3. Tatalakayin ng tagapagsanay ang kahalagahan ng HTTPS at SSL.
4. Ipakikilala ng tagapagsanay ang mga search engine na DuckDuckgo at StartPage.
5. Tatalakayin ng tagapagsanay ang phishing at pekeng mga link kasama ang mga kadalasang scam sa internet.

BUOD NG SESYON

Isinasalin ng internet browser ang code na ginagamit ng mga computer sa paglikha ng mga website sa text, graphics, at iba pang mga feature ng mga webpage na nakasanayan na nating makita. Lubhang umunlad ang mga web browser mula nang una itong ipakilala noong 1990. Ang anumang maayos na web browser ay kailangang napakasegurado at maprotektahan ka nito laban sa anumang mga data breach. Ito ang ilan sa mga iminumungkahing setting:

- Gumamit ng mga open-source na mga web browser tulad ng Brave, Firefox, o Chromium.
- Huwag i-save ang iyong mga password sa iyong browser settings.
- Huwag mag-install ng mga add-on na hindi katiwa-tiwala.
- Isara ang browser history at laging linisin ang iyong mga browser cache at cookie. Bilang kapalit nito, maaari kang gumamit ng pribadong pagba-browse ngunit isaisip na hindi ka gaanong maikukubli nito kumpara sa paggamit ng Tor.
- Huwag paganahin ang Java at Flash kung hindi naman kinakailangan.
- Gumamit ng DuckDuckGo or Startpage para sa privacy sa pages-search.
- Huwag mag-login sa kahit anong site na walang HTTPS. Maging maingat tuwing may transaksiyon sa online.
- Mas segurado ang HTTPS na bersiyon ng web URL kaysa HTTP.
- Maaaring kapareho ng hitsura ng isang lehitimong mga page ang pekeng mga login page. Tingnang maigi ang parte bago ang unang slash (/) sa URL.

SESYON 07

Mga Password, mga Password Manager, at 2FA

Uri ng sesyon: Gawain-Talakayan-Input-Pagpapalalim-Sintesis

INAASAHANG MGA KAHINATNAN NG LEKSIYON

- Makagagawa ang mga kalahok ng mga malalakas na password at pangasiwaan ang mga ito gamit ang isang seguradong password manager. Matututunan ng mga kalahok ang paggamit ng two-factor authentication (2FA).

MGA LAYUNING PAMPAGKATUTO

- Maunawaan ang kahalagahan ng malalakas at walang katulad na mga password.
- Matutunan kung paanong gumawa ng mahusay na password.
- Malaman ang tungkol sa kaligtasan ng password.
- Matutunan ang paggamit ng isang password manager.
- Matutunan ang tungkol sa mga two factor authentication.

KARAGDAGANG MGA SANGGUNIAN

https://keepassxc.org/ Isang open-source na password manager
https://authy.com/ 2FA app at mga gabay
https://ssd.eff.org/en/module/creating-strong-passwords

GABAY NG SESYON

1. Tatalakayin ng tagapagsanay ang kahalagahan ng isang malakas na password at ituro sa mga kalahok kung paano gumawa ng isang seguradong password.
2. Tatalakayin ng tagapagsanay ang mga hakbanging pangkaligtasan na dapat isaalang-alang kung gagamitin ang mga password.
3. Ipakikilala ng tagapagsanay ang KeePassXC (isang open-source na password manager) at magbibigay ng bai-baitang na gabay sa mga kalahok
4. Tatalakayin ng tagapagsanay ang 2FA, bakit ito mahalaga, at kung paano ito isama sa mga gawing pandigital na seguridad.

BUOD NG SESYON

Inilalaan ng mga password ang unang hanay ng depensa laban sa mga hindi awtorisadong pag-access sa iyong computer at personal na impormasyon. Kapag mas malakas ang iyong password, mas protektado ang iyong computer laban sa mga hacker at mga malicious software. Dapat ay panatilihing malalakas ang iyong mga password sa lahat ng mga account mo sa iyong computer. Upang makalikha ng isang malakas na password at masegurado ito, ito ang ilang mga mungkahi:

- Haba – Gumamit ng password na hindi bababa sa 14 na mga character

- Kombinasyon – Gumamit ng mga bilang, simbolo, uppercase at lowercase na mga letra, at mga space kung maaari sa iyong password.
- Random – Huwag gumamit ng kaparehong estruktura sa lahat ng pagkakataon at iwasan ang mga salitang nasa diksiyonaryo.
- Mga ugnayan – Iwasang gumamit ng personal na impormasyon sa iyong password.
- Matatandaan – Gumamit ng password na matatandaan/maalala mo.
- Privacy – Itago ito; huwag ibahagi ang iyong password sa kahit sino.
- Save – Huwag isulat sa papel o ilagay sa isang text file ang iyong password.
- Kakaiba – Huwag gamitin ang magkaparehong password sa kung saan man.
- Kung maaari, magdagdag ng security screen sa iyong device. Pinipigilan nitong masilip ng mga taong malapit sa iyo ang device screen.
- Kapag mag-iinput ng password, seguraduhing walang taong nasa paligid mo para masilip ang iyong password.
- Magtakip habang pinipindot ang iyong PIN sa ATM booth.
- Tiyaking walang mga camera o salamin na malapit sa iyo.
- Huwag magpasok ng password sa isang device na hindi mo pagmamay-ari.
- Intindihin ang proseso ng pag-recover ng password para sa lahat ng iyong mga account.
- Kapag magla-login, seguraduhing gumagamit ng HTTPS protocol ang website at valid ang SSL certificate nito.
- Paganahin ang non-SMS o call-based na 2FA kung maaari. Gumamit ng open-source na app o hardware-based na 2FA.
- Gumamit ng isang open-source na password manager na mag-iingat sa pagiging encrypted ng iyong database. Isang libre at open-source na password manager ang KeePassXC. Nagsimula ito bilang komunidad ng KeePassX. Isa iyong multi-platform na application na mapapatakbo sa Linux, Windows, at macOS.

SESYON 08

Security at Privacy na mga Setting sa Social Media

Uri ng sesyon: Gawain-Talakayan-Input-Pagpapalalim-Sintesis

INAASAHANG MGA KAHINATNAN NG LEKSIYON

- Maisasaayos ng mga kalahok ang kani-kanilang security at privacy setting sa social media.

