EngageMedia

ডিজিটাল নিরাপত্তা প্রশিক্ষণ পাঠ্যক্রম

সংস্করণ ১.১.১

সর্বশেষ সংস্করণ: অক্টোবর ২০২১

এটি EngageMedia দ্বারা তৈরি একটি ডিজিটাল নিরাপত্তা প্রশিক্ষণ ম্যানুয়াল, Greater Internet Freedom (GIF) প্রকল্পের অধীনে অংশীজনদের চাহিদা এবং স্থানীয় প্রেক্ষাপট বিবেচনা করে ভয়েস কর্তৃক বাংলায় অনূদিত।

VOICE
VOICES FOR INTERACTIVE CHOICE & EMPOWERMENT

বাড়ি # ৬৭ (৫ম তলা), ব্লক-ক, পিসিকালচার হাউজিং সোসাইটি, শ্যামলী, ঢাকা-১২০৭
info@voicebd.org; www.voicebd.org, +৮৮-০২-৫৮১৫০৫৮৮

সূচি

১.০ ভূমিকা

১.১ পটভূমি এবং ব্যাপ্তি

গত কয়েক বছরে বিশ্বজুড়ে ইন্টারনেট ব্যবহারকারী সাংবাদিক, ডিজিটাল অধিকার কর্মী, শিক্ষক এবং প্রান্তিক জনগোষ্ঠীসহ অনেকেই ডিজিটাল ঝুঁকির সম্মুখীন হচ্ছেন। এই ধরনের ঝুঁকি প্রায়ই কর্তৃত্ববাদী শাসন থেকে আসে, যারা কঠোর ডিজিটাল নীতির জন্য চাপ সৃষ্টি করে এবং নাগরিকদের মত প্রকাশকে অপরাধের আওতায় গণ্য করে। ফলে নাগরিকের মৌলিক অধিকার ক্ষুন্ন হয়। যেমন সমাবেশের অধিকার, সংগঠন তৈরির অধিকার এবং অনলাইনে মতপ্রকাশের স্বাধীনতার অধিকার। অনেক দেশের সরকার তাদের নীতিগত অবস্থান থেকে ব্যাপক হারে নজরদারির জন্য নতুন নতুন প্রযুক্তি প্রয়োগ করে। ইন্টারনেটে নাগরিকদের অধিকার ও স্বাধীনতা এখন অনেকটাই হুমকির মুখে। Greater Internet Freedom প্রকল্প উপরোক্ত বিষয়গুলো বিবেচনা করে নেওয়া হয়েছে।

এই প্রশিক্ষণ ম্যানুয়াল Greater Internet Freedom (GIF)প্রকল্পের অংশ এবং তা ডিজিটাল প্রযুক্তির নিরাপত্তা বিষয়ে নাগরিক সংগঠন, এনজিও, সাংবাদিকদের দক্ষতা বৃদ্ধিতে সহায়ক হবে। এবং এই প্রশিক্ষণের ফলে অনেকেই ডিজিটাল নিরাপত্তা বিষয়ে দক্ষ হবে এবং স্থানীয় পর্যায়ে তারা এনজিওসহ মিডিয়াকে প্রশিক্ষণ দিতে পারবে।

প্রশিক্ষণে অংশগ্রহণকারীরা নিম্নোক্ত উপায়গুলোর সাহায্যে তাদের জ্ঞান বৃদ্ধি করতে সক্ষম হবে:

- ঝুঁকি মূল্যায়ন
- ডিজিটাল পরিচ্ছন্নতা
- ম্যালওয়্যার এবং সুরক্ষা
- ফ্রি এবং ওপেন সোর্স সফটওয়্যার (FOSS)
- ব্রাউজারের নিরাপত্তা এবং গোপনীয়তা
- পাসওয়ার্ড ব্যবস্থাপনা।
- ফাইল ও ফোল্ডার সুরক্ষা এবং ব্যাকআপ
- ডেটা এবং যোগাযোগ এনক্রিপশন
- পিজিপি এবং ইমেইল এনক্রিপশন
- ইন্টারনেট কীভাবে কাজ করে এবং ভিপিএন ও টর ব্যবহার করে কীভাবে নেটওয়ার্ক এনক্রিপশন করা হয়
- সোশ্যাল মিডিয়ায় গোপনীয়তা এবং নিরাপত্তা।
- মোবাইল ফোন ব্যবহারের সাথে সম্পৃক্ত ঝুঁকি এবং নিরাপদ যোগাযোগ সরঞ্জামের ব্যবহার।
- প্রশিক্ষণের পরিকল্পনা এবং প্রস্তুতি।

১.২ যোগাযোগের দৃষ্টিকোণ

এই প্রশিক্ষণ পাঠ্যক্রমটি পূর্ববর্তী প্রশিক্ষণের অভিজ্ঞতার উপর ভিত্তি করে প্রস্তুত করা হয়েছে। এটি সবসময় প্রশিক্ষণের জন্য উপযুক্ত নাও হতে পারে। প্রয়োজনে, প্রশিক্ষণ পাঠ্যক্রমের সহায়তার জন্য যোগাযোগ করুন।

দায়িত্ব	নাম	যোগাযোগ
প্রকল্প ব্যবস্থাপক	ভিনো লুসেরো	vino@engagemedia.org
ম্যানুয়্যাল প্রস্তুতকারী	মো: আশরাফুল হক	ashraf@engagemedia.org

১.৩ প্রশিক্ষণ ম্যানুয়্যাল তৈরি

EngageMedia এই প্রশিক্ষণ ম্যানুয়ালটি GIF প্রকল্পের অধীনে বিভিন্ন দেশের অংশীজনদের ডিজিটাল নিরাপত্তা প্রশিক্ষণের জন্য তৈরি করেছে। এই প্রশিক্ষন ম্যানুয়্যালটি ওপেন সোর্স, ক্রিয়েটিভ কমন্স BY-SA 4.0 এর অধীনে লাইসেন্সপ্রাপ্ত। অর্থাৎ আপনি যে কোনো উদ্দেশ্যে, এমনকি বাণিজ্যিকভাবে এটি ব্যবহার করতে পারবেন। যে কোনো উদ্দেশ্যে ডকুমেন্টটি শেয়ার এবং প্রয়োজনীয় পরিবর্তন করা যাবে। তবে EngageMedia, এবং ShareAlike কে উপযুক্ত ক্রেডিট দিতে হবে।

২.০ নির্দেশণামূলক বিশ্লেষণ

২.১ প্রয়োজন এবং দক্ষতা বিশ্লেষণ

প্রতিটি প্রশিক্ষণের আগে, অংশগ্রহণকারীদের চাহিদা এবং দক্ষতা নিরুপণ করা প্রয়োজন। প্রত্যেক অংশগ্রহণকারী বৈশিষ্ট্যে ভিন্নতা রয়েছে এবং আলাদা কাজের ক্ষেত্র রয়েছে, তাই তাদের ঝুঁকিও আলাদা। বিষয় এবং প্রশিক্ষণ পদ্ধতি নির্ধারণের জন্য প্রশিক্ষণে অংশগ্রহণকারীদের বিদ্যমান জ্ঞান সম্পর্কে জানা থাকা ভালো।

২.২ ম্যানুয়্যাল তৈরির পদ্ধতি

উপরোক্ত প্রসঙ্গের পরিপ্রেক্ষিতে, এই প্রশিক্ষণ পাঠ্যক্রমটি পুনরায় ডিজাইন করার প্রয়োজন হতে পারে। পাঠ্যক্রম উন্নয়নে সহায়তার জন্য EngageMedia- এর সাথে যোগাযোগ করার আগে চাহিদা এবং দক্ষতা বিশ্লেষণ করুন। জরিপের তথ্যের উপর ভিত্তি করে EngageMedia পরবর্তী সিদ্ধান্ত নেবে।

২.৩ সমস্যা এবং সুপারিশ

প্রশিক্ষণের আগে সম্ভাব্য ঝুঁকিগুলো শনাক্ত করে নিন। মূল্যায়নের উপর ভিত্তি করে অপ্রত্যাশিত কিছু বিষয় মোকাবেলার প্রস্তুতি নিয়ে রাখুন। সবসময় বিকল্প পরিকল্পনা প্রস্তুত রাখুন। প্রশিক্ষণের পরিকল্পনা গ্রহণের সময়, নিম্নোক্ত বিষয়গুলো বিবেচনা করুনঃ

- **কী ধরনের প্রশিক্ষণ কাকে করাবেন?** - অংশগ্রহণকারীদের প্রদত্ত তথ্যের ভিত্তিতে সেশনের পরিকল্পনা করা প্রয়োজন। সংশ্লিষ্ট অংশগ্রহণকারী ও বিষয় নির্বাচন করুন।
- **কে প্রশিক্ষণ করাবেন?** – বিষয় সম্পর্কে দক্ষ ও অভিজ্ঞ প্রশিক্ষক এই প্রশিক্ষণ করাবেন। প্রশিক্ষণের ফলাফল নির্ভর করবে প্রশিক্ষকের ওপর।
- **প্রশিক্ষণের উপকরণ ও উপযুক্ত পরিবেশ কে তৈরী করবেন?** – EngageMedia এই পাঠক্রমের নমুনা তৈরি করেছে, তবে প্রত্যেকটি প্রশিক্ষণের ক্ষেত্রে স্থানীয় প্রেক্ষাপট বিবেচনা করে প্রশিক্ষণ উপকরণ তৈরি করা প্রয়োজন।
- **বৈচিত্র্য** - প্রশিক্ষণে অংশ গ্রহণকারীরা বিভিন্ন সংগঠন থেকে অংশগ্রহণ করবে। তাদের বয়স, লিঙ্গ, বিশ্বাস, কাজের ক্ষেত্র ইত্যাদি আলাদা হতে পারে। বৈচিত্রপূর্ণ বিষয়গুলো প্রশিক্ষণ পরিচালনার ক্ষেত্রে মনে রাখা প্রয়োজন।
- **পরিবেশ** - প্রশিক্ষণ আয়োজনের পূর্বে স্থানীয় রাজনৈতিক ও সামাজিক পরিবেশ সম্পর্কে জানুন।

৩.০ নির্দেশনামূলক পদ্ধতি

৩.১ প্রশিক্ষণ পদ্ধতি

প্রতিটি প্রশিক্ষণের জন্য প্রশিক্ষণের পদ্ধতি সম্পূর্ণ প্রাসঙ্গিক। উল্লেখ্য, মানবাধিকার ইস্যুতে এডভোকেসি এবং দক্ষতা উন্নয়ন প্রশিক্ষণে ADIDS কার্যকরভাবে ব্যবহার করা হয়েছে। ডিজিটাল ও অনলাইন নিরাপত্তার জটিলতাগুলোকে আরও ভালভাবে বুঝতে প্রযুক্তিগত জ্ঞানসহ অংশগ্রহণকারীদের সাহায্য করার জন্য এই প্রশিক্ষণ ম্যানুয়্যালটি কার্যকর হবে। পাঠপরিকল্পনা তৈরির সময় প্রশিক্ষকদের জন্য এটি কাজে দিবে।

ADIDS হল একটি প্রশিক্ষণ পদ্ধতি যার অর্থ দাঁড়ায়: Activity-Discussion-Input-Deepning-Synthesis. বিস্তারিত: https://level-up.cc/before-an-event/preparing-sessions-using-adids/

৩.২ পরীক্ষা এবং মূল্যায়ন

একটি প্রশিক্ষণ পরিচালনা করার জন্য একাধিক পরীক্ষা এবং মূল্যায়ন করা প্রয়োজন। যেমন:

- **প্রশিক্ষণের পূর্বে** - অংশগ্রহণকারীদের বিদ্যমান জ্ঞান সম্পর্কে যাচাই ও প্রশিক্ষণের সেশন সাজানোর জন্য প্রাক-প্রশিক্ষণ প্রয়োজনীয়। এক্ষেত্রে অংশগ্রহনকারীরা তাদের কাজ ও প্রশিক্ষণের বিষয় সম্পর্কে কিছু প্রশ্ন করা যেতে পারে।
- **প্রশিক্ষণ চলাকালীন** - পরবর্তী সেশন আরো ভালো করার জন্য অংশগ্রহণকারীদের কাছ থেকে প্রতিটি অধিবেশনের মূল্যায়ন সংগ্রহ করুন।
- **প্রশিক্ষণোত্তর সময়** - প্রশিক্ষণ শেষে অংশগ্রহণকারীদের কাছ থেকে প্রশিক্ষণের মূল্যায়ন সংগ্রহ করুন।

