অধ্যায় ঃ-০১

সাইবার নিরাপত্তা

ভুমিকাঃ

কম্পিউটার ও ইন্টারনেট কেন্দ্রিক তথ্যব্যাবস্থা, যার মধ্যে কম্পিউটার সিস্টেম, সার্ভার, ওয়ার্ক স্টেশন, টার্মিনাল, স্টোরেজ মিডিয়া, কমিউনিকেশন ডিভাইস, নেটওয়ার্ক রিসোর্স থাকে এবং কম্পিউটার ডাটা আদান প্রদান প্রক্রিয়া বিদ্যমান থাকে, তাকেই সহজ ভাষায় সাইবার জগৎ বলা হয় ।

সাইবার জগতের কথাটি যখন বলা হয়, তখন সাভাবিক ভাবেই এ জগতের নিরাপত্তার প্রসঙ্গটিও চলে আসে অত্যন্ত গুরুত্বে সঙ্গে। নিরাপত্তা কথাটি এ জন্যই আসে যে, সারা দুনিয়ায় এখন সাইবার অপরাধ সংঘটনের নজির দিন দিন বাড়ছে।

কম্পিউটার সিস্টেমে নেটওয়ার্ক ব্যবহার করে কোন ব্যক্তি তার কাজের বিরত রাখা বা কোন কাজ বাধ্য করা, কোন জনগোষ্ঠীকে ভীতি প্রদর্শন করা, প্রতারণা করা ইত্যাদি এ ধরনের আরও অনেক বিষয় আছে, যা সাইবার অপরাধ বলে গণ্য হয়। প্রযুক্তি ভিত্তিক কার্যক্রম দ্রুত বিস্তার লাভ করায়, সাইবার নিরাপত্তা কথাটি এখন মানুষের মুখে মুখে উচ্চারিত হচ্ছে। সাইবার নিরাপত্তা বলতে মূলত বোঝায় কিছু সচেতনতা,কিছু উপায় যার মাধ্যমে ব্যক্তিগত তথ্য কম্পিউটার বিভিন্ন ধরনের ডিজিটাল ডিভাইস কম্পিউটার সিস্টেম ইত্যাদি হ্যাকিং ও বিভিন্ন ধরনের আক্রমণ থেকে নিরাপদ রাখা।

সাইবার নিরাপত্তাঃ

ইন্টারনেট আগমনের পূর্বে, তথ্য সংরক্ষণ করার জন্য আলাদা তথ্য কেন্দ্র ছিল। এসকল তথ্য কেন্দ্রে অ্যাক্সেস খুব নিয়ন্ত্রিত ছিল। শুধুমাত্র অফিসের দায়িত্বে থাকা ব্যক্তিরা ডাটা এক্সেস করতে পারত। বর্তমান ইন্টারনেট অ্যাক্সেস সবকিছুতেই বিদ্যমান। এমনকি প্রত্যেকটি স্মার্ট ডিভাইস থাকে ইন্টারনেট জগতের সাথে সংযুক্ত। সাইবার নিরাপত্তা হলো সব ধরনের তথ্য প্রযুক্তি নির্ভর ডিভাইসের নিরাপদ ব্যবহার, তথ্যকে চুরির হাত থেকে রক্ষা, বিভিন্ন ধরনের ম্যালওয়্যার থেকে নিরাপদ থাকা ইত্যাদি। সাইবার নিরাপত্তার মাধ্যমে নিশ্চিত করা হয়, জেনো বিভিন্ন প্রকার ডিভাইস এবং তার অপব্যবহার না করা হয়। সাইবার নিরাপত্তা সফটওয়্যার এবং হার্ডওয়্যার উভয় ক্ষেত্রে প্রযোজ্য হয়ে থাকে।

সাইবার নিরাপত্তার উপাদানঃ

সাইবার নিরাপত্তা নিশ্চিত করার জন্য বিভিন্ন তথ্য সিস্টেম সমূহের নিরাপত্তা নিশ্চিত করতে হবে। সাইবার নিরাপত্তার প্রধান উপাদান সমূহ হলো---

১। আবেদন নিরাপত্তা

২। তথ্য নিরাপত্তা

৩। নেটওয়ার্ক নিরাপত্তা

৪। অপারেশন নিরাপত্তা

৫। সর্বশেষ ব্যবহারকারীর শিক্ষা ইত্যাদি।

সাইবার নিরাপত্তায় সবচেয়ে সমস্যাযুক্ত উপাদান গুলোর মধ্যে একটি হচ্ছে নিরাপত্তা ঝুঁকি গুলোর ক্রমাগত ক্রমবর্ধমান প্রকৃতি। ঐতিহ্যগত দৃষ্টিভঙ্গির মাধ্যমে গুরুত্বপূর্ণ সিস্টেমের উপাদান গুলো তে সম্পদ গুলো ফোকাস করা হয় এবং সর্বাধিক পরিচিত হুমকি গুলোর বিরুদ্ধে সুরক্ষা প্রদান করা হয় যার অর্থ হলো কম বিপদজনক ঝুঁকিগুলোর বিরুদ্ধে সৃষ্টিগুলোকে অনির্বাচিত করা এবং সিস্টেমগুলো রক্ষা না করা।

বর্তমান পরিবেশ মোকাবেলা করার জন্য অ্যাডভাইজারি সংস্থাগুলো আরো সক্রিয় এবং অভিযোজিত পদ্ধতির প্রচার করছে। উদাহরণস্বরূপ, ন্যাশনাল ইনস্টিটিউট অব স্ট্যান্ডার্ডস এন্ড টেকনোলজি ঝুঁকি মূল্যায়ন কাঠামোতে আপডেট হওয়া নির্দেশিকা জারি করেছে, যা ধারাবাহিক পর্যবেক্ষণ এবং রিয়েল টাইম মূল্যায়ন গুলোর দিকে একটি শিফট সুপারিশ করে।

নিরাপত্তা ঝুঁকির ফলে সাইবার নিরাপত্তা প্রযুক্তি এবং পরিষেবা যেগুলোতে বিনিয়োঘগ বৃদ্ধি পাচ্ছে ২০১৭ সালে গার্টনার ভবিষ্যদ্বাণী করেছিলেন যে তথ্য সুরক্ষা পূর্ণ এবং পরিষেবা দিতে বিশ্বব্যাপী খরচ ৮৩ দশমিক ৪ বিলিয়ন ডলারে পৌঁছাবে ২০১৬ থেকে ৭ শতাংশ বৃদ্ধি পাবে এবং ২০১৮ সালের মধ্যে এটি ৯৩ বিলিয়ন ডলারে উন্নীত হবে।

সাইবার নিরাপত্তায় হুমকি সমূহঃ

সাইবার জগতের সবচেয়ে বড় হুমকি ধরা হয় বিভিন্ন ধরনের নেটওয়ার্কে ইংরেজি Malicious Software এর রূপ হল ম্যালওয়্যার এটি এক ধরনের ক্ষতিকর প্রোগ্রাম বিভিন্ন ধরনের হতে

পারে সব ধরনের মালোওয়ারি সাইবার নিরাপত্তার জন্য হুমকি নিম্নে বিভিন্ন প্রকার সাইবার নিরাপত্তা হুমকি সমূহ আলোচনা করা হলো–

১। অ্যাডওয়ারঃ অ্যাডওয়ার কে সবচেয়ে কম ক্ষতিকর ম্যালওয়্যার ধরা হয় মূলত বিভিন্ন বিজ্ঞাপন দেখায় ভালো না জেনে কোন সফটওয়্যার ইন্সটল কিংবা ব্রাউজার প্লাগিন ইনস্টল করার মাধ্যমে অ্যাডওয়ার সিস্টেমে ঢুকে পড়ে এজন্য ট্রাস্টেড সোর্স ছাড়া সফটওয়্যার ও প্ল্যাগিন ইনস্টল করা কখনোই ঠিক নয়।

২। ভাইরাসঃ ভাইরাস এক ধরনের প্রোগ্রাম, যা সাধারনত অন্য একটি সফটওয়্যার এর সাথে সংযুক্ত অবস্থায় থাকে এবং পরবর্তিতে পুরো সিস্টেমে ছড়িয়ে পড়ে।ভাইরাস বেশির ভাগ সময় সফটওয়ার অথবা ফাইল শেয়ারিং এর মাধ্যমে কম্পিউটার থেকে কম্পিউটারে ছড়িয়ে পড়ে। হোস্টিং অ্যাকাউন্ট নিরাপদ রাখতে ভাইরাস যুক্ত ফাইল কখনই অ্যাকাউন্ট এ আপলোড করা ঠিক নয়।

৩। র‍্যানসমওয়্যারঃ র‍্যানসমওয়্যার সম্পূর্ণ সিস্টেমকে লক করে দেয় এবং সিস্টেমকে আনলক করার জন্য টাকা চায়।এটি বর্তমান সময়ে সবচেয়ে বেশি আরোচিত সাইবার নিরাপত্তা হুমকি।

৪। ব্যাকডোরঃ ব্যাকডোর এমন একটি ব্যবস্থা, যার মাধ্যমে একজন হ্যাকার কিংবা স্প্যামার অন্য কারো নেটওয়ার্ক সংযোগ ব্যবহার করতে পারে।

৫। কী–লগারঃ কী–লগার এর কাজ হলো কম্পিউটারে যা টাইপ করা হয় (যেমন–ইউজার আইডি, পাসওয়ার্ড অথবাযে কোন তথ্য), সবকিছু রেকর্ড করবে এবং পরবর্তীতে কী–লগারের প্রোগ্রামারকে সব তথ্য পাঠিয়ে দিবে।

৬। রুট–কিটঃ এটি ভয়ানক ধরনের মালওয়ার।সহজে এটা ধরা যায়না। রুট–কিট অন্য ম্যালওয়ারকে লুকিয়ে রাখতে সাহাজ্য করে ।

৭। স্পাইওয়্যার ঃ স্পাইওয়্যার বলতে মূলত বোঝায় এটি ইন্টারনেট এক্টিভিটিস থেকে শুরু করে সবকিছু নজরদারি করে।

৮। ট্রোজান হর্সঃ ট্রোজান হর্স এই সময়ের সবচেয়ে ভয়ংকর মালওয়ার। এটা আর্থিক তথ্য চুরি করে এবং সিস্টেমের রিসোর্স ব্যবহার করে। ট্রোজান হর্স বড় কোন সিস্টেম হলেও সিস্টেমকে ডাউন করে দিতে সক্ষম হয়।

৯। ওয়ার্মঃ ওয়ার্ম এক ধরনের খাদক। ওয়ার্ম এর খাবার হল প্রয়োজনীয় ফাইল অ্যাক্টিভ ড্রাইভের যখন ওয়ান ঢুকে পড়ে তখন এটি আস্তে আস্তে সম্পূর্ণ ড্রাইভ টি খালি করে ফেলে।

১০। ফিশিংঃ অনেক সময় চমকপ্রদ অফার দিয়ে ব্যক্তিগত ইমেইল একাউন্টে ব্যাংক পরিচিতি কোন প্রতিষ্ঠান এবং বন্ধুর নাম দেখে মেইল খুলে ক্লিক করা হয় ফিশিং ইমেইলগুলো ব্যক্তিগত তথ্য চুরি করে এজন্য অপরিচিত সন্দেহজনক ইমেইল ওপেন করা ঝুঁকিপূর্ণ।

সাইবার নিরাপত্তার জন্য পদক্ষেপঃ

সাইবার জগতে ব্যক্তিগত কিংবা প্রতিষ্ঠানকে নিরাপদ রাখার জন্য নিম্নোক্ত বিষয় প্রতি খেয়াল রাখতে হবে।

১। ইমেইল এড্রেস,ক্রেডিট কার্ড নাম্বার, পাসপোর্ট নাম্বার, ব্যাংক একাউন্ট নাম্বার ,আইডি কার্ড নাম্বার, ড্রাইভিং লাইসেন্স নাম্বার ইত্যাদি শেয়ার করা থেকে বিরত থাকা।

২। সকাল একাউন্টের ইউজার নেম এবং পাসওয়ার্ড একই না রেখে ভিন্ন ভিন্ন রাখা, যাতে একটি অ্যাকাউন্ট হ্যাক হলেও সমসত একাউন্ট হ্যাক না হয়।

৩। অত্যন্ত ব্যক্তিগত ছবি বা ভিডিও সোশ্যাল মিডিয়াতে শেয়ার করা থেকে বিরত থাকা।

৪। ব্যবসায়িক লেনদেনের ক্ষেত্রে সর্তকতা অবলম্বন করা।

৫। সোশ্যাল মিডিয়াতে সবার জন্য উন্মুক্ত না রাখা

৬। সোশ্যাল মিডিয়াতে অপ নিন্দা এবং অপপ্রচার থেকে বিরত থাকা ।

৭। অপরিচিত ওয়েবসাইট ভিজিট এবং সেখান থেকে ফ্রি সফটওয়্যার ডাউনলোড করা থেকে বিরত থাকা।

৮। ইন্টারনেটের ডকুমেন্ট শেয়ারের ক্ষেত্রে শুধুমাত্র বাছাইকৃতদের দেখার সুযোগ দেয়া ।

৯। রেস্টুরেন্ট ও পাবলিক প্লেস গুলোতে ওয়াইফাই কানেক্টেড থেকে বিরত থাকা।

১০। কোন ওয়েবসাইটে লগইন বা রেজিস্ট্রেশন করার সময় দেখে নেয়া যে সাইটটি সিকিউর কি না।অর্থাৎ এইচটিটিপিএস ব্যবহার করছে কিনা।

১১। স্মার্ট ফোন, ল্যাপটপ, ডেস্কটপ এ ভালো মানের এন্টিভাইরাস ইন্সটল রাখা এবং নিয়মিত আপডেট করা।

১২। সোশ্যাল মিডিয়া এবং ইমেইলসহ সকল সাইটে সম্ভব হলে টু স্টেপ সিস্টেম চালু করা।

১৩। আন–অথেন্টিক কোন পেন ড্রাইভ পিসিতে সংযোগ না করা। করলেও ভালোভাবে স্ক্যান করে নেওয়া।

১৪। ইমেইল অথবা এসএমএসের মাধ্যমে আশা কোন লটারি অথবা অন্য কোন অফারের লিংকে ক্লিক না করা।

সাইবার নিরাপত্তার তিন স্তম্ভঃ

পিপল, প্রসেস এবং প্রযুক্তি এই তিনটি বিষয়কে সাইবার নিরাপত্তার তিন স্তম্ভ বা থ্রি পিলার বলা হয়ে থাকে । কারণ এই তিন ক্ষেত্রে সাইবার নিরাপত্তা সম্পর্কে সচেতন থাকা অতীব জরুরী।

১। পিপল বা ব্যাক্তিঃ প্রতিটি ব্যক্তি বা কর্মচারীকে সাইবার হুমকি গুলো প্রতিরোধ এবং রাস করার ক্ষেত্রে তাদের ভূমিকা সম্পর্কে সচেতন থাকতে হবে। বিশেষ করে প্রযুক্তিগত সাইবার নিরাপত্তা কর্মীদের সাইবার আক্রমণ এবং প্রতিরোধ সম্পর্কে সর্বশেষ দক্ষতা এবং যোগ্যতার সাথে পুরোপুরি আপ-টু-ডেট থাকতে হবে ।

২। প্রসেসঃ কোন সংস্থার তথ্যের ঝুঁকিগুলো রাস করার জন্য কিভাবে সংস্থার ক্রিয়া-কলাপ ভূমিকা এবং ডকুমেন্টেশন ব্যবহার করা হবে সেগুলো সংজ্ঞায়িত করার পদ্ধতি অত্যন্ত গুরুত্বপূর্ণ। সাইবার হুমকি গুলো দ্রুত পরিবর্তিত হয়। তাই প্রসেস গুলোকে তাদের পাশাপাশি মানিয়ে নিতে সক্ষম হওয়ার জন্য ক্রমাগত পর্যালোচনা করতে হয়।

৩। প্রযুক্তিঃ প্রতিষ্ঠান ঝুঁকিগুলো চিহ্নিত করে কি কি নিয়ন্ত্রণ করতে হবে এবং কোন প্রযুক্তি গুলো দ্বারা নিয়ন্ত্রণ করতে হবে তা নির্ধারণ করতে হবে। ঝুঁকির উপর নির্ভর করে সাইবার ঝুঁকিগুলোর প্রভাব হ্রাস করার জন্য প্রযুক্তি স্থাপন করতে হবে।

সাইবার নিরাপত্তা বিশেষজ্ঞঃ

তথ্য সিস্টেম সুরক্ষিত রাখার ক্ষেত্রে সাইবার নিরাপত্তা বিশেষজ্ঞরা গুরুত্বপূর্ণ ভূমিকা পালন করেন। নিরাপত্তা এভেন্ট গুলোর নজরদারি, সনাক্তকরণ, তদন্ত, বিশ্লেষণ, প্রতিক্রিয়া ইত্যাদির মাধ্যমে সাইবার নিরাপত্তা বিশেষজ্ঞরা সাইবার নিরাপত্তা সম্পর্কিত ঝুঁকি, হুমকি এবং দুর্বলতাগুলো থেকে সিস্টেম কে রক্ষা করে। একজন সাইবার নিরাপত্তা বিশেষজ্ঞ মূলত যে সকল কাজ করে থাকেন সেগুলো হলোঃ

১। নিরাপত্তা আপডেট ও এর উন্নয়ন বিশ্লেষণ করেন।

২। নিরাপত্তা অ্যাডমিনিস্ট্রেটর দের দেখাশোনা করেন।

৩। বিভিন্ন সিস্টেমের ক্ষয়ক্ষতি, পরিবর্তন ও অনৈতিক প্রবেশাধিকার নিয়ে গবেষণা করে থাকেন।

৪। বিভিন্ন নিরাপত্তা টুলস ও অ্যাপ্লি-কেশন সঠিকভাবে কাজ করছে কিনা তা দেখাশোনা করেন।

৫। ফায়ারওয়াল একটি ভাইরাস ব্যবস্থাপনায় অ্যান্টিভাইরাস ডেভেলপার ও নেটওয়ার্ক অডিটর কে সাহায্য করেন।

৬। ক্রিপ্টোগ্রাফার, ভালনারেবিলিটি এ্যাসেসর ও সিকিউরিটি এনালিস্ট কে প্রশিক্ষণ দিয়ে থাকেন।

৭। বিভিন্ন কোম্পানির সিস্টেম এর জন্য উপযুক্ত সফটওয়্যার তৈরি করেন।

সাইবার নিরাপত্তার প্রকারভেদঃ

সাইবার নিরাপত্তা বলতে কোন সংস্থার সাইবার আক্রমণ, তথ্য চুরি লংঘন অনুমোদিত একসেস ইত্যাদি থেকে সংস্থার ডিভাইস প্রক্রিয়া অবকাঠামোর সুরক্ষা কথা বোঝায় প্রযুক্তি আবির্ভাব এবং সাংগঠনিক সিস্টেম ও নেটওয়ার্কের ক্রমবর্ধমান আন্তঃসংযোগ এর ফলে কার্যকর সাইবার নিরাপত্তা ব্যবস্থাপনা সব ধরনের প্রতিষ্ঠান জন্য অতীব জরুরী। রিপোর্ট অনুসারে ২০২০ সালে নাগাদ সাইবার নিরাপত্তায় ১৭০ বিলিয়ন ডলারে উন্নতি হতে পারে বলে আশা করা হচ্ছে।বিভিন্ন প্রকার সাইবার নিরাপত্তা সম্পর্কে আলোচনা করা হলো।

১। অ্যাপ্লি-কেশন নিরাপত্তাঃ অ্যাপ্লি-কেশন ডিজাইন, ডেভলপমেন্ট, স্থাপনা, রক্ষণাবেক্ষণ আপগ্রেড ইত্যাদি অ্যাপ্লি-কেশনের ডেভলপমেন্ট পর্যায়ে উদ্ভূত হুমকি এবং দুর্বলতাগুলো মোকাবেলা করার জন্য অ্যাপ্লি-কেশন নিরাপত্তা কৌশল গঠন করা হয়।কয়েকটি অ্যাপ্লি-কেশন নিরাপত্তা কৌশল হলো ব্যবহৃত ইনপুট প্যারামিটার এর বৈধতা, সেশন ব্যবস্থাপনা, ব্যবহারকারী অনুমোদন ইত্যাদি।

২। তথ্য নিরাপত্তাঃ ব্যবহারকারী গোপনীয়তা বজায় রাখার জন্য এবং পরিচয় বা আইডেন্টিটি চুরি প্রতিরোধ করার জন্য অনুমোদিত অ্যাকসেস, লংঘন, চুরি ইত্যাদি থেকে তথ্য এবং ডাটা সুরক্ষার বিষয়টি তথ্য নিরাপত্তা আলোচনা করা হয়।

৩। নেটওয়ার্ক নিরাপত্তা ঃ এটি একটি সংস্থার অভ্যন্তরীণ নেটওয়ার্কের বহিরাগত একসেস পর্যবেক্ষণ এবং প্রতিরোধ ব্যবস্থা। নেটওয়ার্ক নিরাপত্তা নিশ্চিত করে যে অভ্যন্তরীণ নেটওয়ার্ক গুলো নিরাপদ নির্ভরযোগ্য এবং ব্যবহারযোগ্য। অ্যান্টি ভাইরাস এবং অ্যান্টি স্পাইওয়্যার সফটওয়্যার গুলো ভিপিএন আইপিএস ফায়ারওয়াল ইত্যাদি প্রতিষ্ঠানের সবাই হুমকি প্রতিরোধে ব্যবহার করা হয়।

৪। ওয়েবসাইট নিরাপত্তাঃ এটি ইন্টারনেটের সাইবার নিরাপত্তা ঝুঁকি থেকে ওয়েবসাইটগুলোকে সুরক্ষিত করতে ব্যবহার করা হয়। হোলিস্টিক ওয়েবসাইট সুরক্ষা প্রোগ্রাম ওয়েব সাইটের ডাটাবেজ অ্যাপ্লি-কেশন সোর্সকোড এবং ফাইলগুলো কভার করে।গত কয়েক বছরে ওয়েবসাইটগুলোতে ডাটা অবৈধ উপায়ে অ্যাক্সিস এর সংখ্যা ক্রমাগত বৃদ্ধি পেয়েছে। যার ফলে পরিচয় চুরি, ডাউন টাইম, আর্থিক ক্ষতি ইত্যাদি সাইবার হুমকিও বৃদ্ধি পেয়েছে। এর মূল কারণ ওয়েবসাইটের মালিকের মধ্যে একপ্রকার ভুল ধারণা যে,তাদের ওয়েবসাইট টি ওয়েবসাইট হোস্টিং প্রদানকারী সংস্থা দ্বারা সুরক্ষিত।ওয়েবসাইট সুরক্ষার জন্য ব্যবহৃত কয়েকটি গুরুত্বপূর্ণ কৌশল হলো ওয়েবসাইট স্ক্যানিং এবং ম্যালওয়্যার অপসারণ ওয়েবসাইট অ্যাপ্লি-কেশন ফায়ারওয়ার অ্যাপ্লি-কেশন সুরক্ষা যাচাই পদ্ধতি ইত্যাদি।