MGA LAYUNING PAMPAGKATUTO

- Maunawaan ang mga panganib sa paggamit ng mga social network at matuto tungkol sa mga pag-iingat.
- Matutunan ang tungkol sa social engineering.
- Matutunan ang tungkol sa security at privacy na mga setting sa mga social network site.

KARAGDAGANG MGA SANGGUNIAN

https://youtu.be/F7pYHN9iC9I Isang video para sa kamalayan sa social media
https://level-up.cc/curriculum/social-media-safety/
https://www.webroot.com/us/en/resources/tips-articles/what-is-social-engineering
https://www.csoonline.com/article/2124681/what-is-social-engineering.html
https://ssd.eff.org/en/module/protecting-yourself-social-networks

GABAY NG SESYON

1. Magpapalabas ng isang video na may kaugnayan sa kamalayan sa social media ang tagapagsanay.
2. Tatalakayin ng tagapagsanay ang mga bant ana kinahaharap ng mga user sa social media at kung paano ito maiiwasan.
3. Hihikayatin ng tagapagsanay ang mga kalahok na magbahagi ng kani-kanilang personal at pang-organisasyong mga karanasan sa paggamit ng social media at mga nagdaang insidente.
4. Tatalakayin ng tagapagsanay ang konsepto ng social engineering.
5. Gagabayan ng tagapagsanay ang mga kalahok sa bai-baitang na pagsasaayos ng kanilang security at privacy na mga setting sa mga popular na mga social media platform.

BUOD NG SESYON

Isang sining ng pagmamanipula ng mga tao ang social engineering para maisuko sa kanila ang mga kumpidensiyal na impormasyon. Iba't ibang uri ng mga impormasyon ang hinahanap ng mga kriminal na ito, ngunit ang mga indibidwal na tinatarget ng mga kriminal na ito ay karaniwang sinusubukang linlangin ka sa pagbibigay mo ng iyong mga password o impormasyon sa bangko. Maaari rin nilang tangkaing palihim na mag-install ng mga malicious software na magbibigay-kontrol sa iyong computer at ma-access ang iyong personal na impormasyon.

- Kailangang maging malay ka sa mga panganib na ito:
    - o cyberbullying (pambu-bully gamit ang digital na teknolohiya)
    - o pagnanakaw ng impormasyon at identidad
    - o pananalakay ng privacy
    - o nakasasakit na mga imagen at mensaheng nakatarget sa mga bata
    - o presensiya ng mga estranghero na 'naniniktik' ng ibang mga miyembro
- Kumukubli sa maraming mga porma ang mga atakeng social engineering at maaari itong isagawa sa kahit saang may interaksiyon ng mga tao. Minamanipula ng mga social engineer ang damdamin ng mga tao, katulad ng pagkamausisa o pagkatakot, upang isagawa ang mga balak at dalhin ang mga biktima sa kanilang mga patibong. Samakatuwid, maging maingat kapag pakiramdam mo ay naalarma ka sa isang email, inakit ka sa isang alok na ipinakikita sa isang website, o magtaka kapag nakatagpo ka ng kahit anong uri ng digital media.
    - o Huwag magbukas ng mga email at attachment mula sa mga kahina-hinalang nagpadala
    - o Gumamit ng multifactor authentication
    - o Maging mapagmatiyag sa mga nakasisilaw na mga alok
    - o Panatilihing updated ang iyong antivirus at anti-malware na mga software
- Sagana sa panganib ang mga social network, na maaaring magdulot ng mga matitinding kahinatnan sa iyo o sa iyong negosyo. Maaari mong maiwasan ang mga patibong na ito sa pamamagitan lamang ng maingat na paggamit ng mga network na ito. Kadalasang nakatutulong ang mga karagdagang hakbangin na ito:
    - o Ayusin ang iyong mga privacy setting para ang iyong mga kaibigan lamang ang makakakita ng iyong mga post.
    - o Iwasang mag-post ng personal na impormasyon, mga plano sa bakasyon, etc.
    - o Huwag tanggapin ang mga request o mensahe sa mga taong hindi mo naman kilala
    - o Iwasang pindutin ang pinaigsing mga URL
    - o Report suspect or insulting and threatening accounts
    - o Panatilihing magkahiwalay ang mga personal na account sa trabaho

SESYON 09

Kung Paano Gumagana ang Internet

Uri ng sesyon: Gawain-Talakayan-Input-Pagpapalalim-Sintesis

INAASAHANG MGA KAHINATNAN NG LEKSIYON

- Matututunan ng mga kalahok kung paano gumagana ang internet.

MGA LAYUNING PAMPAGKATUTO

- Matutunan kung paanong gumagana ang internet kung paanong naililipat ang datos mula sa isa sa iba pa.
- Malaman kung paanong nagiging kasangkot ang mga actor sa network at ang mga kaakibat nitong mga panganib.
- Maunawaan ang batayang seguridad ng router.

KARAGDAGANG MGA SANGGUNIAN

https://academind.com/tutorials/how-the-web-works/
https://www.youtube.com/watch?v=7_LPdttKXPc
https://vahid.blog/post/2020-12-15-how-the-internet-works-part-i-infrastructure/

GABAY NG SESYON

1. Hihikayatin ang mga kalahok na ibahagi ang kanilang kaalaman at pagkaunawa sa kung paano gumagana ang internet.
2. Magpapalabas ang tagapagsanay ng isang video na nagpapaliwanag kung paanong gumagana ang internet.
3. Ipaliliwanag ng tagapagsanay kung paano kumikilos ang paglilipat ng datos sa internet sa pamamagitan ng pagpapakita ng halimbawa (katulad ng pag-send ng mga email o ang paggamit ng mga web browser) upang ipaliwanag kung paano naglalakbay ang datos mula sa isa hanggang sa isa pa.
4. Tatalakayin ng tagapagsanay ang lahat ng mga posibleng aktor na kasangkot sa isang network at ang mga kaugnay na mga panganib.
5. Tatalakayin ng tagapagsanay ang mga batayang panseguridad na setting ng router.

BUOD NG SESYON

- Isang pandaigdigang computer network ang internet na naghahatid ng sari-saring mga datos at media sa mga magkakakonektang mga device. Guamagana ito sa pamamagitan ng paggamit ng isang packet routing network na sumusunod sa Internet Protocol (IP) at Transport Control Protocol (TCP).
- Isang mas malawak na network ang internet na nagpapahintulot sa mga

computer network na pinatatakbo ng mga kompanya, mga pamahalaan, at ibang mga organisasyon sa iba't ibang panig ng mundo na makipag-ugnayan sa iba pa.