৪.০ প্রশিক্ষণ তথ্যাদি

৪.১ প্রস্তাবিত তথ্যাদি

এখানে প্রশিক্ষণের জন্য কিছু প্রস্তাবিত তথ্য/সোর্স লিঙ্ক রয়েছে।

- https://level-up.cc/
- https://ssd.eff.org/
- https://securityinabox.org/en/
- https://holistic-security.tacticaltech.org/
- https://digitalfirstaid.org/en/index.html
- https://gijn.org/digital-security/
- https://gcatoolkit.org/journalists/
- https://secfirst.org/
- https://www.frontlinedefenders.org/en/digital-security-resources

৪.২ সফটওয়্যার, এ্যাপস, টুলস এবং প্ল্যাটফর্ম

- https://duckduckgo.com/ গুগলের বিকল্প সার্চ ইঞ্জিন
- https://www.malwarebytes.com/ ম্যালওয়্যার অপসারণ সরঞ্জাম
- https://www.avira.com/ ফ্রি এন্টিভাইরাস
- https://www.avast.com/ ফ্রি এন্টিভাইরাস
- https://virustotal.com/ অনলাইন ম্যালওয়্যার স্ক্যানার
- https://brave.com/ ওপেন সোর্স ব্রাউজার
- https://www.mozilla.org/en-US/firefox/new/ ওপেনসোর্স ব্রাউজার
- https://www.eff.org/https-everywhere যেখানে HTTPS ব্রাউজারের জন্য পুর্ননির্দেশ প্রদান করে
- https://adblockplus.org/ ব্রাউজারের জন্য বিজ্ঞাপন এবং ট্র্যাকার অপসারণ এক্সটেনশন
- https://keepassxc.org/ ওপেনসোর্স পাসওয়ার্ড ম্যানেজার
- https://authy.com/ 2FA এপ এবং গাইড
- https://youtu.be/F7pYHN9iC9I সামাজিক যোগাযোগ মাধ্যমের সচেতনতার জন্য ভিডিও
- https://aesencryption.net/ অনলাইন টেক্সট এনক্রিপশন প্ল্যাটফর্ম
- https://aescrypt.com/ পাসওয়ার্ড দিয়ে ফাইল এনক্রিপ্ট করার ছোট টুলস
- https://torproject.org/ টরের অফিসিয়াল সাইট
- https://www.tunnelbear.com/ পেইড ভিপিএন
- https://www.psiphon3.com/ ফ্রি ভিপিএন
- https://veracrypt.fr/ ফাইল ফোল্ডার এনক্রিপশন টুল
- https://www.bleachbit.org/ স্থায়ী ফাইল এবং ফোল্ডার অপসারণ টুল।
- https://ccleaner.com/recuva মুছে ফেলা ফাইল রিকভারি টুল
- http://exif.regex.info/ মেটা ডেটা যাচাই প্ল্যাটফর্ম
- https://duplicati.com/ এনক্রিপ্ট করা ব্যাকআপ তৈরির টুল
- https://www.openpgp.org/ ইমেইল এনক্রিপশন
- https://mailvelope.com/ ইমেইল এনক্রিপশন ব্রাউজার এক্সটেনশন
- https://www.thunderbird.net/ ইমেইল ক্লায়েন্ট
- https://signal.org/ নিরাপদ যোগাযোগ এপ
- https://wire.com/ নিরাপদ যোগাযোগ এপ
- https://briarproject.org/ অফলাইন নিরাপদ যোগাযোগের জন্য মোবাইল এ্যাপ

৫.০ প্রশিক্ষণ পাঠ্যক্রম

সেশন -০১: ব্যক্তিগত পরিচিতি এবং প্রাক-প্রশিক্ষণ পরীক্ষা

সেশনের কাঙ্ক্ষিত ফলাফল	**অংশগ্রহণকারী এবং প্রশিক্ষক একে অপরকে জানতে পারবেন। অংশগ্রহণকারীদের প্রাক প্রশিক্ষণ অবস্থা বোঝা যাবে।**

সেশনের ধরণ:

- ভূমিকা এবং কার্যক্রম।

বিষয়	বর্ণনা
শিখনের উদ্দেশ্য	১ এই প্রশিক্ষণ সম্পর্কে ধারণা পাবে ২ একে অপরের সম্পর্কে জানতে পারবে ৩ কিভাবে একটি প্রাক-প্রশিক্ষণ পরীক্ষা নেয়া যায় সেই সম্পর্কে জানতে পারবে ৪ প্রশিক্ষণে শুরুর সেশন সম্পর্কে ধারণা পাবে এবং পরবর্তী প্রশিক্ষণে ব্যবহার করতে পারবে
অতিরিক্ত তথ্য	• https://internews.org/ • https://engagemedia.org/
সেশন গাইড	• প্রশিক্ষণ সম্পর্কে পরিচিতিমূলক বক্তব্য। • পরিচিতির জন্য অংশগ্রহণকারীদের সুযোগ করে দিন। • প্রশিক্ষণের নিয়মকানুন সম্পর্কে জানান এবং উপযুক্ত পরিবেশ তৈরী করুন। • অনলাইন জরিপ ফর্মের মাধ্যমে প্রাক-প্রশিক্ষণ পরীক্ষা নিন। • অংশগ্রহণকারীদের কাজের ক্ষেত্রের সাথে সম্পর্কিত প্রশ্ন করুন।

অধিবেশনের সার সংক্ষেপ
N/A

সেশন -০২: ডিজিটাল নিরাপত্তার ভূমিকা

সেশনের কাঙ্ক্ষিত ফলাফল	**ডিজিটাল নিরাপত্তা কী এবং কেন এটি গুরুত্বপূর্ণ সে সম্পর্কে অংশগ্রহণকারীরা জানতে পারবেন। এছাড়াও FOSS সম্পর্কে জানবেন।**

সেশনের ধরন:
Activity-Discussion-Input-Deepning-Synthesis.

বিষয়	বর্ণনা
শিক্ষার উদ্দেশ্য	১ সামগ্রিক নিরাপত্তা কি? ২ ব্যাক্তি নিরাপত্তার গুরুত্ব। ৩ কেন এটি আমাদের জন্য প্রাসঙ্গিক। ৪ FOSS সম্পর্কে জানুন (ওপেন সোর্স সফটওয়্যার) ।
অতিরিক্ত তথ্য	https://holistic-security.tacticaltech.org/ https://youtu.be/F7pYHN9iC9I
সেশন গাইড	• ডিজিটাল নিরাপত্তা সম্পর্কে একটি ছোট ভিডিও দেখান। • সামগ্রিক নিরাপত্তা কী এবং কেন আমাদের জন্য নিজ নিরাপত্তা গুরুত্বপূর্ণ সে সম্পর্কে আলোচনা করুন। • অংশগ্রহণকারীরা এই বিষয়ে তাদের চিন্তাভাবনা শেয়ার করবে। • FOSS সম্পর্কে বলুন।

অধিবেশনের সারসংক্ষেপ

ডিজিটাল নিরাপত্তা অনলাইন পরিচয়, ডেটা এবং অন্যান্য সম্পদের সুরক্ষার জন্য সামগ্রিক যার মধ্যে রয়েছে ওয়েব পরিষেবা, এন্টিভাইরাস সফটওয়্যার, স্মার্টফোন সিম কার্ড, বায়োমেট্রিক্স এবং সুরক্ষিত ব্যক্তিগত ডিভাইস।

সংক্ষেপে ডিজিটাল নিরাপত্তা মানে কম্পিউটার, মোবাইল ডিভাইস, ট্যাবলেট এবং অন্য যে কোনো ইন্টারনেট-সংযুক্ত ডিভাইসকে অনুপ্রবেশকারীদের (Hackers) হাত থেকে রক্ষা করা, যা হ্যাকিং, ফিশিং এবং আরও অনেক কিছু হতে পারে। ডিজিটাল নিরাপত্তা কোম্পানির দ্বারা ব্যক্তিগত ডেটা ব্যবহার এবং বিক্রি থেকে রক্ষা করার জন্য ব্যবহার করা যেতে পারে।

সাইবার সিকিউরিটি খুবই গুরুত্বপূর্ণ, কারণ এটি সকল ধরনের তথ্য চুরি এবং ক্ষতি থেকে রক্ষা করে। এর মধ্যে রয়েছে সংবেদনশীল তথ্য, ব্যক্তিগতভাবে শনাক্তযোগ্য তথ্য (Personally Identifiable Information), সুরক্ষিত স্বাস্থ্য তথ্য (Protected Health Information), ব্যক্তিগত তথ্য, বুদ্ধিবৃত্তিক সম্পদ (Intellectual Property), বিস্তৃত এবং গুরুত্বপূর্ণ সরকারি তথ্য কাঠামো। যদি ডিজিটাল নিরাপত্তা দুর্বল হয় তাহলে সকল ধরণের ব্যক্তিগত তথ্য যেমন- ক্রেডিট কার্ড, ব্যাংক একাউন্ট, ইমেইল একাউন্ট ইত্যাদি মারাত্মক ঝুঁকিতে পড়তে পারে।

সামগ্রিক নিরাপত্তা হল ব্যক্তি এবং প্রতিষ্ঠানের ডিজিটাল, শারীরিক এবং মানসিক-সামাজিক নিরাপত্তার একটি সমন্বিত পদ্ধতি। এই সামগ্রিক পদ্ধতির উদ্দেশ্য হলো ইন্টারনেট ব্যবহারকারী ও মানবাধিকার কর্মীদের নিরাপত্তা প্রদান, যার মধ্যে রয়েছে:

- সহিংসতার প্রতিবাদ এবং প্রতিরোধে পরিচালিত কার্যক্রমকে শক্তিশালী করা।
- নিরাপত্তা ও সুরক্ষার জন্য প্রতিরোধমূলক ব্যবস্থা গ্রহণ করে ইন্টারনেট ব্যবহারকারিদের সক্ষমতাকে বৃদ্ধি করা।
- নিরাপত্তা জনিত 'সংকট' মোকাবেলায় প্রতিরোধ করার সক্ষমতাকে বৃদ্ধি করা।

FOSS: ইন্টারনেট ব্যবহারের ক্ষেত্রে ওপেন সোর্স সুবিধাজনক এবং শক্তিশালী নিরাপত্তা প্রদান করে। ওপেন-সোর্স একটি কম্পিউটার সফটওয়্যার যা সুনির্দষ্ট লাইসেন্সের অধীনে ব্যবহৃত এবং কপিরাইট হোল্ডার সফটওয়্যার ব্যবহারকারীদের এই সফটওয়্যার ব্যবহারের অনুমতি দেয় এবং এই সোর্সকোড অন্য ব্যবহারকারীদের যে কোন উদ্দেশে সরবরাহ করতে পারে। ওপেন সোর্স সফটওয়্যারটি একে অপরের সহযোগিতামূলক পদ্ধতিতে তৈরি হতে পারে।

সেশন -০৩: থ্রেট মডেলিং

সেশনের কাঙ্ক্ষিত ফলাফল	অংশগ্রহণকারীরা ঝুঁকিগুলি চিহ্নিত করতে পারবেন।

সেশনের ধরণ:
Activity-Discussion-Input-Deepning-Synthesis.