৫। এন্ড পয়েন্ট নিরাপত্তা ঃএর মাধ্যমে প্রতিষ্ঠানগুলোর তাদের সার্ভার স্টেশন এবং দূরবর্তী ও স্থানীয় সাইবার আক্রমণ থেকে রক্ষা করতে সক্ষম হয় । যেহেতু একটি নেটওয়ার্ক ডিভাইস গুলো সংযুক্ত থাকে তাই একটি হুমকি এবং দুর্বলতার জন্য এন্ট্রিপয়েন্ট তৈরি করে। এন্ড পয়েন্ট নিরাপত্তা এই এন্ট্রি পয়েন্টগুলোর এক্সেস ব্লক করে নেটওয়ার্ক সুরিক্ষিত করে। এন্টিভাইরাস এবং এন্টি-ম্যালওয়ার সফটওয়্যার এর ব্যবহার এন্ড পয়েন্ট নিরাপত্তা অন্যতম কৌশল।

৬। অপারেশন নিরাপত্তা ঃঅপারেটিং নিরাপত্তার মাধ্যমে দুর্বল তথ্য শনাক্ত করা হয় এবং রিসোর্স ট্রাক করে সংস্থার মূল ক্রিয়া-কলাপ গুলো রক্ষা করা হয়।

৭। ক্লাউড নিরাপত্তাঃ ক্লাউড নিরাপত্তা ভিত্তিক এপি-কেশন গুলোকে সুরক্ষা প্রদান করে।

সাইবার নিরাপত্তার প্রয়োজন এবং ভূমিকাঃ

সাইবার নিরাপত্তা শুধু ব্যবসা এবং সরকারের সাথে জড়িত নয় কম্পিউটার ট্যাবলেট এবং সেলফোন এর মধ্যে এমন অনেক তথ্য থেকেই থাকে যা হ্যাকার এবং অন্যান্য অপরাধীরা অ্যাক্সেস করার চেষ্টা করে যেমন অন্য কারও ই-মেইল ঠিকানা নাম জন্মতারিখ ইত্যাদি। উদাহরণস্বরূপ একজন হ্যাকার যদি কারো যোগাযোগ তথ্য অ্যাক্সেস করার অনুমতি পাই তখন হ্যাকার সেই ব্যক্তির নাম ব্যবহার করে তার পরিচিতি প্রত্যেককে একটি ই-মেইল বার্তা পাঠাতে পারে এবং একটি ধারণা কারী লিংকে ক্লিক করার জন্য উৎসাহিত করতে পারে।

১.৩.১ সাইবার নিরাপত্তার ভূমিকা যোগাযোগের জন্য এমন কোন ব্যবস্থা যা ইন্টারনেটের সাথে সংযুক্ত অথবা কোন কম্পিউটার বা স্মার্ট ডিভাইসের সাথে সংযুক্ত সেরকম কোন ব্যবস্থার মাধ্যমে সাইবার নিরাপত্তা বিঘ্নিত হতে পারে। সেই সকল ব্যবস্থার অন্তর্ভুক্ত বিষয়গুলো হলো।

১। যোগাযোগ ব্যবস্থা যেমন ইমেইল ফোন এবং টেক্সট বাত্রা।

২।ট্রাফিক নিয়ন্ত্রণ গাড়ির ইঞ্জিন বিমান নেভিগেশন সিস্টেম সহ পরিবহন ব্যবস্থা।

৩। সামাজিক নিরাপত্তা নম্বর লাইসেন্স রেকর্ডসহ সরকারি ডাটাবেজ।

৪। ব্যাংক একাউন্ট ঋণ এবং পে চেক সহ আর্থিক ব্যবস্থা।

৫। সরঞ্জাম এবং মেডিকেল রেকর্ড সহ চিকিৎসা ব্যবস্থা।

৬। গ্রেড রিপোর্ট কার্ড এবং গবেষণা তথ্য সহ শিক্ষা ব্যবস্থা।

সাইবার নিরাপত্তা তিনটি নীতিঃ

সাইবার নিরাপত্তা কমপক্ষে তিনটি প্রধান নীতি রয়েছে সেগুলো হলো।

১। গোপনীয়তাঃ সংবেদনশীল যে কোন তথ্য শুধুমাত্র একটি সীমিত সংখ্যক মানুষের সাথে ভাগ করা উচিত। উদাহরণস্বরূপ যদি একটি ডেবিট কার্ডের তথ্য কয়েকজন অপরাধীর সাথে ভাগ করা হয় তাহলে বড় ধরনের সমস্যার সম্ভাবনা থাকবে।

২। সম্পূর্ণতাঃ সম্পূর্ণতা হচ্ছে সকল তথ্য পরিবর্তন করে রাখা। যখন ম্যালওয়ার একটি হাসপাতালে কম্পিউটার সিস্টেমকে হিট করে, তখন ঐ রোগীর রেকর্ড লেবেল ফলাফল ছাড়িয়ে দিতে পারেন এবং স্টাফকে রোগীর তথ্য অ্যাক্সেস করতে বাধা প্রদান করতে পারে।

৩। প্রাপ্যতাঃ প্রাপ্যতা প্রায়ই সম্পুর্ণ সম্পর্কিত। তবে সাইবার আক্রমণের সাথে জড়িত লোকেরা নির্দিষ্ট কম্পিউটারগুলোর অ্যাক্সেস করা বা ইন্টারনেট একসেস করতে বাধা দিতে পারে।

তথ্য নিরাপত্তা এবং সাইবার নিরাপত্তার মাঝে পার্থক্যঃ

তথ্য বা ইনফরমেশন কে কোন প্রতিষ্ঠানের হৃদয় বলা হয়, যার মধ্যে ব্যবসার রেকর্ড, ব্যক্তিগত তথ্য ইত্যাদি অর্ন্তভুক্ত থাকে।

তথ্য বা ইনফরমেশন যেকোনো জায়গায় রাখা যায় এবং সেটাকে অনেক উপায় অ্যাক্সেস করা যেতে পারে। কম্পিউটার বা কাগজের রেকর্ড গুলোর মাধ্যমে ডাটা বা উপাত্ত একসেপ্ট করা গেলেও তথ্য ইনফরমেশন একসেপ্ট করার জন্য ডিস্ক, ল্যাপটপ, সার্ভার, ব্যক্তিগত ডিভাইস ইত্যাদি প্রয়োজন হয়। তথ্য বা ইনফরমেশন নিরাপদ রাখা প্রয়োজন এবং নিরাপদ করার প্রক্রিয়াকে তথ্য নিরাপত্তা বলা হয়।

তথ্য নিরাপত্তার দুটি সাব কাটাগরি রয়েছে।প্রথমটি হল, তথ্যের স্থানটির নিরাপত্তা নিশ্চিত করে শারীরিক পরিবেশ সুরক্ষা করা। দ্বিতীয় হল, কেউ যেন বৈদ্যুতিন ভাবে তথ্য অ্যাক্সেস করতে না পারে সেই বিষয়টি নিশ্চিত করা। একে সাইবার নিরাপত্তা বলা হয়।

সাইবার নিরাপত্তা এবং তথ্য নিরাপত্তা শব্দটি অনেক সময় বিভ্রান্তির সৃষ্টি করে। অনেকেই মনে করে যে, সাইবার নিরাপত্তা এবং তথ্য নিরাপত্তা একটি অন্যটির বিপরীত। নিম্নে সাইবার নিরাপত্তা এবং তথ্য নিরাপত্তা মাঝে পার্থক্য আলোচনা করা হলো।

(ক) সাইবার নিরাপত্তা সাইবারস্পেস কে অনুমোদিত ডিজিটাল একসেস থেকে সুরক্ষিত করে। অন্যদিকে, তথ্য নিরাপত্তা তথ্য সম্পর্কে সকল অনুমোদিত অ্যাক্সেস থেকে রক্ষা করে।

(খ) সাইবার নিরাপত্তা এবং তথ্য নিরাপত্তার ক্ষেত্রে সবচেয়ে গুরুত্বপূর্ণ উপাদান তথ্যের ভ্যালু। সাইবার নিরাপত্তা হলো সংস্থার তথ্য এবং সুরক্ষা প্রযুক্তিকে অনুনোমোদিত ডিটেলস থেকে রক্ষা করা। এটি সাইবার স্পেসের মাধ্যমে অ্যাক্সেস করা যেতে পারে। এমন সব কিছুকে অন্তর্ভুক্ত করে। তথ্য নিরাপত্তা মানে কোম্পানির তথ্য সম্পর্কে যেকোনো ধরনের হুমকি থেকে রক্ষা করে।

(গ) সাইবার নিরাপত্তার সঙ্গে পেশাদার নিরাপত্তা মিলে উন্নত ধরনের হুমকি গুলোর সমাধান করে। অন্যদিকে,তথ্য নিরাপত্তা এবং এটি সাথে জড়িত নিরাপত্তা পেশাদারদের হুমকি মোকাবেলার পূর্বে প্রথমে সংস্থান কে অগ্রাধিকার দেওয়া হয়।

(ঘ) সাইবার নিরাপত্তা সামাজিক মিডিয়া একাউন্ট, ব্যক্তিগত তথ্য ইত্যাদি রক্ষা করার মত সাইবার অঞ্চলে বিদ্যমান হুমকি গুলোর সাথে সম্পর্কিত। অন্যদিকে, তথ্য নিরাপত্তা প্রধানত তথ্য সম্পদ এবং তাদের সততা, গোপনীয়তা এবং প্রাপ্যতা ইত্যাদির সাথে সম্পর্কিত। তথ্য নিরাপত্তা তিন ধরনের নিরাপত্তা লক্ষ্যের সমন্বয়।

হ্যাকার সম্প্রদায় সাইবার আক্রমণ নিয়মিত করছে।বিভিন্ন সংস্থা গুলো অনুমোদিত একসেস থেকে তাদের অবকাঠামো রক্ষা করতে এক প্রকার বাধ্য হয়ে থাকে। এখন এটি শুধু ব্যক্তিগত খাতেই সীমাবদ্ধ নয়,বরং সরকারি সংস্থাগুলো এই সাইবার আক্রমণ প্রতিরোধের ক্ষেত্রে সমানভাবে দুর্বল।এটি সাইবার নিরাপত্তা এবং তথ্য নিরাপত্তা বৃদ্ধি করে। সাইবার নিরাপত্তা এবং তথ্য নিরাপত্তা উভয়ই একে অপরের সমর্থক হয়, যদিও দুটির মধ্যে সূক্ষ্ম পার্থক্য বিদ্যমান।সাইবার নিরাপত্তা অনুনোমোদিত ইলেক্ট্রনিক্স থেকে নেটওয়ার্ক, কম্পিউটার এবং ডাটা সুরক্ষার সাথে সম্পর্কিত, অন্যদিকে তথ্য নিরাপত্তা ফিজিক্যাল বা ডিজিটাল ফরমেট এর বিভিন্ন তথ্যের সুরক্ষা প্রদান করে।সাইবার নিরাপত্তা এবং তথ্য নিরাপত্তার জন্যই প্রযুক্তি এবং নিরাপত্তা হুমকি বুঝা অত্যন্ত গুরুত্বপূর্ণ।

কেন তথ্য এবং সাইবার নিরাপত্তা ব্যবস্থা সমাজের জন্য গুরুত্বপূর্ণঃ

যেকোনো কোম্পানিকে স্ক্যাম, তথ্য চুরি এবং অন্যান্য অনলাইন দুর্বলতার হুমকি থেকে রক্ষা করা খুব গুরুত্বপূর্ণ ।হাজার হাজার সাইবার সংক্রমিত ওয়েবপেজ প্রতিদিন আবিষ্কার আবিষ্কার করা হচ্ছে ।গত কয়েকবছরে তথ্য লঙ্ঘনের জন্য লক্ষেরও বেশি রেকর্ড জড়িত রয়েছে এবং এ ধরনের লংঘন থেকে পুনরুদ্ধার করা খুবই কঠিন হয়ে থাকে। অনেক সংগঠন তৈরি হচ্ছে নানা তথ্য বিভিন্ন উপায়ে হ্যাক করছে। কিছু হ্যাকার পাসওয়ার্ড এবং বন্ধ নেটওয়ার্ক অ্যাক্সেস অর্জনে বেশি আগ্রহী, যাতে তারা তথ্য এবং ওয়েবসাইটগুলো ম্যানিপুলেট করতে বা ইচ্ছে মতো প্রয়োজনীয় ফাংশন বন্ধ করতে পারে।

কোন ব্যবসা প্রতিষ্ঠান অথবা সমাজের জন্য নিম্নোক্ত কারণে সাইবার এবং তথ্য নিরাপত্তা অত্যন্ড় গুরুত্বপূর্ণ।

১।প্রতিষ্ঠান বা সমাজের তথ্যের গোপনীয়তা এবং কঠোর এক সে সিভিলিটি নিয়ম সহ, ডাটার সুরক্ষার এক প্রকার স্পষ্ট প্রতিশ্রুতি প্রদর্শন করে।

২। ঝুঁকি পরিচালনা পদ্ধতি প্রদান করে।

৩। গোপন তথ্য নিরাপদ রাখে।

৪। একটি উল্লেখযোগ্য প্রতিযোগিতামূলক সুবিধা প্রদান করে।

৫। তথ্যের নিরাপদ বিনিময় নিশ্চিত করে।

৬। সেবার সামঞ্জস্য সৃষ্টি করে।

৭।প্রতিষ্ঠানের মধ্যে প্রতিষ্ঠান বা দলের মধ্যে আন্ত অপারেশনের জন্য অনুমতি দেয়।

৮। কোম্পানি, সম্পদ, শেয়ার হোল্ডার, কর্মচারী এবং ক্লায়েন্ট রক্ষা করে।

৯। তৃতীয় পক্ষের সরবরাহকারী ডাটা সুরক্ষা কে গুরুত্বসহকারে গ্রহণ করে এবং নিশ্চয়তা দেয়।

বর্তমানে বেশিরভাগ অপরাধী সাইবার জগতের মাধ্যমে হয়। সাইবার নিরাপত্তা জন্য সবচেয়ে জরুরি হলো সামাজিক সচেতনতা।

নিরাপত্তা, পরিচয়, নির্ভরযোগ্যতা, গোপনীয়তা, সম্পূর্ণতা, প্রাপ্যতা, হুমকি, দুর্বলতা, ঝুঁকি ও বিপত্তিঃ

সাইবার নিরাপত্তায় বিভিন্ন প্রকার টার্ম ব্যবহার করা হয়। নিম্নে কিছু কমেন্টও উল্লেখ করা হলো।

১। নিরাপত্তাঃ নিরাপত্তা বলতে মূলত সাইবার নিরাপত্তা বুঝায়, যেখানে সব ধরনের প্রদত্ত প্রযুক্তি নির্ভর ডিভাইসের নিরাপদ ব্যবহার, তথ্যটা চুরির হাত থেকে রক্ষা, বিভিন্ন ধরনের ম্যালওয়্যার থেকে নিরাপদ থাকা ইত্যাদির নিরাপত্তা বুঝায়। সাইবার নিরাপত্তার মাধ্যমে নিশ্চিত করা হয়, যেন বিভিন্ন প্রকার ডিভাইস এবং তার অপব্যবহার করা না হয়।

২। পরিচয়ঃ সাইবার নিরাপত্তায় বিভিন্ন প্রকার পরিচয় বা আইডেন্টিটি রয়েছে, যেমন পরিচয় চুরি, পরিচয়ে প্রতারণা, পরিচয় ক্লোনিং ইত্যাদি। এগুলো বিভিন্ন প্রকার সাইবার অপরাধের অন্ডর্ভুক্ত।

৩। নির্ভরযোগ্যতাঃ পরিচয় বা কোন এনটিটি (ব্যবহারকারী, প্রক্রিয়া বা ডিভাইস) এর অন্যান্য গুণাবলি যাচাই করার প্রক্রিয়াকে নির্ভরযোগ্যতা বলা হয়।

৪। গোপনিয়তাঃ সংবেদনশীল যেকোনো তথ্য শুধুমাত্র একটি সীমিত সংখ্যক মানুষের সাথে ভাগ করাকে সাইবার নিরাপত্তা ভাষায় গোপনীয়তা বুঝায়।

৫। সম্পূর্ণতাঃ সম্পূর্ণতা হচ্ছে সকল তথ্য পরিবর্তন করে রাখা। যখন মাল ওয়ার একটি হাসপাতালে কম্পিউটার সিস্টেমকে হিট করে, তখন এটি রোগীর রেকর্ড, লাব এর ফলাফল ছড়িয়ে দিতে পারে এবং স্টাফকে রোগের তথ্য অ্যাক্সেস করতে বাধা প্রদান করতে পারে।

৬ ।প্রাপ্যতাঃ প্রাপ্যতা প্রায় সম্পন্ন সম্পর্কিত। তবে সাইবার আক্রমণের সাথে জড়িত লোকেরা নির্দিষ্ট কম্পিউটারগুলো অ্যাক্সেস করা বা ইন্টারনেট একসেস করতে বাধা দিতে পারে।

৭। হুমকিঃহুমকি এমন এক পরিস্থিতি বা ঘটনা যা দুর্বলতাকে কাজে লাগিয়ে সাংগঠনিক ক্রিয়া-কলাপ, সম্পদ, ব্যাক্তি, অন্যান্য সংগঠন বা সমাজকে প্রতিকূল ভাবে প্রভাবিত করে।

৮। দুর্বলতাঃ দুর্বলতা একটি সিস্টেমের এক প্রকার ত্রুটি, যা সাইবার আক্রমণ করার জন্য সহায়ক হয়ে থাকে।

৯। ঝুঁকিও বিপত্তি ঃএকটি ঘটনার পরিণতিতে নেতৃত্ব দেওয়ার সম্ভাব্য সম্ভাবনায় হল ঝুঁকি।

অধ্যায় ঃ-০২

ডাটা এবং এভিডেন্স রিকভারি

ভূমিকা ঃ

ডাটা প্রত্যেকের কাছেই অত্যন্ত গুরুত্বপূর্ণ ।কিন্তু অনেকভাবেই আমাদের দৈনন্দিন জীবনের গুরুত্বপূর্ণ,ডাটা হারিয়ে যেতে পারে। ভুলবশত ডাটা ডিলেট হয়ে গেলে, হার্ডড্রাইভ অকেজো হয়ে গেলে,সফটওয়্যার কোনো ক্রুটি থাকলে,ডাটা করাপশন হয়ে গেলে,হ্যাকিং এর কবলে পড়লে, এমনকি সাধারণ বিদ্যুৎ চলে যাওয়া থেকেও ডাটা লস ঘটতে পারে ।প্রায় যে কোনো প্রকার হারিয়ে যাওয়া ডাটা রিকভার করা সম্ভব। ডাটা রিকভারি হলেঅ লজিক্যাল,ফিজিক্যাল বা উপরোল্লেখিত যে-কোনো কারণে লস হয়ে যাওয়া ডাটা পুনরুদ্ধারের একটি প্রক্রিয়া ।হারিয়ে যাওয়া ডাটাগুলো যদি কোনো হার্ডড্রাইভ,সলিড-স্টেট ড্রাইভ, পেনড্রাইভ বা যে কোনো মিডিয়া স্টোরেজের সাথে জড়িত থাকে, তবে বেশিরভাগ সময়েই সেই ডাটাগুলোকে বিভিন্ন উপায়ে রিকভার করা সম্ভব হয়।

তবে সবসময় ডাটা রিকভার করা সম্ভব হয় না ।অনেক সময় সিস্টেম এতোটাই অকেজো হয়ে পড়তে পারে,যেখান থেকে কোনো ডাটা পুনরুদ্ধার করা অসম্ভব ।বর্তমানে ডাটা রিকভারের জন্য অনেক উন্নত প্রযুক্তি ব্যবহার করা হয় ।যেমন–Kroll Ontrack নামক এক অস্ট্রেলিয়ান ডাটা রিকভারি কোম্পানি আছে,যারা ৯৯% পর্যন্ত যে কোনো হার্ডড্রাইভ থেকে ডাটা রিকভার করার নিশ্চয়তা প্রদান করে থাকে।

ফাইল রিকভারি এবং ফাইল রিকভারির বিভিন্ন প্রক্রিয়ার শ্রেণিবিভাগ

যদি সিস্টেম থেকে কোনো ফাইল লস হয়ে যায় (যেমন– ভুলবশত ডিলিট হয়ে গেলে, হার্ডড্রাইভ/সফট্রয়্যারে কোনো ক্রুটি থাকলে ইত্যাদি),তবে সেই ফাইল পুনরুদ্ধার করার প্রক্রিয়াকে ফাইল রিকভারি বলা হয়। বর্তমানে সকল অপারেটিং সিস্টেমই ডিলিট হয়ে যাওয়া ফাইলটি স্থায়ীভাবে ডিলিট করার জন্য পুনরায় ব্যবহারকারীর নিশ্চিতকরণের জন্য অপেক্ষা করে ।ডিলিট করা ফাইলগুলোর মেমরি স্পেস যদি অন্য কোনো নতুন ফাইল দ্বারা ওভাররাইট করা না হয়, তবে সেই ফাইলগুলেঅ বিভিন্ন উপায়ে পুনরুদ্ধার করা যায় ।একটি ফাইল কেবলমাত্র তখনই পুনরুদ্ধার করা যায়,যতক্ষণ পর্যন্ত এটি নূন্যতম ডিগ্রি অতিক্রম না করে ।তবে যদি হার্ডড্রাইভ/সফটওয়্যার ডিভাইস নষ্ট হওয়ার কারণে ডাটা পুনরুদ্ধার করার প্রয়োজন হয়, সেক্ষেত্রে বিশেষ সরঞ্জাম এবং ডাটা পুনরুদ্ধার সংস্থা কর্তৃক বিভিন্ন কৌশলের প্রয়োজন হয়।

ফাইল রিকভারির বিভিন্ন প্রক্রিয়া ঃ ফাইল রিকভারি বিভিন্ন উপায়ে সম্পন্ন করা হয়। ফাইল রিকভারি করার প্রক্রিয়া মূলত নির্ভর করে ফাইল হারানো বা লস এর ধরনের উপর।প্রধানত ফাইল রিকভারির প্রক্রিয়াকে দুটি ভাগে ভাগ করা হয়, যথা– সফওয়্যার রিকভারি এবং হার্ডওয়্যার রিকভারি। ইচ্ছা বা অনিচ্ছায় ফাইল ডিলিট করা কিংবা ফাইল ওভাররাইট হওয়ার কারণে যে রিকভারি সম্পন্ন করা হয়, তাকে হার্ডওয়্যার রিকভারি বলে। নিম্নে বিভিন্ন প্রকার ফাইল রিকভারি পদ্ধতি আলোচনা করা হলো ঃ