- Simpleng inililipat ng internet ang data mula sa isang pook sa isa pa, para magawa nating makipag-chat, mag-browse, at magbahagi ng impormasyon.
- Sa pisikal, ang internet ay isang koleksyon ng mga computer na nagpapagalaw ng mga bit sa mga kawad, kable, at mga radio signal.
- Direktang kumokonekta ang isang wireless router sa isang modem sa pamamagitan ng kable. Pinahihintulutan nitong makatanggap ng impormasyon mula — at maghatid ng impormasyon — sa internet. Saka lilikha at makikipagkomunika ang router sa iyong Wi-Fi network sa bahat sa pamamagitan ng mga built-in na antenna. Ang resulta nito, lahat ng iyong mga device sa inyong home network ay may access sa internet.
- Ganito mo bina-browse ang isang website: Iyong device <-> Router <-> ISP <-> DNS <-> Web Server
- Hindi laging segurado ang internet. Kung hindi mag-iingat, maaaring makakuha ng access sa iyong hindi naka-encrypt na personal na impormasyon ang ibang tao.
- Batayang mga router security setting:

    o Palitan ang default na password.

    o Palitan ang default na pangalan ng wifi

    o Gumamit ng mahusay na password para sa wifi

    o Gumamit ng WPA2/3 encryption at umiwas sa WEP.

    o Itago ang wifi ID kung kinakailangan.

    o Huwag ibahagi ang iyong network sa iba. Kung kinakailangan, gumawa ng isang guest network.

SESYON 10

Encryption at Pag-eencrypt ng Daloy ng Internet

Uri ng sesyon: Gawain-Talakayan-Input-Pagpapalalim-Sintesis

INAASAHANG MGA KAHINATNAN NG LEKSIYON

- Matututunan ng mga kalahok kung ano ang encryption at kung paano nila ma-eencrypt ang kanilang daloy ng internet.

MGA LAYUNING PAMPAGKATUTO

- Maunawaan kung ano ang encryption.
- Maunawaan kung ano ang isang VPN at kung paano pumili ng isang mahusay na VPN.
- Maunawaan kung ano ang TOR at kung paano ito gumagana.

KARAGDAGANG MGA SANGGUNIAN

https://aesencryption.net/ Isang online text encryption platform
https://aescrypt.com/ Munting mga kasangkapan sa pag-encrypt ng mga file na may gamit na password
https://torproject.org/ Opisyal na site ng TOR
https://www.tunnelbear.com/ Bayad na VPN

- https://engagemedia.org/tunnelbear – libreng isang-taong subscription ng TunnelBear VPN

https://www.psiphon3.com/ Libreng VPN
https://www.f-secure.com/en/home/articles/6-things-to-consider-when-choosing-a-vpn
https://engagemedia.org/2021/indonesia-vpn/
https://www.eff.org/pages/tor-and-https Kung paano gumagana ang HTTPS at Tor

GABAY NG SESYON

1. Hihikayatin ang mga kalahok na ipaliwanag kung paano nila nauunawaan ang encryption.
2. Tatalakayin ng tagapagsanay kung ano ang encryption at kung bakit ito mahalaga
3. Hihikayatin ang mga kalahok na magbahagi kung nakaranas na sila na ma-block ang pinupuntang website o nilinlang nito, at kung nakaranas na, paano nila ito nasolusyonan.
4. Tatalakayin ng tagapagsanay kung ano ang VPN, paano ito gumana, at bakit kailangan nating gumamit ng VPN. Ipaliliwanag ng tagapagsanay kung ano ang mga salik na isasaalang-alang sa pagpili ng isang VPN.
5. Ipaliliwanag ng tagapagsanay kung paano gumagana ang TOR network.

BUOD NG SESYON

- Encryption ang proseso ng pagkuha ng isang payak na text, tulad ng text message o email, at paguguluhin ang pagkakaayos nito tungo sa isang hindi mabasang format na binansagang “cipher text.” Tinutulungan nitong maprotektahan ang pagiging kumpidensiyal ng digital data na nakaimbak sa mga computer system o ipinapadala sa pamamagitan ng isang network tulad ng internet.
- A virtual private network (VPN) protects your identity and browsing activity from hackers, businesses, government agencies, and other snoops. When connecting to the internet, your data and IP address are hidden by a type of virtual tunnel. This keeps others from spying on your online activity.
- Kapag namimili ng VPN:
    - o Tingnan ang karanasang panseguridad ng VPN provider
    - o Tingnan ang patakaran sa privacy ng iyong pipiliing VPN
    - o Tingnan ang bilang nga mga lokasiyon ng server
- Isang libre at open-source na software na nagpapahintulot sa isang walang pangalang komunikasyon ang Tor. Idinidirekta nito ang daloy ng internet sa pamamagitan ng isang libre, pandaigdigan, at boluntaryong overlay network na binubuo ng higit 7,000 mga relay upang ikubli ang lokasiyon at paggamit ng isang user mula sa kahit sinong nagsasagawa ng pangmamatiyag sa network o pag-aanalisa ng daloy.
- Paano gumagana ang Tor:
    - o Naglulunsad ito para sa iyo ng mga koneksiyon sa pamamagitan ng tatlong random na mga Tor node.
    - o Hindi alam na kahit ano sa mga node ang pinagmulan at pupuntahan ng kahit anong koneksiyon.
    - o Naka-encrypt ang lahat ng iyong daloy mula sa iyo hanggang sa huling node.

SESYON 11
Seguridad ng File at Folder

Uri ng sesyon: Gawain-Talakayan-Input-Pagpapalalim-Sintesis

INAASAHANG MGA KAHINATNAN NG LEKSIYON
- Matitiyak ng kalahok ang seguridad ng file at folder.

MGA LAYUNING PAMPAGKATUTO
- Maunawaan ang kahalagahan ng seguridad ng datos.
- Malaman kung ano ang metadata at bakit ito mahalaga
- Matutunan kung paano mag-encrypt ng mga file at folder gamit ang mga kasangkapang pang-encrypt.
- Matutunan kung paano mag-recover ng tinanggal na mga file.

