প্রশিক্ষণার্থীদের করা প্রশ্ন ও তার সম্ভাব্য উত্তরঃ
বরিশাল

প্রশ্ন ১) সাইবার নিরাপত্তা কি? ইন্টারনেট জগতে নিরাপদ থাকব কিভাবে?

উত্তরঃ সাইবার নিরাপত্তা বলতে মূলত বুঝায় সচেতনতা এবং উপায় যার মাধ্যমে আমরা আমাদের ব্যক্তিগত তথ্য, কম্পিউটার, আমাদের বিভিন্ন ধরনের ডিজিটাল ডিভাইসকে হ্যাকিং ও বিভিন্ন ধরনের সাইবার আক্রমন থেকে নিরাপদ রাখতে পারি। অতএব, সাইবার নিরাপত্তা বলতে সব ধরনের তথ্য প্রযুক্তি নির্ভর ডিভাইস এর নিরাপদ ব্যবহার, তথ্য কে চুরির হাত থেকে রক্ষা, বিভিন্ন ধরনের ম্যালওয়্যার থেকে নিরাপদ রাখাকে বুঝায়। একটি মাউস ক্লিক সুগম করে দিতে পারে শক্তিশালী একটি ম্যালওয়্যার এর আগমন। তাই সাইবার নিরাপত্তার হুমকি গুলো সম্পর্কে স্পষ্ট ধারণা থাকলে, এই জগতে নিরাপদ থাকা সহজ হবে।

ইন্টারনেট জগতে নিরাপদ থাকতে করণীয়ঃ ইন্টারনেট জগতে নিজেকে নিরাপদ রাখতে নিম্নোক্ত বিষয়ে খেয়াল রাখতে হবে-

১। আপনার ডিভাইসের অপারেটিং সিস্টেম আপ টু ডেট রাখুন।
২। অবশ্যই এন্টিভাইরাস ব্যবহার করতে হবে। কখনই ক্র্যাক ভার্সন ব্যবহার করবেন না।
৪। ব্যক্তিগত তথ্য নেটওয়ার্ক সংযুক্ত যন্ত্রে না রাখাই ভাল।
৫। ক্রেডিট কার্ড ও ব্যাংকিং সহ সকল আর্থিক তথ্য কোথাও ইনপুট দেয়ার আগে কয়েকবার চেক করে নিন কোন ওয়েব সাইট এ দিচ্ছেন। পার্সোনাল ফায়ারওয়াল থাকলে ভাল এক্ষেত্রে।
৬। যে কোনো ধরনের বিজ্ঞাপন এ ক্লিক করবেন না।
৭। অপরিচিত ইমেইল খুলবেন না। শুধু মাত্র ইমেইল ওপেন করার কারনেই আপনার তথ্য চলে যেতে পারে হ্যাকার এর কাছে।
৮। পাসওয়ার্ড ব্রাউজারে অটো সেইভ করে না রাখাই ভাল।
৯। ফাইল ফরম্যাট দেখেই ভাববেন না ওপেন করার কথা। যেমন ধরুন একটি পি ডি এফ ফাইল ওপেন করলেও আপনার নেটওয়ার্ক এ ম্যালওয়্যার ইন্সটল হয়ে যেতে পারে আপনার অজান্তে।
১০। সব শেষে সামাজিক মাধ্যম ব্যবহারে সচেতন হতে হবে অনেক বেশি। অনেক সময় দেখা যায় ধর্মীয় অথবা মানবিক আবেগ কে পুঁজি করে, জঙ্গি অথবা চরমপন্থি গোষ্ঠী আপনার অজান্তে আপনাকে ব্যবহার করতে পারে। তাই এ বিষয়ে সচেতন হতে হবে।

প্রশ্ন ২) ডিনাইয়াল অফ সার্ভিস অ্যাটাক (DNS attack) কী?

