প্রশিক্ষণার্থীদের প্রশ্ন ও তার সম্ভাব্য উত্তরঃ
চাঁপাইনবাবগঞ্জ

প্রশ্ন ১) সাইবার বুলিং কী? কারা এবং কোন কোন উপায়ে এর শিকার হয়ে থাকে? সাইবার বুলিং এর সামাজিক প্রভাব কি? সাইবার বুলিং হতে শিশুদের কিভাবে নিরাপদ রাখা যায়?

উত্তরঃ সাইবার বুলিং একধরণের অনলাইন ভিত্তিক অপরাধ। মূলত সাইবার বুলিং' হচ্ছে অনলাইনে কোনো শিশু বা ব্যক্তিকে প্রলুব্ধ বা হেয় প্রতিপন্ন করা, ভয় দেখানো এবং মানসিক নির্যাতন করা। তবে, অধিকাংশ ক্ষেত্রে শিশুরাই সাইবার বুলিং এর শিকার হয়ে থাকে।

যেভাবে সাইবার বুলিং করা হয়ে থাকেঃ শুরুতে কিশোর-কিশোরীরাই কেবল এ ধরনের কাজে জড়িত থাকে ভেবে বুলিং সংজ্ঞায়িত করা হলেও পরে দেখা যায় অনেক ক্ষেত্রে স্বনামে বা ফেক আইডির আড়ালে প্রাপ্তবয়স্ক অনেকেও এ ধরনের হীন কাজে জড়িত থাকে।সাইবার বুলিংয়ের ঘটনা বেশির ভাগ ক্ষেত্রে সামাজিক যোগাযোগ মাধ্যমগুলোতে ঘটলেও ফোনে কিংবা ইমেইলেও অনেক সময় এ ধরনের নির্যাতনের ঘটনা ঘটে থাকে।

সাইবার বুলিং এর সামাজিক প্রভাবঃ সাইবার বুলিংয়ের কোনো সূত্র পাওয়া গেলে বা এ ধরনের ঘটনা একবার ঘটলে বিকৃত ও অসুস্থ মানসিকতার আরো অনেকের কাছে আক্রান্ত ব্যক্তির খোঁজ বা যোগাযোগের তথ্য চলে যায় বলে ধীরে ধীরে এর মাত্রা বাড়তেই থাকে। এর ক্রমবর্ধমান চাপে শিশুদের মাঝে হতাশা,লেখাপড়ার প্রতি অনীহা, ইনসমনিয়া থেকে শুরু করে আত্মহত্যার প্রবণতা পর্যন্ত তৈরি হতে পারে।

সাইবার বুলিং থেকে শিশুদের কিভাবে নিরাপদ রাখার উপায়ঃ সাইবার বুলিং প্রতিরোধে এ বিষয়ে মা-বাবার ধারণা থাকা, সন্তান ইন্টারনেটে (কম্পিউটার এবং মোবাইলে) কী করছে তা জানা এবং সন্তানদের সাথে বন্ধুসুলভ সুসম্পর্ক বজায় রাখা উচিত। এছাড়াও কেউ সাইবার বুলিং এর শিকার হলে সাথে সাথেই বিষয়টি অভিভাবককে জানানো উচিত।

প্রশ্ন ২) Covid-19 এর কারণে বর্তমানে শিক্ষা গ্রহণের জন্য আমরা প্রায় সবাই তথ্য প্রযুক্তির উপর নির্ভরশীল হয়ে পড়েছি। এ ক্ষেত্রে আমাদের মাঝে অনেকে জেনে অথবা না জেনে বিভিন্ন ধরনের অপরাধে জড়িয়ে পড়েছে । এ ব্যাপারে আমরা কিভাবে তাদের সচেতন করতে পারি অথবা কীভাবে তাদেরকে এসব অনৈতিক কাজ থেকে ফিরিয়ে আনতে পারি?