KARAGDAGANG MGA SANGGUNIAN
https://veracrypt.fr/ Kasangkapang pang-encrypt ng File folder
https://cryptomator.org/
https://www.bleachbit.org/ Permanenteng pantanggal ng file at folder
https://ccleaner.com/recuva Kasangkapan sa pag-recover ng binurang file
http://exif.regex.info/ Platform ng pagbeberipika ng metadata
https://ssd.eff.org/en/module/why-metadata-matters

GABAY NG SESYON
1. Hihikayatin ang mga kalahok na ibahagi ang kanilang mga gawi sa seguridad ng file at folder.
2. Tatalakayin ng tagapagsanay ang seguridad ng locally stored information.
3. Tatalakayin ng tagapagsanay ang metadata at kung bakit kailangang maging malay tayo dito.
4. Ipakikita ng tagapagsanay ang mga tagubilin kung paano mag-recover ng mga tradisyunal na binurang mga file at kung paanong permanenteng tanggalin ang mga ito sa computer.
5. Magbibigay ng bai-baitang na gabay ang tagapagsanay sa mga kasangkapang pang-encrpyt ng file/folder katulad ng Veracrypt.

BUOD NG SESYON

Sa panahon ngayon ng kaligirang digital, winiwika nang mas mamahalin umano ang datos kaysa langis dahil sa kabatiran at kaalaman na maaaring mahango mula rito. At napakadali na rin para sa mga cyber criminal na i-hack ang iyong account at pasukin ang iyong Negosyo sa pagkakataong makolekta na nila ang iyong sensitibong impormasyon. Ito ang dahilan kung bakit napakahalaga ng cyber security para sa lahat na iyong kumokonektang mga device.

Data security is when protective measures are put in place to keep unauthorised access out of computers, websites, and databases. This process also provides a mechanism for protecting data from loss or corruption.

- Napakahalagang mabawasan ang panganib ng data breach at mga atake nito. Napakaimportante ang paglalapat ng panseguridad na mga control upang mapigilan ang hindi awtorisadong pag-access sa mga sensitibong impormasyon.
- Ang pagiging kumpidensiyal, pagkakaroon ng integridad, at pagiging bukas ang batayang mga simulain ng seguridad sa impormasyon.
- Kapag magdi-delete ng file sa tradisyunal na pamamaraan (i.e., ilipat ito sa trash folder), hindi talaga ito nabubura. Maaari pang mai-recover ang isang file na binura sa ganitong paraan. Ang permanenting pagbubura ng isang file sa isang normal na magnetic hard disk (HDD) ay nangangailangan ng pag-ooverwrite sa kaparehong lokasiyon.
- Mag-ingat sa mga file katulad ng Temporary / History / Cache / Logs, atbp. Dala-dala ng mga ito ang iba pang mahahalagang impormasyon katulad ng history ng iyong browser at mga chat log.
- Ang metadata ay impormasyon tungkol sa mga komunikasyong digital na iyong ipinadadala o tinatanggap. Nagdadala ang metadata ng napakaraming mahahalagang impormasyong maaaring magdala ng banta sa iyong seguridad. Tiyaking subukan ang pagdi-delete o pagmiminimisa ng metadata. Narito ang ilang mga halimbawa ng metadata:

  o ang paksa (subject) ng iyong mga email

  o ang haba ng iyong pag-uusap

  o ang panahon kung saan nangyari ang isang pag-uusap

  o ang iyong lokasiyon kapag nakikipag-usap (pati na rin kung kanino)

- Paganahin ang encryption kung sinusuportahan ito ng iyong operating system. O gumamit ng libre at open-source na software tulad ng Veracrypt, na nagbibigay ng on-the-fly na encryption. Makalilikha ito ng isang birtwal na encrypted disk sa loob mismo ng file o mag-encrypt ng bahagi o ng buong storage device na may pre-boot na awtentikasyon.
- Bilang pamalit, maaari ka ring gumamit ng Cryptomator upang panatilihing encrypted ang iyong datos. Kung gagamit ka ng Cryptomator, makagagawa ka ng mga vault nan aka-host sa isang birtwal na drive. Ang mga datos na nakaimbak sa vault ay saka ieencrypt. Maaaring tukuyin ng user ang lokasiyon ng vault, katulad ng isang cloud provider, halimbawa.

SESYON 12
Pagba-backup ng Datos

Uri ng sesyon: Gawain-Talakayan-Input-Pagpapalalim-Sintesis

INAASAHANG MGA KAHINATNAN NG LEKSIYON
- Malalaman ng mga kalahok ang kahalagahan ng mga backup at kung paano ito gawin nang wasto.

MGA LAYUNING PAMPAGKATUTO
- Maunawaan ang kahalagahan ng pagba-backup.
- Matutunan kung paano gumawa at mag-imbak ng mga backup nang segurado.

KARAGDAGANG MGA SANGGUNIAN
https://duplicati.com/ Isang kasangkapang naka-encrypt para sa paggawa ng backup
https://www.duplicati.com/articles/Getting-Started/
https://support.microsoft.com/en-us/windows/backup-and-restore-in-windows-10-352091d2-bb9d-3ea3-ed18-52ef2b88cbef

GABAY NG SESYON
1. Tatanungin ang mga kalahok tungkol sa kanilang kasalukuyang mga gawi sa pagba-backup ng datos.
2. Tatalakayin ng tagapagsanay ang kahalagahan ng pagba-backup.
3. Magpapakita ng bai-baitang na gabay ang tagapagsanay sa paggamit ng isang open-source na kasangkapang naka-encrypt para sa paggawa ng backup tulad ng Duplicati.

BUOD NG SESYON

Ano ang kahalagahan ng pagba-backup ng datos? Lumilikha ang data backup ng isang seguradong sinupan ng iyong mga mahahalagang impormasyon – maging kumpidensiyal na mga dokumento ng iyong megosyo o pinahahalagahang litrato ng iyong pamilya – para sa mabilisan at tuloy-tuloy na pagsasabalik ng iyong device sa dati mangyari mang mawala ang mga datos.

- Mahalaga sa pangangasiwa ng mga datos ang paggawa ng mga backup ng mga nakolektang datos. Mapoprotektahan ito ng backup laban sa mga pagkakamali ng tao, pagbagsak ng hardware, pag-atake ng virus, pagkawala ng kuryente, at mga likas na sakuna.
- Maaaring masira, manakaw, o mawala ang iyong device na naglalaman ng mahahalagang mga file. Makatitipid sa oras at pera ang mga backup upang maibalik ang mahahalagang mga impormasyon kung may mangyari mang pagkawala nito.