বিষয়	বর্ণনা
শিক্ষার উদ্দেশ্য	১ থ্রেট মডেলিং সম্পর্কে জানতে পারবেন। ২ ব্যক্তিগত ও সাংগঠনিক ঝুঁকি মূল্যায়ন করার উপায় সম্পর্কে জানতে পারবেন।
অতিরিক্ত তথ্য	• https://ssd.eff.org/en/module/your-security-plan
সেশন গাইড	• প্রশিক্ষক থ্রেট মডেলিং ফ্লোচার্ট উপস্থাপন করবেন এবং ধাপে ধাপে এর প্রক্রিয়া নিয়ে আলোচনা করবেন। • উদাহরণস্বরুপ প্রশিক্ষক প্রাতিষ্ঠানিক এবং ব্যক্তিগত ঝুঁকি উপস্থাপন করবেন। • অংশগ্রহণকারীদের মডেলের মধ্যে উল্লেখিত ঝুঁকি মূল্যায়ন করতে বলা হবে। • যদি অংশগ্রহণকারীরা কোন ভুল করে থাকে সেসব সম্পর্কে প্রশিক্ষক আলোচনা করবেন।

অধিবেশনের সার সংক্ষেপ

নিজস্ব নিরাপত্তা এমন একটি প্রক্রিয়া যেখানে সুচিন্তিত একটি পরিকল্পনার মাধ্যমে, আপনি আপনার জন্য সঠিক একটি পরিকল্পনা তৈরি করতে পারেন। নিরাপত্তা কেবল ব্যবহৃত সরঞ্জাম বা ডাউনলোডকৃত সফটওয়্যার সম্পর্কে নয় বরং এটি অন্যান্য ইন্টারনেট বিরজমান হুমকি এবং কীভাবে সেসব হুমকি মোকাবেলা করা যায় সে সম্পর্কে জানতে সাহায্য করবে।

- আমি কি কি সুরক্ষিত করতে চাই?
- কার থেকে আমি সুরক্ষিত করতে চাই?
- যদি আমি ব্যর্থ হই তার ফল কতোটা খারাপ হবে?
- কেন আমাকে রক্ষা করতে হবে?
- সম্ভাব্য হুমকি প্রতিরোধের জন্য আমি কতটা অসুবিধার মুখোমুখি হতে রাজি?

সেশন -০৪: ডিজিটাল পরিচ্ছন্নতা সম্পর্কে সচেতনতা ও প্রস্তুতি

সেশনের কাঙ্ক্ষিত ফলাফল	**অংশগ্রহণকারীরা সচেতন হবেন এবং ডিজিটাল পরিচ্ছন্নতা সম্পর্কে নিজেদের প্রস্তুত করবেন।**

সেশনের ধরণ:
Activity-Discussion-Input-Deepning-Synthesis.

বিষয়	বর্ণনা
শিক্ষার উদ্দেশ্য	১ ডিজিটাল নিরাপত্তা সম্পর্কে মৌলিক সচেতনতা অর্জন করতে পারবেন। ২ ডিজিটাল পরিচ্ছন্নতা অনুশীলন সম্পর্কে জানতে পারবেন।
অতিরিক্ত তথ্য	• https://coconet.social/digital-hygiene-safety-security/
সেশন গাইড	• প্রশিক্ষক ডিজিটাল সুরক্ষার জন্য প্রাথমিক সচেতনতাসহ হার্ডওয়্যার এবং সফটওয়্যার, কি করা যাবে এবং কি করা যাবে না, আচরণগত পরিবর্তন ইত্যাদি নিয়ে আলোচনা করবেন। • অংশগ্রহণকারীদের তাদের বর্তমান অনুশীলন সম্পর্কে আলোচনা করতে বলা হবে। • অংশগ্রহণকারীদের মতামতের উপর ভিত্তি করে প্রশিক্ষক বিস্তারিত আলোচনা করবেন।

অধিবেশনের সারসংক্ষেপ

- কারো সাথে আর্থিক তথ্য শেয়ার করবেন না।
- ইমেইল খোলার সময়, প্রেরকের বিস্তারিত বিবরণ অবশ্যই যাচাই করে নিবেন।
- উদ্দেশ্য নিশ্চিত হওয়ার আগে কোন লিঙ্কে ক্লিক করবেন না।
- এ্যাটাচমেন্ট বিপজ্জনক হতে পারে, তাই খোলার আগে এন্টিভাইরাস দিয়ে স্ক্যান করে নিন।
- সবসময় মূল (অফিসিয়াল) ওয়েবসাইট থেকে সফটওয়্যার ডাউনলোড করবেন।
- ওপেন সোর্স সফটওয়্যারকে অগ্রাধিকার দিন।
- অনলাইন এবং অফলাইন অভ্যাসে পরিবর্তন করুন।
- কম্পিউটার বন্ধ করার আগে সমস্ত একাউন্ট থেকে সাইন আউট/ লগ আউট করুন।
- সব সময় সতর্ক থাকুন। কোথায় ক্লিক করছেন তা আগে জেনে নিন। ক্লিক করার আগে চিন্তা করুন।
- অন্য কারো কম্পিউটার বা মোবাইলে আপনার একাউন্ট খুলবেন না এবং ব্যবহার করবেন না।
- কারো কাছে আপনার ডিভাইস ধার দিবেন না। অন্যদের আপনার ডিভাইসটি ধার দেওয়ার ক্ষেত্রে বিশেষভাবে সতর্ক থাকুন।
- আপনার ডিভাইস নিয়মিত আপডেট করুন।
- যদি ভিপিএন বা টর ব্যবহার না করেন তবে, ডিভাইস সুরক্ষিত রাখার জন্য হোটেল, সাইবার ক্যাফে বা পাবলিক নেটওয়ার্ক ব্যবহার করবেন না। যদি আপনার অন্যের কম্পিউটার ব্যবহার করার প্রয়োজন হয়, তাহলে নিরাপদ এবং পোর্টেবল OS (অপারেটিং সিস্টেম) ব্যবহার করুন।
- আপনি অনলাইনে কি প্রকাশ করছেন সে সম্পর্কে সচেতন থাকুন।
- শুধুমাত্র প্রয়োজনীয় ব্যক্তিগত তথ্য সাথে রাখুন।
- ছদ্মনাম ব্যবহার করুন এবং গোপনীয়তা বজায় রাখুন।
- তথ্য বিনিময় করতে এনক্রিপশন ব্যবহার করুন।
- ডিজিটাল নিরাপত্তা কেবল ব্যক্তিগত বিষয় নয়, অন্যকেও জানাতে চেষ্টা করুন।

সেশন -০৫: ম্যালওয়্যার, এন্টিভাইরাস এবং ম্যালওয়্যার অপসারণ সরঞ্জাম

সেশনের কাঙ্ক্ষিত ফলাফল	**অংশগ্রহণকারীরা এন্টিভাইরাসের গুরুত্ব এবং ম্যালওয়্যারের প্রকারভেদ সম্পর্কে জানতে পারবেন।**

সেশনের ধরণ:
Activity-Discussion-Input-Deepning-Synthesis.

বিষয়	বর্ণনা
শিক্ষার উদ্দেশ্য	১ ইন্টারনেট এবং দৈনন্দিন ডিভাইসে বিপদ। ২ ম্যালওয়্যারের প্রকারভেদ ৩ এন্টিভাইরাস এর গুরুত্ব ৪ পেইড এবং নন-পেইড এন্টিভাইরাসের মধ্যে পার্থক্য ৫ ম্যালওয়্যার অপসারণ টুলস এবং পদ্ধতি
অতিরিক্ত তথ্য	• https://www.malwarebytes.com/ ম্যালওয়্যার অপসারণ ট্যুলস • https://www.avira.com/ ফ্রি/পেইড এন্টিভাইরাস • https://www.avast.com/ ফ্রি/পেইড এন্টিভাইরাস • https://virustotal.com/ অনলাইন ম্যালওয়্যার স্ক্যানার • https://level-up.cc/curriculum/ ম্যালওয়্যার-সুরক্ষা
সেশন গাইড	• প্রশিক্ষক অনলাইন এবং দৈনন্দিন ডিভাইসে যে সকল হুমকি রয়ছে, সে সম্পর্কে আলোচনা করবেন। • প্রশিক্ষক ম্যালওয়ারের প্রকারভেদ সম্পর্কে আলোচনা করবেন। • অংশগ্রহণকারীদের ম্যালওয়্যার এবং বিভিন্ন পদক্ষেপ সম্পর্কে অভিজ্ঞতা শেয়ার করতে বলা হবে। • এন্টিভাইরাসের গুরুত্ব আলোচনা করা হবে, পেইড এবং নন-পেইড এন্টিভাইরাসের মধ্যে পার্থক্যউপস্থাপন করা হবে। • অংশগ্রহণকারীদের ম্যালওয়্যার অপসারণ সম্পর্কে পরিচয় করিয়ে দেওয়া হবে এবং সেশন চলাকালীন ম্যালওয়্যার স্ক্যান করতে বলা হবে।

অধিবেশনের সারসংক্ষেপ

- ফাইলের নামের শেষ অংশটি লক্ষ্য করুন (এক্সটেনশন)।
- শুধু ফাইল আইকন দেখে সিদ্ধান্ত নেবেন না।
- যদি ফাইল এক্সটেনশন গোপন থাকে, তাহলে তা চালু করুন।
- বেশিরভাগ ক্ষেত্রে, আপনার কম্পিউটার বহিরাগত ডিভাইস সংযুক্ত করে সংক্রমিত হয়।
    - কম্পিউটারের অপারেটিং সিস্টেম আপডেট রাখুন।
    - কম্পিউটারে অটোরান অপশন নিষ্ক্রিয় করুন।
    - এক্সটার্নাল ডিভাইস খোলার আগে এন্টিভাইরাস ব্যবহার করুন এবং সঠিকভাবে স্ক্যান করুন।
- কোন অবিশ্বস্ত (Not Trusted) মাধ্যমের সফটওয়্যার ব্যবহার করবেন না। এটি নিজেই ম্যালওয়্যার বহন করতে পারে।
- সম্ভব হলে এন্টিভাইরাস কিনুন অথবা ফ্রী ভার্সন ব্যবহার করুন। পৃষ্ঠা নং XX এ প্রস্তাবিত তালিকা দেখুন।
- এন্টিভাইরাস ডাটাবেস নিয়মিত আপডেট রাখুন।
- ম্যালওয়্যার অপসারন করার টুল সংক্রামিত ফাইল/ সিস্টেমকে ঠিক করতে পারে। তবে এটি কোনভাবেই একটি এন্টিভাইরাসের বিকল্প নয়।
- বেশিরভাগ এন্টিভাইরাস কোম্পানি বিভিন্ন ধরণের বিনামূল্যে ম্যালওয়্যার অপসারণ সরবরাহ করে।
- ম্যালওয়্যার বা ফিশিং লিঙ্ক থেকে নিরাপদ থাকার জন্য, যেকোন ফাইল, লিংক বা লগইন পৃষ্ঠা খোলার আগে স্ক্যান করুন।

সেশন -০৬: ব্রাউজার এবং এর নিরাপত্তা

সেশনের কাঙ্ক্ষিত ফলাফল	**অংশগ্রহণকারীরা ওয়েব ব্রাউজারের নিরাপত্তা এবং গোপনীয়তা সম্পর্কে জানতে পারবেন।**

সেশনের ধরণ:
Activity-Discussion-Input-Deepning-Synthesis.

