প্রশিক্ষণার্থীদের করা প্রশ্ন ও তার সম্ভাব্য উত্তরঃ
বরগুনা

প্রশ্ন ১) কিভাবে ই-মেইল স্পুফিং (Spoofing) করা হয়? আমরা ই-মেইল স্পুফিং (Spoofing) থেকে কিভাবে রক্ষা পেতে পারি?

উত্তরঃ 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 ২) কোন এ্যাপের Crack ভার্সন ডাউনলোড করা নিরাপদ কিনা?

উত্তরঃ এ্যাপ ডাউনলোড এর সময় কোন এ্যাপের Crack ভার্সন ডাউনলোড করা নিরাপদ নয়। যেকোন এ্যাপ ইনস্টলের ক্ষেত্রে এক্সেস প্রদানের সময় অনুমতি প্রদান করতে হয়। এ সময় এধরণের অনুমতি প্রদানের ক্ষেত্রে যাচাই-বাছাই করে নেয়া উচিত। এ্যাপ ডাউনলোড এর ক্ষেত্রে সবসময় লাইসেন্সড এ্যাপ ডাউনলোড করতে হবে। কোন ফ্রি এ্যাপ ডাউনলোড এবং ব্যবহার করার আগে অবশ্যই সচেতন হতে হবে।

প্রশ্ন ৩) সাইবার অপরাধ থেকে আমরা কিভাবে নিজেদের নিরাপদ রাখতে পারি?

উত্তরঃ সাইবার অপরাধ থেকে নিজেদের নিরাপদ রাখতে হলে সবার আগে প্রয়োজন ব্যক্তিগত সচেতনতা তৈরি। 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 কেউ 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।

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।

প্রশ্ন ৪) আমাদের আশে পাশে কেউ সাইবার অপরাধ সংঘটিত করলে 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 ৫) কেউ যদি আমার অ্যাকাউন্ট হ্যাক করে তাহলে এর আইনী প্রতিকার কী?

উত্তরঃ ফেসবুক একাউন্ট সুরক্ষা রাখার সব ধরনের ব্যবস্থা করে রাখলেও অনেক সময় একাউন্ট হ্যাক হয়ে যায়। তাই হ্যাক হওয়া মাত্রই আপনি প্রয়োজনীয় আইনী পদক্ষেপ গ্রহণ করতে পারেন।

আইনগত প্রতিকারঃ

ডিজিটাল নিরাপত্তা আইন ২০১৮ এর ৩৪ ধারা অনুযায়ী হ্যাকিং একটি আমলযোগ্য অপরাধ। সুতরাং ডিজিটাল নিরাপত্তা আইন অনুসারে প্রয়োজনীয় আইনগত ব্যবস্থা গ্রহণ করা যাবে।