১। **ডিলিট হয়ে যাওয়া ফাইল রিকভারি ঃ** যখন একটি ফাইল ডিলিট করা হয়,ফাইলটি আসলে স্থায়ীভাবে ততক্ষণ পর্যন্ত ডিলিট হয় না, যতক্ষণ পর্যন্ত না সেখানে কোনো ফাইল/ডাটা ওভাররাইট করা হয়। এজন্য যদি কোনো ফাইল ভুলক্রমে ডিলিট হয়ে যায়,সাথে সাথে সেই ফাইলটি কোনো ভালো রিকভারি সফটওয়্যার দিয়ে রিকভারি করে নেয়া সম্ভব।কারণ রিকভারি করতে যত বেশি দেরি হবে, ফাইলটির সেই স্থানে ওভাররাইট হওয়ার সম্ভাবনা বেশি থাকবে।এখানে একটি গুরুত্বপূর্ণ বিষয় হলো,যদি ডিলিট করা ফাইলটির সাইজ খুব বড় হয়, তবে ফাইলটি কিন্ত স্থায়ীভাবে ডিলিট হয়ে যেতে পারে। সেক্ষেত্রে রিকভারি করা অনেকটাই কঠিন হয়ে যায়।

২। **ওভাররাইট হওয়া ফাইল রিকভারি ঃ** ফাইল ওভাররাইট হয়ে গেলে সেক্ষেত্রে রিকভারি করা একটু জটিল। এক্ষেত্রে ব্যবহার করা অ্যাপ্লিকেশনের ফাইলটি কীভাবে সংরক্ষিত হয়েছে তার উপর নির্ভর করে। একটি ফাইল ওভাররাইট করা আর একটি ফাইল ডিলিট করে নতুন তৈরি করা কিন্তু এক কথা নয়। একটি ফাইল ডিলিট করা মানে হলো ফাইলটি ব্যবহারের জন্য প্রস্তুত আছে কিন্তু মডিফিকেশন করা যাবে না। অন্যদিকে ওভাররাইট মানেই হলো ফাইলটির পরিবর্তন। ফাইল ওভাররাইট হয়ে গেলেও বিভিন্ন প্রকার ফাইল রিকভারি সফটওয়্যারের মাধ্যমে ফাইলটি রিকভারি করা সম্ভব। তবে অনেক সময় ফাইলটি রিকভারি করা সম্ভব নাও হতে পারে।

৩। **নষ্ট হওয়া ফাইল রিকভারি ঃ** যদি হার্ড ডিস্ক এর কোনো ড্রাইভ নষ্ট হয়ে যায়, কিংবা ফাইল ফরম্যাট নষ্ট হয়ে যায়,তবে ফাইল ফিরে পাবার ক্ষেত্রে নির্ভর করে ফাইলটি ঠিক কতটা ক্ষতিগ্রস্ত হয়েছে তার উপর। যদি ফাইল রিকভারি সফটওয়্যার ক্ষতিগ্রস্ত ফাইলটি থেকে যথেষ্ট তথ্য উদ্ধার করতে সক্ষম হয়, তবে ধ্বংস হওয়া ফাইলটি ব্যবহারের যোগ্য হতে পারে।তারপরও ফাইল রিকভারি সফটওয়্যার আগের ফাইলটি অর্থাৎ ধ্বংস হওয়ার আগের ভার্সনটি খোঁজার চেষ্টা করে এবং যদি খুঁজে পায় তখন পার্টিশন টেবিল ঠিক করে ফাইলটি রিকভারি করা সম্ভব হয়।

৪। **ফিজিক্যালি ড্যামেজ হওয়া ফাইল রিকভারি ঃ** ডিলিট হওয়া বা ফরম্যাটিং/করাপ্টেড ফাইল রিকভারি করা, আর সম্পূর্ণ ফিজিক্যালি ধ্বংস হওয়া হার্ডড্রাইভ থেকে ফাইল রিকভারি করা কিন্তু এক নয়। এই অবস্থায় সাধারণ ডাটা রিকভারি সফটওয়্যার বা টেকনিক্যাল জ্ঞান তেমন কোনো কাজে লাগবে না। ফিজিক্যালি ড্যামেজ থেকে ফাইল রিকভার করার সবচেয়ে উত্তম পন্থা হবে ড্রাইভটি কোনো রিকভারি বিশেষজ্ঞ বা রিকভারি প্রতিষ্ঠান থেকে রিকভার করিয়ে নেয়।অনেকভাবে একটি সিস্টেম ফিজিক্যালি ড্যামেজ হতে পারে। অনেক সময় শুধু হয়তো ড্রাইভটির কন্ট্রোলার বোর্ড বা হেড ড্যামেজ হয়।এই অবস্থায় এগুলোকে পরিবর্তন করে ড্রাইভটি রিপেয়ার করা যেতে পারে। কিন্তু এই পরিবর্তনগুলো করাতে বা যে কোনো গুরুতর ড্যামেজ থেকে ড্রাইভটিকে সারাতে অবশ্যই বিশেষজ্ঞদের সাহায্য নেওয়া উচিত।

ডাটা রিকভারি এবং ফরেনসিক টুল কিটঃ

ডাটা লস যে-কোনো সময়েই ঘটতে পারে। কেবল হার্ড ডিস্ক ক্র্যাশ না, ডাটা লস হতে পারে অপারেটিং সিস্টেম ক্র্যাশ, র‍্যানসমওয়্যার আক্রমণ, ভুলক্রমে ডিলিট কিংবা ডিভাইস চুরি বা হারানো যাওয়ার ফলেও। আর ডাটা লসে কেবল পার্সোনাল ডাটাই নয়, হারাতে পারে অফিসিয়াল এবং ক্লায়েন্ট ডাটাও। ডাটা রিকভারি হলো নষ্ট হয়ে যাওয়া হার্ড ড্রাইভ/পেন ড্রাইভ/অপারেটিং সিস্টেম কিংবা ভুলক্রমে ডিলিট হয়ে যাওয়া ডাটা থেকে যতটুকু সম্ভব ডাটা ফিরিয়ে নিয়ে আসার প্রক্রিয়া।

কীভাবে ডাটা রিকভারি কাজ করে ঃ যখন কোনো ডাটা সিস্টেম থেকে ডিলিট করা হয়,সেটি প্রথমে কম্পিউটারের রিসাইকেল বিন-এ জমা হয়। পরবর্তীতে প্রয়োজন হলে রিস্টোর দিয়ে রিসাইকেল বিন থেকে যে-কোনো সময় সেই ডাটা ফেরত আনা যায়।এজন্য কোনো ফোল্ডারকে ডিলিট করে রিসাইকেল বিন-এ পাঠালেও ড্রাইভে কোনো খালি স্পেস দেখায় না। স্পেস সম্পূর্ণ খালি করতে হলে প্রয়োজন রিসাইকেল বিন থেকেও ডাটা ডিলিট করা।আবার রিসাইকেল বিন থেকে ডিলিট করলে দেখা যায় স্পেস আসলেই খালি হয়েছে,কিন্তু আসলে ডাটা সম্পূর্ণরূপে সরে যায়নি। ড্রাইভের সেই স্পেসটুকু আসলে খালি হিসাবে মার্ক করা হয়েছে। তখন আসলে বুঝানো হয় যে চাইলে,এই জায়গায় নতুন ডাটা রাখা যাবে।

ডাটা যেখানে ছিল সেই স্পেসটি খালি হয়ে যায়,কিন্তু ডাটার অস্তিত্ব তখনও থেকে যায়।শুধুমাত্র ডাটা বা ফাইলের পয়েন্টারগুলো চলে যায়।পয়েন্টার হলো কম্পিউটারের আরেক ধরনের ডাটা,যেগুলো মেমরিতে থাকা ফাইলগুলোর ডিরেক্টরিকে পয়েন্ট করে বা নির্দেশ করে।ফ্রি হওয়া ড্রাইভে নতুন কিছু ডাটা ঢুকালে পুরাতন ডাটা ফেরত পাবার হার কমতে থাকবে।অর্থাৎ ডিলিট

করার পর যতক্ষণ পর্যন্ত না সেই ড্রাইভে নতুন কোনো ডাটা ঢুকানো হচ্ছে,ততক্ষণ পর্যন্ত ডাটা রিকভারি সফটওয়্যার ব্যবহার করে খুব সহজেই ডাটা রিকভার করা যায় ।ডাটা রিকভাবি সফটওয়্যারগুলো অনেক জটিল অ্যালগরিদম ব্যবহার করে ড্রাইভে পড়ে থাকা পুরাতন ডাটাগুলো খোঁজার চেষ্টা করে এবং ডিলিট হওয়া ডাটার ফিজিক্যাল লোকেশন অনুমান করে। যদি সফটওয়ার সঠিক লোকেশন অনুমান করতে সক্ষম হয়,তবে নিঃসন্দেহে ডাটা ফিরে পাওয়া যাবে। আর যদি অনুমান করতে না পারে, কিংবা যদি হার্ড ডিস্ক ক্র্যাশ, অপারেটিং সিস্টেম ক্র্যাশ ইত্যাদি ফিজিক্যালি কোনো সমস্যার কারণে ডাটা লস হয়,তাহলে বিভিন্ন প্রকার ডাটা রিকভারি টুলস, টেকনিক এবং ডাটা রিকভারি বিশেষজ্ঞ দ্বারা ডাটা রিকভারি করানোই সবচেয়ে ভালো পন্থা।

কমন ডাটা লস ফ্যাক্টর ঃ

বিভিন্ন কারণে ডাটা লস হতে পারে এবং সেই ডাটা পুনরুদ্ধারেরও আলাদা আলাদা ব্যবস্থা রয়েছে ।নিম্নে কিছু কমন ডাটা লস ফ্যাক্টর আলোচনা করা হলো ঃ

১। **ডাটা ডিলিট ঃ** আমরা জানি যে, যখন কোনো ডাটা ড্রাইভ থেকে ডিলিট করে দেয়া হয়, তখন উক্ত ডাটা ড্রাইভে ততোক্ষণ পর্যন্ত থেকেই যায়, যতক্ষণ না অন্য কোনো ডাটা এসে সেটির উপর প্রতিস্তাপিত না হয়।

অর্থ্যৎ ভুলবশত ডিলিট করা ফাইল বা ডাটা পুনরুদ্ধার করতে দ্রুত পদক্ষেপ গ্রহণ করা হলে ডাটা ফিরে পাবার সুযোগ অনেক বেড়ে যায় ।ডিলিট হওয়া ডাটা পুনরুদ্ধার করার জন্য কোনো ভালো ডাটা রিকভারি সফটওয়্যার ব্যবহার করা যেতে পারে। কোনো গুরুত্বপূর্ণ ফাইল বা ডাটা ডিলিট হয়ে যাওয়ার পরে কম্পিউটারের সাথে যে-কোনো কার্যকলাপ সেই ডাটাকে চিরতরে হারিয়ে ফেলার জন্য দায়ী হতে পারে। কারণ এতে নতুন ডাটা ওভাররাইট হওয়ার সুযোগ থাকে ।এমনকি ইন্টারনেট ব্রাউজিং করলেও পুরাতন বা হারিয়ে যাওয়া ক্যাশ ফাইল বা কুকিজগুলো ওভাররাইট হয়ে যেতে পারে। ফলে আর সেগুলো ফিরে পাওয়া যাবে না ।ডাটা রিকভারি সফটওয়্যারগুলো শুধু সেই ডাটাকেই পুনরুদ্ধার করতে পারে,যা ওভাররাইট হয়নি।

আবার ডিলিট হওয়া ডাটা কতটা দ্রুত ফিরে পাওয়া যাবে, সেটা অনেক সময় নির্ভর করে ফাইল সিস্টেমের উপরে ।উদাহরণস্বরূপ ঃ উইন্ডোজ এনটিএফএস ফাইল সিস্টেম কোনো ফাইল কিংবা সেই ফাইলের ডাটা ডিলিট হওয়ার পরেও বিবরণী তথ্য সংরক্ষণ করে রাখে। ফলে যে-কোনো ডাটা রিকভারি সফটওয়্যারের কাছে ফাইলটি খুঁজে পাওয়া অনেক সুবিধাজনক হয়ে যায়।

২। **ডাটা করাপশন ঃ** যদি কম্পিউটার বারবার মেসেজ আসতে শুরু করে "আপনার হার্ডড্রাইভ করাপ্টেড হয়ে গেছে", তাহলে যে-কোনো কম্পিউটার ব্যবহারকারীর কাছে এটি একটি দুঃস্বপ্নের ব্যাপার। তবে সেক্ষেত্রে ডাটাগুলো পুনরুদ্ধারিত করার সুযোগ রয়েছে। প্রথমই হার্ডড্রাইভটি অন্য একটি কম্পিউটারের সাথে লাগিয়ে চেক করে দেখতে হবে।যদি শুধু ঐ ড্রাইভটির অপারেটিং সিস্টেম করাপ্টেড হয়,তবে অনেক সহজেই বাকি ডাটাগুলো কপি করে নেয়া যাবে। কিন্তু যদি হার্ডড্রাইভের পার্টিশন টেবিল করাপ্টেড হয়ে যায়, তাহলে সেখান থেকে ডাটা রিকভারি করা একটু জটিল এবং কষ্টকর।তখন পার্টিশন টেবিল থেকে ডাটা উদ্ধার করার চেষ্টা করা হয়।যদি রিকভার করা ডাটা করাপ্টেড হয়, তবে ডাটা রিকভারি সফটওয়্যার ব্যবহার করে সেগুলোকে ব্যবহারযোগ্য করা সম্ভব।

৩। **ফাইল সিস্টেম ফরম্যাট ঃ** ডিলিট হওয়া ডাটা অনেকটাই নির্ভর করে ডাটার ফাইল সিস্টেমের উপর।যেমন– এফএটি ফাইল সিস্টেমে কোনো বড় ডাটা ডিলিট করে দিলে ড্রাইভের সেই অংশকে অংশকে সম্পূর্ণ জিরো দ্বারা ওভাররাইট করে দেয়া হয়।ফলে আগের ফাইলটি ফিরে পাওয়া অনেক কঠিন হয়ে যায়। কিন্তু এনটিএফএস ফাইল সিস্টেমে কোনো ডাটা রিকভার করা অনেক সহজ হয়ে থাকে।

যদি কোনো ডাটা ধ্বংস হয়ে যায়, তবে সেটি ফিরে পাবার ক্ষেত্রে নির্ভর করে ডাটা বা ফাইলটি ঠিক কতটা ক্ষতিগ্রস্ত হয়েছে তার উপর। যদি ডাটা রিকভাবি সফটওয়্যার ক্ষতিগ্রস্ত ডাটাগুলো থেকে যথেষ্ট পরিমাণ ডাটা উদ্ধার করতে সক্ষম হয়,তবে ধ্বংস হওয়া ডাটা ব্যবহারের যোগ্য হতে পারে।

৪। **ফিজিক্যাল হার্ডড্রাইভ ড্যামেজ ঃ** অনেকভাবে একটি হার্ডড্রাইভ ফিজিক্যালি ড্যামেজ হতে পারে।অনেক সময় শুধুমাত্র ড্রাইভটির কন্ট্রোলার বোর্ড বা হেড ড্যামেজ হয়।এই অবস্থায় এগুলোকে পরিবর্তন করে ড্রাইভটি রিপেয়ার করা যেতে পারে।কিন্তু এই পরিবর্তনগুলো করাতে বা যে-কোনো গুরুতর ড্যামেজ থেকে ড্রাইভটিকে সারাতে অবশ্যই বিশেষজ্ঞদের সাহায্য নেওয়া উচিত। ড্যামেজ বা ধ্বংস হওয়া হার্ডড্রাইভ থেকে ডাটা রিকভার করা অনেক কঠিন কাজ। শুধুমাত্র ডাটা রিকভারি বিশেষজ্ঞরাই এটি করে থাকেন। তারা একটি বদ্ধ এবং অত্যন্ত পরিষ্কার রুমে এই কাজটি সম্পন্ন করে থাকেন। এই রুমটি অত্যন্ত নিয়ন্ত্রিত পরিবেশের হয়ে থাকে এবং সকল প্রকারের প্রাকৃতিক দূষণমুক্ত হয়ে থাকে।এই অবস্থায় একটি সামান্য ধূলিকণাও হার্ড ড্রাইভটিকে সম্পূর্ণ অকেজো করতে পারে। ডাটা রিকভারি বিশেষজ্ঞগণ বিভিন্ন ধাপ অনুসরণ করে ড্রাইভটি ফিক্সট করানোর চেষ্টা করে।প্রথম এর ফিজিক্যালি ড্যামেজ ঠিক করে এবং পরে ড্রাইভটি রান করিয়ে সেটা

থেকে স্পেশাল সফটওয়্যার ব্যবহার করে ডাটাগুলোকে রিকভার করানোর চেষ্টা করে ।এই সম্পূর্ণ প্রসেসটি একটি নিয়ন্ত্রিত কক্ষে করা হয়। তবে এ প্রক্রিয়াটি ব্যয়বহুল হয়ে থাকে।

৫। **সলিড স্টেট ড্রাইড রিকভারি ঃ** বর্তমানে সলিড স্টেট ড্রাইভগুলো অনেক বেশি জনপ্রিয় হয়ে উঠছে। বিশেষ করে বর্তমান নতুন আল্ট্রাবুকগুলোতে সলিড স্টেট ড্রাইভ থাকছে প্রধান চমক হিসেবে ।এসএসডি থেকে ডাটা রিকভার করা যে-কোনো ট্র্যাডিশনাল হার্ডড্রাইভ থেকে অনেক সহজ এবং কার্যকরী। ডিলিট হওয়া বা ফরম্যাট হওয়া ডাটা রিকভারি করার প্রসেস এখানেও একই। তবে ফিজিক্যালি ড্যামেজ হওয়া সলিড স্টেট ড্রাইভ থেকে ডাটা রিকভার করা অনেক ব্যবহুল।

এ ছাড়াও ডাটা রিকভারি যে-সকল ডিভাইস থেকে করা সম্ভব সেগুলো হলো ঃ হার্ড ডিস্ক ড্রাইভ, সলিড স্টেট ডিভাইস, ইউএসবি, ফ্ল্যাশ ড্রাইভ, এক্সটারনাল হার্ড ড্রাইভ, এসডি কার্ড বা মেমরি কার্ড, ডিজিটাল ক্যামেরা, সিডি বা ডিভিডি, স্মার্টফোন,ট্যাবলেট, আইফোন, অ্যান্ড্রয়েড, ল্যাপটপ, ব্যাকআপ ড্রাইভ ইত্যাদি।

ডাটা রিকভরির সীমাবদ্ধতা ঃ

ডাটা রিকভারি সবসময় ডাটা পুনরুদ্ধারের নিশ্চয়তা প্রদান করে না ।ডিলিট করা বা ফরম্যাট করা ডাটাকে ততক্ষণ পর্যন্ত পুনরুদ্ধার করা যায়, যতক্ষণ না এটি ওভাররাইট করা হয়। কিন্তু ডাটা রিকভারির কিছু উল্লেখযোগ্য সীমাবদ্ধতা রযেছে, যা নিম্নে উল্লেখ করা হলো ঃ

১. গুরুতর ক্ষতিগ্রস্ত স্টোরেজ ডিভাইস হলে ডাটা রিকভারি করা অসম্ভব হয়ে পড়ে।
২. রিকভারি প্রোগ্রাম দ্বারা ডাটা স্টোরেজের অবস্থান চিহ্নিত করা যায় না।
৩. ডাটা ওভাররাইট করা হলে প্রায় সময়ই ডাটা রিকভার করা যায় না।
৪. ফাইল এবং ফোল্ডার বেশি সংক্রামিত হলে হেডার ফাইলে প্রবেশ করা যায় না ।
৫. Storage device পুড়ে গেলে Data recovery প্রায় অনম্ভব।

ডাটা লস প্রতিহত করার উপায় ঃ ডাটা লস প্রতিহত করার সবচেয়ে ভালো উপায় ডাটা ব্যাকআপ। জনপ্রিয় তিনটি ডাটা ব্যাকআপ পদ্ধতি হলো ঃ

১. এক্সটার্নাল ড্রাইভের মাধ্যমে ব্যাকআপ
২. সার্ভারের মাধ্যমে ব্যাকআপ
৩. ক্লাউড স্টোরেজের মাধ্যমে ব্যাকআপ।

পার্সোনাল ও অফিসিয়াল ডাটা হলে এক্সটার্নাল ড্রাইভে ব্যাকআপ করে রাখা যায়। আবার কোম্পানির সার্ভার থাকলে কর্পোরেট ডাটা সেখানেও তুলে রাখা যায়। সার্ভার না থাকলে বা নিজের ডাটা হলে ক্লাউড স্টোরেজ যেমন - গুগল ড্রাইভ, ওয়ান ড্রাইভ এসবেও সংরক্ষণ করা যায়।

ফরেনসিক টুল কিট ঃ

কম্পিউটার বা স্মার্টফোন বা ডিজিটাল কোনো ডিভাইস ব্যবহার করে কোনো অপরাধ সংগঠিত হলে স্মার্ট ডিভাইস বা কম্পিউটার ফরেনসিক করা হয় এবং খুন হলে মৃতদেহ পরীক্ষা করার পাশাপাশি তার কম্পিউটার ও স্মার্টফোনেরও ফরেনসিক করা হয়। অর্থাৎ, মৃত্যু/অপরাধ সংঘটিত হওয়ার সময়ে/আগে ভিক্টিম/অপরাধীর সাথে কারোর যোগাযোগ হয়েছিল কি না তা চেক করা হয় ।ভিক্টিম/অপরাধীর সংরক্ষিত ডাটা , কল লিস্ট, রেকর্ড, ফোন বুকসহ সবকিছুই খুটিয়ে দেখা হয়। কারোর সাথে ই-মেইল আদান-প্রদান করে থাকলে তা দেখা হয়। ঘটনার শুরু থেকে শেষ পর্যন্ত যা করেছে, তা ভিক্টিম/আসামীর কম্পিউটার-স্মার্টফোন ব্যবহার করে সকল তথ্য রিকভারি করে প্রাসঙ্গিক তথ্য খুঁজে বের করা হয় ।এটি ডিজিটাল ফরেনসিক বা কম্পিউটার ফরেনসিক নামে পরিচিত।