বিষয়	বর্ণনা
শিক্ষার উদ্দেশ্য	১ সঠিক ব্রাউজার বেছে নিতে শিখুন। ২ ব্রাউজারের নিরাপত্তা সেটিংস এবং এক্সটেনশন ব্যবহার করে ব্রাউজারে গোপনীয়তা সম্পর্কে জানুন। ৩ HTTP এবং HTTPS এর মধ্যে পার্থক্য শিখুন। ৪ ফিশিং এবং ভূয়া লিঙ্কগুলি সনাক্ত করতে শিখুন। ৫ গুগলের পরিবর্তে DuckDuckGo বা StartPage বা Quant কে সার্চ ইঞ্জিন হিসেবে ব্যবহার করুন।
অতিরিক্ত তথ্য	• https://brave.com/ ওপেনসোর্স ব্রাউজার • https://www.mozilla.org/ ওপেনসোর্স ব্রাউজার • https://www.eff.org/https-everywhere ব্রাউজারের জন্য HTTPS পুন-নির্দেশ এক্সটেনশন • https://duckduckgo.com/ গুগলের বিকল্প সার্চ ইঞ্জিন • https://adblockplus.org/ ব্রাউজারের জন্য বিজ্ঞাপন এবং ট্র্যাকার অপসারণ এক্সটেনশন • https://level-up.cc/curriculum/safer-browsing/
সেশন গাইড	• প্রশিক্ষক কয়েকটি ওপেনসোর্স ওয়েব ব্রাউজার সম্পর্কে আলোচনা করবেন এবং সেগুলি ব্যবহার করতে উৎসাহিত করবেন। • এই সময়ে প্রশিক্ষক ব্রাউজার নিরাপত্তা এবং গোপনীয়তা সেটিংস সম্পর্কে আলোচনা করবেন। • HTTPS এবং SSL এর গুরুত্ব আলোচনা করবেন। • DuckDuckgo, StartPageএবং Quant অংশগ্রহণকারীদের নিকট পরিচয় করাবেন। • প্রশিক্ষক ইন্টারনেটে স্ক্যাম, ফিশিং এবং ভূয়া লিঙ্ক সম্পর্কে আলোচনা করবেন।

অধিবেশনের সারসংক্ষেপ

- ওপেনসোর্স ওয়েব ব্রাউজার ব্যবহার করুন যেমন, Brave, Firefox or Chromium
- ব্রাউজারে কখনোই আপনার পাসওয়ার্ড সেভ করবেন না।
- বিশ্বস্ত নয় এমন ‘এডঅন’ ইনস্টল করবেন না।
- ব্রাউজারের হিস্টোরি বন্ধ রাখুন এবং আপনার ব্রাউজারের ক্যাশ (cache)এবং কুকিজ নিয়মিত পরিষ্কার করুন। বিকল্পভাবে, প্রাইভেট ব্রাউজার (incognito mode) ব্যবহার করতে পারেন কিন্তু মনে রাখবেন যে এটি টর-এর মতো আপনার গোপনীয়তা বজায় রাখবে না।
- প্রয়োজন না হলে জাভা এবং ফ্ল্যাশ নিষ্ক্রিয় করুন।
- অনুসন্ধানের গোপনীয়তার জন্য DuckDuckGo, StartPageবা Quant ব্যবহার করুন।
- এমন কোন সাইটে লগইন করবেন না যেখানে HTTPS নেই। অনলাইন লেনদেনের সময় সতর্ক থাকুন।
- HTTP- এর থেকে ওয়েব URL-এর HTTPS ভার্সন বেশি নিরাপদ।
- ফেক লগইন পৃষ্ঠাগুলি দেখতে ঠিক একই রকম হতে পারে। প্রথম স্ল্যাশের(/)আগের অংশটি লক্ষ্য করুন ।

সেশন -০৭: পাসওয়ার্ড, পাসওয়ার্ড ম্যানেজার এবং টু ফ্যাক্টর অথেনটিকেশান (2FA)

সেশনের কাঙ্ক্ষিত ফলাফল	**অংশগ্রহণকারীরা সঠিক পাসওয়ার্ড তৈরি করতে শিখবে এবং নিরাপদ পাসওয়ার্ড ম্যানেজারের মাধ্যমে পাসওয়ার্ড পরিচালনা করতে পারবে। এছাড়াও Two Factor Authentications ব্যবহার করতে শিখবে।**

সেশনের ধরন:
Activity-Discussion-Input-Deepning-Synthesis.

বিষয়	বর্ণনা
শিক্ষার উদ্দেশ্য	১ শক্তিশালী এবং ইউনিক পাসওয়ার্ডের গুরুত্ব। ২ কিভাবে একটি ভালো পাসওয়ার্ড তৈরি করবেন। ৩ পাসওয়ার্ড নিরাপত্তা। ৪ পাসওয়ার্ড ম্যানেজারের পরিচিতি। ৫ Two Factor Authentications এর ভূমিকা।
অতিরিক্ত তথ্য	• https://keepassxc.org/ ওপেনসোর্স পাসওয়ার্ড ম্যানেজার • https://authy.com/ 2FA অ্যাপ এবং গাইড • https://ssd.eff.org/en/module/creating-strong-passwords
সেশন গাইড	• প্রশিক্ষক শক্তিশালী পাসওয়ার্ডের গুরুত্ব সম্পর্কে আলোচনা করবেন এবং কীভাবে একটি ভাল পাসওয়ার্ড তৈরি করবেন তা শেখাবেন। • পাসওয়ার্ড ব্যবহারের সময় কোন নিরাপত্তা ব্যবস্থা গ্রহণ করা উচিত সে বিষয়ে সংক্ষিপ্ত আলোচনা করবেন। • Keepass (একটি ওপেনসোর্স পাসওয়ার্ড ম্যানেজার) সম্পর্কে ধারণা প্রদান করা হবে এবং প্রশিক্ষক ধাপে ধাপে এর সম্পর্কে বিস্তারিত আলোচনা করবেন। • Two Factor Authentications কী, কেন এটি গুরুত্বপূর্ণ এবং কীভাবে কাজে লাগানো যায় তা নিয়ে আলোচনা করবেন।

অধিবেশনের সারসংক্ষেপ

- পাসওয়ার্ড হচ্ছে সমস্ত তথ্যের মূল চাবিকাঠি এবং ডিজিটাল নিরাপত্তার গুরুত্বপূর্ণ অংশ।
- দৈর্ঘ্য- কমপক্ষে ১৪ অক্ষরের একটি পাসওয়ার্ড ব্যবহার করুন।
- মিশ্রন- পাসওয়ার্ডে সংখ্যা, চিহ্ন, বড় হাতের এবং ছোট হাতের অক্ষর এবং সম্ভব হলে স্পেস ব্যবহার করুন।
- এলোমেলো- সব ক্ষেত্রে একই রকম কাঠামো ব্যবহার করবেন না এবং অভিধানে থাকা শব্দগুলি এড়িয়ে চলুন।
- সম্পর্ক- ব্যক্তিগত তথ্য এড়িয়ে চলুন।
- মনে রাখবেন– এমন একটি পাসওয়ার্ড ব্যবহার করুন যা আপনি মনে রাখতে পারেন।
- গোপনীয়তা- পাসওয়ার্ড গোপন রাখুন, এটি কারও সাথে শেয়ার করবেন না।
- সংরক্ষণ করুন- কাগজে বা ফাইলে লিখবেন না।
- অনন্য- একই পাসওয়ার্ড অন্য কোথাও ব্যবহার করবেন না।
- যদি সম্ভব হয়, আপনার ডিভাইসে একটি নিরাপত্তা স্ক্রিন যুক্ত করুন। যা আশেপাশের লোকজনকে আপনার ডিভাইসের স্ক্রিন দেখতে বাধা দেয়।
- পাসওয়ার্ড দেওয়ার সময় নিশ্চিত হয়ে নিন যে আপনার আশেপাশে কেউ বসে নেই বা লক্ষ্য করছে না।
- এটিএম বুথে পিন দেয়ার সময় উপরের দিকে ঢেকে রেখে পিন দিন যেনো এটি সিসি ক্যামেরায় বুঝা না যায়।
- আশেপাশে কোন ক্যামেরা বা আয়না নেই তা নিশ্চিত করুন।
- নিজস্ব কোন পাসওয়ার্ড কখনোই অন্যের ব্যবহৃত ডিভাইসে অন্তর্ভুক্ত করবেন না।
- প্রতিটি পাসওয়ার্ডের জন্য পুনরুদ্ধার প্রক্রিয়া জেনে নিন।
- কোথাও লগ ইন করার সময়, HTTPS প্রোটোকল ব্যবহার নিশ্চিত এবং SSL সার্টিফিকেটের বৈধতা যাচাই করুন।
- সম্ভব হলে নন-এসএমএস/কল ভিত্তিক Two Factor Authentications একটিভ করুন। ওপেন সোর্স এপ বা হার্ডওয়্যার ভিত্তিক Two Factor Authentications ব্যবহার করুন।
- একটি পাসওয়ার্ড ম্যানেজার ব্যবহার করুন যা ওপেনসোর্স এবং ডাটাবেস এনক্রিপ্ট করে রাখে।

সেশন -০৮: সোশ্যাল মিডিয়ায় নিরাপত্তা এবং গোপনীয়তা সেটিংস

সেশনের কাঙ্ক্ষিত ফলাফল	**অংশগ্রহণকারীরা সামাজিক যোগাযোগ মাধ্যমে নিরাপত্তা সম্পর্কে এবং গোপনীয়তা কিভাবে বজায় রাখতে হয় তা জানতে পারবেন।**

সেশনের ধরন:
Activity-Discussion-Input-Deepning-Synthesis.

বিষয়	বর্ণনা
শিক্ষার উদ্দেশ্য	১ সামাজিক যোগাযোগ মাধ্যমের ঝুঁকি এবং সতর্কতা। ২ সামাজিক প্রকৌশল (Social engineering) কি? ৩ সামাজিক নেটওয়ার্ক সাইটে নিরাপত্তা এবং গোপনীয়তা।
অতিরিক্ত তথ্য	• https://youtu.be/F7pYHN9iC9I সামাজিক যোগাযোগ মাধ্যমের সচেতনতার জন্য ভিডিও • 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
সেশন গাইড	• প্রশিক্ষক শক্তিশালী পাসওয়ার্ডের গুরুত্ব সম্পর্কে আলোচনা করবেন এবং কীভাবে একটি ভাল পাসওয়ার্ড তৈরি করবেন তা শেখাবেন। • পাসওয়ার্ড ব্যবহারের সময় কোন নিরাপত্তা ব্যবস্থা গ্রহণ করা উচিত সে বিষয়ে সংক্ষিপ্ত আলোচনা করবেন। • Keepass (একটি ওপেনসোর্স পাসওয়ার্ড ম্যানেজার) সম্পর্কে ধারণা প্রদান করা হবে এবং প্রশিক্ষক ধাপে ধাপে এর সম্পর্কে বিস্তারিত আলোচনা করবেন। • Two Factor Authentications কী, কেন এটি গুরুত্বপূর্ণ এবং কীভাবে কাজে লাগানো যায় তা নিয়ে আলোচনা করবেন।

অধিবেশনের সারসংক্ষেপ

- যেসব ঝুঁকি সম্পর্কে সচেতন হতে হবে তা হল:
  - সাইবার বুলিইং (ডিজিটাল প্রযুক্তি ব্যবহার করে হয়রানি)
  - তথ্য এবং পরিচয় চুরি।
  - গোপনীয়তায় হস্তক্ষেপ।
  - শিশু-কিশোরদের মাঝে আপত্তিকর ছবি এবং বার্তা।
  - অপরিচিতদের উপস্থিতি যারা অন্য সদস্যদের 'হীন' করতে পারে।

Social engineering এর আক্রমণ যেখানেমানবীয় যোগাযোগ আছে সেখানে হতে পারে বিভিন্ন উপায়ে। মানবীয় অনুভূতি যেমন কৌতূহল, ভয়, এগুলোকে ব্যবহার করে Social Engineer রা মানুষকে নিজেদের স্বার্থে ব্যবহার করে এবং ফাঁদে ফেলে। সুতরাং যখনই কোনো ইমেইল বা ওয়েবসাইটের বিজ্ঞাপনে আকৃষ্ট হন, তখনই সাবধান হন।

  - সন্দেহজনক উৎস থেকে ইমেল এবং ফাইল খুলবেন না
  - মাল্টিফ্যাক্টর যাচাইকরী ব্যবহার করুন
  - লোভনীয় অফার থেকে সাবধান থাকুন
  - আপনার অ্যান্টিভাইরাস/অ্যান্টিম্যালওয়্যার সফটওয়্যার আপডেট রাখুন

- সামাজিক যোগাযোগ মাধ্যমগুলো নানারকম বিপদের ফাঁদ পাতা থাকে যা আপনার ব্যবসায় চরম প্রভাব ফেলতে পারে। নেটওয়ার্কগুলো সাবধানতার সাথে ব্যবহার করে এই বিপদগুলি এড়াতে পারবেন। নিম্নলিখিত ব্যবস্থাগুলি প্রায়ই সাহায্য করে:
  - গোপনীয়তা সেটিংস প্রয়োগ করুন যাতে শুধু মাত্র আপনার বন্ধুরাই আপনার পোস্টগুলি দেখতে পায়।
  - ব্যক্তিগত তথ্য, ছুটির পরিকল্পনা ইত্যাদি পোস্ট করা থেকে বিরত থাকুন।
  - আপনি যাদের চেনেন না, তাদের কাছ থেকে রিকোয়েস্ট বা ম্যাসেজ গ্রহণ করবেন না।
  - সংক্ষিপ্ত ইউআরএলে ক্লিক করা থেকে বিরত থাকুন এবং সন্দেহজনক অথবা মানহানিকর বা ভীতিকর একাউন্ট রিপোর্ট করুন
  - ব্যক্তিগত এবং কাজের অ্যাকাউন্ট আলাদা রাখুন

কর্মচারীদের জন্য সামাজিক মিডিয়া প্রশিক্ষণের ব্যবস্থা করুন, বিশেষ করে ডেটা নিরাপত্তার বিষয়ে।

সেশন -০৯: ইন্টারনেট কিভাবে কাজ করে

সেশনের কাঙ্ক্ষিত ফলাফল	অংশগ্রহণকারীরা জানতে পারবে কিভাবে ইন্টারনেট কাজ করে।

সেশনের ধরণ:
Activity-Discussion-Input-Deepning-Synthesis.