ডিনাইয়াল অফ সার্ভিস অ্যাটাক (DNS attack) হলো কোনো কম্পিউটার সিস্টেমের কোনো রিসোর্স বা সেবার (service) প্রকৃত ব্যবহারকারীদের বাধা দেয়ার একটি কৌশল। কোনো কম্পিউটার বা সিস্টেম বা ইন্টারনেট ওয়েসাইটে এই আক্রমণ চালানোর মাধ্যমে ঐ সিস্টেম বা সাইটের যথাযথ কার্যক্রমকে ধীর গতির, বা অনেক ক্ষেত্রে পুরোপুরি বন্ধ করে দেয়া হয়। এই আক্রমণ চালানোর একটা বেশ জনপ্রিয় পদ্ধতি হলো বাইরে থেকে ঐ সিস্টেম বা সাইটের সাথে যোগাযোগের জন্য অসংখ্য বার্তা পাঠাতে থাকা। একটি বার্তা বিশ্লেষণ করতে করতে আরো বেশ কয়েকটি বার্তা যদি এসে পড়ে, তখন ঐ সিস্টেমটি আক্রমণকারীর পাঠানো বার্তা বিশ্লেষণেই ব্যস্ত থাকে এবং প্রকৃত ব্যবহারকারীরা ধীর গতির সম্মুখীন হন।

ডিনাইয়াল অফ সার্ভিস অ্যাটাক (DNS attack) এর প্রধান দুটি মাধ্যম হলোঃ

১. টার্গেট করা কম্পিউটারকে রিসেট করে দেয়া অথবা তার সীমিত রিসোর্সগুলোকে ব্যবহার করে অন্যদের ব্যবহারের অযোগ্য করে ফেলা।
২. আক্রমণের লক্ষ্য যে সিস্টেম বা সাইট, তার সাথে প্রকৃত ব্যবহারকারীদের যোগাযোগের মাধ্যম বন্ধ করে দেয়া।

প্রশ্ন ৩) এড ওয়্যার, ব্যাকডোর, কি-লগার, রুট কিট এবং স্পাইওয়্যার বলতে কি বুঝায়?

উত্তরঃ ক) এড ওয়্যারঃ এটি এক ধরণের ক্ষতিকর কম্পিউটার প্রোগ্রাম। তবে একে সব চেয়ে কম ক্ষতিকর ম্যালওয়্যার হিসেবে বিবেচনা করা হয়। এড ওয়্যার মূলত আপনাকে বিভিন্ন বিজ্ঞাপন দেখাবে। ভাল না জেনে কোন সফটওয়্যার ইন্সটল কিংবা ব্রাউজার প্লাগিন ইন্সটল করার মাধ্যমে এড ওয়্যার ঢুকে পড়বে আপনার সিস্টেমে। তাই ট্রাস্টেড সোর্স ছাড়া সফটওয়্যার ও প্লাগিন ইন্সটল কখনই ঠিক নয়।
খ) ব্যাকডোরঃ ব্যাকডোর এমন একটি ব্যবস্থা যার মাধ্যমে একজন হ্যাকার কিংবা স্প্যামার আপনার নেটওয়ার্ক সংযোগ ব্যবহার করতে পারবে।
গ) কি লগারঃ এটি এক ধরণের ক্ষতিকর কম্পিউটার প্রোগ্রাম যার মাধ্যমে কোণ ডিভাইস বা কম্পিউটারে টাইপকৃত সকল তথ্য ব্যবহারকারীর অজান্তেই অপর কোন ব্যক্তির নিয়ন্ত্রণে চলে যায়। কি লগারের কাজ হল কম্পিউটারে যা ই টাইপ করা হবে, ইউজার আই ডি, পাসওয়ার্ড অথবা যেকোনো স্পর্শকাতর তথ্য, সব কিছু রেকর্ড করবে এবং পরবর্তীতে কি লগারের প্রোগ্রামার কে পাঠিয়ে দিবে সব তথ্য।
ঘ) রুট কিটঃ রুট-কিট হলো ক্ষতিকর সফটওয়্যার। হ্যাকার যদি একবার আপনার মোবাইল বা, কম্পিউটারে এটি install করিয়ে দেয় তাহলে, এটি hide হয়ে (লুকিয়ে) থেকে কাজ করে যাবে। সাধারন সফটওয়্যার দেখা গেলেও রুট-কিট hide হয়ে চোখের আড়ালে কাজ করে। রুট-কিটের কাজ হলো-