কম্পিউটার ফরেনসিক সম্পন্ন করার উদ্দেশ্যে তৈরিকৃত একপ্রকার টুল হলো FTK বা ফরেনসিক টুল কিট ।এটি তদন্তকারীদের সকল ফরেনসিক সরঞ্জামগুলোকে এক জায়গায় একত্রিত করার সুবিধা প্রদান করে ।ফরেনসিক সম্পন্ন করার উদ্দেশ্যে কোনো পাসওয়ার্ড ক্র্যাক করা, ই-মেইল বিশ্লেষণ করা, কোনো ফাইলে নির্দিষ্ট অক্ষরের সন্ধান করা সহ বিভিন্ন ক্ষেত্রে FTK ব্যবহার করা হয় ।কিছু পার্থক্য রয়েছে যা অন্যন্ত্র টুল থেকে FTK- কে পৃথক করে। ডিস্ট্রিবিউটিং প্রসেসিং পদ্ধতি সাবস্ক্রাইব করা, মাল্টি কোর CPU- কে সমান্তরালভাবে ব্যবহার করা ইত্যাদি ফিচারের জন্য এটি অন্যান্য ফরেনসিক টুলস থেকে ব্যতিক্রম। FTK - এর আরেকটি অনন্য বৈশিষ্ট্য হলো এটি শেয়ারকৃত কেস ডাটাবেস ব্যবহার করে। ডাটাসেটগুলোর একাধিক কাজ কপি করার পরিবর্তে, FTK শুধুমাত্র একটি একক কেন্দ্রীয় ডাটাবেস ব্যবহার করে ।নিম্নে FTK এর বিভিন্ন প্রকার ব্যবহার উল্লেখ করা হলো ঃ

১. **ই-মেইল বিশ্লেষণ ঃ** FTK ফরেনসিক পেশাদারদের জন্য ই-মেইল বিশ্লেষণের একটি ইন্টারফেস প্রদান করে। এতে নির্দিষ্ট শব্দগুলোর জন্য ই-মেইল বিশ্লেষণ করার ক্ষমতা, সোর্স আইপি অ্যাড্রেসের জন্য শিরোনাম বিশ্লেষণ ইত্যাদি ব্যবস্থা রয়েছে।

২. **ফাইল ডিক্রিপশন ঃ** FTK এর একটি কেন্দ্রীয় বৈশিষ্ট্য হলো ফাইল ডিক্রিপশন ।পাসওয়ার্ড ক্র্যাক বা সম্পূর্ণ ফাইল ডিক্রিপ্ট করতে চাইলে, FTK এর উত্তর প্রদান করে থাকে। FTK এর মাধ্যমে ১০০ টির বেশি অ্যাপ্লিকেশনের পাসওয়ার্ড পুনরুদ্ধার করা যায়।

৩. **ডাটা কারভিং করা ঃ** FTK এর একটি শক্ত ডাটা কারভিং ইঞ্জিন ব্যবস্থা রয়েছে ।অনুসন্ধানকারীদের আকার, ডাটা টাইপ এবং পিক্সেল আকারের উপর ভিত্তি করে ফাইল অনুসন্ধান করার জন্য বিকল্প ব্যবস্থা রয়েছে।

৪. **তথ্য ভিজুয়ালাইজেশন ঃ** পাঠ্য তথ্য বিশ্লেষণ করার পরিবর্তে ফরেনসিক বিশেষজ্ঞরা এখন বিভিন্ন তথ্য কল্পনা কৌশল ব্যবহার করে একটি মামলার জন্য আরো স্বজ্ঞাত চিত্র তৈরি করতে পারেন। FTK ব্যবহারকারীদেরকে টাইমলাইন নির্মাণ, ক্লাস্টার গ্রাফ এবং জিওলোকেশনের ক্ষমতা প্রদান করে।

৫. **ওয়েব ভিউয়ার ঃ** FTK ওয়েব ভিউয়ার টুল-এর মাধ্যমে রিয়েল টাইমে কেস ফাইলগুলোকে অ্যাক্সেস প্রদানের মাধ্যমে কেস মূল্যায়ন ত্বরান্বিত করে ।এটি মাল্টি কেস অনুসন্ধানের জন্যও অনুমোদন করে, যার অর্থ হচ্ছে বিভিন্ন ক্ষেত্রে ম্যানুয়ালি ক্রস রেফারেন্স প্রমাণ করতে হবে না।

৬. **সারবেরাস ঃ** FTK এর শক্তিশালী স্বয়ংক্রিয় ম্যালওয়্যার শনাক্তকরণ বৈশিষ্ট্য রয়েছে, যার নাম সারবেরাস এটি কম্পিউটারে ম্যালওয়্যার স্নিফার করার জন্য মেশিন বুদ্ধিমত্তা ব্যবহার করে, পরে পাওয়া গেলে এটি মোকাবেলা করার জন্য পদক্ষেপ গ্রহণ করে।

৭. **অপটিক্যাল ক্যারেক্টার চিহ্নিতকরণ ঃ** FTK এর অপটিক্যাল ক্যারেক্টার চিহ্নিতকরণ ইঞ্জিন ইমেজকে পঠনযোগ্য টেক্সটে রূপান্তর করে ।এতে একাধিক ভাষা সমর্থন করা হয়।

বিভিন্ন প্রকার কম্পিউটার ফরেনসিক টুলস ঃ

ডিজিটাল কোনো ডিভাইস ব্যাবহার কওে কোনো আপরাধ সংঘঠিত হলে স্মাট কম্পিউটার ফরেনসিক সম্পুন্ন করতে কিছু টুলস ব্যবহার করা হয়, যাদেও কম্পিউটার ফরেনসিক টুলস বলা হয় ।নিম্নে এনকম কিছু টুলস উল্লেখ করা হলোঃ

P2 Explorer : এটি আকর্ষণীয় একটি ডিস্ক ইমেজ ব্রাউজ করার অনুমতি প্রদান করে। যেহেতু এটি একটি ডিস্ক ইমেজ,সেজন্য এটি কেবল মাত্র রিট করতে

পারে ।এর মানে বিষয়বস্তু পরীক্ষা করার পর এটিতে পরিবর্তন করা যাবে না ।এটি একটি গুরুত্বপূর্ণ টুল, যেখানে ।নেক কম্পিউটার ডিস্ক আছে। p2 Explorer ফ্রি এবং পেইড উভয় সংকরণে পাওয়া যায় ।ফ্রি সংস্করণ শুধুমাত্র ৩২- বিট উপারেটিং সিস্টেমে চালানো যায়।

Digital Forensic Framwork: এটি একটি ওপেন সোর্স সফটওয়্যার, যা নিম্নক্ত আনুমতি প্রদান করেঃ

১। রাইট ব্লক করা।

২। উইন্ডোজ অপারেটিং সিস্টেম থেকে লিনাক্স ফাইল পুনরুদ্ধার করা।

৩। ডিস্ক এবং ড্রাইভের দূরবর্তী অ্যাক্সেস।

৪। ডিলিট এবং হিডেন ফাইল পুনোরুদ্ধার এবং পরীক্ষা করে দেখা।

Freeware Hex Editor and Disk Editor (Hxd): এটি এমন আরেকটি টুল, যা ফাইল সিস্টেম এবং উদ্দেশ্য বিশ্লেষণ করে। এটি যে কোনো আকারের ফইলগুলোকে পরিচালনা করতে পারে ।এর ইন্টারফেস ব্যবহার করা সহজ ।কম্পিউটারটি কীভাবে কাজ কওে তার সামান্য জ্ঞান থাকলেও এটি ব্যবহার করা যায়।

Plain Slight: এটি একটি ওপেন সোর্স টুল ।এটি সমগ্র সিস্টেমের বিভিন্ন উপায়ে পূর্বরূপ দেখতে সহায়তা করে ।এর ইন্টার ফেস ব্যবহার সহজ । এটি ডিলিট করা ফাইল পুনরুদ্ধার,হিডেন ফাইল এবং ফোল্ডার পুনরুদ্ধার,হার্ড ডিক্স তথ্য প্রাপ্তি, USB স্টোরেজ তথ্য পরীক্ষাসহ বিভিন্ন কাজ করতে পারে।

Bulk Extractor: এটি হিডেন, সিস্টেম এবং ডিলেট করা ফাইল রেকর্ড করতে সক্ষম হয়।

কম্পিউটার ফরেনসিক বনাম কম্পিউটার নিরাপত্তাঃ যদিও কম্পিউটার ফরেনসিক প্রায়ই কম্পিউটার নিরাপত্তার সাথে যুক্ত থাকে, তবে দুটি ভিন্ন। কোথাও একটি অননুমোদিত অ্যাক্সেস বা ব্যাবহার ঘটার পর কম্পিউটার ফরেনসিক প্রাথমিকভাবে একটি ডিজিটাল অপরাধ প্রমাণের সঠিক অধিগ্রহন, সংরক্ষন এবং বিশ্লেষণ করে। আর অননুমোদিত অ্যাক্সেসের অথবা সাইবার অপরাধ প্রতিরোধ করার পাশাপাশি কম্পিউটার সিস্টেমের গোপনীয়তা, সততা এবং প্রাপ্যতা রক্ষণাবেক্ষণের জন্য কম্পিউটার নিরাপত্তা ব্যবহার করা হয় । যাইহোক, কম্পিউটার নিরাপত্তা

এবং কম্পিউটার ফরেনসিক একে অপরের সাথে সম্পর্কিত। কম্পিউটার নিরাপত্তায় অপরাধ ঠেকাতে সাধারণত কম্পিউটার, নেটওয়ার্ক এবং অন্যান্য ডিভাইসগুলোর অ্যাক্সেস এবং ব্যাবহাওে যথাযথ নিয়ন্ত্রণই কম্পিউটার ফরেনসিক।

এক জন কম্পিউটার ফরেনসিক এক্সপার্টকে নিম্নক্ত বিষয়সমূহে পারদর্শী হতে হয় ঃ

১। নেটওয়ার্কিং, নেটওয়ার্ক কমিউনিকেশন, টিসিপি/আইপি প্রটকল, নেটওয়ার্ক ট্রেসিং ইত্যাদি সম্পর্কে দক্ষ হতে হবে।

২। উইন্ডজ, ইউনিক্স, লিনাক্স্ বেং অ্যান্ড্রয়েড অপারেটিং সিস্টেমে দক্ষ হতে হবে।

৩। সিসি প্লাস প্লাস, সি শার্প, জাভা এবং পাইথন প্রোগ্রামিং ভাষার উপর দক্ষ হতে হবে।

৪। কম্পিউটার হার্ডওয়্যার ও সফটওয়্যার সিস্টেম সম্পকে জানতে হবে।

৫। অপারেটিং সিস্টেম ইনস্টলেশম, প্যাচিং ও কনফিগারেশন করার দক্ষতা থাকতে হবে।

৬। ব্যাকআপ ও আর্কাইভিং টেকনোলজি সম্পর্কে জানতে হবে।

৭। ক্রিপ্টোগ্রাফির সূত্র, এসকেসি, পিকেসি এবং সাইফার জানতে হবে।

৮। ই-ডিসকভারি অ্যাপ্লিকেশনের (যেমন এনইউঅইএক্স, রিলেটিভিটি, ক্লিয়ারওয়েলে ইত্যাদি) ব্যবহার এর উপর যথেষ্ট পরিমান দক্ষ হতে হবে।

৯। বিভিন্ন ধরনের ফরেনসিক সফটওয়্যার অ্যাপ্লিকেশনের কাজে দক্ষ হতে হবে।

১০। এনকেইস, এফটিকে, হেলিক্স, সেলিব্রাইট, এক্সআরওয়াইযের মতো সফটওয়্যারের কাজ সম্পকে জানতে হবে।

১১। ডাটা প্রসেসিং ও ইলেকট্রনিক ডিসক্লোসার এনভারনমেন্ট সম্পকে জানতে হবে।

১২। এভিডেন্স হ্যান্ডেলিং প্রসিডিউর ও এসিপিও গাইডলাইন সম্পকে জানতে হবে।

১৩। ক্লাউড কম্পিউটিং ও ক্লাউড সার্ভার সম্পকে জানতে হবে।

বিভিন্ন প্রকার ব্যাক্তিগত শনাক্তকরণযোগ্য তথ্য ঃ

ব্যক্তিগতভাবে শনাক্তকরনযোগ্য তথ্য বা (PII) হলো কোনো নিদিষ্ট ব্যবহারকারী বা ব্যক্তির সাথে যোগাযোগ, শনাক্তকরণ বা চিহ্নিত করতে ব্যবহা করা কিছু নির্দিষ্ট ডাটার সমষ্টি ।কোনো নিদিষ্ট ব্যাবহারকারী বা ব্যক্তি শনাক্ত করার জন্য ব্যবহৃত উপাদান কয়েকটি উপাদান হলো বায়োমেট্রিক ডাটা, আঙ্গুলের ছাপ, নাম, টেলিফোন নাম্বার, ই-মেইল ঠিকানা ইত্যাদি। এটি এক ধরনের গ্রাহক তথ্য নিরাপত্তা । ব্যক্তিগত শনাক্তকরণযোগ্য তথ্য মূলত দুই প্রকার,যথা-

১। **সেনসেটিভ ব্যক্তিগত শনাক্তকরন তথ্য ঃ** সেনসেটিভ ব্যক্তিগত তথ্যগুলেতে পূর্ণ নাম, সামাজিক নিরাপত্তা নাম্বার (এসএসএন), ড্রাইভিং লাইসেন্স, মেইলিং ঠিকানা, ক্রেডিট কার্ড তথ্য, পাসপোর্ট তথ্য এবং আর্থিক তথ্য ইত্যাদি অন্তর্ভুক্ত থাকে।

২। **নন-সেনসেটিভ ব্যক্তিগত শনাক্তকরণযোগ্য তথ্য ঃ** এই প্রকার ব্যক্তিগত তথ্যগুলো সহজেই ফোনবুক, ইন্টারনেট এবং কর্পোরেট ডিরেক্টরিগুলোর মতো উৎস থেকে অ্যাক্সেস করা যায়। জিপ কোড, জাতি, লিঙ্গ, জন্ম তারিখ ইত্যাদি নন-সেনসিটিভ ব্যক্তিগত তথ্য।

বিভিন্ন ধরনের ই-মেইল থ্রেড ঃ

ই-মেইল থ্রেড হলো একই ধরনের ই-মেইল বার্তাগুলোর একটি গ্রুপ ।ই-মেইল থ্রেড প্রেরিত সমস্ত ই-মেইল ধারন করে থাকে এবং ডকুমেন্টেশনের উদ্দেশ্যে খুব দরকারি, অতীত কথোপকতন ট্র্যাক করে রাখার অনুমতি প্রদান করে থাকে। কিন্তু যকন বিষয়টি বন্ধ হয়ে যায় বা কথোপকথন বেশ লম্বা হয়ে যায়, তখন ই-মেইল থ্রেডিং একটি বিরক্তিকর কারণ হতে পারে। ই-মেইল থ্রেডিংকে কথোপকথন থ্রেডিংও বলা হয়; কারন এটি কেবল ই-মেইলের সাথেই নয়, ইন্টরনেট ফোরাম, নিউজগ্রুপ এবং অন্যান্য অংশ যা ব্যবহারকারীরা তথ্য ভাগ কওে বা প্রশ্ন করে ।নিম্নে বিভিন্ন ধরনের ই-মেইল থ্রেড উল্লেখ করা হলোঃ

Ois ডিভাইসে ই-মেইল থ্রেডিং ঃ অ্যাপল Ois এর বিল্ট-ইন মেইল অ্যাপ্লিকেশনটিতে ই-মেইল থ্রেডিং নিয়ন্ত্রণে বেশ কয়েকটি সিটিংস রয়েছে। ই-মেইল থ্রেডিং বাই ডিফল্ট চালু থাকে।

- Settings প্রেস কওে তারপর Mail অপশনে যেতে হবে।
- Threading Section এ স্ক্রোল করে নিম্নের একটি অপশন সিলেক্ট করতে হবে।

(ক) Organize by thread ঃ এই সেটিংসটি ই-মেইলগুলোতে থ্রেডিং ব্যাবহার করা হয় কিনা তা নিয়ন্ত্রন করে।

(খ)Most Recent Message on Top ঃ এটি ডিফল্টভাবে বন্ধ থাকে, তবে এটি একটি ভাল বিকল্প থ্রেডিং চালু করার জন্য

(গ) Complete Threads ঃ এই সেটিংস অন্য মেইলবক্স থেকে উদ্ধৃত হলেও বার্তাকে থ্রেড গুলোতে ই-মেইল করে।

Android ডিভাইসে ই-মেইল থ্রেডিং ঃ অ্যান্ড্রয়েড ৫.০ ললিপপে জিমেইল অ্যাপ্লিকেশনু এর ব্যবহার শুরু হয়। অ্যান্ড্রয়েডের জিমেইলে ই-মেইল থ্রেডিং ডিফল্ট ভাবে বন্ধ করে দেওয়া হয় ।একটি অ্যান্ড্রয়েড ডিভাইসে নিম্ন ই-মেইল থ্রেডিং নিয়ন্ত্রন করা হয়ঃ

১। জিমেইল খুলে ইনবক্সের বামে তিন-লাইনের আইকনে ক্লিক করতে হবে।

২। আতীতের সকল ফোল্ডার স্ক্রোল করে সিটিং নির্বাচন করতে হবে।

৩। কনভার্সন ভিউ এর পাশে চেকবক্সটিতে টিক দিতে হবে।

৪। থ্রেড ই-মেইল কথোপকথন দেখতে পুনরায় ই-মেইলে ফিরে যেতে হবে।

অধ্যায় ঃ ০৩

সাইবার অপরাধ

ভূমিকা :

ইন্টারনেটকে বলা হয় তথ্য প্রযুক্তির সূতিকাগার। এটা জ্ঞানের অবারিত হাজার দরজা খুলে দিচ্ছে আমাদের সামনে। এ মাধ্যমে মানব সভ্যতা যেমন উপকৃত হচ্ছে , তেমনি এর চরম অপকারিতা ও রয়েছে। এর মধ্যে সাইবার অপরাধ বা সাইবার ক্রাইম শব্দটি প্রতিটি দেশেই অনেক পরিচিত এবং ভীতিজনক একটি শব্দ। এই শব্দে সাথে পরিচিত হোক বা না হোক, প্রতিদিন লক্ষ লক্ষ লোক এ শিকার হচ্ছে। সাইবার অপরাধ বিশ্বের কোন নতুন ধরনের অপরাধ নয়। তথ্য চুরি, তথ্য বিকৃতি, জালিয়াতি, ব্ল্যাকমেইল, মানি লন্ডারিং ইত্যাদি অপরাধ গুলো ইন্টারনেটের মাধ্যমে করা হলে সেটি সাইবার অপরাধ হিসাবে গণ্য করা হয়।

সাধারণ ভাষায় বলা যায় যে, ইন্টারনেটের মাধ্যমে যে-কোনো অপরাধ সংঘটিত হলে তাকে সাইবার অপরাধ বলে। সাইবার অপরাধ এমন একটি অপরাধ, যাতে প্রধানত

কম্পিউটার বা অন্য কোনো ইলেকট্রনিক যন্ত্র ব্যবহৃত হয় এবং অপরাধীরা বিশ্বব্যাপি অপরাধে ইন্টারনেট ব্যবহার করে। বর্তমানে উন্নত দেশগুলোতে সাইবার অপরাধকে অপরাধের তালিকায় শীর্ষে স্থান দেওয়া হয়েছে। তৈরি হয়েছে সাইবার অপরাধ রোধের জন্য নতুন নতুন নিয়ম ও আইন। অন্যান্য দেশে মতো বাংলাদেশেও সাইবার ক্রাইম এবং এ সংক্রান্ত অপরাধগুলো দমনের আইন প্রণয়ন করা আছে।

সাইবার অপরাধঃ

সাইবার ক্রাইম একটি ইংরেজি শব্দ, যার অভিধানিক অর্থ ভার্চূয়াল জগতের অপরাধ। নেটওয়ার্ক সংযোগ মাধ্যমে অথবা নেটওয়ার্ক সংযোগ ব্যতীত কম্পিউটার, অথবা মোবাইল মাধ্যমে কারো অনুমতি ব্যাতীত ভার্চূয়াল জগতের তথ্য চুরি, বিকৃতি, সংযোগ ধ্বংস করাকে সাইবার ক্রাইম বলে বিবেচিত। যারা এগুলোর সাথে জরিত তাদের সাইবার ক্রিমিনাল বলা হয়। বিভিন্ন প্রকার ক্রাইমের মধ্যে উল্লেখযোগ্য ক্রাইম হচ্ছে হ্যাকিং, ফিশিং, সাইবার বুলিং ইত্যাদি।

David Bohm ও Nikki Haley সাইবার অপরাধকে এভাবে সংজ্ঞায়িত করেছেন যে, কম্পিউটার প্রযুক্তি ব্যবহারের মাধ্যমে অপরাধ সংগটন করাকে বল হয় সাইবার অপরাধ।

তবে সাইবার অপরাধ ও কম্পিউটার দ্বারা কৃত অপরাধের মধ্যে কিছু পার্থক্য রয়েছে। শুধুমাএ কম্পিউটার ব্যবহারের মাধ্যমে অনেক অপরাধ করা সম্ভব হলেও, ইন্টারনেট ব্যবহারের মাধ্যমে এই অপরাধের পরিমাণ বহুগুন বাড়ানো যায়। সেদিক থেকে কম্পিউটার প্রযুক্তির সাথে তথ্য প্রযুক্তির সমন্বয়ের মাধ্যমে যে-সব অপরাধ সংগটিত হয়, সেগুলো হবে সাইবার অপরাধ বা সাইবার ক্রাইম।

সাইবার অপরাধসমূহঃ সাইবার অপরাধ বিভিন্ন প্রকার হয়ে থাকে, যেমনঃ

১। মোবাইলে মেসেজে কারও সম্পর্কে অশালীন বা কুরুচিকর মন্তব্য।

২। ই-মেইলে কারো সম্পর্কে অশালীন বা কুরুচিকর মন্তব্য।

৩। ফেসবুকে হোয়াটসঅ্যাপে কুরুচিকর ছবি বা মেসেজ পাঠানো।

৪। কারো ছবি সুপার-ইমপোজ করে ছড়ানো।

৫। কম্পিউটার সিস্টেমের আইপি কোড চুরি বা হ্যাক করা।

৬। এটিএমের পিন নাম্বার জেনে প্রতারণা।

৭। ব্যক্তিগত বা আপত্তিজনক ছবি না জানিয়ে প্রকাশ্যে আনা।

৮। সরকারি তথ্য বিক্রি করার চেস্টা করা।

৯। সরকার বা সরকারি পদাধিকারীর বিরুদ্ধে গুজব ছড়ানো।

এছাড়া অনলাইনে যে-কোনো অপরাধমূলক কর্মকান্ডে জড়িত হলে সবাই সাইবার অপরাধের অন্তভূক্ত।

সাইবার অপরাধের কারনসমূহ: যেসব কারনে সাইবার অপরাধ সংগঠিত হয়, এর মধ্যে উল্লেখযোগ্য কারনসমূহ হলো:

