প্রশিক্ষণার্থীদের প্রশ্ন ও তার সম্ভাব্য উত্তরঃ
পটুয়াখালী

প্রশ্ন ১) সাইবার বুলিং কী? সাইবার বুলিং হতে কিভাবে নিরাপদ থাকা 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। 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 থেকে শিশুদের কিভাবে নিরাপদ রাখার উপায়ঃ সাইবার বুলিংয়ের ফলে শিশুর মাঝে হতাশা, পড়াশুনার প্রতি অনীহা, ইনসমনিয়া থেকে শুরু করে আত্মহত্যার প্রবণতা পর্যন্ত তৈরি হতে পারে। 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) ফেসবুক আইডি থেকে ছবি নিয়ে যদি ভুয়া ফেসবুক আইডি কিংবা Fake conversation বানানো হয় তখন কি করতে পারি?
উত্তরঃ অন্য কারোর ছবি নাম দিয়ে অনেকেই ফেসবুক আইডি খুলে বিভিন্ন অপ্রীতিকর পোস্ট বা কথোপকথনের মাধ্যমে অপর ব্যক্তিকে বিরক্ত করে থাকে। ফেসবুকে আপনার নাম বা ছবি ব্যবহার করে কেউ ফেক আইডি খুললে আপনি ফেসবুক এ রিপোর্ট করার মাধ্যমে তা বন্ধ করতে পারেন। এক্ষেত্রে নিম্নোক্ত পদ্ধতিতে রিপোর্ট করবেন-

১. প্রথমে যেই আইডিতে রিপোর্ট করতে চান তার প্রোফাইলে যান। এবার ওপর থেকে More অপশনে ক্লিক করুন।
২. এবার Find support or report profile ক্লিক করুন।
৩. এখানে নিম্নোক্ত অপশন গুলো পাবেন -

ক) Pretending to be someone: যদি কেউ আপনার নামে ফেক ফেসবুক আইডি খোলে তাহলে Pretending to be someone ক্লিক করে নিচে থেকে **me** সিলেক্ট করুন।

খ) Fake account: আপনার নাম ব্যবহার করে কোন আইডিকে যদি ভুয়া হিসেবে চিহ্নিত করতে পারেন তবে উক্ত আইডিকে Fake account অপশনে গিয়ে রিপোর্ট করতে পারেন।

গ) Fake name: যদি কেউ আপনার নাম বা ছবি ব্যবহার করে আইডি তৈরি করে কিংবা কোন অশ্লীল নামে আইডি তৈরী করে আপনাকে ফ্রেন্ড রিকুয়েস্ট পাঠায় তখন তাকে Fake name অপশনে গিয়ে রিপোর্ট করতে পারেন।

প্রশ্ন ৩) ই-মেইল স্পুফিং কী? এর শিকার হলে করণীয় কী?

উত্তরঃ স্পুফ (Spoof) অর্থ প্রতারণা করা বা ধোঁকা দেওয়া। সাইবার জগতে স্পুফিং(Spoofing) মানে কোন অনলাইন ব্যবহারকারি কে বা কম্পিউটার সিস্টেম কে ধোঁকা দেওয়া। স্পুফিং (Spoofing) এর অনেক পদ্ধতি রয়েছে তবে সবচেয়ে বেশি স্পুফিং(Spoofing) ইমেইলের মাধ্যমে করা হয় । নিজের তথ্যসমূহ আড়াল করে অন্যের Email Address ব্যবহার করে কাউকে ইমেইল করার নামই Email Spoofing। ইমেইল স্পুফিং খুব সহজ একটি পদ্ধতি হলেও ইন্টারনেটে সব থেকে ভয়ংকর ক্রাইম এর মধ্যে এটি একটি অন্যতম। বর্তমানে যত ক্রেডিট কার্ড ও পেপাল একাউন্ট হ্যাক করার ক্ষেত্রে এই ইমেইল স্পুফিং এর ব্যবহার করা হয়ে থাকে।

কিভাবে ইমেইল স্পুফিং (Spoofing) করা হয়?

হ্যাকাররা বিভিন্ন ধরণের অ্যাপস, ওয়েবসাইট এবং টুলস দিয়ে ইমেইল স্পুফিং করে থাকে । স্পুফ করা মেইলে মেইল অ্যাড্রেস সহ, মেইলটি কোথা থেকে এসেছে, মেইলকারীর নাম এইসবই স্পুফ করা হয়। এক্ষেত্রে ভিক্টিম প্রাপ্ত ই-মেইলের রিপ্লাই দিলে মেইলটি সাধারণত আরেক মেইল অ্যাড্রেসে চলে যায় যার মাধ্যমে হ্যাকার ভিক্টিমের ইউজার নেম, পাসওয়ার্ড অন্যান্য গোপনীয় তথ্য যেমন ব্যাংক অ্যাকাউন্ট নম্বর, এক্সপায়ার ডেট, সিকিউরিটি কী ইত্যাদি পেয়ে যায়। তাছাড়া মেইল স্পুফিং করার সময় সার্ভার আইপি অ্যাড্রেস ও নকল করা হয়, সত্যি বলতে কোন এক্সপার্ট যদি মেইল স্পুফ করে, সেটা বোঝা অনেক বেশি কষ্টের ব্যাপার হয়ে যায় যতক্ষণ পর্যন্ত ঐ আসল ব্যাক্তির নিকট হতে ই-মেইল প্রেরণের বিষয়ে নিশ্চিত হওয়া যায়। ই-মেইল স্পুফিং এর সময় হ্যাকাররা তাদের নিজস্ব SMTP ("Simple Mail Transfer Protocol") ব্যবহার করে স্পাম মেসেজ পাঠিয়ে থাকে।

করণীয়ঃ

১) অজানা বা অদ্ভুত ঠিকানা (spoofed email addresses) থেকে আসা ই-মেইল গুলো বিশেষ ভাবে লক্ষ্য করুন। এসব ই-মেইলের প্রেরকের নাম ও ই-মেইল ঠিকানা খেয়াল করুন। আপনি কোন উদ্বেগ ছাড়াই ই-মেইলটি পড়তে পারবেন। তবে এ জাতীয় ই-মেইলের সাথে থাকা লিঙ্ক ও সংযুক্তি পরিহার করুন।

২) আক্রমণকারী অনেক সময় এমন সব ই-মেইলের ঠিকানা ব্যবহার করে যা দেখতে পরিচিত বা বৈধ মনে হবে। যাদের সাথে ব্যবহারকারী প্রায়ই যোগাযোগ করেন এরকম ঠিকানা থেকেও ফিশিং ই-মেইল পেতে পারেন। সেক্ষেত্রে বানান, বিরামচিহ্ন এবং ব্যাকরণগত ত্রুটি লক্ষ্য করুন।

৩) সন্দেহজনক ই-মেইলের সংযুক্তি ও লিঙ্ক এড়িয়ে চলুন

৪) সর্বদা সক্রিয় ও হালনাগাদ অ্যান্টি-ভাইরাস সফ্টওয়ার ব্যবহার করুন।

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।

আইন প্রয়োগকারী সংস্থাসমূহের পাশাপাশি আপনি সাইবার ট্রাইব্যুনালে পিটিশন মামলা দায়ের করতে পারেন। অন্যদিকে টেলিযোগাযোগ নিয়ন্ত্রক সংস্থা বিটিআরসিতে অভিযোগ করতে পারেন, সমাধান মিলবে। এছাড়াও পুলিশের কাউন্টার টেরোরিজম ইউনিট, 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 আইডি বা বা অন্য কোন 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।
5. 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 করবেন না।