- মোবাইল বা, কম্পিউটারে আপনি কখন কি করছেন সে তথ্য হ্যাকারের কাছে পাঠিয়ে দেয়া।
- ডিভাইসে Anti-Virus সফটওয়্যারকে অকার্যকর করে দেওয়া।
- ব্যবহারকারীর বিভিন্ন অ্যাকাউন্টের পাসওয়ার্ড জেনে তা হ্যাকারের কাছে পাঠিয়ে দেয়া ইত্যাদি।

এটি ভয়ানক ধরনের ম্যালওয্যার যা সহজে ধরা যায় না। এটি অন্য ম্যালওয্যার কে লুকিয়ে রাখতে সাহায্য করে।
ঙ) স্পাইওয্যারঃ এটি একধরণের কম্পিউটার ম্যালওয়্যার যার সাহায্যে কোন ব্যক্তির অ্যাকাউন্টে ইন্টারনেট এক্টিভিটিস থেকে শুরু করে সবকিছু গুপ্তচরবৃত্তি করা হয়।

প্রশ্নঃ ৪) বিভিন্ন সামাজিক যোগাযোগ মাধ্যমে গ্রুপ আইডি ব্যবহারের ক্ষেত্রে হ্যাকিং কিংবা নিরাপত্তার ঝুঁকি রয়েছে কিনা?

বিভিন্ন সামাজিক যোগাযোগ মাধ্যমে গ্রুপ আইডি বলতে এমন একটি সেবাকে বোঝানো হয়েছে যার মাধ্যমে এক গ্রুপের সদস্যরা একে অন্যের সঙ্গে বার্তা আদান-প্রদান করতে পারেন। ২০১৮ সালের অক্টোবরে গ্রুপের সদস্যদের মধ্যে রিয়েল টাইম যোগাযোগকে ত্বরান্বিত করতে ‘চ্যাট ইন ফেসবুক গ্রুপস’ অপশনটি চালু করেছিল ফেসবুক। সাধারণ ফেসবুক আইডির ন্যায় ‘ফেসবুক গ্রুপ’ ও একধরণের আইডি। তাই ফেসবুকের ন্যায় ‘ফেসবুক গ্রুপ’ ও হ্যাক হতে পারে। তাই সাধারণ ব্যক্তিগত ফেসবুক আইডির ন্যায় ‘ফেসবুক গ্রুপ’ এর জন্য নিরাপত্তামূলক ফিচারসমূহ ব্যবহার করুন।

প্রশ্ন ৫) যদি কারো ছবি ব্যবহার করে ফেইক অ্যাকাউন্ট খুলে তাহলে এর আইনগত প্রতিকার কী?

উত্তরঃ ফেসবুক কারো নাম বা ছবি ব্যবহার করে কেউ ফেইক একাউন্ট খুললে তা একধরণের পরিচয় প্রতারণা বা ছদ্মবেশ ধারণের শামিল। এ বিষয়ে বাংলাদেশের প্রচলিত আইনে শাস্তির বিধান রয়েছে।

আইনগত প্রতিকারঃ ডিজিটাল নিরাপত্তা আইন ২০১৮ এর ২৪ ধারা অনুযায়ী পরিচয় প্রতারণা বা ছদ্মবেশ ধারন একটি আমলযোগ্য অপরাধ। সুতরাং ডিজিটাল নিরাপত্তা আইনে প্রয়োজনীয় আইনগত ব্যবস্থা গ্রহন করা যাবে। যদি কোনো ব্যক্তি ২৪ ধারা এর অধীন কোনো অপরাধ সংঘটন করেন, তাহা হইলে তিনি অনধিক ৫ (পাঁচ) বৎসর কারাদণ্ডে, বা অনধিক ৫ (পাঁচ) লক্ষ টাকা অর্থদণ্ডে, বা উভয় দণ্ডে দণ্ডিত হইবেন। উল্লিখিত অপরাধ দ্বিতীয়বার বা পুনঃপুন সংঘটন করেন, তাহা হইলে তিনি অনধিক ৭ (সাত) বৎসর কারাদণ্ডে, বা অনধিক ১০ (দশ) লক্ষ টাকা অর্থদণ্ডে, বা উভয় দণ্ডে দণ্ডিত হইবেন।