১। অপরাধীর প্রযুক্তি বিষয়ে দক্ষতা।

২। গতানুগতিক পদ্ধিতিতে অপরাধ সংগটনের সুযোগ ও ক্ষেএ কমে যাওয়া।

৩। সমাজে কম্পিউটার ও তথ্যপ্রযুক্তির ব্যাপক বিস্তার।

৪। এ ধরনের অপরাধের ক্ষেত্রে ঝুঁকি কম থাকা বা না থাকা।

৫। অপরাধীর বিরুদ্ধে আইনগত ব্যরস্থা গ্রহনে জটিলতা।

৬। প্রচুর আর্থিক লাভের সস্ভাবনা।

৭। কম্পিউটার ও তথ্যপ্রযুক্তি ব্যবহারকারীদের অসর্তকতা ও অদক্ষতা।

৮। সাইবার অপরাধকে সংজ্ঞায়িত করার ক্ষেত্রে অপরাধ আইনের অপর্যাপ্ততা।

৯।প্রকৃত অপরাধী নির্নয়ে সমস্যা।

১০। অপরাধের নতুন নতুন কৌশল উদ্ভাবন ও আইন প্রয়োগকারী সংস্থার দূর্বলতা।

১১। কিছু কিছু সাইবার অপরাধের ক্ষেত্রে ক্ষতিগ্রস্থ ব্যক্তির আইনি ব্যবস্থা গ্রহনে অনাগ্রহ ইত্যাদি সাইবার অপরাধ সংগঠনের প্রধান কারন।

বাংলাদেশে সাইবার অপরাধের আইন: সাইবার অপরাধ বলতে ইন্টারনেট ব্যবহার করে যে অপরাধ করা হয়, তাকেই বুঝানো হয়েছে। উন্নত বিশ্বে সাইবার অপরাধকে তালিকায় শীর্ষে স্থান দেয়া হয়েছে। তৈরি করা হয়েছে সাইবার অপরধীদের জন্য নতুন নতুন আইন। বাংলাদেশে সাইবার অপরাধের পরিচিতি বা এ সংক্রান্ত অপরাধ দমনের জন্য আইন রয়েছে। তথ্য ও যোগাযোগ প্রযুক্তি আইন ২০০৬ এ বিষয়ে নির্দেশনা দেয়। এই আইনে অপরাধের শাস্তিগুলো নিম্নরুপ:

(ক) ৫৪ ধারা অনুযায়ী কম্পিউটার বা কম্পিউটার সিস্টেম ইত্যাদির ক্ষতি, অনিষ্ট সাধন যেমন-ই-মেইল পাঠানো, ভাইরাস ছড়ানো, সিস্টেমে অনাধিকার প্রবেশ বা সিস্টেমের ক্ষতি করা ইত্যাদি অপরাধ। এর শাস্তি সর্বোচ্চ ১৪ বছর কারাদন্ড এবং সর্বনিম্ন ৭ বছর কারাদন্ড বা ১০ লাখ টাকা পর্যন্ত জরিমানা।

(খ) ৫৬ ধারা অনুযায়ী-কেউ যদি ক্ষতি করার উদ্দেশ্যে এন কোনো কাজ করে, যার ফলে কোনো কম্পিউটারে রির্সোসের কোনো তথ্য বিনাশ, বাতিল বা পরিবর্তিত হয় বা এর উপযোগিতা হ্রাস পায় অথবা কোনো কম্পিউটার, সার্ভার নেটওয়ার্ক বা কোনো ইলেকট্রনিক সিস্টেমে অবৈধভাবে প্রবেশ করে, তবে এটি হবে হ্যাকিং অপরাধ। এর শাস্তি সর্বোচ্চ ১৪ বছর কারাদন্ড এবং সর্বনিম্ন ৭ বছর কারাদন্ড বা ১ কোটি টাকা পর্যন্ত জরিমানা।

(গ) ৫৭ ধারা অনুযায়ী- কোনো ব্যক্তি যদি ইচ্ছাকৃতভাবে ওয়েবসাইটে বা অন্য কোনো ইলেকট্রনিক বিন্রাস কোনো মিথ্যা বা অশ্লীল কিছু প্রকাশ বা সম্প্রচার করে, যার দ্বারা মানহানি ঘটে, আইনশৃঙ্খলার অবনতি হয় অথবা রাষ্ট্র বা ব্যক্তির ভাবমূতি ক্ষুণ্ন হয়, তাহলে গুলো হবে অপরাধ। এর শাস্তি সর্বোচ্চ ১৪ বছর কারাদন্ড এবং সর্বনিম্ন ৭ বছর কারাদন্ড বা ১ কোটি টাকা পর্যন্ত জরিমানা।

সাইবার বুলিং, সাইবার একটরশন, ফিশিং, আইডেন্টিটি চুরি, স্ক্যামিং, সাইবার লন্ডারিং (মানি লন্ডারিং ২.০), ডিডস আক্রমন ইত্যাদি

বিভিন্ন প্রকার সাইবার অপরাধঃ

প্রযুক্তির ব্যবহার বাড়ার সঙ্গে সঙ্গে জামিতিক হারে বাড়ছে সাইবার অপরাধ। এই অনুচেছদে বিভিন্ন প্রকার সাইবার অপরাধ সম্পর্কে আলোচনা করা হলোঃ

(ক) সাইবার বুলিংঃ বুলিং বলতে সাধারনত বুঝায়, দুজন ব্যক্তির মধ্যে তর্ক বা কথা কাটাকাটি জের ধরে একজন ব্যক্তিকে সুনির্দিষ্ট ভাবে সবার সামনে দোষারোপ বা খারাপ ভাষায় আক্রমন করা। সাইবার বুলিং হলো অনলাইন টেকনোলজির মাধ্যমে আক্ররমন বা হ্যারজমেন্ট করা, যা সাধারণত হয়ে থাকে ই-মেইল এবং মেসেজসহ বিভিন্ন অনলাইন প্লাটফরর্মের মাধ্যমে। অনেক সময় ব্যক্তিগত তথ্য, ভিডিও, ছবি এবং স্ট্যাটাস্ এর মাধ্যমে আক্রমন করা হয়ে থাকে। শুরুতে কিশোর-কিশোরীরাই কেবল এ ধরনের কাজে জড়িত থাকে ভেবে বুলিং সংজ্ঞায়িত করা হলেও, পরে সাইবার বুলিং-এর ঘটনা বেশিভাগ ক্ষেত্রে সামাজিক যোগাযোগ মাধ্যম গুলোতে ঘটলেও, ফোনে কিংবা ই-মেইলে ও অনেক সময় এ ধরনের নির্যাতনের ঘটনা ঘটে থাকে। সাইবার বুলিং-এর কোনো সূত্র পাওয়া গেলে বা এধরনের ঘটনা একবার ঘটলে, বিকৃত ও অসুস্থ মানসিকতার আরো অনেকের কাছে আক্রান্ত ব্যক্তির খোঁজ বা যোগাযোগের তথ্য চলে যায়। যার ফলে ধীরে ধীরে অপরাধের মাত্রা বাড়তে থাকে।

(খ) সাইবার একটরশন : এটি এমন সাইবার অপরাধ, যার অর্থের চাহিদা বা অন্য কোনো প্রতিক্রিয়ার জন্য করা হয়ে থাকে। বর্তমানে সাইবার একটরশনের মাধ্যমে র র‍্যানসমওয়্যার অন্যতম। র‍্যানসমওয়্যার হচ্ছে একপ্রকার ম্যালওয়্যার বা ক্ষতিকর সফটওয়্যার, যা একটি কম্পিউটারের সংরক্ষিত ডাটা বা তথ্যকে এনক্রিপ্ট করে ফেলে বা বলা যেতে পারে তালা মেরে আটকে দেয়। এটা অনেকটা এই রকম, যেমন- একজনের বাড়িতে ঢুকে আরেকজন লোক সব তালা-চাবি ভেঙ্গে ফেলে নতুন তালা-চাবি লাগিয়ে দিল। তখন কম্পিউটারের আসল ব্যবহার কারী নিজে তার কম্পিউটারের কোথাও ঢুকতে পারে না। হ্যাকাররা সেই ব্যবহারকারীর প্রবেশাধিকার ফিরিয়ে দেবার জন্য এ ধরনের মুক্তিপণ হিসাবে অর্থ দাবি করে।

(গ) ফিশিং: ফিশিং হচ্ছে এমন এক প্রকার কাযক্রম যাতে ইলেকট্রনিক যোগাযোগ ব্যবস্থায় তথ্যাদি সংগ্রহের জন্য কোনো বিশ্বস্ত মাধ্যমে ছদ্মবেশ ধারণ করা হয়। সাধারণত জনপ্রিয় সামাজিক যোগাযোগ মাধ্যম, ব্যাংক, আইটি অ্যাডমিনিস্ট্রটেরদের ওয়েবসাইটের মাধ্যমে জনসাধারনকে প্রলোভন দেখানো হয়। ফিশিং সাইটের লিঙ্কগুলো সাধারনত ই-মেইল ইনস্ট্যান্ট মেসেজিং-এর মাধ্যমে প্রেরণ করা হয় ই-মেইলে প্রেরিত লিংকে ক্লিক করলে ইউজারকে নকল ফিশিং ওয়েবসাইটটিতে নিয়ে যাওয়া হয় , যা দেখতে হুবহু আসল অফিশিয়াল ওয়েবসাইটের মতো। ফিশিং এর মাধ্যমে বর্তমান ইন্টারনেট পরিস্থিতির দুর্বল নিরাপওা ব্যবস্থাকে অবৈধভাবে নিজের কাজে ব্যবহার করা হয়। ফিশিং পদ্ধতির বিভিন্ন ধরন রয়েছে। নিচে এসব ধরনের মধ্যে কিছু ফিশিং পদ্ধতি উল্লেখ করা হলো :

(১) **Spare phishing:** এ প্রকার ফিশিং-এ কিছু ব্যক্তি মিলে বা একটি কোম্পানি কোনো বিশেষ ব্যক্তি সম্পর্কে তথ্য যোগাড় করে সম্ভাব্য সাফল্য পাওয়ার জন্য।

(২) **Clone phishing:** এ প্রকার ফিশিং-এ পূবে প্রেরিত কোনো ই-মেইল ক্লোন করে এর কন্টেন্টসমূহ বা লিংকসমূহ পরিবর্তনের পর অন্য ই-মেইল আড্রেস থেকে প্রেরণ করা হয়, যেন ও মনে হয় এটা অরিজিনাল আড্রেস থেকে পেরিত।

(৩)**Link manipulation:** এর মাধমে ভিকটিম কোনো ম্যালিশিয়াস ওয়েবসাইটে রিডিরেস্ট হতে পারেন। ফিশার সাধারনত ভুল অথবা অন্য লিঙ্ক অথবা সাবডোমেইন সমূহ ব্যবহার করে থাকে।

(৪) **Filter evasion:** ফিশাররা লেখার বদলে ইমেজ লিঙ্ক হিসেবে ব্যবহার করতে শুরু করে যেন অ্যান্টি ফিশিং ফিল্টারের কাছে ধরা না পরে।

(৫) **Websiteforgery:** ফিশাররা জাভা স্ক্রিপ্ট ব্যবহার করতে পারে আড্রেস বার পরিবর্তনের জন্য। এছাড়া ও ফ্ল্যাশ টেকনোলজির মাধ্যমে ফ্ল্যাশ ফিশিং ব্যবহার করা হয় অ্যান্টি ফিশিং পদ্ধতি গুলোকে ধোকা দিতে।

(৬) **Phone phishing:** এ প্রকার ফিশিং-এর জন্য ওয়েবসাইটের প্রয়োজন হয় না। এ ক্ষেত্রে কোনো ব্যক্তির ফোন নাম্বার সংগ্রহের পর তাকে ফোন করে বিভিন্ন তথ্য বলতে বা ডায়াল করে প্রদান করতে প্ররোচিত করে।

(ঘ) **আইডেন্টিটি চুরি**ঃ আইডেন্টিটি চুরি এমন এক প্রকার সাইবার অপরাধ, যা কেএন্ ব্যক্তির পরিচয়ের অপব্যবহার হিসাবে অখ্যায়িত করা হয়। আইডেন্টিটিশব্দটির মধ্যে একজন ব্যক্তির নাম, জন্মতারিখ, ঠিকানা, আর্থিক তথ্য যেমন- ক্রেডিট কার্ড বিবরণ, সামাজিক নিরাপওা নম্বর বা অন্য ব্যক্তির পরিচয় সম্পর্কিত তথ্য অন্তর্ভূক্ত করে। কোনো ব্যক্তির এসকল তথ্য চুরি করে এর অপব্যবহার করাই এ প্রকার সাইবার অপরাধের অন্তর্ভূক্ত।

(ঙ) **স্ক্যামিং**ঃ স্ক্যামিং শব্দের অর্থ ধোঁকাবাজি বা প্রতারনা। এই প্রকার সাইবার অপরাধে পুরষ্কারের লোভ দেখিয়ে প্রতারণার মাধ্যমে অর্থ হাতিয়ে নেয়া হয়। এটি এসএমএস বা মেইলের মাধ্যমেই সবচেয়ে বেশি হয়ে থাকে।

৩.৩ ম্যালওয়্যারের সংজ্ঞা ও বিভিন্ন প্রকার ম্যালওয়্যারের বর্ণনাঃ

(ক) ভাইরাসঃ

কম্পিউটারের পরিভাষায় ভাইরাস (Virus) শব্দটিকে ভাঙলে পাওয়া যায় ’’ভাইটাল ইনফরমেশন রিসোর্স আন্ডার সিজ’’ বা **V**ital **I**nformation **R**esources **under S**eize = **VIRUS**. অথ্যার্ৎ গুরুত্বপূর্ণ উৎসগুলো বাজেয়াপ্ত করা হয়েছে। প্রখ্যাত গবেষক প্রেড কোহেন ভাইরাস এর নামকরণ করেন। আবার অনেকেই VIRUS কে Very Important Resource under Seize নামেও অভিহিত করে থাকেন।

(খ) কম্পিউটার ওয়ার্ম ঃ

কম্পিউটার ওয়ার্ম হচ্ছে নিজেই নিজের অনুরূপ আরেকটি তৈরি করতে পারে এমন একটি প্রা ্রোম। এটি নিজের প্রতিলিপি অন্য (নেটওয়ার্কভুক্ত কম্পিউটার) জন্য একটি নেটওয়ার্ক ব্যবহার করে এবং তা কোন মধ্যবর্তী ব্যবহারকারী ছাড়াই। ভাইরাসের মতা এটিকে একটি সক্রিয় প্রোগ্রামের সাথে সংযুক্ত হতে হয় না। ওয়ার্ম প্রায় সব সময়ই নেটওয়ার্কের কিছু না কিছু ক্ষতি করে, যদি কিছু না পারে তাহলে ব্যান্ডউইথ নষ্ট করে,

যেখানে ভাইরাস সব সময় নির্দিষ্ট কম্পিউটারের ফাইল ক্ষতি করে অথবা সম্পূর্নভাবে নষ্ট করে দেয়।

অধিকাংশ নিরাপত্তা বিশেষজ্ঞরা সকল ওয়ার্মকে ম্যালওয়্যার হিসেবে দেখেন।

(গ) ট্রোজান হর্স ঃ

ট্রোজান ম্যালওয়্যারের নামকরণ করা হয়েছে ট্রোজান হর্স থেকে। ট্রোজান হর্স সম্পর্কে যারা জানেন না তাদের জন্য ট্রোজান হর্স বিষয়ে সামান্য কিছু ধারনা দেওয়া থেকে আমি লোভ সামলাতে পারছিনা। আপনারা হয়তো ঐতিহাসিক ট্রয় এবং ট্রোজানদের যুদ্ধের কাহিনী জানেন। ট্রোজানরা যখন ট্রয় নগরী আক্রমন করতে আসে তখন ট্রয় নগরীর চারপাশের প্রাচীর ভেদ করে ট্রোজানরা ভেতরে প্রবেশ করতে পারছিলো না। পরে তারা বুদ্ধি করে নিজেদের যুদ্ধ জাহাজগুলোকে লুকিয়ে রেখে সমুদ্রতীরে বিশাল এক কাঠের ঘোড়া তৈরী করে। যার ভেতরে ট্রোজান বীরগণ লুকিয়ে ছিলেন। ট্রয় নগরীর রাজা যখন বুঝতে পারলেন যে ট্রোজানরা পালিয়ে গেছে এবং তিনি সমুদ্রতীরে একটি কাঠের বিশাল আকৃতির ঘোড়া দেখতে পেলেন। তিনি সেটাকে দেবতার আশির্বাদ ভেবে ট্রয় নগরীর ভেতরে নিয়ে আসলেন। তারপর রাতের অন্ধকারে ট্রোজান সৈন্যরা ঘোড়া ভেঙ্গে বের হয়ে আসলো এবং দুর্গের দরজা ভেতর থেকে খুলে দিয়ে ট্রোজান সেনাবাহিনীল ভেতরের ঢুকার রাস্তা বের করে দেয়। এভাবেই ট্রয় নগরী বায়রের শক্তিশালী প্রাচীর থাকা সত্ত্বেও অরক্ষিত অবস্থায় ধ্বংস হয়ে যায়।

(ঘ) স্পাইওয়্যার ঃ

স্পাইওয়্যার নামটি থেকেই তার কাজ সম্পর্কে আংশিক ধারনা পাওয়া যায়। যদিও অধিকাংশ স্পাইওয়্যার তুলনামুলকভাবে ক্ষতিকর হয়না, তবুও কিছু কিছু স্পাইওয়্যার খুব মারাত্বক সিকিউরিটি রিস্কের কারন হয়ে দাড়ায়। স্পাইওয়্যার মুলত আপনার ইন্টারনেট সার্ফিং এর উপর নজরদারী করে এবং অ্যাড রিলেটেড ব্যাপারগুলোর সাথে সম্পৃক্ত থাকে। স্পাইওয়্যার মাঝে মাঝে ট্রোজান হর্সের চেয়েও ক্ষতিকর হয়ে যায়, যখন এটা আপনার কম্পিউটারের গুরুত্বপূর্ণ তথ্য, ছবি, ইমেইল, ব্যাংক ইনফোরমেশন সার্ভার কিংবা অন্য ব্যবহারকারীর কাছে পাঠিয়ে দেয়।

স্পাইওয়্যার সাধারনত কম্পিউটারে সফটওয়্যার ডাউনলোডের সময়, এডনস ডাউনলোডের সময় এবং অধিকাংশ ফ্রিওয়্যার কিংবা শেয়ার ওয়্যারের সাথে আপনার পিসিতে চলে আসে।

পাসওয়ার্ড ক্র্যাকিং ঃ

পাসওয়ার্ড ক্র্যাকিং কী তা জানার আগে জেনে নেয়া যাক ওয়েবসাইটগুলোতে কীভাবে পাসওয়ার্ড সংরক্ষণ করা হয় সেই সম্পর্কে। ওয়েবসাইটে পাসওয়ার্ড সংরক্ষণের অনেক উপায় আছে। হ্যাশিং, সল্টিং, টোকেইন, টু ফ্যাক্টর অথেনটিকেশন্ এগুলোই বেশি ব্যবহার করা হয়। প্রথমেই হ্যাশিং কী তা একটু জানা যাক। আমরা সাধারণত যেসব শব্দ ব্যবহার করে নতুন পাসওয়ার্ড নির্বাচন করি ঠিক সেভাবে পাসওয়ার্ডগুলোকে ওয়েবসাইটগুলো সংরক্ষণ করে না। এই পাসওয়ার্ডগুলোকে সাইটের সার্ভারে সংরক্ষণ করা হয় একটি বিশেষ এনক্রিপশন অ্যালগরিদমের মাধ্যমে। সেই অ্যালগরিদমকে বলা হ্যাশিং বা হ্যাশ ফাংশন। এই অ্যালগরিদমের কাজ খুবই সাধারণ। আমাদের ইনপুট দেয়া প্লেইন টেক্সট বা সাধারণ অক্ষরগুলোকে এই অ্যালগরিদম একটি নির্দিষ্ট দৈর্ঘের কিছু দুর্বোধ্য কোড বা সংকেতে পরিণত করে। যেমন, abc123 এই পাসওয়ার্ডটির জন্য হ্যাশ হবে e99a18c428cb38d5f260853678922e03 (এমডি৫ হ্যাস অ্যালগরিদম অনুযায়ী)। কিন্তু এই হ্যাশিং আবার পর্যায়ক্রমিক হয় না, যেমন “password” শব্দটির হ্যাশ 5f4dcc3b5aa765d61d8327deb882cf99, কিন্তু “password1” শব্দটির হ্যাস 7c6a180b36896a0a8c02787eeafb0e4c। দুটি সম্পূর্ণ আলাদা হয়ে যাবে কেবল একটি মাত্র শব্দ বেশি ব্যবহারের জন্য। এই হ্যাশ পদ্ধতির জন্য বেশ কিছু জনপ্রিয় অ্যালগরিদম হল এমডি ৫, এসএইচএ ১, এসএইচএ ২ সহ এমন আরো বেশ কিছু। এগুলো হল ওয়ান ওয়ে ফাংশন, যার অর্থ হল পাসওয়ার্ড একবার হ্যাশ করা হয়ে গেলে সেটি থেকে আবার পুনরায় প্লেইন টেক্সট আকারে পাসওয়ার্ড ফেরত পাওয়া যায় না।

(ক) ব্রুটফোর্স অ্যাটাক ঃ

হ্যাকার যদি একটি ওয়েবসাইটের সার্ভার থেকে ইউজারদের পাসওয়ার্ড ফাইল সংগ্রহ করে ফেলতেও পারে, তারপরও কিন্তু সে পাসওয়ার্ডগুলো ব্যবহার করতে পারবে না। তার কারণ সেগুলো এনক্রিপ্ট করা। আর এখন কাজে আসবে ব্রুট ফোর্স অ্যাটাক। ব্রুট ফোর্স

অ্যাটাকের ধারণাটাও খুব সহজ। এটি কিন্তু একটি অনুমান নির্ভর প্রক্রিয়া। আরেকটু পরিষ্কার করা যাক। ব্রুট ফোর্স অ্যাটাকে হ্যাকার একটি সফটওয়্যারের সাহায্য নেয় যেটি একের পর এক পর্যায়ক্রমে সম্ভাব্য পাসওয়ার্ড তৈরী করে তা হ্যাশ করে সার্ভারের হ্যাশের সাথে মিলাতে থাকে। আর এই প্রক্রিয়া চলতে থাকে সঠিক পাসওয়ার্ডটি মিলে যাবার আগপর্যন্ত।

একটি উদাহরণ দেয়া যাক, যদি হ্যাকারের সফটওয়্যার অনুমান aaaa থেকে শুরু হয় আর তারপর aaab, তারপর aaac এবং এভাবে সেটা zzzz পর্যন্ত পরীক্ষা করে দেখতে থাকবে। এখানে ৪টি অক্ষরের জন্য এমনটা হবে। আর ধীরে ধীরে তার দৈর্ঘ্য কিন্তু বাড়তে থাকবে। কিন্তু প্রশ্ন হলো, এই প্রক্রিয়া চলতে কতটা সময় নেয়?