- Panatilihin ang palagiang pagba-backup. Inirerekomenda ang higit sa isang paggawa nito.
- Huwag ipagsama sa magkaparehong lugar ang orihinal at naka-backup na datos.
- Seguraduhing naka-encrypt ang backup.
- Gumamit ng maayos at maaasahang mga kasangkapan sa pagba-backup.
- Mga uri ng backup:
    - o Ganap (Full) na backup
    - o Padagdag-dagdag (Incremental) na backup
    - o Magkakaibang (Differential) backup
- Maaari mong gamitin ang built-in na backup feature sa Windows operating system. Gayunpaman, tiyaking huwag ibackup ang mga file sa parehong hard disk na kung saan naka-install ang Windows. Halimbawa, huwag ibackup ang mga file sa isang pang-recovery na partition. Laging itago ang media na ginagamit sa mga backup (mga external hard disk, mga DVD, o mga CD) sa isang seguradong lugar upang maiwasan ang pag-access ng mga file ng mga hindi awtorisadong mga tao; inirerekomenda rin ang isang iwas-sunog na lokasiyon na malayp sa iyong computer. Isaalang-alang mo rin ang pag-eencrypt ng datos sa iyong backup.
- Isang libre at open-source na backup client ang Duplicati na seguradong nagtatago ng mga naka-encrypt, padagdag, at siniksik na mga backup sa isang cloud storage na mga service at malalayong mga file server. Tinitipon ng Duplicati ang lahat ng mga file na ibabackup, dine-deduplicate, at sinisiksik, saka ipadadala sa lokasiyon ng iyong backup nang bloke-bloke o tipak-tipak para itago sa pinakamataas na kahusayan, Hindi lamang iba't ibang mga online backup service ang sinusuportahan ng Duplicati katulad ng OneDrive, Amazon S3, Backblaze, Rackspace Cloud Files, Tahoe LAFS, at Google Drive, kundi pati ring kahit anong mga server na sumusuporta ng SSH/SFTP, WebDAV, o FTP.

SESYON 13
Pag-eencrypt ng Email

Uri ng sesyon: Gawain-Talakayan-Input-Pagpapalalim-Sintesis

INAASAHANG MGA KAHINATNAN NG LEKSIYON
- Matututunan ng mga kalahok kung paano iencrypt ang kanilang komunikasyon sa email.

MGA LAYUNING PAMPAGKATUTO
- Maunawaan kung paanong ipinapadala, rinuruta, at natatanggap ang email, pati na kung saan at paanong mababasa ang mga nilalaman ng email.
- Matuttunan ang mga paraan sa pagmiminimisa ng pagkakalantad ng email sa hindi ginustong pagsisiyasat.
- Maintindihan kung ano ang GPG/PGP at kung paano ito gumagana, kasama na ang iba't ibang mga isyu na may kaugnayan sa paggamit nito (e.g., potensyal na "pagtawas sa iyong atensiyon" ng iyong paggamit nito, ang limitasyon ng maaaring pagkagamit nito sa mobile na mga device, atbp.)
- Matutunan kung paano gumawa ng isang pribado/publikong keypair, mag-upload ng pampublikong key sa isang keychain, maghanap at mag-download ng mga pampublikong key ng iba, at mag-awtentika ng mga key at pagkakakilanlan ng iba.
- Matutunan kung paano magpadala at tumanggap ng mga email na nilagdaan o in-encrypt gamit ang GPG/PGP.

KARAGDAGANG MGA SANGGUNIAN
https://www.openpgp.org/ Encryption ng email
https://mailvelope.com/ Isang email encryption na browser extension
https://www.thunderbird.net/ Isang open-source na mail client na sumusuporta ng PGP.

GABAY NG SESYON
1. Tatalakayin ng tagapagsanay kung paano gumagana ang komunikasyon sa email, ang proseso ng pagpapadala ng email mula sa nagpadala patungo sa tatanggap, ang mga sangkot na panganib sa seguridad, at kung paano mapagaan ang mga panganib na ito.
2. Magpapakita ang tagapagsanay ng isang bai-baitang na gabay sa paggamit ng Mailvelope, isang open-source na email security browser extension.
3. Magpapakita ang tagapagsanay ng isang bai-baitang na gabay sa paggamit ng Thunderbird, isang open-source na email client na sumusuporta sa openPGP.

BUOD NG SESYON

Ayon sa **IRONSCALES report** na ito, higit 90% ng mga atake laban sa mga organisasyon ay nagsisimula sa isang malicious email. Mahalaga ang pagpoprotekta sa email dahil sa mga cyber threat katulad ng mga atakeng sosyal na umaasinta sa mga organisasyon sa pamamagitan ng email. Halimbawa, maaaring linlangin ng mga phisihing email ang mga user sa pagbibigay nila ng sensitibong impormasyon, pag-apruba sa mga pekeng kuwenta, o pagdownload ng mga malware na makahahawa sa network ng iyong kompanya.

- Laging dumadaan sa isang taong hindi natin kilala ang ating mga email, usapan sa chat, at instant na mga mensahe dahil sa kung paanong gumagana ang internet.

    o Nakadisenyo na ang pag-access nito ng ilang mga tao, e.g., ang ating ISP o mobile service provider.

    o Maaaring mayroon sila nito dahil sa mataas na antas ng pag-access, na maaaring sa pamamagitan ng legal na pamamaraan, katulad ng isinapublikong utos ng korte na subpoena o mga serbisyong pang-intelihensiya, o sa extralegal na pamamaraan.

    o Ma-aaccess ito ng iba dahil sa kahinaan ng system nito, e.g. mga hacker.

- Isang sistemang pang-encryption ang Pretty Good Privacy (PGP) na ginagamit sa parehong pagpapadala ng mga naka-encrypt na email at pag-eencrypt ng sensitibong mga file.

- Pinahihintulutan ng browser extension na Mailvelope ang isang seguradong komunikasyon sa email na nakabatay sa pamantayan ng OpenPGP. Maaari itong magamit gamit ang kasalukuyan mong email upang mag-encrypt at lumagda ng mga elektronikong mensahe, kasama na ang mga kalakip na file, kahit hindi gumamit ng hiwalay at native na email client.

- May built-in na support ang Thunderbird 78 para sa dalawang mga standard ng encryption, OpenPGP at S/MIME. Pinahihintulutan bilang default ang OpenPGP simula sa version 78.2.