উত্তরঃ বর্তমান Covid-19 পরিস্থিতির কারণে আমাদের মধ্যে তথ্য প্রযুক্তির উপর নির্ভরশীলতা বেড়ে যাবার পাশাপাশি সাইবার অপরাধের সাথে যুক্ত হবার প্রবণতাও বেড়েছে। অনেকেই জেনে বা না জেনেই সাইবার অপরাধের সাথে যুক্ত হচ্ছে। তবে এসব সাইবার অপরাধ থেকে নিজেদের নিরাপদ রাখ সবার আগে প্রয়োজন ব্যক্তিগত সচেতনতা। এর পরই আসবে পারিবারিক ও প্রাতিষ্ঠানিক শিক্ষা প্রদান, প্রযুক্তি বিষয়ে সক্ষমতা গড়ে তোলা এবং এবং আইনের কঠোর প্রয়োগ। তবে, সাইবার অপরাধ থেকে বাঁচতে থামো, ভাবো, সংযোগ দাও (Stop, Think, Connect) মূলনীতি অনুসরণ করা বা মেনে চলা খুবই গুরুত্বপূর্ণ। ইন্টারনেটে কোন কিছু শেয়ার করার পূর্বে সে বিষয়ের সত্যতা সম্পর্কে নিশ্চিত হতে হবে। এছাড়াও ব্যক্তিগত পর্যায়ে নিম্নোক্ত বিষয়সমূহ অনুসরণ করতে হবে-

১. শক্তিশালী পাসওয়ার্ড ব্যবহার করতে হবে। প্রতি তিন মাস অন্তর পাসওয়ার্ড পরিবর্তন করতে হবে। নিজের ব্যক্তিগত একাউন্টসমূহের পাসওয়ার্ড কখনোই কারো সাথে শেয়ার করা যাবেনা।
২. নিজের কম্পিউটার বা অন্য কোন ডিভাইসে লাইসেন্সযুক্ত এন্টিভাইরাস সফটওয়ার ব্যবহার করতে হবে। ডিভাইসের পাসওয়ার্ড কারো সাথেই শেয়ার করা যাবেনা।

৩. ই-মেইল বা অন্য কোন অনলাইন একাউন্ট আপডেট করার জন্য কোন অপরিচিত লিংকে ক্লিক করা যাবেনা। ই-মেইল বা মেসেজের মাধ্যমে কউ কোন অর্থ প্রাপ্তি বা লটারী জেতার কথা বলতে তা বিশ্বাস করা যাবেনা।
৪. ব্রাউজার নিয়মিত হালনাগাদ করতে হবে এবং কোন ওয়েবসাইটে লগ-ইন করার পূর্বে ওয়েব এড্রেস https/ secure কিনা তা যাচাই করে নিন। শিক্ষামূলক ও নির্ভরযোগ্য ওয়েবসাইটসমূহ ব্যবহার করুন।
৫. অনলাইন একাউন্টে ওয়ান টাইম পাসওয়ার্ড বা টু ফ্যাক্টর অথেনটিকেশন সিস্টেম চালু করে নিন।
৬. সামাজিক যোগাযোগ মাধ্যমে বা অন্যান্য সোশ্যাল মিডিয়া একাউন্টের নিরাপত্তা সেটিংসগুলো নিয়মিত যাচাই করুন।
৭. কারো প্ররোচনায় বা অনুরোধ যাই হোক না কেন ওয়েব ক্যামেরা বা অন্য কোন ডিভাইসের ক্যামেরার সামনে কোন ধরণের শারীরিক অঙ্গ ভঙ্গি করা থেকে বিরত থাকতে হবে।
৮. পাবলিক প্লেসে ফ্রি ওয়াইফাই নেটওয়ার্ক ব্যবহার থেকে বিরত থাকুন। কোন ভাবেই পাবলিক ওয়াইফাই নেটওয়ার্ক ব্যবহার করে অনলাইনে আর্থিক লেনদেন করবেন না।
৯. নিজের মোবাইল ব্যাংকিং একাউন্টের পিন নম্বর বা একাউন্ট ব্যালেন্স কোন ভাবেই অপর কাউকে জানাবেন না। কখনো কারো কথায় বা নির্দেশনায় কোন নম্বরে ডায়াল করা বা ব্যক্তিগত তথ্য প্রদান করা থেকে বিরত থাকুন।
১০. সব সময় নিরাপদ ও শিক্ষামূলক ওয়েবসাইটসমূহ ভিজিট করা।
১১. ইন্টারনেটে বিভিন্ন ধরণের গেমস খেলা থেকে বিরত থাকা।

প্রশ্ন ৩) সাইবার অপরাধের শিকার হলে আমাদের করনীয় কী?