আরস টেকনিকা কয়েকজন হ্যাকারকে নিয়ে একটি পরীক্ষা চালায়। সেই পরীক্ষায় একজন সাধারণ হ্যাকার ১০,২৩৩টি পাসওয়ার্ড ক্র্যাক করতে সক্ষম হন, তাতে সময় লাগে মাত্র ১৬ মিনিট। আর তাছাড়া এই প্রক্রিয়া পুরোটা হ্যাকারের উপর নির্ভর করে না, কারণ হ্যাকারের কম্পিউটারের হার্ডওয়্যার, ইন্টারনেট সংযোগ যত উন্নত হবে, প্রক্রিয়াটি তত দ্রুত কাজ করতে পারবে। কিন্তু পাসওয়ার্ডের অক্ষর সংখ্যা যত বেশি হবে, এতে সময় তত বেশি লাগবে। ব্রুট ফোর্স তাই কাজ করে ৮ অক্ষরের কম পাসওয়ার্ডে।

(খ) ডিকশনারি অ্যাটাক ঃ

ডিকশনারি অ্যাটাককে ব্রুট ফোর্সেরই একটি অংশ বলা চলে। ডিকশনারি অ্যাটাকে সাধারণ কিছু পাসওয়ার্ডের একটি ডিকশনারি তৈরি করে হ্যাকার। এর মাধ্যমে অনেক দ্রুত এবং দুর্বল পাসওয়ার্ডগুলো খুব সহজে ক্র্যাক করে করে ফেলা যায়। কত দ্রুত? ৬.২ বিলিয়নপাসওয়ার্ড ম্যাচ করতে পারে প্রতি সেকেন্ডে। সাধারণ পাসওয়ার্ডের মধ্যে পড়ে নিজের নাম, কোনো সাধারণ শব্দ বা নিজের নামের সাথে কোনো সংখ্যা এগুলোই। তো আপনি এরকম কিছু পাসওয়ার্ড হিসেবে ব্যাবহার করছেন না তো?

ডিকশনারি অ্যাটাককে আরেকটু কার্যকরী এবং আরেকটু কঠিন পাসওয়ার্ড ক্র্যাক করতে সাহায্য করে হাইব্রিড অ্যাটাক। এর সাহায্যে ডিকশনারি অ্যাটাকে ব্যবহৃত শব্দগুলোকে একটু ভিন্নভাবে সাজানো হয়। সাধারণ শব্দগুলোতে ব্যবহার করা হয় নাম্বার, বিশেষ চিহ্ন ইত্যাদি।

যেমন, ডিকশনারি অ্যাটাকে কেবল password123 চেক করলে হাইব্রিড অ্যাটাকে চেক করা হয় p@$$word123, অর্থাৎ a, s, এবং o এর স্থলে ব্যবহার করা হয়েছে @, $ এবং 0 ।

(গ) রেইনবো অ্যাটাক ঃ

নাম শুনে যতটা নিরীহ মনে হয় ততটা নিরীহ নয় এই রেইনবো টেবিল। এতক্ষণ যেসকল প্রক্রিয়ার কথা জানলেন আপনি সেসকল ক্ষেত্রেই প্রথমে একটি পাসওয়ার্ড অনুমান করে সেটিকে হ্যাশ করে সার্ভারের হ্যাশের সাথে মিলিয়ে দেখার কাজটি করাতো হ্যাকার তার সফটওয়্যার দিয়ে। কিন্তু হ্যাশিং করে তা আবার মিলিয়ে দেখতে অনেক সময় অপচয় হয়। তো কেমন হয় যদি কয়েক মিলিয়ন হ্যাশ করা পাসওয়ার্ডের একটি টেবিল পাওয়া যেত! রেইনবো টেবিল সেই চাহিদা পূরণ করে।

অধিক ব্যবহৃত প্রি-হ্যাশড কয়েক মিলিয়ন পাসওয়ার্ড থাকে এই টেবিলে, যার ফলে নতুন করে আর হ্যাশ করা লাগে না হ্যাকারের সফটওয়্যারকে। আর তাছাড়া যেহেতু দুটো হ্যাস মিলে গেলেই হল, তাই হ্যাকারকে আসল পাসওয়ার্ড কী তা জানার দরকারও পড়ে না। প্রায় ৩২ বিলিয়ন পাসওয়ার্ড প্রতি সেকেন্ডে ম্যাচ করতে পারা যায় রেইনবো টেবিলের মাধ্যমে। তো আপনার পাসওয়ার্ড এখন কতটুকু নিরাপদ মনে হচ্ছে!

(ঘ) সল্টিং অ্যাটাক ঃ

না, খাবার লবণের কথা বলছি না। এটাকে পাসওয়ার্ডের লবণ বলা যেতে পারে। কারণ এটি পাসওয়ার্ডের স্বাদ কিছুটা বদলে দেয়। আরেকটু পরিষ্কার করা যাক।

হ্যাশিং করা হয় কেবলমাত্র প্লেইন টেক্সটকে একটি অ্যালগরিদম দ্বারা এনক্রিপ্ট করে। কিন্তু দেখা গেলো এটি বিশেষ সুবিধার নয়। আর তাই সল্টিং করা হয় পাসওয়ার্ড এবং সেটির হ্যাশকে। এটি বেশি জটিল কিছু না, কেবলমাত্র আসল পাসওয়ার্ডের সাথে কয়েকটি অক্ষর জুড়ে এটিকে হ্যাশ করা হয় এবং সেই হ্যাশের সাথে আরো কিছু অক্ষর যোগ করা হয়।

একটি উদাহরণ দেয়া যাক। আপনার পাসওয়ার্ড যদি হয় abc123 (আশা করা যায় বাস্তবেই এটি আপনার পাসওয়ার্ড না), তাকে সল্ট করা হয়। ধরা যাক, সল্ট করার পর এটি হল 2abc123। এরপর সেটিকে হ্যাশ করে সেই হ্যাশের সাথে আবারো 2 যোগ করাই হলো

সল্টিং হ্যাশ। আর এটি একেক ইউজারের ক্ষেত্রে একেক রকম হতে পারে। এটি হ্যাকারকে বেশ ধীর করে দেয়। কিন্তু ব্রুট ফোর্স আর ডিকশনারি অ্যাটাক এর কিছু ক্ষেত্রে কাজে দিলেও রেইনবো টেবিল কোনোই কাজে আসে না। কারণ এক্ষেত্রে আগে হ্যাকারকে জানতে হয় সল্ট কোথায় যোগ করা হয়েছে, সল্টিং অক্ষরটি কী, কত অক্ষর পর যোগ করা হয়েছে ইত্যাদি।

১. কেবলমাত্র পাসওয়ার্ডে বিশেষ চিহ্ন ব্যবহার করলেই চলবে না। খেয়াল রাখতে হবে পাসওয়ার্ড যেন সহজ না হয়।

২. সর্বনিম্ন ৮ অক্ষরের পাসওয়ার্ড নির্বাচন করুন। পাসওয়ার্ড যত বড় হবে হ্যাকারের তা বের করতে তত বেশি সময় লাগবে।

৩. প্রয়োজনে বাক্য ব্যবহার করুন। হতে পারে তা কোনো কবিতার চরণ বা গল্পের লাইন কিংবা নিজের বানানো কোনো উক্তি।

৪. প্রতি মাসে অন্তত একবার পাসওয়ার্ড পরিবর্তন করুন। একই পাসওয়ার্ড বার বার ব্যবহার করবেন না।

৫. মনে রাখতে সহজ হবে ভেবে সহজ পাসওয়ার্ড ব্যবহার করবেন না। আপনার কাছে যেটা সহজ সেটা হয়ত আগেই কোনো হ্যাকার ক্র্যাক করে রেখেছে।

৬. ভিন্ন ভিন্ন ওয়েবসাইটের জন্য বা ব্যাংক একাউন্টের জন্য ভিন্ন ভিন্ন পাসওয়ার্ড বা পিন কোড ব্যবহার করুন। ভুলে যাওয়া যদি আপনার অভ্যাস হয় তাহলে আপনার জন্য আছে অনেক পাসওয়ার্ড ম্যানেজার, যেগুলাতে আপনি কেবল একটি পাসওয়ার্ডের মাধ্যমে সব সাইটের পাসওয়ার্ড সংরক্ষণ করে রাখতে পারবেন।

অধ্যায়-৪

হ্যাকিং

ভূমিকা:

তথ্য প্রযুক্তির ছোঁয়ায় মানুষের জীবন হয়ে উঠেছে সহজ থেকে সহজতর । কিন্তু তথ্যপ্রযুক্তির অগ্রসরের সাথে সাথে আরেকটি বিষয়ও সামনে চলে এসেছে , আর সেটি হচ্ছে হ্যাকিং । হ্যাকিং বলতে মূলত বুঝায় , কোনো অনুমতি ছাড়া অন্য কারো অ্যাকাউন্ট / নেটওয়ার্কে /কম্পিউটারে প্রবেশ করে সেখান থেকে গুরুত্বপূর্ণ তথ্য গ্রহণ করা , মুছে দেওয়া বা এমন খারে পরিবর্তন করা , যা ওই ব্যক্তি বা প্রতিষ্ঠানের জন্য ক্ষতিকর হয় । হ্যাকিং বলতে শুধু কোনো ওয়েবসাইট হ্যাক করা বা কম্পিউটার নেটওয়ার্ক হ্যাক করাই বুঝায় না , হ্যাকিং অনেক ধরনের হতে পারে । মোবাইল ফোন , ল্যান্ড ফোন , গাড়ি ট্র্যাকিং , বিভিন্ন ইলেকট্রনিক্স ও ডিজটাল যন্ত্র বৈধ অনুমতি ছাড়া ব্যবহার করলে সেটিও হ্যাকিং এর আওতায় পড়ে । হ্যাকাররা সাধারণত এসব ইলেকট্রুনক যন্ত্রের ত্রুতি বের করে তা দিয়েই হ্যাক করে । অনলাইন অ্যাকাউন্ট থেকে টাকা চুরি , ব্যক্তিগত তথ্য সংগ্রহ , ভাইরাস , ম্যালওয়্যার আক্রমণ সবকিছু হ্যাকিং এর মাধ্যমে করা সম্ভব ।

হ্যাকিং এবং এর প্রকারভেদ:

" হ্যাক" মানে কোসো জিনিসকে নিজের মতো করে পরিবর্তন করা । আর হ্যাক করার পদ্ধতিই হলো হ্যাকিং । অন্য ভাষায় বলা যায় , হ্যাকিং হলো এমন একটি প্রক্রিয়া যেখানে কেউ বৈধ্য অনুমতি ছাড়া কোনো কম্পিউটার বা কম্পিউটার নেটওয়ার্কে প্রবেশ করে । অনেকেই হ্যাকিং বলতে শুধু ফেসবুক আইডি বা মেইল আইডি হ্যাকিং বা ওয়েবসাইট হ্যাকিংকেই বঝে থাকে । বাস্তবে হ্যাকিং কিন্তু শুধু এই সামান্য গন্ডিতেই সীমাবদ্ধ না । যারা হ্যাকিং করে তাদের বলে হ্যাকার । একজন হ্যাকার স্কাইপ অ্যাকাউন্ট হ্যাক করে যেমন স্কাইপ ব্যবহারকারীর কথা শুনতে পারে তেমনি অনলাইন ওয়েব ক্যাম হ্যাক করে ব্যবহারকারীকে সরাসরি দেখতেও পারে ।

হ্যাকিং-এর উৎপত্তি: ১৯৫০ থেকে ১৯৬০ এর দশকে এমআইটি ইঞ্জিনিয়াররা প্রথম হ্যাকিং শব্দটির প্রচেলন শুরু করেন। এটা মূলত শুরু করা হয় মেইনফ্রেম কম্পিউটারের কোডিং ভাঙ্গার জন্য এবং শুধুই মজার করার উদ্দেশ্য। পরের দশকে কিছু নীতিহীন হ্যাকার অনৈতিক উদ্দেশ্য মোবাইল ফোন হ্যাক শুরু করে। আগে কম্পিউটারের এত বহ্যল প্রচলন না থাকায়, তখন হ্যাকাররা ফোন হ্যাকিং করত । ফোন হ্যাকারদের বলা হত ফ্রিকার এবং এ প্রক্রিয়াকে বলা হতো ফ্রিকিয়। এরা বিভিন্ন টেলিকমিউনিকেশন সিস্টেমকে হ্যাক করে নিজেদের প্রচোজনে ব্যবহার করত।

হ্যাকিং-এর প্রকারভেদ: কী হ্যাক করা হচ্ছে তার ভিত্তিতে হ্যাকিংকে বিভিন্ন বিভোগে ভাগ করা যায় –

১. ওয়েবসাইট হ্যাকিং: ওয়েবসাইট হ্যাকিং মানে হলো ওয়েব সার্ভার এবং তার সংশ্লিষ্ট সফটওয়্যার (যেমন অনুনমোদিত এবং অন্যান্য ইন্টারফেস) –এর নিয়ন্ত্রণ গ্রহণ।

২. নেটওয়ার্ক হ্যাকিং: নেটওয়ার্ক হ্যাকিং হচ্ছে নেটওয়ার্কে ক্ষতিসাধন করার লক্ষ্য টেলনেট, এনএস লিংক, পিং, ট্রাচার, নেটস্ট্যাট ইত্যাদির সাহায্য এ একটি নেটওয়ার্ক সম্পকিত তথ্য সংগ্রহ করা এবং এটির মূল অপারেশনকে ব্যাহাত করা।

৩. ই-মেইল হ্যাকিং: ই-মেইল অ্যাকাউন্টে অননুমোদিত আক্সেস এবং দার মালিকের সম্মাত ছাড়া ব্যবহার করাই ই-মেইল হ্যাকিং।

৪. ইথিক্যাল হ্যাকিং: নৈতিক হ্যাকিং বা ইথিক্যাল হ্যাকিং একটি কম্পিউটার বা নেটওয়ার্ক সিস্টেমর মধ্যে দুর্বলতা খোঁজার জন্য ব্যবহৃত হয় এবং অবশেষে তাদের সংশোধন করা হয়।

৫. পাসওয়ার্ড হ্যাকিং: এটি কম্পিউটার সিস্টেম দ্বারা সংরক্ষিত তথ্য থেকে গোপন পাসওয়ার্ড পুনরুদ্ধারের প্রক্রিয়া।

৬. কম্পিউটার হ্যাকিং: এই হ্যাকিং পদ্বতি প্রয়োগ করে কম্পিউটার সিস্টেমের অননুমোদিত অ্যাক্সেস লাভ করা হয় মাধ্যমে আইডি এবং পাসওয়ার্ড চুরি করা যায়।

হ্যাকিং এবং এর স্বপক্ষে যুক্তি:

অনেক কারণেই হ্যাকিং করা হয়। অযৌক্তিক এবং যৌক্তিক দুই ধরনের কারণেই হ্যাকিং – এর সঙ্গে জড়িত। হ্যাকিং-এর উল্লেখযোগ্য কারণ হলো:

- নিজেদের দক্ষতা প্রমাণের উদ্দেশ।
- অনেকের কাছে হ্যাকিং করাটা এক ধরনের বিনোদন।
- নিজেদের স্কিল প্র্যাকটিস করার জন্য।
- তথ্য চুরি জন্য।
- আর্থিক ভাবে লাভবান হওয়ার উদ্দেশ্য, যেমন- ক্রেডিট কার্ড হ্যাকিং।
- কেনো কাজের প্রতিবাদ করার উদ্দেশ্য।

কোনো সন্দেহ নেই যে, হ্যাকিং (অন- ইথিক্যাল) অবশ্যই একটি অপরধি। একজনের প্রাইভেসিতে হাত দেয়ার অধিকার আরেকজনের নেই। যারা হ্যাকিংয়ের মাধ্যমে

অন্যের ক্ষতি করে, আইনের চোখে তারা সাইবার ক্রিমিন্যাল হিসেবে পরিচিতি। তারপরও হ্যাকিং কিছু ক্ষেত্রে অত্যন্ত প্রয়োজনীয়:

● হারিয়ে যাওয়া তথ্য পুনরুস্থান জন্য, যেমন: পাসওয়ার্ড হারিয়ে গেলে।

●কম্পিউটার এবং নেটওয়ার্ক সুরক্ষা শক্তিশালী করার জন্য অনুপ্রবেশ পরীক্ষা সঞ্চালন।

● নিরাপত্তার ভাঙ্গন প্রতিরোধ করার জন্য পর্যাপ্ত প্রতিরোধ মূলক ব্যবস্থা রাখা।

●ব্লাক হ্যাট হ্যাকাররা অ্যাক্সেস লাভ কবতে বাধা দেয় এমন একটি কম্পিউটার সিস্টেস।

বিভিন্ন প্রকার হ্যাকিং পদ্ধতি যেমন- ভালনরেবিলিটি স্ক্যানিং, ব্রোট ফোর্স আক্রমণ, ডিকশনারি অ্যাটাক, পাসওয়ার্ড ক্র্যাকিং, প্যাকেট স্নিফার, স্পেফিং আক্রমণ (ফিশিং), প্রোগ্রামড থ্রেটস, সোশ্যালি ইঞ্জিনিয়ারিং ইত্যাদি:

হ্যাকিং করার জন্য হ্যাকাররা বিভিন্ন প্রক্রিয়া অনুসরণ করে থাকে। নিম্নে বিভিন্ন প্রকার হ্যাকিং প্রক্রিয়া সম্পর্কে আলোচনা করা হলো:

(ক) ভালনারেবিলিপি স্ক্যানিং: কম্পিউপার নিরাপত্তার দুর্বলতা শনাক্ত করতে ব্যবহৃত একটি নিরাপত্তা কৌশল। কোনো ব্যক্তি বা নেটওয়ার্ক অ্যাডমিনিস্ট্রেটর সিস্টেমের মাঝে কোনো দুর্বলতা আছে কি না সেটি চেক করার জন্য ভালনারেবিলিটি স্ক্যানিং করে থাকে। আবার হ্যাকররা কম্পিউটার সিস্টেমে অননুমোদিত অ্যাক্সেস পাওয়ার জন্য ভালনারেবিলিটি স্ক্যানিং করে থাকে।

(খ) ব্রন্ট ফোর্স অ্যাটাক: হ্যাকার যদি একটি ওয়েবসাইটের সার্ভার থেকে ইউজারদের পাসওয়ার্ড ফাইল সংগ্রহ করে ফেলতেও পারে, তারপরও কিন্তু সে পাসওয়ার্ড গুলো ব্যবহার করতে পারবে রা। তার কারণ সেগুলো এনক্রিপ্ট করা। কিন্তু ব্রন্ট ফোর্স অ্যাটাকে হ্যাকার একটি সফটওয়্যারের সাহায্য নেয়, যেটি একের পর এক পর্যায়ক্রমে সম্ভাব্য পাসওয়ার্ড তৈরী করে তা হ্যাশ করে সার্ভারের হ্যাশের সাথে মিলত থাকে। আর এই প্রক্রিয়া চলতে থাকে সঠিক পাসওয়ার্ডটি মিলে যাবার আগ পর্য্ন্ত।

একটি উদাহরণ দেয় যাক। যদি হ্যাকারের সফটওয়্যার অনুমান aaaa থেকে শুরু হয় আর তারপর aaab, তারপর aaac এবং এভাবে সেটা zzzz পর্য্ন্ত পরীক্ষা করে দেখতে থাকবে। এখানে ৪টি অক্ষরের জন্য এমনটা হবে। আর ধীরে ধীরে তার দৈর্ঘ্য বাড়তে থাকবে।

(গ) ডিকশনারি অ্যাটাক: ডিকশনারি অ্যাটাককে ব্রন্ট ফোর্স এর একটি অংশই বলা চলে । ডিকশনারি অ্যাটাকে হ্যাকাররা সধারণ কিছু পাসওয়ার্ডের একটি ডিকশনারি তৈরী করে। এর মাধ্যমে অনেকে দ্রুত এবং দুর্বল পাসওয়ার্ডগুলো খুব সহজে ক্র্যাক করে ফেলা যায় ।সেই ডিকশনারির মাধ্যমে ৬.২ বিলিয়ন পাসওয়্যার্ড ম্যাচ করতে করতে পারে প্রতি সেকেন্ড। সাধারণ পাসওয়ার্ডের মধ্যে পড়ে নিজের নাম, কোনো সাধারণ শব্দ বা নিজের নামের সাথে কোনো সংখ্যা এগুলোই ।

ডিকশনারি অ্যাটাককে আরেকটু কার্য্করী এবং আরেকটু কঠিক পাসওয়ার্ড ক্র্যাক করতে সাহায্য করে হাইব্রিড অ্যাটাক । এর সাহায্যে ডিকশনারে অ্যাটাকে ব্যবহৃত শব্দগুলোকে একটু ভিন্ন ভাবে সাজানো হয় । সাধারণ শব্দগুলোতে ব্যবহার করা হয় নাম্বার, বিশেষ চিহ্ন ইত্যাদি । যেমন – ডিকশনারি অ্যাটাকে কেবল passw0rd123 চেক করলে হাইব্রিড অ্যাটাকে চেক করা হয় p@$$word123 অর্থ্যাৎ a, s এবং এর স্থলে ব্যবহার করা হয় o @, $ এবং 0 ।

(ঘ) পাসওয়ার্ড ক্র্যাকিং : আমরা সাধারণত যে সব শব্দ ব্যবহার করে নতুন পাসওঁয়ার্ড নির্বাচন করি ঠিক সেভাবে পাসওয়ার্ডগুলোকে ওয়েবসাইড গুলো সংরক্ষণ করে না। এই পাসওয়ার্ডগুলোকে সাইটের সংরক্ষণ করা হয় একটি বিশেষ এনক্রিপশন অ্যালগরিদমের মাধ্যমে । ওয়েবসাইটে পাসওয়ার্ড সংরক্ষণ করার জণ্য। আর এই পদ্ধতি গুলোর প্রয়োজনীয়তা হলো হ্যাকার হাত থেকে পাসওয়ার্ড সুরক্ষিত রাখা । কারণ পাসওয়ার্ড ফাইলগুলো জমা রাখা হয় ওয়েব সাইট এর সার্ভারে ; আর সে সব সার্ভার হ্যাক করা যায়। এজন্য হ্যাকারদের থামানোর জন্য এই পদ্ধতি। কিন্তু তারপরও হ্যাকাররা এই হ্যাশ কোডকে ডিক্রিপ্ট করে ফেলে। আর এটিই হলো পাসওয়ার্ড ক্র্যাকিং ।