- Huwag ibahagi sa iba ang iyong pribadong mga key.

- Kung ayaw mong gumamit ng Thunderbird o Mailvelope, gumamit ng seguradong mail service tulad ng Protonmail. Ngunit isaisip na tanging ang mga mail na ipinapadala at galing sa Protonmail ay naka-encrypt at segurado. Ang ibig sabihin nito, kapag nagpadala ka ng email galling sa iyong Protonmail account patungong Gmail, Yahoo, Hotmail, o iba pang email services, hindi ito ma-eencrypt.

SESYON 14
Seguridad ng Mobile Phone

Uri ng sesyon: Talakayan-Input-Pagpapalalim-Sintesis

INAASAHANG MGA KAHINATNAN NG LEKSIYON
- Matututunan ng mga kalahok ang tungkol sa seguridad ng mobile phone.

MGA LAYUNING PAMPAGKATUTO
- Maunawaan ang mga nauugnay na mga panganib sa pagdadala at paggamit ng mga mobile phone.
- Malaman kung paanong mabawasan ang mga panganib na ito.

KARAGDAGANG MGA SANGGUNIAN
https://level-up.cc/curriculum/mobile-safety/
https://ssd.eff.org/en/playlist/privacy-breakdown-mobile-phones
https://securityinabox.org/en/guide/basic-security/android/
https://securityinabox.org/en/guide/basic-security/ios/

GABAY NG SESYON
1. Tatalakayin ng tagapagsanay ang iba't ibang mga uri ng mga panganib na maiuugnay sa paggamit ng mga mobile phone.
2. Magpepresenta ang tagapagsanay ng mga iminumungkahing setting para sa mobile phone para sa privacy at security, na susundin ng mga kalahok.

BUOD NG SESYON

Malaking bahagi na ng ating pang-araw-araw na buhay ang pagkakaroon ng isang mobile phone. Maraming nagmamaliit sa totoong halaga ng isang phone pagdating sa nakaimbak na impormasyon. Nasa iyong phone ang iyong buong buhay – ito ay isang mobile bank, device na pangkomunikasyon, at isang social network na hub. Sa napakaraming gamit sa iisang device, mahalagang maprotektahan ang impormasyong nakalagak dito.

Isang hakbangin upang protektahan laban sa malawak na sakop ng mga panganib na layong manira sa iyong privacy at makakuha ng access sa iyong phone ang mobile na seguridad. Layon ng mga atakeng ito sa iyong mobile device na agawin ang iyong pribadong impormasyon katulad ng impormasyon sa bangko, impormasyon sa pag-login, at iba pang mga datos.

Isang paraan ng cyber-attack na tumatarget ng mga mobile device tulad ng mga smartphone at tablet ang mobile security threat. Katulad ng paghahack sa isang PC o enterprise server, pinagsasamantalahan nito ang mga kahinaan ng mga mobile software, hardware, at mga koneksiyon sa network na nagpapahintulot ng mga kahina-hinala at hindi awtorisadong mga gawain sa target device.

Posible para sa mga hacker na ma-access sa iyong mobile phone at gawin ang anumang gusto nila, tulad ng pakikinig sa iyong boses gamit ang mic, i-record ang iyong mga tawag, kumuha ng mga litrato, o mag-record ng mga video. Makatatawag din sila o kaya'y makakapag-send ng SMS galing sa iyong device.

Narito ang ilang mga suhestiyon upang maprotektahan ang iyong privacy:

- Panatilihing updated ang OS ng iyong device.
- Laging gumamit ng password sa iyong mobile phone.
- Huwag hayaang gamitin ng iba ang iyong mobile phone.
- Sa pag-install ng isang mobile app, isaalang-alang ang mga permisong pahihintulutan.
- Paganahin ang full disk encryption.
- Isara ang GPS.
- Huwag i-jailbreak o i-root ang iyong phone.
- Mag-ingat sa mga hindi pamilyar na mga mensahe o media.
- Huwag ikonekta ang iyong phone sa public wifi.
- Ioptimisa ang seguridad ng iyong lock screen.
- Huwag dalhin ang iyong phone kahit saan. Kung nais mong dumalo isang seguradong pagpupulong o protesta at ayaw mong ipabunyag ang iyong lokasyon, iwanan sa bahay ang iyong phone.

SESYON 15

End-to-end na Pag-eencrypt at Mobile na Komunikasyon

Uri ng sesyon: Gawain-Talakayan-Input-Pagpapalalim-Sintesis

INAASAHANG MGA KAHINATNAN NG LEKSIYON

- Matututunan ng mga kalahok ang tungkol sa end-to-end na encryption at kung paano sila makakapagkomunika nang segurado sa pamamagitan ng encrypted na mga app.

MGA LAYUNING PAMPAGKATUTO

- Maunawaan ang pamamaraan ng end-to-end na encryption.
- Pumili ng mga encrypted na app para sa mobile na komunikasyon.

KARAGDAGANG MGA SANGGUNIAN

https://protonmail.com/blog/what-is-end-to-end-encryption/
https://ssd.eff.org/en/module/deep-dive-end-end-encryption-how-do-public-key-encryption-systems-work Isang key exchange system (advanced)
https://signal.org/ Isang secure communication app
https://wire.com/ Isang secure communication app
https://briarproject.org/ Mobile app para sa offline secure communication

GABAY NG SESYON

1. Tatalakayin ng tagapagsanay kung ano ang end-to-end na encryption, paano ito gumagana, at bakit ito mahalaga para sa seguridad at privacy.
2. Magbabahagi ang tagapagsanay ng mga mobile communication app na sumusuporta ng end-to-end na encryption.
3. Hihikayatin ang mga kalahok na i-download ang mga app at gagawa ng isang group sa Signal/Wire para sa komunikasyon ng mga kalahok o pagtuturo mula sa tagapagsanay sa hinaharap.

BUOD NG SESYON

Isang paraan ng seguradong komunikasyon ang end-to-end encryption (E2EE) na pumipigil sa mga third party sa pag-access ng data habang naglilipat ng impormasyon mula sa isang one end system o device sa iba pa. Sa E2EE, naka-encrypt ang data sa system o device ng nagpadala at tanging ang makatatanggap lamang ang makakapag-decrypt nito. Sa ngayon, pinakaseguradong paraan ng paglilipat ng kumpidensiyal na datos ang end-to-end encryption, kaya naman maraming mga serbisyong pangkomunikasyon ang lumilipat sa mga ito.

