২.৫ পাসওয়ার্ড এবং এ সম্পর্কিত কিছু তথ্য

পাসওয়ার্ড আমাদের ডিভাইস ও ডাটা সিকিরিটির অন্যতম ও প্রথম ধাপ। তাই একটি জটিল শক্তিশালী ও দীর্ঘ পাসওয়ার্ড ব্যবহার করা উচিৎ। হ্যাকাররা বা সাইবার ক্রিমিনালরা আপনার অ্যাকাউন্টগুলিতে প্রবেশ করার জন্য আপনার পাসওয়ার্ডটি ধারনা করার চেষ্টা করে এবং এর জন্য এরা একাধিক পদ্ধতি ব্যবহার করে। সর্বাধিক ব্যবহৃত পদ্ধতি হ'ল, আপনার সাথে সম্পর্ক যুক্ত বিভিন্ন অক্ষর, সংখ্যা এবং প্রতীক ম্যানুয়ালি টাইপ করা। আরও সবচেয়ে উন্নত পদ্ধতিটি হল "ব্রুট ফোর্স আক্রমণ"। এই কৌশলটিতে, একটি কম্পিউটার প্রোগ্রাম আপনার পাসওয়ার্ডটি ক্র্যাক করার জন্য খুব দ্রুত অক্ষর, সংখ্যা এবং প্রতীকগুলির সম্ভাব্য সংমিশ্রণ (কম্বিনেশন) তৈরি করে এবং তা আপনার অ্যাকাউন্ট পাসওয়ার্ডটির সাথে তুলনা করে। আপনার পাসওয়ার্ডটি যত বড় এবং জটিল হবে, এই প্রক্রিয়াটি সম্পন্ন হতে ততো বেশি সময় নেবে। তিনটি অক্ষরযুক্ত পাসওয়ার্ডগুলি ক্র্যাক করতে এক সেকেন্ডেরও কম সময় লাগে।

ব্যক্তিগত তথ্য এড়িয়ে চলুনঃ

আপনার সম্পর্কে যেসব তথ্য সহজে জোগাড় করা সম্ভব সেসব তথ্য যেমনঃ জন্মদিন, কওন বার্ষিকী, ঠিকানা, জন্মের শহর, উচ্চ বিদ্যালয় এবং পোষা প্রাণীর' নাম ইত্যাদি পাসওয়ার্ডে ব্যবহার না করা। আবার যদি কোন অ্যাকাউন্ট খুলতে সিকিউরিটি প্রশ্ন ও উত্তর দিতে হয় সেইসব ক্ষেত্রেও এই সকল তথ্য ও আপনার সোশ্যাল মিডিয়াতে পাওয়া যায় এমন সব তথ্য ব্যবহার এড়িয়ে চলুন।

পাসওয়ার্ডটি বড় করুনঃ

আগে যেমনটা বলেছি ব্রুট ফোর্স আক্রমণ মাত্র এক সেকেন্ডেরও কম সময় লাগে। পাসওয়ার্ড তৈরির পূর্বে এটা অবশ্যই মাথায় রাখবেন। একটি বড় বা লং পাসওয়ার্ড আপনার অ্যাকাউন্ট হ্যাকের ঝুঁকি কমায়।

পুরাতন পাসওয়ার্ড বারবার ব্যবহার না করাঃ

হ্যাকাররা যখন বড় আকারের হ্যাকগুলি সম্পন্ন করে, যেমন জনপ্রিয় ই-মেইল সার্ভার ইয়াহু ও এর অন্যান্য সার্ভিস টাম্বলার, ফ্যান্টাসি ও ফ্লিকারও হ্যাক করে এবং এর সমস্ত ই-মেইল অ্যাড্রেস এবং পাসওয়ার্ডগুলি অনলাইনে ফাঁস করে দেয়। যদি আপনার অ্যাকাউন্টটি এর মধ্যে থাকে এবং আপনি এই ইমেল ঠিকানা এবং পাসওয়ার্ডটি অন্যান্য সাইটগুলিতে ব্যবহার করেন তবে আপনার হ্যাক হওয়া তথ্য দিয়ে সহজেই ওই সব অ্যাকাউন্টে প্রবেশ করে ফেলতে পারে। তাই একই পাসওয়ার্ড বিভিন্ন সার্ভিস বা সাইটে ব্যবহার না করে অন্যান্য পাসওয়ার্ড ব্যবহার করুন।

পাসওয়ার্ডের গোপনীয়তাঃ

আপনার পাসওয়ার্ড অন্য কারও সাথে শেয়ার করবেন না। যদি অন্য কেউ আপনার সামনে থাকেন ও আপনার ডিভাইসটি (যেমনঃ কম্পিউটারের কীবোর্ড বা ফোন ইত্যাদি) তার নজরে থাকে তবে আপনার পাসওয়ার্ডটি ডিভাইসে টাইপ করবেন না। এবং আপনার অফিস কম্পিউটারে স্টিকি নোটে আপনার পাসওয়ার্ডটি লাগিয়ে রাখবেন না।

আপনার পাসওয়ার্ডটি নিদিষ্ট সময় পর পর বদলানঃ

আপনার তথ্য যত সংবেদনশীল বা গোপনীয়, তত বেশি বার আপনার পাসওয়ার্ড নিদিষ্ট সময় পর পর পরিবর্তন করা উচিত। একবার পরিবর্তিত পাসওয়ার্ডটি দীর্ঘ সময়ের জন্য পুনরায় ব্যবহার করবেন না।

জটিল ও শক্তিশালী পাসওয়ার্ড তৈরির কিছু টেকনিকঃ

সংখ্যা, প্রতীক বা চিহ্ন, ছোট বা বড় হাতের শব্দ ব্যবহারঃ

পাসওয়ার্ডকে শক্ত বা জটিল করতে শব্দের সাথে সংখ্যা ও প্রতীক ব্যবহার করুন যেমন ও (O) এর পরিবর্তে শুন্য(0-), এ (A-a) এর পরিবর্তে @ চিহ্ন অথবা ই (E) এর পরিবর্তে ৩ ইত্যাদি ব্যবহার করতে পারেন। আবার যদি আপনার পাসওয়ার্ডটি যদি কোন বাক্য হয় তবে বাক্যের প্রতিটি শব্দের প্রথম অক্ষর বড় হাতের করতে পারেন। উদাহরণ সরূপ ILik3Pink@ppl3 – I like pink apple. এটি একটি যুক্তিহীন বাক্য কিন্তু সহজে মনে রাখার মতো আবার একটি স্ট্রং পাস্বওয়ার্ড।

একটি অযৌক্তিক বাক্য দিয়ে পাসওয়ার্ড তৈরি করুনঃ

দীর্ঘ বা লং (Long) পাসওয়ার্ড ভাল; তাই অযৌক্তিক এলোমেলো শব্দ এবং বাক্যাংশ দিয়ে দীর্ঘ পাসওয়ার্ড তৈরি করা ভাল। যদি আপনার পাসওয়ার্ডের, বাক্যের অক্ষরগুলির কম্বিনেশন ডিকশনারিতে না থাকে বা সাহিত্যে প্রকাশিত কোন বিখ্যাত উক্তিএ,না হয় কিংবা ব্যাকরণগতভাবে সঠিক না হয়, তবে এই পাসওয়ার্ডগুলি ক্র্যাক করা কঠিন হয়। এছাড়াও কীবোর্ডে সিকয়েন্সিয়াল অক্ষরগুলি ব্যবহার এক বারেই করবেন না যেমন 12345,54321, qwert, ‘;lkj, zxcvb ইত্যাদি।