(ঙ) প্যাকেট স্নিফার: হ্যাকিং য়ের ভাষায় স্নিফিং হলো গুরুত্বপূর্ণ তথ্য হাতিয়ে নেওয়া । স্নিফিং আক্রমণ হলো এমন এক পদ্ধতি, যেটাতে কোনো কম্পিউটার নেটওয়ার্ক দিয়ে প্রবহিত ডাটা ক্যাপচার করে । আর যে ডিভাইস বা সফটওয়্যার ব্যবহার করে এটি করা হয, সেটিকে প্যাকেট স্নিফার বলা হয় ।

(চ) স্পেফিং আক্রমণ (ফিশিং): ফিশিং হচ্ছে এমন একপ্রকার কার্য্ক্রম, যাতে ইলেকট্রনিক যোগাযোগ ব্যবস্থায় তথ্যদি সংগ্রহের জন্য কোনো বিশ্বস্ত মাধ্যমের ছদ্মবেশ ধারণ করা হয়। সাধারণত জনপ্রিয় সামাজিক যোগাযোগ ব্যবস্থা, ব্যাংক, আইটি অ্যাডমিনিস্ট্রেটরদের ওয়েবসাইট-এর মাধ্যমে জনসাধারণরত প্রলোভন দেখানো হয়। ফিশিং সাইট এর লিংক গুলো সাধারণত ই-মেইল বা ইন্টারনেট মেসেজিং এর মাধ্যমে প্রেরণ করা হয়। ই-মেইলে প্রেরিত লিংকে ক্লিক করলেই ইউজারকে নকল ফিশিং ওয়েবসাইটতে নিয়ে যাওয়া হয়, যা তেখতে হুবহু আসল অফিশিয়াল ওয়েবসাইটটির মত । ফিশিং এর মাধ্যমে বর্তমান ইন্টারনেট পরিস্থিতির দুর্বল নিরাপত্তা ব্যবস্থাতে অবৈধভাবে নিজের কাজ ব্যভহার করা হয় ।

(ছ) প্রোগ্রামড থ্রেটস : কোনো প্রোগ্রামের সম্পূর্ণ কোড বা কোডের একাংশ , যা (সেটি হতে পারে এক্সিকিউটেবিল কোড , নন- এক্সিকিউটেবিল কোড ইত্যাদি) কম্পিউটারের

জন্য ক্ষতি কর তাই হলো প্রোগ্রাম থেট্রস। কিছু উল্লেখযোগ্য প্রোগ্রাম থ্রেটস হলো ভাইরাস, ট্রোজান হর্স, ব্যাকটেরিয়া, ওয়ার্ম ইত্যাদি।

(জ) সোশ্যাল ইঞ্জিনিয়ারিং: এক ধরনের মনোবিজ্ঞানিক কৌশল, যেখানে অত্যন্ত চতুরতার সঙ্গে ভিকটিমের গুরুত্বপূর্ণ তথ্য বের করে আনা হয়। এই তথ্য দেওয়ার কাজটা ভিকটিম নিজের অজান্তে নিজেই করে থাকে। যেমন, ফেসবুক অ্যাকাউন্ট এর " সিকি্উরিপি কোয়েশ্চন " – এ মায়ের জন্মস্থান কোথায় ? এর উত্তর কেও প্রদান করল ঢাকা। যদি উত্তরটি শতভাগ সঠিক এবং সত্যি হয়ে থাকে, তাহলে একজন হ্যাকারের পক্ষে সোশ্যাল ইঞ্জিনিয়ারিং র্ব্যবহার করে খুবব সহজেই এই উত্তরটা অনুমান করা সম্ভব।

হ্যাকার:

উইকিপিডিয়ার ভাষ্য অনুযায়ী, হ্যাকার হচ্ছেন সেই ব্যক্তি যিনি নিরাপত্তা / অনিরাপত্তার সঙ্গে জড়িত এবং নিরাপত্তা ব্যবস্থার দুরাবল দিক খুঁজেবের করায় বিশেষ ভাবে দক্ষ। এ্রিই সঙ্গে অন্য কম্পিউটার ব্যবস্থায় অবৈধ অনুপ্রবেশ করতে সক্ষম বা এর সম্পর্কে গভীর জ্ঞানের অধীকারী। সহজ ভাষায় বলা যায়, হ্যাকিং একটি প্রক্রিয়া যেখানে কেউ কোনো বৈধ অনুমতি ছাড়া কোনো কম্পিউটার বা কম্পিউটার নেটওয়ার্কের প্রবেশ করে। যারা এ হ্যাকিং করে তাদের বলা হয় হ্যাকার। এরা যে সিস্টেম হ্যাকিং করবে, ঐ কম্পিউটার সিস্টেমের গঠন, কার্য্প্রণালী, কীভাবে কাজ করে ইত্যাদি সকল তথ্য সম্পর্কে অবগত থাকে। কোনো কম্পিউটার সিস্টেম বা কম্পিউটার নেটওয়ার্ক এর দুর্বলতা খুঁজে বের করে, সেটির নিরাপত্তা ভাঙ্গাই হ্যাকারদের কাজ।

কোনো মিডিয়া ম সফটওয়্যার বা ওয়েব সাইট তৈরীর সময় বা ব্যবহারের ভুলের কারণে অনেক জায়গায় দুর্বলতা বা ভুল থেকে যায়। হ্যাকাররা ঐ দুর্বল জায়গাতেই তাদের হ্যাকিং কৌশল ব্যবহার করে মিডিয়া ডিভাইস, মফটওয়্যার বা ওয়েবসাইট নিজের নিয়ন্ত্রণ নিয়ে নেয় বা নিজের মতো করে পরিবর্তন করে নেয়।

কয়েকজন বিখ্যাত হ্যাকার: নিম্নে কয়েকজন বিখ্যাত হ্যাকার সম্পকে আলোচনা করা হলো:

(ক) কেভিন মিটনিক: হ্যাকিং জগতের সবচেয়ে বিখ্যাত ব্যক্তি কেভিন মিটনিক। তাকে বলা হয় ' ফাদার আব আল হ্যাকার '। তার হ্যাকিং জীবন শুরু হয় সোশ্যাল ইঞ্জিনিয়ারিং ব্যবহার করে লস অ্যাঞ্জলাসের বাসে পাঞ্চ কার্ড হ্যাকিংয়ের মাধ্যমে। তিনি মটোরোলা, নাকিয়া, ফজিৎসুর মতো বড় বড় প্রতিষ্ঠানের কম্পিউটার সিস্টেম হ্যাক করেছিলেন। আমেরিকার ন্যাশনাল সিকিউরিটি সিস্টেমেও তার অবৈধ বিচরণ ছিল। ২০০০ সাল থেকে ২০০৩ সাল পর্য্ন্ত তার উপর কম্পিউটার, সেল ফোন এবং ইন্টারনেটযুক্ত ডিভাউজ ব্যবহারের উপর নিষেধাজ্ঞা আরোপ করা হয়। মিটানিকের জীবনী নিয়ে ২০০০ সালে তৈরী হয় ' ট্রেকডাউন ' চলচ্চিত্র।

(খ) গ্যারি ম্যাককিনল: বিশ্বের ইতিহাসে সবচেয়ে বড় মিলিটারি কম্পিউটার হ্যাকার সঙ্গে জড়িয়ে ছিলেন এই ব্যক্তি। মার্কিন যুক্তরাষ্ট্র এর আর্মি, নৌবাহিনী, নাসার মতো বড় বড় সরকারী দপ্তর এর ৯৭ টি কম্পিউটার হ্যাক করে ছিলেন তিনি।

গ) জনাথন জেমস: জনাথন জেমস মাত্র ১৬ বছর বয়সে সাইবার ক্রাইমের জন্য জেলে গিয়েছিলেন েএই ব্যক্তি । ১৫ বছর বয়সে বেল – সাউথ, মিয়ামি ডেড, আমেরিকার প্রতিরক্ষা বিভাগে এবং নাসা ওয়েব সাইট হ্যাক করেন । জেমস নাসার ওয়েব সাইট হ্যাক করে সেখান থেকে প্রায় ১.৭ মিলিয়ন ডলার সমপরিমান মূল্যের একটি সফটওয়্যার এর সোর্স কোড ডাউন লোড করেন ।

নাসার মতো জেমস যে সফটওয়্যারটি চুরি করেছিলেন সেগুলো দিয়ে ইন্টারন্যাশনাল স্পেস স্টেশন নিয়ন্ত্রণ করা হয় । জেমস নাসার ওয়েব সাইট যে ক্ষতি করেছিলেন সেটি ঠিক করতে নাসার ওয়েব সাইট তিন সপ্তাহ বন্ধ রাখতে হয়ে ছিল । ২০০৮ সালের ১৮ মে মাত্র ২৪ বছর বয়সে েএই প্রতিভাবান হ্যাকার আত্মহত্যা করেন ।

(ঘ) ভ্লাদিমির লেভিন: রাশিয়ান এই হ্যাকার ১৯৯৪ সালে মিটি ব্যাংকের বেশ কয়েক জন কর্পোরেট ইউজারের পাসওয়ার্ড হ্যাক করে তাদের অ্যাকাউন্ট থেকে সরিয়ে ফেলেন ১০.৭ মিলিয়ন পলার । ১৯৯৫ সালে লেবিন ধরা পড়েন এবং বিচার এ তার ৩ বছরের জেল হয় ও ২.৫ লাখ ডলার জরিপানা হয় ।

(ঙ) আদ্রিয়ান লামো: 'দ্য হোমালেস হ্যাকার 'হিসেবে বিখ্যাত আদ্রিয়ান লামো মাইক্রোসফট, ইয়াহু সহ বড় বড় কোম্পানীর ওয়েবসাইট হ্যাক করেন। এছাড়া তিনি হ্যাক করেছেন ব্যাংক অব আমেরিকা, সিটি গ্রুপ, নিউইয়র্ক টাইমস, এমসিআই ওয়ার্ল্ডকমের মতো বিখ্যাত সব ওয়েব নাইট ।

(চ) মাইকেল কেল্স: ইন্টারনেট দুনিয়ার 'মাফিয়া বয়' হিসেবেই পরিচিত। এই কানাডিয়ান 'মাফিয়া বয়' DdoA Attack এর মাধ্যমে অ্যামাজন, ডেল, ইবে, সিএনএনের মতো বিশ্বের বড় বড় কোম্পানী হ্যাক করেছিলেন ।

(ছ) অ্যাস্ট্রা: অ্যাস্ট্যা একজন গ্রিক গণিত বিদ, যার আসল নাম খানা কখনোই প্রকাশিত হয় নি । তিনি ফ্রান্স এর প্রতিরক্ষা বাএ্রীনির ওয়েব সাইট গ্যাক করে সমস্ত অস্ত্র এর ডিজাইনসংক্রান্ত ডাটা নিজের দখলে নিয়ে আসেন এবং বিশ্বের বিভিন্ন কাস্টামারের কাছেই সেই ডাটা ৩৬১ মিলিয়ন ডলারে বিক্রি করেন । গ্রিসের এথন্স শহরের একটি অ্যাপার্টমেন্ট থেখে ২০০৮ সালে তিনি নিরাপত্তা বাহিনীর হাতে গ্রেফকার হন।

(জ) অ্যালবার্ট গঞ্জালেজ: ক্রেডিট কার্ড হ্যাকিংয়ের জন্য কুখ্যাত । ২০05 থেকে ২০07 সাল, মাত্র ২ বছরে গঞ্জালেজ ও তার গ্রুপ ১৭০ মিলিয়ন ক্রেডিট কার্ড এবং এটিএম নম্বর জালিয়াতি করেন । ২০১০ সালে তাকে ২০ বছরের জন্যে জেলে পাঠানো হয় ।

(ঝ) ডেভিড স্মিথ: তিনি ম্যালিনা ভাইরাস এর স্রষ্টা । ভাইরাসটি ইন্টারনেটে ঢুকে ব্যাপক ক্ষতি সাধন করে এবং প্রায় ৩০০ টি বড় বড় কর্পোরেট প্রতিষ্ঠানের নেটওয়ার্ক

গামলা চালায় । এর মধ্যে মাইক্রোসফট, ইন্টেল, লুসেন্ট টেকনোলজির মতো কোম্পানীও ছিল ।

(ঞ) ম্যাথিউ বেভান ও রিচার্ড প্রাইস: ১৯৯৬ সালে গ্রেফতার হবার পর যখন মিডিয়াতে আসেন তখন দুজনের বয়স ছিল যথাক্রমে ২১ ও ১৭ বছর । সেই সময় তারা হ্যাক করেন ইউএস মিলিটারি কম্পিউটার সিস্টেম । িএ ছাড়া কোরিয়ার সরকারি নিরাপত্তা কাজে নিয়োজিত কম্পিউটারও হ্যাক করেছিলেন ।

বিভিন্ন প্রকার হ্যাকার যেমন – স্ক্রিপ্ট কিডি, হোয়াইট হ্যাট (ইথিক্যাল হ্যাকার), ব্ল্যাক হ্যাট (ক্র্যাকারস), গ্রে হ্যাট, গ্রিন হ্যাট, রেড হ্যাট, ব্লু হ্যাট ইত্যাদি:

একটি সিস্টেম এর হ্যাকিং এর উপর ভিত্তি করে হ্যাকারদের বিভিন্ন শ্রেণীতে শ্রিণীবদ্ধ করা হয় । নিম্নে বিভিন্ন প্রকার হ্যাকারদের সম্পর্কে আলোচনা করা হলো:

স্ক্রিপ্ট কিডি: এই ধরনের হ্যাকাররা প্রোগ্রামিং এ তেমন দক্ষ নয় । এরা নিজেরা কোনো টুলস তৈরী করতে পারে না । অন্যের বাননো টুলস বা স্ক্রিপ্ট ব্যবহার করে এরা হ্যাকিং করে থাকে । কোনো সিস্টেম হ্যাক কিরার পর এরা সঠিক ভাবে নিজেদির লুকিয়েও নিতে পারে না। সিকিউরিটি হলো সেই

হোয়াইট হ্যাট হ্যাকার: হোয়াইট হ্যাট হ্যাকার হলো সেই ব্যক্তি, যিনি কোনো সিকিউরিটি সিস্টেমের দুর্বলতা খুজে বের করে ঐ সিকিউরিটি সিস্টেমের মালিককে বা সংশ্লিষ্ট কর্মকর্তাদের ত্রুটি গুলো সম্পর্কে অবহিত করেন । এই সিকিউরিটি সিস্টেমটি হতে পারে কোনো কম্পিউটার বা কোনো কম্পিউটার নেটওয়ার্কের ওয়েব সাইট, বা অন্য কোনো প্রোগ্রাম । হোয়িইট হ্যাট হ্যাকাররা মূলত সাইবার ওয়াল্ড এ নিরাপত্তাপ্রদান করে । এদেরকে ইথিক্যাল হ্যাকারও বলা হয় । এরা বিভিন্ সিস্টেমের নিরাপত্তা প্রদান করাই এদের কাজ ।

ব্ল্যাক হ্যাট হ্যাকার: হ্যাকার বলতে মূলত এদেরকেই বোঝায় । এরা বিভিন্ সিস্টেমের দুর্বলতা খুঁজে বেড়াই শুধু মাত্র নিজেদের আর্থিক অথবা ব্যক্তিগত স্বর্থসিদ্ধির জন্য । এরা কোনো সিকিউরিটি সিস্টেমের ক্রতি গুলো বের করলে তা নিজেদের স্বর্থে লাজে লাগায় । ঐ সিস্টেমের ডাটাবেস নষ্ট করে, কখনো বা বিভিন্ন ভাইরাস ছড়িয়ে দেয় । অথবা কোনো নতুন ত্রুটি তৈরী করে রাখে, যাতে ভবিষ্যতে আবার সেই সিস্টেমে প্রবেশ করতে পারে ।

গ্রে হ্যাট হ্যাকার: এরা হলো হোয়াইট হ্যাট হ্যাকার এবং ব্ল্যাক হ্যাকার মাঝামাঝি অবস্থা । অর্থ্যাৎ এরা ভালো এবং খারাপ দুটোই করে থাকে । বেশীর ভাগ হ্যাকাররাই এই ক্যাটাগরিতে পড়ে । এরা কোনো সিস্টেমের ত্রুটি সাধান করে কখনো ঐ সিস্টেমের

মালিককে জানায়, কখনো নিজেদের স্বার্থে ব্যবহার করে সিস্টেমের ক্ষতি সাধন করে। দিনে ভালো রাতে খারাপ, এরা হলো এই টাইপির হ্যাকার।

গ্রিন হ্যাট হ্যাকার: এ ধরনের হ্যাকাররা হ্যাকিং এ খুব বেশী পারদর্শী হয় না। এদরকে নবগত হ্যাকার হিসেবে বিবেচনা করা হয়।

রেড হ্যাট হ্যাকার: এ ধরনের হ্যাকাররা অন্য দেশের ওয়েব সাইট এবং অনলাইন সেবা হ্যাক করে থাকে।

বলু হ্যাট হ্যাকার: এরা বিভিন্ন কোম্পানীর হয়ে সিকিউরিটি রক্ষার করে। এরা অত্যন্ত মেধাসম্পন্ন হয়। এদের হ্যাকিং জ্ঞান সীমিাবদ্ধ। বর্তমানে মাইক্রোসফটও এ ধরনের হ্যাকারদেরকে সিকিউরিটি চেক করার জন্য নিয়োজিত রেখেছে।

এছাড়া আরও কয়েক প্রকারের হ্যাকার রয়েছে, যেমন -

এলিট হ্যাকার: এরা খুবই দক্ষ হ্যাকার। কোনো সিস্টেমকে হ্যাক করার পাশাপাশি দক্ষতার সাথে লুক্কায়িত হতে পারে। এরা নিত্যনতুন হ্যাকিং কৌশল আবিষ্কার করে। একই সাথে কোনো মেথকে আরো নিখুঁত করার চেষ্টা করে থাকে। এরা প্রোগ্রামিং এ বিশেষ দক্ষ। বিভিন্ন ধরনের হ্যাকিং টুলস এবং এক্সপ্লয়েট মূলত এরাই তৈরী করে থাকে।

ক্রাকার হ্যাকার: ব্ল্যাক হ্যাট হ্যাকাররাই মূলত ক্রাকার। এদের কাজ হলো বিভিন্ন ক্ষতিকারক প্রোগ্রাম তৈরী করা এবং অনুমতি ছাড়া কোনো কাপিরাইট প্রটেক্টেড সফটওয়্যারের কোড ভেঙ্গে ফেলা।

নিওফাইট: এরা হলো হ্যাকিং এ নতুন শিক্ষার্থী। হ্যাকিং এর প্রয়োজনীয় জ্ঞান বা অভিজ্ঞতা কোনোটাই এতের নেই এদেরকে নিউবি বা নবুও বলা হয়।

অধ্যায়: ০৫

প্রাথমিক নিরাপত্তা

ভূমিকা ঃ

প্রযুক্তির অগ্রসর হওয়ার সাথে সাথে কিছু মানুষ প্রযুক্তিকে ক্ষতিকর কাজের উদ্দেশ্যে ব্যবহার করতে শুরু করে এবং সৃষ্টি করে আইসিটি সেক্টর এর নেতিবাচক বিভিন্ন দিক। কম্পিউটার ভাইরাস মূলত প্রোগ্রামারদের ডেভলপ করা ক্ষতিকর প্রোগ্রাম ছাড়া আর কিছুই নয়। এ ধরনের নেতিবাচক বা ক্ষতিকর প্রোগ্রামের কার্যক্রম অব্যাহত থাকে প্রযুক্তির উৎকর্ষ যত উন্নত হচ্ছে তার সাথে পাল্লা দিয়ে ক্ষতিকর প্রোগ্রাম উন্নত থেকে উন্নততর ক্ষতিকর কর্মকান্ডের পারদর্শী ভাইরাস বা ক্ষতিকর প্রোগ্রাম তৈরি করে

ইন্টারনেটে ছেড়ে দিচ্ছে । এর ফলে কম্পিউটার ব্যবহারকারীদের তথ্য অ্যাড্রেস পাসওয়ার্ড ব্যাংক অ্যাকাউন্ট গুরুত্বপূর্ণ সন্ত্রাসীচক্রের নাগালে পৌঁছে যাচ্ছে ।

অন্যদিকে সাইবার অপরাধের প্রতিহত করার জন্য প্রতিনিয়ত করা হচ্ছে নিত্যনতুন ক্ষমতা বৈশিষ্ট্য প্রযুক্তির মধ্যে উল্লেখযোগ্য । কম্পিউটার জগতে উদাহরণ দিতে গেলে মনের আগুন ভেতরে প্রবেশ করতে দেয়না ভিতর আগুন বাইরে যেতে দেনা । কম্পিউটারের ক্ষেত্রে ফায়ারওয়াল প্রটেকশন ইন্টারনেটের ব্যবহার করা সময় অনাকাঙ্ক্ষিত সফটওয়্যার অনুমতিতে প্রবেশ করার জন্য বাধা প্রদান করে থাকে যোগাযোগের সর্বক্ষনিক ভাবে মনিটর এবং অন্যান্য উৎস থেকে আগত অবৈধ অনুপ্রবেশ প্রতিহত করে|

ফায়ারওয়াল এবং আক্রমণ প্রতিরোধ ঃ

ফায়ারওয়াল ঃ কথাটির শব্দের অর্থ হল আগুনের দেয়াল অতীত ইতিহাসে রাজা বাদশাহ বাড়ির নিরাপত্তার জন্য তাদের প্রসারে চারপাশে পরীক্ষার খনন করা হতো যাতে কেউ তাদের প্রসাদের অযাচিতভাবে ঢুকতে না পারে| কম্পিউটারে রক্ষার জন্য সেই পদ্ধতির উদ্দেশ্য নিয়ে কিন্তু বিভিন্ন সিস্টেমের মাইক্রোসফট কর্পোরেশন তাদের অপারেটিং সিস্টেম উইন্ডোজ এক্সপির নিরাপত্তা ব্যবস্থা তৈরি করেছে যাকে বলা হয় উইন্ডোজ ফায়ারওয়াল মাইক্রোস|

ফায়ারওয়াল হলো এক বিশেষ নিরাপত্তা ব্যবস্থা যাতে এক নেটওয়ার্ক থেকে আরেক নেটওয়ার্কে ডাটা প্রবাহিত নিয়ন্ত্রণ করা যায়| সেখানে দুটি নেটওয়ার্কের মাঝে একটি থাকে এর ফলে একটি নেটওয়ার্ক থেকে আরেক নেটওয়ার্কে কোন ডাটা প্রবাহিত হলে সেটিকে অবশ্যই ফায়ারওয়াল অতিক্রম করতে হবে| তার নিয়ম অনুসারে ডাটা পরীক্ষা-নিরীক্ষা করে এবং যদি দেখার গন্তব্য যাওয়ার অনুমতি আছে তাহলে সেটি যেতে পারে আর না থাকলে সেটি ওখানে আটকে রাখে|