- Iwasan ang regular na pagtawag sa cellular kung gusto mong panatilihing pribado ang iyong impormasyon.
- Laging gumamit ng mga apps na open

source at sumusuporta ng end-to-end encryption para sa mobile na komunikasyon.

- Isang libre at nakapokus sa privacy na messaging at voice talk app ang Signal na maaaring gamitin sa Apple at Android na mga smartphone at pati na rin sa desktop. Phone number lang ang iyong kailangan para makasali. Encrypted na end-to-end ang mga komunikasyon sa Signal, ibig sabihin ay ang mga makakakita lamang ng nilalaman ng mga mensaheng ipadadala ay ang mga tatanggap lamang – kahit ang kompanya ay hindi rin ito makikita.

- Kapareho ng Signal ang Wire, ngunit pwede kang gumawa ng account sa Wire kahit walang mobile phone number. Pwede kang gumamit ng alinman sa email address o phone number upang makagawa ng account.

- Dinisenyo naman ang messaging app na Briar para sa mga aktibista, peryodista, at sinumang nangangailangan ng isang ligtas, madali, at matibay na paraan ng pakikipagkomunika. Hindi tulad ng mga traditional na messaging app, hindi umaasa ang Briar sa isang central na server – sinisingkronisa ang mga mensahe nang direkta sa device ng mga gumagamit. Kapag walang internet, makakapag-sync ang Briar gamit ang Bluetooth o WiFi, habang pinapanatili ang pagdaloy ng impormasyon sa isang krisis. Kapag gumagana na ang internet, makakapag-sync ang Briar gamit ang Tor network habang pinoprotektahan nito ang mga user at ang kanilang mga kasamahan mula sa pangmamatiyag.

SESYON 16

Paanong Maghanda para sa mga Susunod na Pagsasanay

Uri ng sesyon: Talakayan-Input-Pagpapalalim-Sintesis

INAASAHANG MGA KAHINATNAN NG LEKSIYON

- Mas mahusay na pagganap ng mga kalahok sa pagsasagawa ng pagsasanay

MGA LAYUNING PAMPAGKATUTO

- Matutunan ang batayang mga panuntunan sa mas mahusay na pagganap habang nagsasanay.
- Matuto kung paanong gumawa ng isang maayos na presentasyon.
- Alamin ang iba't ibang mga bagay na isasaalang-alang bago, habang, at pagkatapos na magsanay.
- Matuto kung paanong magplano ng isang sesyon.
- Matuto kung paano pangasiwaan ang mga tanong sa panahon ng pagsasanay

KARAGDAGANG MGA SANGGUNIAN

https://level-up.cc/before-an-event/preparing-sessions-using-adids/
https://level-up.cc/you-the-trainer/golden-rules-of-effective-training/

GABAY NG SESYON

1. Magpapakita ang tagapagsanay ng iba't ibang mga tip sa mga kalahok na may kinalaman sa pagpaplano at pagsasagawa ng kanilang susunod na pagsasanay,
2. Sasagutin ng tagapagsanay ang mga tanong mula sa mga kalahok at magbigay ng mga halimbawa kung kinakailangan.

BUOD NG SESYON

- Pangangasiwa sa oras:
  - o Bantayan ang oras. Hikayatin ang mga kalahok na sundin ang wastong oras at iskedyul.
  - o Mag-iskedyul batay sa nilalaman ng pagsasanay.
  - o Maglaan ng oras para sa mga tanong.
  - o Sandaling huminto kung kinakailangan
- Mga Kalahok:
  - o Magpakita ng respeto sa mga kalahok.
  - o Seguruhing nauunawaan nila ang mga paksa.
  - o Magtanong at hikayatin silang magtanong.
  - o Bigyang pansin ang kanilang kalagayang emosyonal (halimbawa, kung sila ay naiinis).

- Pag-uunawa sa sitwasyon:

  o Hindi lahat ay maayos at tuloy-tuloy. Maghanda sa pagbabago ng mga plano.

  o Maging malikhain at mapag-angkop depende sa sitwasyon.

  o Baguhin ang nilalaman batay sa mga kahingian o sitwasyon ng mga kalahok.

  o Ayusin ang mga paksa sa mga paraang organisado at nauugnay.

  o Magsama ng mga ice breaker at maglibang upang mapanatiling gising ang mga kalahok

- Mga kagamitan at kinakailangang pagsasaayos:

  o Gawin ang mga kinakailangang pag-iingat sa seguridad.

  o Seguraduhing gumagana ang mga gagamiting device.

  o Tiyaking mayroong mga kinakailangang kagamitan para sa lahat ng mga kalahok.

- Paglikha ng presentasyon:

  o Panatilihing simple at malinis ang presentasyon.

  o Gumamit ng magkakatulad na mga font. Iwasang gumamit ng mga extra color.

  o Huwag sobrahan ang text; magdagdag na lamang ng mga larawan.

  o Panatilihin ang pagpapatuloy ng paksa. Talakayin muna ang suliranin saka ipakita ang solusyon.

  o Maging updated sa mga pinakabagong balita tungkol sa digital security.

  o Magbigay ng halimbawang may kinalaman sa mga work area at context ng kalahok.

  o Huwag magsama ng anumang materyal na nang-aagrabyado ng iba pang mga kalahok.

  o Maglagom sa pagwawakas ng bawat seksiyon

5.0 *Glosaryo*

2FA	Ang two-factor authentication (2FA) ay isang sistemang panseguridad na nangangailangan ng dalawang magkahiwalay at magkaibang mga porma ng pagkilala upang makapasok sa anumang bagay.
Antivirus	Antivirus software, kilala rin bilang anti-malware, ay isang computer program na ginagamit upang mapigilan, matitikan, at mananggal ng malware.
DNS	Ang Domain Name System (DNS) ay ang “phone book” ng internet.
DuckDuckGo	Isang internet search engine ang DuckDuckGo at pinahahalagahan nito ang privacy ng mga searcher at iniiwasan din nito ang filter bubble ng isinapersonal na mga search result.
E2EE	Ang end-to-end encryption ay isang sistema ng komunikasyon na kung saan ang mga communicating user lamang ang makababasa ng mga mensahe.
Encryption	Ang encryption ay isang paraan ng pagpapalit ng katumbas ng impormasyon tungo sa isang sekretong code na kumukubli sa totoong kahulugan nito. Cryptography ang bansag sa agham ng pag-eencrypt at pagde-decrypt ng impormasyon.
FTP	Isang pamantayan sa protocol ng komunikasyon ang File Transfer Protocol na ginagamit sa paglipat ng mga computer file mula sa isang server tungo sa client na nasa computer network.
GPS	Ipinakikita ng Global Positioning System (GPS) sa iyo kung nasaang bahagi ka ng daigdig.
HRD	Human rights defenders, mga tagapagtanggol ng karapatang pantao.