উত্তরঃ কোন ব্যক্তি যদি সাইবার অপরাধ করে থাকে তবে এক্ষেত্রে প্রতিকারের উপায় রয়েছে। এক্ষেত্রে সাইবার অপারধের শিকার ব্যক্তিকে অবশ্যই যথেষ্ট তথ্য-প্রমাণসহ অবিলম্বে অপরাধ সংঘটনের বিষয়টি সংশ্লিষ্ট আইন প্রয়োগকারী সংস্থা বা কর্তৃপক্ষকে জানাতে হবে। এছাড়াও ডিজিটাল নিরাপত্তা আইন, ২০১৮ অনুসারে সংশ্লিষ্ট ব্যক্তি বা ব্যক্তিগণের বিরুদ্ধে মামলা করতে পারেন। তবে এসব ক্ষেত্রে যত বেশি সম্ভব তথ্য-প্রমাণাদি সংগ্রহ করে রাখুন। তথ্য প্রমাণাদি সংগ্রহের ক্ষেত্রে-

১. সংশিষ্ট আইডির ইউ আর এলসহ স্ক্রীনশট সংগ্রহ করে রাখুন।
২. পোস্টের তারিখ ও সময়সহ ইউ আর এল সংবলিত তথ্যের এক বা একাধিক কপি প্রিন্ট করে রাখুন।
৩. কোন ভাবেই সংশ্লিষ্ট তথ্য প্রমাণ মুছে ফেলবেন না বা ডিলিট করবেন না।

এছাড়াও আইন প্রয়োগকারী সংস্থাসমূহের পাশাপাশি আপনি সাইবার ট্রাইব্যুনালে পিটিশন মামলা দায়ের করতে পারেন। অন্যদিকে টেলিযোগাযোগ নিয়ন্ত্রক সংস্থা বিটিআরসি, পুলিশের কাউন্টার টেরোরিজম ইউনিটে ও অভিযোগ করতে পারেন, সমাধান মিলবে। এছাড়াও, ৩৩৩, ৯৯৯ ইত্যাদি নাম্বারে আপনার হয়রানীর বিষয় জানিয়ে তাদের নিকট অভিযোগ দায়েরের বিষয়ে সহায়তা চাইতে পারেন।

প্রশ্ন ৪) কোন ব্যক্তি আমার ফেসবুকের পাসওয়ার্ড বা অন্য কোন আইডি বা অনলাইন একাউন্টের পাসওয়ার্ড জেনে গেলে আমার করণীয় কি?

উত্তরঃ এতে আপনার ফেসবুক বা বা অন্য যেকোন আইডি বা অনলাইন একাউন্টের নিয়ন্ত্রন খুব সহজেই অন্য কেউ নিয়ে নিতে পারে। এক্ষেত্রে আপনার আইডির মাধ্যমে যেকোন ধরণের সাইবার অপারাধ সংগঠিত হবার ঝুকি রয়েছে। কোন কারণে ফেসবুক বা অন্য যেকোন ধরনের সামাজিক যোগাযোগ মাধ্যমে বা অনলাইন একাউন্টের পাসওয়ার্ড জেনে গেলে-

১. সাথে সাথে আপনার ফেসবুক বা অন্য কোন আইডি বা অনলাইন একাউন্টের পাসওয়ার্ড পরিবর্তন করে ফেলুন।
২. আপনার আইডিতে ‘টু ফ্যাক্টর অথেন্টিকেশন’ সিস্টেম চালু করে নিন।
৩. অন্য সব ডিভাইস হতে আপনার আইডি লগ আউট করে নিন।

৪. নাম্বার, ক্যারেক্টার এবং চিহ্ন ব্যবহার করে নিজের ফেসবুকের বা অন্য কোন সামাজিক যোগাযোগ মাধ্যমের জন্য শক্তিশালী পাসওয়ার্ড তৈরি করে নিন।

এছাড়া বিশেষভাবে মনে রাখতে হবে যে, যত কাছের মানুষই হোক না কেন, কখনোই তার সাথে আপনার ফেসবুক বা অন্য যেকোন ধরনের সামাজিক যোগাযোগ মাধ্যমে বা ক্রেডিট/ডেবিট কার্ড বা ই-মেইলের পাসওয়ার্ড শেয়ার করা যাবেনা।