বিষয়	বর্ণনা
শিখনের উদ্দেশ্য	১ ইন্টারনেট কীভাবে কাজ করে এবং কীভাবে আমাদের ডেটা এক প্রান্ত থেকে অন্য প্রান্তে স্থানান্তরিত হয় তা জানবে। ২ ইন্টারনেটের ডাটা প্রবাহে কতগুলো মাধ্যম জড়িত এবং এর ঝুঁকিগুলো সম্পর্কে জানবে ৩ বেসিক রাউটারের নিরাপত্তা সম্পর্কে জানবে।
অতিরিক্ত তথ্য	• 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/
সেশন গাইড	• ইন্টারনেট কীভাবে কাজ করে সে বিষয়ে অংশগ্রহণকারীদের জ্ঞান দান করা হবে। • ইন্টারনেট কিভাবে কাজ করে তা ধাপে ধাপে ব্যাখ্যা করে একটি ভিডিও উপস্থাপন করা হবে। • কিভাবে ডেটা সঞ্চালন করে এবং এক প্রান্ত থেকে অন্য প্রান্তে প্রেরণ করে সে বিষয়ে প্রশিক্ষক একটি ইমেইল বা ওয়েবসাইট উদাহরণস্বরূপ উপস্থাপন করবেন। • নেটওয়ার্কের সাথে জড়িত সকল সম্ভাব্য বিষয়ে এবং সংশ্লিষ্ট ঝুঁকি নিয়ে আলোচনা করা হবে। • বেসিক রাউটারের নিরাপত্তা সেটিংস উপস্থাপন করা হবে।

অধিবেশনের সারসংক্ষেপ

- ইন্টারনেট হল একটি বৃহত্তর নেটওয়ার্ক যা বিশ্বব্যাপী কম্পিউটার নেটওয়ার্কগুলি যেমন কোম্পানি, সরকার, বিশ্ববিদ্যালয় এবং অন্যান্য সংস্থা দ্বারা পরিচালিত নেটওয়ার্ককে একত্রিত করে একে অপরের সাথে তথ্য আদান প্রদানের সুযোগ করে দেয়।
- ইন্টারনেট কেবল এক স্থান থেকে অন্য স্থানে তথ্য স্থানান্তর করে, যাতে আমরা চ্যাট, ব্রাউজ এবং শেয়ার করতে পারি।
- ইন্টারনেট হাজার হাজার কম্পিউটারের একটি নেটওয়ার্ক যা এক কম্পিউটার থেকে আরেক কম্পিউটারে তার, এবং বেতার তরঙ্গের মাধ্যমে বিটস স্থানান্তর করে।
- ডিভাইস<->রাউটার<->ইন্টারনেট সরবরাহকারী<->ডিএনএস<->সার্ভার
- বেসিক রাউটারের নিরাপত্তা-
    - আগেই দেওয়া (Default)পাসওয়ার্ড পরিবর্তন করুন।
    - আগেই দেওয়া (Default)ওয়াইফাই-এর নাম পরিবর্তন করুন।
    - ওয়াইফাই এর জন্য শক্তিশালী পাসওয়ার্ড ব্যবহার করুন।
    - WPA-2/3 এনক্রিপশন ব্যবহার করুন, WEP এড়িয়ে চলুন।
    - প্রয়োজনে ওয়াইফাই আইডি গোপন রাখুন।
    - আপনার নেটওয়ার্ক অন্যদের সাথে শেয়ার করবেন না, প্রয়োজনে গেস্ট/অতিথিদের জন্য আলাদা নেটওয়ার্ক তৈরি করুন।

সেশন -১০: এনক্রিপশন কি? ইন্টারনেট ট্রাফিক এনক্রিপশন

সেশনের কাঙ্ক্ষিত ফলাফল	অংশগ্রহণকারীরা এনক্রিপশন কী এবং কীভাবে তাদের ইন্টারনেট ট্র্যাফিক এনক্রিপ্ট করতে হয় তা শিখতে পারবেন।

সেশনের ধরণ:
Activity-Discussion-Input-Deepning-Synthesis.

বিষয়	বর্ণনা
শিখনের উদ্দেশ্য	১ এনক্রিপশন কি? ২ ভিপিএন কি? কীভাবে একটি ভাল ভিপিএন নির্ণয় করবেন। ৩ টর (TOR)কী এবং এটি কীভাবে কাজ করে?
অতিরিক্ত তথ্য	• https://aesencryption.net/ অনলাইন টেক্সট এনক্রিপশন প্ল্যাটফর্ম • https://aescrypt.com/ পাসওয়ার্ড দিয়ে ফাইল এনক্রিপ্ট করার ছোট টুলস • https://torproject.org/ TOR এর অফিসিয়াল সাইট • https://www.tunnelbear.com/ পেইড ভিপিএন • https://engagemedia.org/tunnelbear- বিনামূল্যে ১ বছরের TunnelBear ভিপিএন সাবস্ক্রিপশন • https://www.psiphon3.com/ ফ্রি ভিপিএন • https://www.f-secure.com/en/home/articles/6-things-to-consider-when-chusing-a-vpn • https://engagemedia.org/2021/indonesia-vpn/ • https://www.eff.org/pages/tor-and-https কিভাবে HTTPS এবং টর কাজ করে
সেশন গাইড	• অংশগ্রহণকারীদের এনক্রিপশন সম্পর্কে জিজ্ঞাসা করা হবে। • এনক্রিপশন কেন গুরুত্বপূর্ণ তা নিয়ে প্রশিক্ষক আলোচনা করবেন। • অংশগ্রহণকারীদের পূর্বে কোনো ওয়েবসাইটে ব্লক বা বাধার সম্মুখীন হয়েছিল কি না তা জিজ্ঞাসা করা হবে। যদি হ্যাঁ হয়, তারা কিভাবে এটি সমাধান করেছিল তা জানাবে। • ভিপিএন (VPN) কিভাবে কাজ করে এবং কেন ভিপিএন ব্যবহার করতে হবে তা প্রশিক্ষক আলোচনা করবেন। ভিপিএন নির্বাচন করার সময় কোন বিষয়গুলো বিবেচনা করা উচিত তা অংশগ্রহণকারীদের সাথে আলোচনা করবেন। • TOR নেটওয়ার্ক সম্পর্কে অংশগ্রহণকারীদের মধ্যে বিস্তারিত ব্যাখ্যা করা হবে।

অধিবেশনের সারসংক্ষেপ

- এনক্রিপশন হলো একটি বার্তা যা টেক্সট বা ইমেইলে পাঠানো বার্তাকে একটি প্রক্রিয়ার মাধ্যমে পাঠঅযোগ্য বিন্যাসে রূপান্তর করে- যাকে "সাইফার টেক্সট" বলা হয়।এটি ডিজিটাল তথ্যের গোপনীয়তা রক্ষা করতে সাহায্য করে। এটি কম্পিউটার সিস্টেমের মতো সংরক্ষিত এবং ইন্টারনেটের মতো বিভিন্ন তথ্য সংরক্ষণ করে থাকে।
- ভার্চুয়াল প্রাইভেট নেটওয়ার্ক, যা ভিপিএন নামে পরিচিত, আপনার পরিচয় এবং ব্রাউজিং কার্যকলাপকে হ্যাকার, ব্যবসায়ী, সরকারী সংস্থা এবং অন্যান্য ছদ্মবেশীদের থেকে রক্ষা করে। ইন্টারনেটের সাথে সংযুক্ত হবার পর, আপনার তথ্য এবং আইপি ঠিকানা এক ধরনের 'ভার্চুয়াল টানেল' দ্বারা গোপন থাকে।
- যখন VPN- নির্বাচন করবেন:
  - ভিপিএন সরবরাহকারীর নিরাপত্তা অভিজ্ঞতা পরীক্ষা করুন।
  - আপনার ভিপিএন এর গোপনীয়তা নীতি দেখুন।
  - সার্ভারের অবস্থানগুলোর সংখ্যা দেখুন।
- টর (TOR) একটি ফ্রি ওপেন সোর্স সফটওয়্যার যার মাধ্যমে পরিচয় গোপন রেখে যোগাযোগ করা সম্ভব। এখানে বিশ্বব্যাপী, স্বেচ্ছাসেবী ওভারলে নেটওয়ার্কের (Overlay network) মাধ্যমে ইন্টারনেট ট্র্যাফিক পরিচালনা করা হয়, যার মধ্যে সাত হাজারেরও বেশি রিলে(Relay) থাকে। এর ফলে ব্যবহারকারীর অবস্থান এবং নেটওয়ার্ক নজরদারি থেকে নিজেকে গোপন রাখা যায়।
- কিভাবে এটা কাজ করে:
  - তিনটি আলাদা টর 'নোড' (Nodes)এর মাধ্যমে আপনার জন্য সংযোগ তৈরি করে।
  - এই নোডগুলো কোনটিই একে অপরের সংযোগের উৎপত্তি এবং গন্তব্য জানে না।
  - আপনার থেকে শেষ নোড পর্যন্ত সমস্ত ট্র্যাফিক এনক্রিপ্ট করা থাকে।
- ফলাফল: এনক্রিপশন এবং গোপনীয়তা।

সেশন -১১: ফাইল এবং ফোল্ডার নিরাপত্তা

সেশনের কাঙ্ক্ষিত ফলাফল	অংশগ্রহণকারীরা ফাইল এবং ফোল্ডার নিরাপত্তা নিশ্চিত করতে পারবেন।

সেশনের ধরণ:
Activity-Discussion-Input-Deepning-Synthesis.