HTTP	Isang application-layer na protocol ang Hypertext Transfer Protocol (HTTP) para sa pagpapadala ng hypermedia na mga dokumento, katulad ng HTML. Dinisenyo ito para sa komunikasyon sa pagitan ng mga web browser at web server, ngunit maaari rin itong gamitin sa iba pang mga bagay.
HTTPS	Ekstensiyon ng Hypertext Transfer Protocol ang Hypertext Transfer Protocol Secure. Ginagamit ito para sa seguradong komunikasyon sa isang computer network, at malawakang ginagamit sa internet, Sa HTTPS, naka-encrypt ang communication protocol gamit ang Transport Layer Security, o may dating bansag na Secure Sockets Layer.
IP	Isang numerikal tatak ang Internet Protocol address tulad ng 192.0.2.1 na konektado sa isang computer network na gumagami ng Internet Protocol para sa komunikasyon. Dalawa ang ginagampanang gamit ng IP address: pagkilala sa host o network interface at paghahanap ng address.
ISP	Tumutukoy sa isang kompanya na nagbibigay ng access sa internet para sa parehong personal at pangnegosyong mga costumer ang terminong Internet Service Provider (ISP).
Jailbreak	Sa mga Apple device na tumatakbo sa iOS na operating system, ang pagje-jailbreak ay isang pribilehiyadong pagpaparami na pinakikilos upang tanggalin ang mga restriksiyon sa software na itinakda ng manufacturer.
Malware	Ang malware ay kahit anong software na dinisenyo upang sadyang manira ng computer, server, client, o computer network.
Metadata	Ibinibigay ng data na metadata ang impormasyon tungkol sa ibang mga datos, ngunit hindi ang nilalaman nito, katulad ng teksto ng mensahe o ang mismong imahen.
Open-source software	Isang computer software ang open-source computer software na isinasapubliko sa ilalim ng isang awtorisasyon na kung saan ipinagkakaloob ng may-ari nito ang karapatan sa paggamit, pag-aaral, pagbabago, at pagbabahagi ng software at source code nito sa kahit sino at sa kahit anong dahilan. Maaaring linangin ang isang open-source software sa isang paraang kolaboratibo at pampubliko

OpenPGP	Isang bukas at libreng bersiyon ng Pretty Good Privacy (PGP) standard na tumutukoy sa mga format ng pag-eencrypt na nagpapahintulot sa kakayahang magmensahe nang pribado para sa email at iba pang message encryption.
OS	Pinangangasiwaan ng isang operating system (OS) ang hardware ng computer, software resources, at nagbibigay ito ng mga karaniwang serbisyo para sa mga computer program.
PGP	Isang encryption program ang Pretty Good Privacy (PGP) na nagbibigay ng cryptographic privacy at authentication para sa data communication.
Phishing	Isang uri ng social engineering ang phishing na kung saan ay magpapadala ang umaatake ng mapanlinlang na mensahe na nilikha upang linlangin ang isang tao sa pagpapabunyag nito ng kaniyang sensitibong impormasyon o mag-deploy ng malicious na software (katulad ng ransomware) sa impraestruktura ng biktima.
Root	Pinahihintulutan ng proseso ng pagru-root ang mga gumagamit ng Android mobile operating system na makakuha ng pribilehiyadong kontrol (kilala bilang root access) sa iba't ibang mga subsystem ng Android.
SFTP	Isang file transfer protocol na magpupuwersa sa isang set ng mga utility ang SFTP (Secure File Transfer Protocol) na nagbibigay ng access sa isang remote na computer na maghatid ng seguradong komunikasyon.
SMTP	Isang internet standard communication protocol ang Simple Mail Transfer Protocol para sa transmisyon ng elektronikong mail. Ginagamit ng mga mail server at iba pang mga ahente ng pagpapadala ng mensahe ang SMTP sa pagpapadala at pagtanggap ng mga mensaheng mail.
SSH	Isang cryptographic network protocol ang Secure Shell para sa seguradong pag-ooperate ng mga network service sa isang hindi seguradong network. Ang mga karaniwang aplikasyon niyo ay ang remote command-line, login, at remote na command execution, ngunit maseseguro rin ng SSH ang kahit anong network service.

SSL	Ang SSL (Secure Sockets Layer) at ang humalili rito na TLS (Transport Layer Security), ay mga protocol na naglulunsad ng awtentikado at naka-encrypt na mga ugnayan sa pagitan ng naka-network na mga computer
Startpage	Ang Startpage ay isang nakabaseng Olandes na kompanya ng search engine at itinatampok nito ang privacy bilang isang katangi-tanging feature.
TCP	Isa sa mga pangunihing mga protocol ng internet protocol suite ang Transmission Control Protocol. Nagumumula ito sa inisyal na network implementation na kung saan pinupunan nito ang Internet Protocol. Samakatuwid, ang buong suite ay karaniwan nang binabansagan bilang TCP/IP.
Tor	Tor, pinaigsing The Onion Router, ay isang libre at open-source na software na nagpapahintulot sa isang walang pangalang komunikasyon.
VPN	Pinalalawig ng isang virtual private network (VPN) ang isang pribadong network na nakapaloob sa isang pampublikong network at pinahihintulutan nito ang mga user na magpadata at makatanggap ng datos sa kabila ng isang nakabahagi o pampublikong mga network na para bang direktang nakakonekta sa isang private network ang kanilang mga computing device.
WebDAV	Karugtong ng WebDAV ang Hypertext Transfer Protocol at pinahihintulutan nito ang mga client na magsagawa ng mga operasyong remote Web content authoring.
WEP	Ang Wired Equivalent Privacy ay isang security algorithm para sa mga IEEE 802.11 wireless network.
WPA	Wi-Fi Protected Access, Wi-Fi Protected Access II, at Wi-Fi Protected Access 3 ay ang tatlong mga security at security certification program na ginawa ng Wi-Fi Alliance para sa seguridad ng mga wireless computer network.