বিষয়	বর্ণনা
শিক্ষার উদ্দেশ্য	১ ডেটা নিরাপত্তার গুরুত্ব। ২ মেটা-ডেটা কী এবং কেন এটি গুরুত্বপূর্ণ। ৩ কিভাবে এনক্রিপশন টুল দিয়ে ফাইল এবং ফোল্ডার এনক্রিপ্ট করবেন। ৪ কিভাবে স্থায়ীভাবে ফাইল/ফোল্ডার মুছে ফেলবেন। ৫ মুছে ফেলা ফাইল পুনরুদ্ধার কিভাবে করবেন।
অতিরিক্ত তথ্য	• https://veracrypt.fr/ ফাইল ফোল্ডার এনক্রিপশন টুল • https://cryptomator.org/ • https://www.bleachbit.org/ স্থায়ী ফাইল এবং ফোল্ডার অপসারণ টুল। • https://ccleaner.com/recuva মুছে ফেলা ফাইল রিকভারি টুল • http://exif.regex.info/ মেটা ডেটা যাচাই প্ল্যাটফর্ম • https://ssd.eff.org/en/module/why-metadata-matters
সেশন গাইড	• অংশগ্রহণকারীদের তাদের ফাইল ফোল্ডার নিরাপত্তার বর্তমান অবস্থা সম্পর্কে জিজ্ঞাসা করা হবে। • প্রশিক্ষক স্থানীয়ভাবে সংরক্ষিত তথ্যের নিরাপত্তা নিয়ে আলোচনা করবেন। • মেটা-ডেটা এবং কেন এটি সম্পর্কে সচেতন হওয়া দরকার তা নিয়ে আলোচনা করা হবে। • প্রশিক্ষক উপস্থাপন করবেন কিভাবে একটি সাম্প্রতিক মুছে ফেলা ফাইল পুনরুদ্ধার করা যায় এবং কিভাবে কম্পিউটার থেকে স্থায়ীভাবে সেগুলি সরিয়ে ফেলা যায়। • ওপেনসোর্স ফাইল/ফোল্ডার এনক্রিপশন ট্যুল 'Veracrypt'-এর ধাপে ধাপে নির্দেশিকা উপস্থাপন করবেন।

অধিবেশনের সারসংক্ষেপ

- তথ্য চুরির ঝুঁকি হ্রাস করা খুবই গুরুত্বপূর্ণ। সংবেদনশীল তথ্যে অননুমোদিত প্রবেশাধিকার রোধ করতে নিরাপত্তা নিয়ন্ত্রণ প্রয়োগ করা শেখানো হবে।
- তথ্য নিরাপত্তার মৌলিক নীতি হল গোপনীয়তা, অখণ্ডতা এবং প্রাপ্যতা।
- যখন আপনি সাময়ীকভাবে একটি ফাইল মুছে ফেলেন, এটি আসলে তা মুছে দেয় না, বরং সেটি পুনরুদ্ধার করা সম্ভব। একটি স্বাভাবিক হার্ড ডিস্কে (HDD) স্থায়ীভাবে একটি ফাইল মুছে ফেলার জন্য একই স্থানে কিছু প্রতিস্থাপন করা প্রয়োজন।
- অস্থায়ী/ হিস্ট্রি/ ক্যাশে/ লগ ইত্যাদি ফাইল থেকে সাবধান থাকুন। এগুলি আপনার ব্রাউজারের হিস্ট্রি, চ্যাট লগ সহ অন্যান্য গুরুত্বপূর্ণ তথ্য বহন করে।
- মেটা-ডেটা হল আপনার পাঠানো এবং প্রাপ্ত ডিজিটাল যোগাযোগের তথ্য। মেটা-ডেটা অনেক গুরুত্বপূর্ণ তথ্য বহন করে। যা আপনার নিরাপত্তার জন্য হুমকি হতে পারে। মেটাডেটা মুছে ফেলার বা ছোট করার চেষ্টা করুন। মেটাডেটার কিছু উদাহরণের মধ্যে রয়েছে:
  - আপনার ইমেলের সাব্জেক্ট লাইন
  - আপনার কথোপকথনের দৈর্ঘ্য
  - যে সময়ে কথোপকথন পরিচালিত হয়েছিল
  - যোগাযোগ করার সময় আপনার অবস্থান (পাশাপাশি কার সাথে)
- আমাদের অপারেটিং সিস্টেম এনক্রিপশন সমর্থন করলে তা চালু করে রাখুন। অথবা ফ্রি ওপেনসোর্স সফটওয়্যার ভেরাক্রিপ্ট (Varacrypte)ব্যবহার করুন যা চলন্ত ডাটাকে এনক্রিপশন প্রদান করে। এটি প্রি-বুট অথেনটিকেশন এর মাধ্যমেএটি একটি ফাইলকে ভার্চুয়ালি এনক্রিপ্ট ডিস্ক তৈরি অথবা পার্টিশন তৈরি অথবা পুরো স্টোরেজ ডিভাইসটি এনক্রিপ্ট করতে সক্ষম।
- এছাড়াও, আপনি আপনার ডেটা এনক্রিপ্ট রাখতে ক্রিপ্টোমেটর (Cryptomator) ব্যবহার করতে পারেন। আপনি যদি ক্রিপ্টোমেটর ব্যবহার করেন, তাহলে আপনি ভার্চুয়াল ড্রাইভে হোস্ট করা ভল্ট তৈরি করতে পারেন। ভল্টে সংরক্ষিত ডেটা এনক্রিপ্ট করা হয় এবং ব্যবহারকারী ভল্টের অবস্থান নির্দিষ্ট করতে পারে, যেমন- ক্লাউড সরবরাহকারী।

সেশন -১২: ডেটা ব্যাকআপ

সেশনের কাঙ্ক্ষিত ফলাফল	**অংশগ্রহণকারীরা ব্যাকআপের গুরুত্ব এবং কীভাবে এটি সঠিকভাবে করতে হয় তা শিখবেন।**

সেশনের ধরন:
Activity-Discussion-Input-Deepning-Synthesis.

বিষয়	বর্ণনা
শিখনের উদ্দেশ্য	১ ব্যাকআপের গুরুত্ব। ২ কিভাবে নিরাপদে ব্যাকআপ তৈরি এবং সঞ্চয় করতে হয়।
অতিরিক্ত তথ্য	• https://duplicati.com/ এনক্রিপ্ট করা ব্যাকআপ তৈরির টুল • 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
সেশন গাইড	• অংশগ্রহণকারীদের তাদের বর্তমানে অনুশীলন ডাটা ব্যাকআপ সম্পর্কে জিজ্ঞাসা করা হবে। • ব্যাকআপের গুরুত্ব সম্পর্কে প্রশিক্ষক আলোচনা করবেন। • ওপেনসোর্স এনক্রিপ্টেড ডেটা ব্যাকআপ নকল করার সরঞ্জাম ধাপে ধাপে প্রশিক্ষক উপস্থাপন করবেন।

অধিবেশনের সারসংক্ষেপ

- তথ্য ব্যবস্থাপনার জন্য সংগৃহীত তথ্যের ব্যাকআপ তৈরি করা অত্যন্ত গুরুত্বপূর্ণ। তথ্য ব্যাকআপ বিভিন্ন কারণে যেমন-হার্ডওয়্যার ব্যর্থতা, ভাইরাস আক্রমণ ইত্যাদি দুর্যোগ থেকে রক্ষা করে। ব্যাকআপ থাকলে এসব দূর্যোগ ঘটলেও সময় এবং অর্থ সাশ্রয় করতে সহায়তা করে।
- আপনার ডিভাইস নষ্ট, চুরি বা হারিয়ে যেতে পারে। অথবা গুরুত্বপূর্ণ ফাইল হারিয়ে যেতে পারে।
- নিয়মিত ব্যাকআপ রাখুন। একাধিক হলে ভাল হয়।
- মূল তথ্য এবং ব্যাকআপ তথ্য একই জায়গায় রাখবেন না।
- নিশ্চিত করুন যে ব্যাকআপ এনক্রিপ্ট করা আছে।
- ব্যাকআপের জন্য ভালো এবং নির্ভরযোগ্য টুলস ব্যবহার করুন।
- ব্যাকআপের ধরন-
    - সম্পূর্ণ ব্যাকআপ
    - ক্রমবর্ধমান ব্যাকআপ
    - ডিফারেনশিয়াল ব্যাকআপ
- উইন্ডোজ অপারেটিং সিস্টেমে অন্তর্নির্মিত (Built-in) ব্যাকআপ ব্যবহার করতে পারবেন। কিন্তু ফাইল ব্যাকআপ একই হার্ড ডিস্কে করবেন না যেখানে উইন্ডোজ ইনস্টল করা হয়েছে। বহিরাগত ব্যক্তিদের ফাইল অ্যাক্সেস করা থেকে বিরত রাখার জন্য সর্বদা ব্যাকআপের জন্য ব্যবহৃত মিডিয়া (বাহ্যিক হার্ড ডিস্ক, ডিভিডি বা সিডি) আলাদা রাখুন। আপনি আপনার ব্যাকআপের ডাটা এনক্রিপ্ট করেওরাখতে পারেন।
- 'ডুপ্লিকাটি' একটি ফ্রি, ওপেন সোর্স, ব্যাকআপ ক্লায়েন্ট যা ক্লাউড স্টোরেজ সার্ভিস এবং রিমোট ফাইল সার্ভারে এনক্রিপ্ট, ইনক্রিমেন্টাল, কম্প্রেসড ব্যাকআপ নিরাপদে সংরক্ষণ করে।

সেশন -১৩: ইমেল এনক্রিপশন

সেশনের কাঙ্ক্ষিত ফলাফল	অংশগ্রহণকারীরা তাদের ইমেইল যোগাযোগ এনক্রিপ্ট করতে শিখবেন।

সেশনের ধরণ:
Activity-Discussion-Input-Deepning-Synthesis.

বিষয়	বর্ণনা
শিখনের উদ্দেশ্য	১ কীভাবে ইমেইল পাঠানো হয়, ইমেইলের কোথায়, কীভাবে পাঠানো হয়, পাঠানোর পর কোথায় যায়, কীভাবে ইমেল বিষয়বস্তু পড়া যায় তা জানবেন। ২ ইমেল অনাকাঙ্ক্ষিত নজরদারির হাতে পড়ার হার কমানোর উপায় সম্পর্কে জানবেন। ৩ GPG / PGP কি এবং এটি কিভাবেমোবাইল ডিভাইসে ব্যবহার করবে তা সম্পর্কে জানবে। ৪ ব্যক্তিগত/সর্বজনীন কী-পেয়ার তৈরি করতে, কী-চেইনে একটি পাবলিক কী আপলোড করতে পারবেন।অন্যদের পাবলিক কীগুলি খুঁজে পেতে ও ডাউনলোড করতে, অন্যদের পরিচয়জানতে এবং কী-গুলি যাচাই করতে সক্ষম হবেন। ৫ GPG/PGP ব্যবহার করে স্বাক্ষরিত বা এনক্রিপ্ট করা ইমেল পাঠাতে এবং গ্রহণ করতে সক্ষম হবেন।
অতিরিক্ত তথ্য	• https://www.openpgp.org/ ইমেইল এনক্রিপশন • https://mailvelope.com/ ইমেইল এনক্রিপশন ব্রাউজার এক্সটেনশন • https://www.thunderbird.net/ PGP সাপোর্ট সহ মেইল ক্লায়েন্ট খোলা।
সেশন গাইড	• ইমেল যোগাযোগ কিভাবে হয় তা নিয়ে প্রশিক্ষক আলোচনা করবেন। কিভাবে একটি ইমেল প্রেরক থেকে প্রাপকের নিকটযায়, এর মধ্যে নিরাপত্তা ঝুঁকিগুলি কী এবং কীভাবে সেগুলি হ্রাস করা যায়তাজানতেপারবেন। • ওপেনসোর্স ইমেইল সিকিউরিটি ব্রাউজার এক্সটেনশান মেইলভেলপের ধাপে ধাপে নির্দেশিকা উপস্থাপন করা হবে। • OpenPGP সাপোর্ট দিয়ে ওপেনসোর্স ইমেল ক্লায়েন্টের ধাপে ধাপে নির্দেশিকা উপস্থাপন করা হবে। উপস্থাপনার মাধ্যমে থান্ডারবার্ড দেখানো হবে।

অধিবেশনের সারসংক্ষেপ

- 90% এর বেশি সংস্থা করাপ্টেড ইমেইল থেকে আক্রমনের শিকার হয়।
- সবসময় ইন্টারনেট, ইমেইল, চ্যাট কথোপকথন এমন ব্যক্তি বা মাধ্যমে স্থানান্তর হয়, যাকে আমরা জানি না। কারণ ইন্টারনেট এভাবেই কাজ করে।
    - ISP বা মোবাইল পরিষেবা প্রদানকারী কিছু প্রতিষ্ঠানের এই ধরনের সুযোগ আছে কারণ ইন্টারনেটের ব্যবস্থাপনা প্রক্রিয়ায় জড়িত।
    - উচ্চ পর্যায়ের অনেকে আইনীভাবে বা "কম আইনি" উপায়ে যেমন প্রকাশ্যে আদালতের আদেশপ্রাপ্ত প্রতিষ্ঠান, বা গোয়েন্দা বিভাগে কাজ করার সূত্রে এই সুযোগ পায়।
    - হ্যাকারদের মতো অনেকে সিস্টেমে দুর্বলতার কারণে এধরণের প্রবেশগম্যতা পেতে পারে।
- প্রিটি গুড প্রাইভেসি (পিজিপি) একটি এনক্রিপশন সিস্টেম যা এনক্রিপ্ট করা ইমেল পাঠানো এবং সংবেদনশীল ফাইল এনক্রিপ্ট করা উভয়ের জন্য ব্যবহৃত হয়। এটি এনক্রিপ্ট করা ইমেল প্রেরণ এবং গ্রহণের জন্য ব্যবহৃত হয়। বার্তা প্রেরকের পরিচয় যাচাই করা হয়। আপনার ডিভাইসে বা ক্লাউডে এনক্রিপ্ট করা ফাইল জমা হয়।
- ‘মেইলভেলপ’ হল একটি ব্রাউজার এক্সটেনশন যা OpenPGP স্ট্যান্ডার্ডের উপর ভিত্তি করে নিরাপদ ইমেইল যোগাযোগের অনুমতি দেয়। এটি আপনার বর্তমান ইমেলের সাথে একটি পৃথক, স্থানীয় ইমেল ক্লায়েন্ট ব্যবহার না করে সংযুক্ত ফাইল সহ বার্তাগুলি এনক্রিপ্ট করতে ব্যবহার করা যেতে পারে।
- “থান্ডারবার্ড 78 এ দুটি এনক্রিপশন স্ট্যান্ডার্ড, OpenPGP এবং S/MIME এর জন্য বিল্ট-ইন সাপোর্ট রয়েছে।
- সংস্করণ 78.2 থেকে OpenPGP স্বয়ংক্রিয়ভাবে সক্রিয় করা হয়েছে।
- আপনার গোপন পাসওয়ার্ড অন্যদের কাছে আদান প্রদান করবেন না।

সেশন -১৪: মোবাইল ফোনের নিরাপত্তা

সেশনের কাঙ্ক্ষিত ফলাফল	**অংশগ্রহণকারীরা মোবাইল ফোনের নিরাপত্তা সম্পর্কে জানতে পারবেন।**

সেশনেরধরণ:
Activity-Discussion-Input-Deepning-Synthesis.

বিষয়	বর্ণনা
শিখনের উদ্দেশ্য	১ মোবাইল ফোন বহন ও ব্যবহারের ঝুঁকি জানতে পারবেন। ২ কীভাবে সেই ঝুঁকিগুলি কমানো যায় তা জানতে পারবেন।
অতিরিক্ত তথ্য	• 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/
সেশন গাইড	• প্রশিক্ষক মোবাইল ফোনের সাথে সম্পর্কিত বিভিন্ন ধরনের ঝুঁকি নিয়ে আলোচনা করবেন। • প্রশিক্ষক গোপনীয়তা এবং নিরাপত্তার জন্য মোবাইলে কয়েকটি সেটিংস উপস্থাপন করবে, অংশগ্রহণকারীরা ধাপগুলি অনুসরণ করবে।

অধিবেশনের সার সংক্ষেপ

- মোবাইল নিরাপত্তা হুমকি বলতে বোঝায় এক ধরণের সাইবার-আক্রমণ যেখানে স্মার্টফোন এবং ট্যাবলেটের মতো মোবাইল ডিভাইস গুলিকে টার্গেট করা হয়। এটি পিসি বা এন্টারপ্রাইজ সার্ভারে হ্যাকিং আক্রমণের অনুরূপ। হ্যাকাররা মোবাইল সফটওয়্যার, হার্ডওয়্যার এবং নেটওয়ার্ক সংযোগের দুর্বলতাকে কাজে লাগায় যাতে টার্গেটেড ডিভাইসকে দূষিত, অননুমোদিত ক্রিয়াকলাপে সক্ষম করে।
- হ্যাকারদের পক্ষে আপনার মোবাইলের ঢোকা সম্ভব এবং তারা যা চায় তা করতে পারে। উদাহরণস্বরূপ- মাইকে আপনার ভয়েস শোনা, আপনার কল রেকর্ড করা, ছবি তোলা বা ভিডিও রেকর্ড করা এবং তারা এমনকি আপনার ডিভাইস থেকে কল বা এসএমএসও পাঠাতে পারে।
- আপনার ডিভাইসের অপারেটিং সিস্টেম আপটুডেট রাখুন।
- সর্বদা আপনার মোবাইল ফোনে পাসওয়ার্ড ব্যবহার করুন।
- অন্য কাউকে ডিভাইস ব্যবহার করতে দেবেন না।
- অ্যাপ ইনস্টল করার সময়, আপনি কি কি অনুমতি দিচ্ছেন তা বিবেচনা করুন।
- ফুলডিস্ক এনক্রিপশন চালু করুন।
- জিপিএস বন্ধ করুন।
- 'জেলব্রেক' করবেননা বা আপনার ফোন রুট করবেন না।
- অপরিচিত সূত্র থেকে পাওয়া বার্তা বা মিডিয়া থেকে সাবধান।
- পাবলিক ওয়াইফাই ব্যবহার করবেন না।
- আপনার লক স্ক্রিন নিরাপত্তা অপ্টিমাইজ করুন।
- মোবাইল ফোন যেখানে সেখানে বহন করবেননা। আপনি যদি কোনো নিরাপদ মিটিং বা প্রতিবাদে অংশ নিতে চান এবং আপনি আপনার অবস্থান প্রকাশ করতে না চান, তাহলে আপনার মোবাইল ফোন বাড়িতে রেখে দিন।

সেশন -১৫: এন্ড-টু-এন্ড এনক্রিপশন এবং মোবাইল যোগাযোগ

সেশনের কাঙ্ক্ষিত ফলাফল	**অংশগ্রহণকারীরা এন্ড-টু-এন্ড এনক্রিপশন সম্পর্কে জানতে পারবেন এবং তারা এনক্রিপ্ট করা অ্যাপ ব্যবহার করে নিরাপদে যোগাযোগ করতে পারবেন।**

সেশনেরধরণ:
Activity-Discussion-Input-Deepning-Synthesis.

বিষয়	বর্ণনা
শিখনের উদ্দেশ্য	১ এন্ড-টু-এন্ড এনক্রিপশনের পদ্ধতি জানতে পারবেন। ২ মোবাইল যোগাযোগের জন্য এনক্রিপ্ট করা অ্যাপস বেছে নিতে পারবেন।
অতিরিক্ত তথ্য	• 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 key exchange system. (advance) • https://signal.org/ নিরাপদ যোগাযোগ অ্যাপ • https://wire.com/ নিরাপদ যোগাযোগ অ্যাপ • https://briarproject.org/ অফলাইন নিরাপদ যোগাযোগের জন্য মোবাইল অ্যাপ
সেশন গাইড	• প্রশিক্ষক এন্ড-টু-এন্ড এনক্রিপশন কী, এটি কীভাবে কাজ করে এবং কেন এটি নিরাপত্তা ও গোপনীয়তার জন্য গুরুত্বপূর্ণ তা উপস্থাপন করবেন। • প্রশিক্ষক এন্ড-টু-এন্ড এনক্রিপশন সমর্থিত মোবাইল কমিউনিকেশন অ্যাপ সম্পর্কে বিস্তারিত আলোচনা করবেন। • অংশগ্রহণকারীদের অ্যাপ ডাউনলোড করতে বলবেন এবং অংশগ্রহণকারীদের মধ্যে ভবিষ্যতের যোগাযোগের জন্য বা প্রশিক্ষকেরকাছ থেকে পরামর্শের জন্য একটি গ্রুপ তৈরি করা হবে।

অধিবেশনের সারসংক্ষেপ

- এন্ড-টু-এন্ড এনক্রিপশন (E2EE) নিরাপদ যোগাযোগের একটি পদ্ধতি যা তৃতীয়পক্ষকে ডেটা অ্যাক্সেস করতে বাধা দেয়। E2EE তে, প্রেরকের সিস্টেম বা ডিভাইসে ডেটা এনক্রিপ্ট করা হয় এবং শুধুমাত্র প্রাপকই এটি ডিক্রিপ্ট করতে পারবেন।
- এন্ড-টু-এন্ড এনক্রিপশন বর্তমানে গোপনীয় তথ্য স্থানান্তর করার সবচেয়ে নিরাপদ উপায়, এবং সেজন্যই আরও বেশিসংখ্যক যোগাযোগ পরিষেবা এতে চলে আসছে।
- তথ্য গোপন রাখতে চাইলে নিয়মিত ‘সেলুলারকল’ এড়িয়ে চলুন।
- মোবাইল যোগাযোগের জন্য একটি ওপেনসোর্স এবং এন্ড-টু-এন্ড এনক্রিপশন সমর্থিত অ্যাপ ব্যবহার করবেন।
- সিগন্যাল হল একটি ফ্রি, গোপনীয়তা-ভিত্তিক মেসেজিং এবং কল করার অ্যাপ যা আপনি অ্যাপল এবং অ্যান্ড্রয়েড স্মার্টফোনে এবং ডেস্কটপের মাধ্যমে ব্যবহার করতে পারেন। যোগদান করার জন্য আপনার শুধু একটি ফোন নম্বর প্রয়োজন। সিগন্যালের যোগাযোগ এন্ড-টু-এন্ড এনক্রিপ্ট করা হয়, যার অর্থ কেবল যারা বার্তাগুলো আদান-প্রদান করছেন তারাই বিষয়বস্তু দেখতে পারবেন। এমনকি কোম্পানিও দেখতে পারবেন না।
- ওয়্যার হলো সিগন্যালের অনুরূপ অ্যাপ কিন্তু মোবাইল ফোন নম্বর ছাড়াই ওয়্যারে অ্যাকাউন্ট তৈরি করতে পারবেন। অ্যাকাউন্ট তৈরির জন্যই ইমেল অথবা ফোন নম্বর- যে কোনো একটা ব্যবহার করতে পারবেন।
- ব্রায়ার হল একটি মেসেজিং অ্যাপ যা অধিকারকর্মী, সাংবাদিক এবং অন্য যে কারও যোগাযোগের জন্য একটি নিরাপদ, সহজ এবং শক্তিশালী উপায়। সাময়িক মেসেজিং অ্যাপের বিপরীতে, ব্রায়ার কেন্দ্রীয় সার্ভারের উপর নির্ভর করেনা - বার্তাগুলি সরাসরি ব্যবহারকারীদের ডিভাইসের মধ্যে সিঙ্ক্রোনাইজ করা হয়। যদি ইন্টারনেট বন্ধ থাকে, সংকটের মুহূর্তে যোগাযোগ চালু রাখতে ব্রায়ার ব্লুটুথ বা ওয়াই-ফাইয়ের মাধ্যমেও সিঙ্ক করতে পারে, যদি ইন্টারনেট চালু থাকে, ব্রায়ার টর নেটওয়ার্কের মাধ্যমে সিঙ্ক করতে পারে, ব্যবহারকারীদের এবং তাদের সম্পর্ক কে নজরদারি থেকে রক্ষা করতে পারে।

সেশন -১৬: পরবর্তী প্রশিক্ষণের জন্য কীভাবে নিজেকে প্রস্তুত করবেন

সেশনের কাঙ্ক্ষিত ফলাফল	প্রশিক্ষক হিসেবে অংশগ্রহণকারীরা আরও ভালো করবেন।

সেশনেরধরণ:
Activity-Discussion-Input-Deepning-Synthesis.

বিষয়	বর্ণনা
শিখনের উদ্দেশ্য	১ প্রশিক্ষণের সময় আরও ভাল করার জন্য মৌলিক নিয়মগুলি শিখবেন। ২ কীভাবে একটি ভালো উপস্থাপনা তৈরি করতে হয় তা জানবেন। ৩ প্রশিক্ষণের আগে, চলাকালীন এবং পরবর্তি বিষয় বিবেচনা করা উচিত। ৪ কীভাবে একটি সেশনের পরিকল্পনা করবেন তা জানবেন। ৫ প্রশিক্ষণের সময় প্রশ্নগুলি কীভাবে পরিচালনা করবেন তা জানবেন।
অতিরিক্ত তথ্য	• https://level-up.cc/before-an-event/preparing-sessions-using-adids/ • https://level-up.cc/you-the-trainer/golden-rules-of-effective-training/
সেশন গাইড	• প্রশিক্ষক অংশগ্রহণকারীদের তাদের পরবর্তী প্রশিক্ষণের জন্য বিভিন্ন টিপস উপস্থাপন করবেন। • প্রশিক্ষক উদাহরণসহ বিভিন্ন প্রশ্নের উত্তর দিবেন।

অধিবেশনের সারসংক্ষেপ

- সময় ব্যবস্থাপনা:
  - সময়ের ব্যবস্তাপনায় সতর্ক থাকুন। অংশগ্রহণকারীদের সঠিক সময় অনুসরণ করতে উৎসাহিত করুন।
  - বিষয়বস্তু অনুযায়ী সময়সূচী ঠিক করুন।
  - প্রশ্নের জন্য সময় রাখুন।
  - প্রয়োজনে বিরতি দিন।
- অংশগ্রহণকারী:
  - অংশগ্রহণকারীদের প্রতি সম্মান প্রদর্শন করুন।
  - নিশ্চিত করুন যে তারা বিষয়গুলো বুঝতে পেরেছে।
  - প্রশ্ন জিজ্ঞাসা করুন এবং তাদের প্রশ্ন করতে উৎসাহিত করুন।
  - খেয়াল করুন তারা যেন বিরক্ত বোধ না করে।
- পরিস্থিতি বোঝাঃ
  - সবসময় সবকিছু স্বাভাবিকভাবে চলতে পারেনা। পরিকল্পনা পরিবর্তন করতে প্রস্তুত থাকুন।
  - পরিস্থিতির উপর নির্ভর করে সৃজনশীল এবং নমনীয় হন।
  - চাহিদা বা পরিস্থিতি অনুযায়ী বিষয়বস্তু পরিবর্তন করুন।
  - প্রাসঙ্গিকতা বিবেচনা করে বিষয়গুলি পরিকল্পনা করুন।
  - অংশগ্রহণকারীদের সক্রিয় রাখতে আইসব্রেকিং এবং মজা করার সময় রাখুন।
- সরঞ্জাম এবং প্রয়োজনীয় ব্যবস্থা:
  - সাবধানতা অবলম্বন করুন।
  - আপনার প্রয়োজনীয় ডিভাইসগুলো কাজ করছে কিনা তা নিশ্চিত করুন।
  - সমস্ত অংশগ্রহণকারীদের জন্য প্রয়োজনীয় সরঞ্জামগুলি নিশ্চিত করুন।
- উপস্থাপনা সৃষ্টি:
  - এটা সহজ এবং পরিষ্কার রাখুন।
  - অনুরূপ ফন্ট ব্যবহার করুন। অতিরিক্ত রং ব্যবহার এড়িয়ে চলুন।
  - খুব বেশি টেক্সট যোগ করবেন না, কিছু ছবি যোগ করুন।
  - বিষয়ের ধারাবাহিকতা বজায় রাখুন। প্রথমে সমস্যা নিয়ে আলোচনা করুন তারপর সমাধান করুন।
  - আপটুডেট রাখুন।
  - অংশগ্রহণকারীদের সাথে সম্পর্কিত উদাহরণ দিন।
  - অংশগ্রহণকারীকে অসন্তুষ্ট করে এমন কিছু অন্তর্ভুক্ত করবেন না।

দক্ষতা মূল্যায়ন টেমপ্লেট:

আপনার দক্ষতা এবং চাহিদা নির্ধারণ করতে দয়া করে নিম্নোক্ত প্রশ্নের উত্তর দিন। এই মূল্যায়নের ফলাফল আমাদের আপনার জন্য একটি ভালো প্রশিক্ষণ ডিজাইন করতে সাহায্য করবে। এছাড়াও, দয়া করে মনে রাখবেন যে কিছু প্রশ্নের একাধিক বা খুব কাছাকাছি একাধিক সঠিক উত্তর থাকতে পারে, আপনি যা ভাল মনে করেন তা চয়ন করুন।

১. ডিজিটাল নিরাপত্তার সবচেয়ে গুরুত্বপূর্ণ নীতি কী?
- অ্যান্টিভাইরাস প্রোগ্রাম আপডেট
- অপারেটিং সিস্টেম আপডেট
- কাওকে বিশ্বাস না করা
- ইমেল সংযুক্তি না খোলা

২. আপনার পাসওয়ার্ড কমপক্ষে কতগুলো অক্ষর হওয়া উচিত?
- ৮ অক্ষর
- ১০ অক্ষর
- ২০ অক্ষর
- ২৫ অক্ষর

৩. জটিল পাসওয়ার্ড তৈরি করা কেন গুরুত্বপূর্ণ?
- এটা পাসওয়ার্ড শক্তিশালী করে যা ব্রুট ফোর্সের মতো সফটওয়্যার ব্যবহার করে পাসওয়ার্ড ভাঙাকে করা আরও কঠিন করে তোলে
- এটি পাসওয়ার্ড এনক্রিপশনকে আরও কঠিনতর করে
- এটি পাসওয়ার্ড অনুমান করা আরও কঠিন করে
- এটি পাসওয়ার্ড বুঝতে আরও কঠিন করে

৪. কীভাবে আপনার কম্পিউটারকে ফিজিক্যাল টেম্পারিং থেকে রক্ষা করবেন?
- আপনার হার্ড ডিস্ক ফরম্যাট করবেন
- আপনার সম্পূর্ণ হার্ডডিস্ক এনক্রিপ্ট করবেন
- আপনার নথি এনক্রিপ্ট করবেন
- আপনার কম্পিউটার লক করবেন

৫. আপনি আপনার ব্যাকআপ ফাইল কোথায় রাখবেন?
- একই কম্পিউটারে আলাদা ড্রাইভে।
- একই কম্পিউটারে লুকানো ফোল্ডারে।
- আমি কোনো ব্যাকআপ রাখি না
- পৃথক ডিভাইস এবং লোকেশানে।

৬. কোনো ওয়েবসাইটে https সঠিক কিনা তা আমি কীভাবে পরীক্ষা করব?
- আমি হেডারে https চেক করি
- আমি URL- এ কী লক দেখি
- আমি ডিজিটাল সার্টিফিকেট চেক করি
- আমি URL- এ নাম চেক করি

৭. ইমেল প্রেরণ এবং গ্রহণের জন্য একটি নিরাপদ উপায় কী?
- নিরাপদ মেইল
- SMTP
- এফটিপি

- পিজিপি

৮. আপনাকে একটি এনক্রিপ্ট করা ইমেল পাঠানোর জন্য আমার কী প্রয়োজন?
- আপনার ব্যক্তিগত কী
- আপনার পাবলিক কী
- উপরের দুটিই
- কোনটিই নয়

৯. আপনার কম্পিউটার বন্ধ করার আগে আপনি আপনার খোলা অ্যাকাউন্ট (ইমেল, টুইটার, ফেসবুক ...) কী করবেন?
- শুধু ল্যাপটপের ঢাকনা বন্ধ করবেন
- ব্রাউজার বন্ধ করে তারপর কম্পিউটার বন্ধ করবেন।
- অ্যাকাউন্ট থেকে লগআউট করে ব্রাউজার বন্ধ করবেন তারপর কম্পিউটার বন্ধ করবেন।
- কম্পিউটার বন্ধ না হওয়া পর্যন্ত পাওয়ার বোতাম টিপুন।

১০. এ্যাকাউন্টে সহজে প্রবেশের জন্য ব্রাউজারে কি পাসওয়ার্ড সেভ করা উচিত?
- হ্যাঁ
- না

১১. প্রতিটি অ্যাকাউন্টের জন্য আপনার কি আলাদা পাসওয়ার্ড ব্যবহার করা উচিত? অথবা সব এ্যকাউন্টের জন্য একটি পাসওয়ার্ড যাতে আপনি এটি ভুলে না যান এবং আপনার অ্যাকাউন্ট না হারান? *
- সবগুলোর জন্য একটি।
- প্রতিটি অ্যাকাউন্টের জন্য আলাদা পাসওয়ার্ড।

১২. আপনার কম্পিউটারে কোন অপারেটিং সিস্টেম আছে তা আপনি কীভাবে জানতে পারেন?
- উৎপাদনকারী সংস্থার সাথে যোগাযোগ করে।
- এটা কম্পিউটারের পিছনে লেখা আছে।
- মাই কম্পিউটারে রাইট বাটন ক্লিক করে এবং প্রোপার্টিজে চেক করে।
- আমি এটি মেরামতের দোকানে নিয়ে গেলে তারা আমাকে বলবে।

১৩. একাধিক অ্যান্টি-ভাইরাস প্রোগ্রাম ব্যবহার করলে অধিক সুরক্ষা পাওয়া যায়।
- হ্যাঁ
- না

১৪. রুট কিটস কী করে?
- ভাইরাস এবং ট্রোজানকে লুকিয়ে রাখে
- ফাইল লুকিয়ে রাখে
- অ্যান্টিভাইরাস প্রোগ্রাম বন্ধ করে দেয়
- ম্যালওয়্যার ইনস্টল করে

১৫. আমার ডেটা মুছে ফেলার জন্য ফরম্যাট কি যথেষ্ট?
- হ্যাঁ
- না

১৬. ইউএসবি এবং সিডিকে ভাইরাস থেকে রক্ষা করার জন্য?
- আমার কোন ইউএসবি ব্যবহার করা উচিত নয়
- আমার উইন্ডোতে অটোরান নিষ্ক্রিয় করা উচিত
- আমার কম্পিউটার স্ক্যান করা উচিত

- আমার কিছু করা উচিত নয়

১৭. যদি আপনি আপনার বন্ধুর কাছ থেকে ই-মেইলে একটি অনাকাঙ্ক্ষিত লিঙ্ক বা এ্যাটাচমেন্ট পান যা আপনি কী করবেন?

- এটি যাচাই করবেন এবং খুলবেন কিনা সিদ্ধান্ত নিবেন।
- আপনি এটি খুলবেন কারণ আপনার কম্পিউটারকে রক্ষা করার মত একটি ভালো অ্যান্টি ভাইরাস রয়েছে।
- প্রেরকের সাথে যোগাযোগ করুন এবং তিনি পাঠিয়েছেন কিনা তা যাচাই করে খুলুন।
- এটি খুলুন, কারণ এটি যে ফায়ারওয়াল এক্টিভেট করেচে তা আপনার কম্পিউটারের ক্ষতি থেকে রক্ষা করবে।

১৮. আপনি আপনার মোবাইলে একটি অ্যাপ ইনস্টল করার আগে আপনার কী পরীক্ষা করা উচিত?

- এর কী অনুমতি দরকার
- কে এটি প্রকাশ করেছে
- এটি কি আমার অবস্থান প্রকাশ করে
- এটি কি প্রচুর ব্যান্ডউইথ ব্যবহার করে

১৯. যদি আপনার গুরুত্বপূর্ণ মিটিং থাকে এবং আপনি না চান যে মোবাইল কোম্পানি আপনার অবস্থান জানুক?

- মোবাইলের জিপিএস বন্ধ করুন,
- আমার ফোন পুরনো এবং জিপিএস নেই তাই তারা আমার অবস্থান জানতে পারবেনা।
- মিটিং শুরুর আগে ফোন বন্ধ করুন এবং সিম কার্ড খুলে ফেলুন
- বাসা থেকে বের হওয়ার আগে মোবাইল বন্ধ করে ব্যাটারি খুলুন

২০. মোবাইলকে অন্যের ব্যবহার থেকে রক্ষা করতে:

- একটি পাস কোড ব্যবহার করুন
- সম্পূর্ণ ডিভাইস এনক্রিপশন ব্যবহার করুন
- সিমকার্ডের জন্য পাসকোড ব্যবহার করুন
- ফোন খুলতে একটি প্যাটার্ন ব্যবহার করুন