ফায়ারওয়াল এর প্রয়োজনীয়তাফট কর্পোরেশন তাদের অপারেটিং সিস্টেমের এটা শুরু করলেও অনেক এন্টিভাইরাস থার্ডপার্টি সফটওয়্যার সেবা দিয়ে থাকে বাইরের আক্রমণ থেকে কম্পিউটারকে রক্ষা করার জন্য হার্ডওয়ার সফটওয়্যার ব্যবহারের ক্ষেত্রে তথ্য নিরাপত্তা রক্ষার এ কাজের অংশ|

ফায়ারওয়াল এর প্রয়োজনীয়তা ঃ

অনেক সময় দেখা যায় কোন সফটওয়্যার ইন্সটল করার সময় বারবার সফটওয়্যার এর জন্য অনুমতি দিতে হয় ,অথবা বারবার পপ-আপ আসে ইত্যাদি | বর্তমান সময়ে কম্পিউটারে যে কোনভাবে যেকোনো স্থান থেকে সাইবার আক্রমণ আসতে পারে| সে আক্রমণ প্রতিরোধ করার জন্য অবশ্যই ভালো প্রটেকশন ব্যবস্থা থাকা জরুরি| ব্যবস্থা যার মাধ্যমে অনাকাঙ্ক্ষিত সফটওয়্যার ইত্যাদি বাধা প্রদান করা হয় কারণ হ্যাকাররা যে কোনো অনাকাঙ্ক্ষিত সফটওয়্যার ইত্যাদি কম্পিউটারে প্রবেশ করিয়ে ডাটা অনলাইন একাউন্ট ইনফর্মেশন ইনফরমেশন চুরি করতে পারে| আবার অনেক সময় কম্পিউটার সফটওয়্যার অ্যান্টিভাইরাস রূপ ধারণ করে | কিন্তু এই সফটওয়্যার গুলো নিয়ে থাকে কখনো কখনো কোন সাইটে প্রবেশ করলে সামনে মেসেজ আসে সেই ইউর সিস্তেম মেমোরি অথবা আপনি ডিভাইসটি ভাইরাস দ্বারা আক্রান্ত হয়েছে| এক্ষুনি পরিষ্কার করে নিন ইত্যাদি | এসকল মেসেজ পড়ে যখনই সে গুলোতে ক্লিক করা হয় তখনই ব্যবহারকারীর কম্পিউটারে কোন সফটওয়্যার ডাউনলোড করা হয়ে যায় এবং মেমোরি ক্লিন না করে উল্টো করে ফেলে এজন্য সকল প্রকার অনাকাঙ্ক্ষিত থেকে বাঁচতে কম্পিউটার ফেয়ারওয়েল চালু করতে অনেক বেশি জরুরী| এছাড়াও নিম্নে কারণসমূহ জন্য ফায়ারওয়াল ব্যবহার করার প্রয়োজন |

- **রিমোট অ্যাক্সেস থেকে কম্পিউটারকে রক্ষা ঃ** যদি কেউ দূরবর্তী অবস্থান থেকে কোন ব্যবহারকারীর কম্পিউটার নিয়ন্ত্রণ করার চেষ্টা করে কিংবা নিয়ে, নে তাহলে এটি হবে একজন কম্পিউটার ব্যবহারকারীর কাছে সবচেয়ে ভয়ঙ্কর ব্যাপার| এটির ভালো কনফিগারেশনের দূরবর্তী ডেস্কটপ অক্ষম করে দেই এবং এভাবে কম্পিউটার ডাটা গ্রহণ করে থেকে প্রতিরোধ করে থাকে |

- **অবাঞ্চিত বিষয়বস্তুর সাথে সংযোগ ব্লক ঃ** এখনো অনেক মানুষ উইন্ডোজের পুরনো সংরক্ষণ গুলো ব্যবহার করে| আরো খারাপ বিষয় যে তারা এক্সপিতে কোন ফায়ারওয়াল ব্যবহার করছে না এবং বিল্ট-ইন ফেয়ারওয়েল ফায়ারওয়াল ডিফল্ট ভাবে সক্রিয় করা থাকে না | এমন অরক্ষিত পিসির অপেক্ষার অপরাধীরা তাই এসকল পিসিটি একটি ডেডিকেটেড ফেয়ারওয়েল ইনস্টল করা প্রয়োজন |

- **অনলাইন গেমিং নিরাপত্তা ঃ** এখন অনেক জনপ্রিয়| কিন্তু এতে ডাটা নিরাপত্তা ঝুঁকির সম্ভাবনা অনেক বেশি অনেক অনলাইন গেম সার্ভার ব্যবহার করে কিন্তু ফেয়ারওয়েল এটা হতে দেয় না| ফলে এটি অনলাইন গেমিং নিরাপদ করে|

- **অনুপযুক্ত কনটেন্ট ব্লক ঃ** অ্যাপ্লিকেশন একটা অপশন আছে যেটা দিয়ে বিশেষ অনলাইন লোকেশন কে ব্লক করা যায় ফলে বন্ধ করা রাখা যায় ঝুঁকিপূর্ণ ওয়েবসাইটকে| ব্যবহারকারী ছাড়াও অন্য কেউ যদি এমন ব্লক করা সাইটের ঢোকার চেষ্টা করে ফায়ারওয়াল সেই চেষ্টা নষ্ট করে দেয়|

ফায়ারওয়াল এর প্রকারভেদঃ

ফায়ারওয়াল সাধারণত দুই প্রকারের দেখা দেখা যায়| একটি হলো হার্ডওয়ার নির্ভর ফায়ারওয়াল এবং আরেকটি হল সফটওয়্যার নির্ভর ফেয়ারওয়েল| নিম্নে উভয় প্রকারের সম্পর্কে বিস্তারিত আলোচনা করা হলো ঃ-

হার্ডওয়ার নির্ভর ফায়ারওয়াল ঃ হানিফার ফেয়ারওয়েল সাধারণত রাউটার দেখা যায়| তাছাড়া আলাদা ডেডিকেটেড ডিভাইস বাজারে কিনতে পাওয়া যায় এবং এই ডিভাইসের একপ্রকার হার্টের প্রটেকশন প্রদান করে থাকে যদি একটি রাউটার সংযোগ করা থাকে এবং যদি ফায়ারওয়াল চালু করা থাকে তবে রাউটার সংযোগ করা দশটি দিব তাই নিয়ে আসবে| কয়েকটি হার্ডওয়ার নির্ভর ফায়ারওয়াল হলো ঃ-

সফটওয়্যার নির্ভর ফায়ারওয়াল ঃ বিভিন্ন অ্যান্টিভাইরাস নির্মাতা কোম্পানি যেমন এভাস্ট নর্টন এভিজি ম্যাকাফি ইত্যাদি| সাধারণত তাদের অ্যান্টিভাইরাসের সুরক্ষা প্রদান করে থাকে তাছাড়া উইন্ডোজ এর ভিতরে সুবিধা থাকে কয়েকটি সফটওয়্যার নির্ভর ফায়ারওয়াল সেগুলো হলো ঃ-

- প্যাকেট ফিল্টার এটি প্রতিটা প্যাকেট এর দিকে লক্ষ্য রাখে নেটওয়ার্ক প্রবেশ ও বের হওয়ার সময়|

- অ্যাপ্লিকেশন গেটওয় ftp.net সার্ভারের মতো অ্যাপ্লিকেশনের ওপর সিকিউরিটি মেকানিজম প্রয়োগ করে|

- সার্কিট লেভেল গেটওয় এটা যখন টি সি পি বাইউ ডিপি কানেকশন স্থাপিত হয় তখন সিকিউরিটি মেকানিজম প্রয়োগ করে|

- প্রক্সি সার্ভার এটি নেটওয়ার্কের মধ্যে প্রবেশ ও বের হওয়ার সময় প্রতিটা মেসেজ চেক করে|

বিভিন্ন প্রকার ফায়ারওয়াল **এর মধ্যে তুলনা** ঃ-

ফায়ারওয়াল সাধারণত এপ্লাই করা হয় হার্ডওয়ার সফটওয়্যার দুটি উপায়| ইন্টারনেটে প্রবেশ করে এবং বের হয়ে যায় শহরের মধ্যে আসা-যাওয়া করে| ফেল পর্যবেক্ষণ করে প্রতিটা ম্যাচে সিকিউরিটি নিয়মকানুন মেনে চলে কি না| নিম্নে বিভিন্ন ধরনের মধ্যে তুলনা করা হলো ঃ-

- **প্যাকেট ফিল্টার** ঃ এটি প্রতিটা প্যাকেট এর দিকে লক্ষ্য রাখে নেটওয়ার্ক প্রবেশ ও বের হওয়ার সময় ইউজারের দেয়া নিয়ম-কানুন ভিডিও ভিত্তিতে তাকে অ্যাকসেপ্ট রিজেক্ট| প্যাকেটের মধ্যে অ্যাডমিনিস্ট্রেটরের ইচ্ছামত নতুন নিয়ম কানুন নির্ধারণ করা হয় অথবা ডিলেট করে দিতে পারেন| প্যাকেট ফিল্টেরিং ও কার্যকরী ব্যবস্থা কিন্তু এটি কনফিগার করা কঠিন এছাড়া এই আইপি ওপর নির্ভর করে|

- **অ্যাপ্লিকেশন গেটওয়** ঃ এটি ftp.net সার্ভারের মত অ্যাপ্লিকেশন এর উপর সিকিউরিটি মেকানিজম প্রয়োগ করা হয়| অপ্রয়োজনীয় বা বাজে কনটেন্টগুলো পর্যবেক্ষণ করে ফায়ারওয়াল নেটওয়ার্কের কম্পিউটার ব্যাপক হারে ছড়িয়ে দিতে করে| এটা খুবই কার্যকর ব্যবস্থা কিন্তু বিভিন্ন ধরনের অ্যাপ্লিকেশন এর উপর একসাথে কাজ করতে গিয়ে পারফরমেন্স অনেকটা কমিয়ে দেই|

- **সার্কিট ডেভেলপমেন্ট গেটওয়ে** ঃ যখন টিসিপি কানেকশন স্থাপন করা হয় তখন এটি সিকিউরিটি মেকানিজম পরে| যখন কানেকশন তৈরি হয়ে যায় তখন প্যাকেটগুলো হোস্টের মধ্যে ইচ্ছামত আসা-যাওয়া করতে পারে কোন প্রকার চেকিং ছাড়াই ।

- **প্রক্সি সার্ভার** ঃ এটি নেটওয়ার্কের মধ্যে প্রবেশ ও বের হওয়ার সময় প্রতিটা মেসেজ চেক করে| প্রক্সি সার্ভারের সত্তিকারের নেটওয়ার্ক ঠিকানা নিখুঁতভাবে লুকাতে পারে|

প্রাথমিক অনলাইন নিরাপত্তা ঃ

প্রযুক্তি ভিত্তিক কার্যক্রম দ্রুত বিস্তার লাভ করা অনলাইন নিরাপত্তা কথাটি এখন মানুষ মুখে মুখে উচ্চারিত হচ্ছে অনলাইন নিরাপত্তা বলতে মূলত বোঝায় সেই সচেতনতার কিছু উপায় যার মাধ্যমে ব্যক্তিগত তথ্য কম্পিউটারে বিভিন্ন ধরনের ডিজিটাল ডিভাইস কম্পিউটার সিস্টেম ইত্যাদি বিভিন্ন ধরনের আক্রমণ থেকে নিরাপদ রাখা। একজন ব্যবহারকারীর যে সমস্যার সম্মুখীন হয় তার মধ্যে অন্যতম হচ্ছে কোন আইডি হ্যাক হওয়া প্রদান করা ফাইল চুরি করা। এসব সমস্যার সম্মুখীন কিছু উল্লেখযোগ্য কারণ নিম্নে আলোচনা করা হল ঃ

(ক)ম্যালওয়্যার ঃ এল এর পুরো নাম মেলিসিয়াস সফটওয়্যার। এটি কম্পিউটারের একটি ক্ষতিকর প্রোগ্রাম যা ব্যবহারকারীর অনুমতি ছাড়া পরিকল্পিত কোন নেটওয়ার্কের জায়গায় আঘাত করে যেকোনো ডাটা তথ্য চুরি চুরি করে নেয় কম্পিউটার প্রোগ্রামের ক্ষতি করে। বিভিন্ন ধর্মের মধ্যে কয়েকটি উল্লেখযোগ্য হলো ঃ-

- **ভাইরাস ঃ** ভাইরাস শব্দের পুরো অর্থ হল ভাইরাস ইনফর্মেশন রেসোর্স অন্ড সাইজ তথ্যের উৎসগুলো বাজেয়াপ্ত করা হয়েছে একটি কম্পিউটার জরুরী তথ্য নষ্ট করে কম্পিউটার স্লো করে দেয়।

- **ওয়ার্মস ঃ** এটি সাধারণত নিজেকে প্রচার করার চেষ্টা করে অর্থাৎ কোন কম্পিউটার যদি ওয়ার্ম দ্বারা আক্রমণ হয় তবে এটি কম্পিউটার অনেকগুলো একই ফাইল তৈরি করে এবং সিস্টেম ফ্লো করে দিবে।

- **ট্রোজান হর্স ঃ** ব্যবহারকারীর অগোচরে এ ভাইরাস কম্পিউটারে ঢুকে পড়ে কম্পিউটারের স্বাভাবিক প্রক্রিয়া বাধা দেওয়ার পাশাপাশি গুরুত্বপূর্ণ ফাইল চুরি করে অন্য কম্পিউটার কাছে পাঠিয়ে দেয়।

- **স্পাইওয়্যার ঃ** একবার সুপার কম্পিউটার ইন্সটল হয়ে গেলে ডিভাইসে থাকা সকল তথ্য অনায়াসেই অন্য কারো কাছে পাচার করে দিতে পারে। খুব গোপনে এর মাধ্যমে খুব সহজেই ব্ল্যাকমেইল করা সম্ভব যা মাঝে মাঝে প্রাণনাশের কারণ হতে পারে।

(খ) হ্যাকিংঃ হ্যাকিং বলতে মূলত বোঝায় কোন অনুমতি ছাড়া কোন কারনে ফায়ারওয়াল কে কম্পিউটার প্রবেশ করা এর মাধ্যমে উক্ত সিস্টেমের গুরুত্বপূর্ণ তথ্য গ্রহণ করা মুছে দেওয়া এমন ভাবে পরিবর্তন করা যা| যা ঐ ব্যাক্তি বা প্রতিষ্ঠানের জন্য ক্ষতিকর হয় হ্যাকিং বলতে শুধু করা বা কম্পিউটার নেটওয়ার্কিং অনেক ধরনের হতে পারে|

(গ) ফিশিংঃ ফিশিং হচ্ছে এমন এক প্রকার কার্যক্রম যাতে ইলেকট্রনিক যোগাযোগ ব্যবস্থায় তথ্যাদি সংগ্রহের জন্য কোন বিশ্বস্ত মাধ্যমে ছদ্মবেশ ধারণ করা হয় সাধারণ জনপ্রিয় সামাজিক এতে কোনো জনপ্রিয় সাইটের মত সাইট তৈরি করে| তাতে লগইন করার মাধ্যমে আইডি-পাসওয়ার্ড চুরি করে যোগাযোগ মাধ্যম ব্যাংক ওয়েবসাইটের মাধ্যমে দেখানো হয়|

(ঘ) **সোশ্যাল ইঞ্জিনিয়ারিং ঃ** সোশ্যাল ইঞ্জিনিয়ারিং এক ধরনের মনোবৈজ্ঞানিক কৌশল জাতি যেখানে অত্যান্ত চতুর্থ সঙ্গে ভিকটিমের গুরুত্বপূর্ণ তথ্য বের করে আনা হয়| এই তথ্য দেয়ার কাজটা ভিকটিম নিজের অজান্তেই নিজেই করে থাকে|

অনলাইন নিরাপত্তা জন্য পদক্ষেপঃ অনলাইন জগতে ব্যক্তিগত কিংবা প্রতিষ্ঠানের নিরাপদ রাখার জন্য নিম্নোক্ত বিষয় প্রতি খেয়াল রাখা জরুরী ঃ

1. ব্যবহৃত বিভিন্ন একাউন্ট এর ইউজার নেম এবং পাসওয়ার্ড ভিন্ন রাখা|
2. সব অ্যাকাউন্ট যাতে একসাথে হ্যাক না হয়|
3. ব্যক্তিগত ছবি ভিডিও সোশ্যাল মিডিয়াতে শেয়ার করা থেকে বিরত থাকা|
4. ব্যবসায়িক তথ্য লেনদেনের ক্ষেত্রে সর্তকতা অবলম্বন করা|
5. অপরিচিত সাইট ভিজিট যেখানে থেকে ফ্রি সফটওয়্যার ডাউনলোড থেকে বিরত থাকা|
6. ইমেইল এড্রেস ক্রেডিট কার্ড নম্বর পাসপোর্ট নাম্বার ব্যাংক অ্যাকাউন্ট নম্বর আইডি কার্ড নম্বর ড্রাইভিং লাইসেন্স নাম্বার ইত্যাদি অনলাইনে শেয়ার করা থেকে বিরত থাকা|

হ্যাকারদের উদ্দেশ্য ঃ

হ্যাক মানে কোন জিনিস কে নিজের মতো করে পরিবর্তন করা | হ্যাক হ্যাক করার পদ্ধতি হলো হ্যাকিং | অন্য ভাষায় বলা যায় হ্যাকিং হল এমন এক প্রকার প্রক্রিয়া যেখানে কেউ বৈধ অনুমতি ছাড়া কোন কম্পিউটার বা কম্পিউটার নেটওয়ার্কে প্রবেশ করে আর যে হ্যাক করে | তাকে হ্যাকার বলা হয় একজন হ্যাকার বিভিন্ন ধরনের একজন হ্যাকার বিভিন্ন কারণে বিভিন্ন উদ্দেশ্য নিয়ে হ্যাকিং করে থাকে যার মধ্যে নিম্নলিখিত কয়েকটি উল্লেখযোগ্য ঃ-

1. নিজের দক্ষতা প্রমাণের উদ্দেশ্য |
2. কোন কাজের প্রতিবাদ করার উদ্দেশ্য |
3. আর্থিক উদ্দেশ্য |
4. গুপ্তচর ভিত্তিক কাজের জন্য |
5. মজা করার উদ্দেশ্য |
6. অন্যান্য কারণ |

আক্রমণ প্রতিরোধ প্রক্রিয়া হিসেবে ফায়ারওয়াল ঃ

ফায়ারওয়াল বাইরের আক্রমণ থেকে কম্পিউটার রক্ষা করার জন্য হার্ডওয়ার এবং সফটওয়্যার এর মিলিত প্রয়াস ।

(ক)হার্ডওয়ার ফায়ারওয়াল ঃ মাধ্যমে সুরক্ষা যখন কোন ওয়েবসাইটে প্রবেশ করার জন্য বায়ু থেকে রিকুয়েস্ট পাঠানো হয় তখন সেভ করা রিকুয়েস্ট সাথে নেটওয়ার্কে যুক্ত হয়ে যায় এবং রিকোয়েস্ট পাঠিয়ে দেই| সার্ভার থেকে যখন ফিরতি কাছে পৌঁছায় তখন সেই প্যাকেট নেটওয়ার্ক যুক্ত থাকে| আসলে চিনতে পারে এবং সেগুলো সেন্ড করে দেয় | এমন কোন প্যাকেজে যাতে নেটওয়ার্ক আইডি নেই তবে সেটিকে তাৎক্ষণিক ব্লক করে দিবে |

(খ)সফটওয়্যার ফায়ারওয়াল ঃ এর মাধ্যমে সুরক্ষা সিস্টেম বা কম্পিউটারে ইনস্টল থাকা কোন গেম বা সফটওয়্যার যদি কোন ইন্টারনেট সংযোগের জন্য রিকোয়েস্ট করে তবে কম্পিউটারে অবাঞ্চিত ফেয়ারওয়েল থেকে ব্যবহারকারীদের কাছে একটি পপ-আপ আইপি অনুমতি চেয়ে| প্রদান না করা পর্যন্ত ইনস্টল করা সফটওয়্যার ইন্টারনেটের মাধ্যমে রিসিভ করতে পারেনা| উইন্ডোজ ফায়ারওয়াল সবসময় এটি মনিটর করে যে কম্পিউটার আউটগোয়িং ট্যারিফ এবং ইনকামিং ট্রাফিক তাদের উৎস কোথায় এবং তাদের আছে কিনা বা কোন ইনকামিং ট্রাফিক অনাকাঙ্ক্ষিত সফটওয়্যার ইন্সটল করছে কিনা | এ সকল বিষয়ের উপর নির্ভর করে সিদ্ধান্ত নিয়েছে এবং কোন কোন গুলো ব্লক করবে |

অ্যাধায় ঃ-০৬

সাইবার নৈতিকতা

ভূমিকাঃ

বর্তমান সময়কে প্রযুক্তির সোনালি যুগ বলা হল। দিন দিন প্রযুক্তি প্রসারে প্রায় পুরো পৃথিবী এখন হাতের মুঠোয়। শত বছর আগে যে সকল চিন্তা মানুষের বাইরে ছিল, আজ তার বাস্তব প্রয়োগ দেখছে। ব্যাপকভাবে প্রযুক্তি প্রচার এবং প্রসারের ফলে শহর থেকে শুরু করে প্রত্যান্ত অঞ্চলেও পৌছে গেছে ইন্টারনেট সুবিধা। হাতে হাতে পৌছে গেছে কম্পিউটার, স্মার্টফোনসহ বিভিন্ন ডিজিটাল ডিভাইস। কিন্তু ইন্টারনেট ব্যবহারকারীর বড় একটি অংশ হলো প্রযুক্তির ই সুবিধাকে কাজে লাগিয়ে বিবিন্ন প্রকার সাইবার অপরাধ করা হচ্ছে। ইন্টারনেটের মাধ্যমে যে অপরাধ সংঘটিত হলে তাকে সাইবার অপরাধ বলে।

সাইবার নৈতিকতা ঃ

সাইবার নৈতিকতা হলো কম্পিউটার সম্পর্কিত এক প্রকার নীতিশাস্ত,সেখানে ব্যবহার কারীকে কম্পিউটারের সঠিক ব্যাবহার এবং এর মাধ্যমে কীভাবে ব্যক্তি এবং সমাজকে প্রভাবিত করে সে সম্পর্কে বিস্তারিত আলোচনা করা হয়। বিবিন্ন সংস্থা সাইবার নৈতিকতা সম্পর্কিত বিষয়গুলো বিবিন্নভাবে ব্যাখ্যা করে এবং সে অনুযায়ী সেই দেশের সরকার আইন প্রনয়ন করে। এক কথায় সাইবার নৈতিকতা বলতে সাইবার জগত যা কিছু আছে সবকিছুর দায়িত্বশীল ব্যবহারকে বুঝায়।

সাইবার নৈতিকতার কিছু কাজঃ

অনলাইনে অন্য কারও ক্ষতি হয় এমন সকল কাজই সাইবার নৈতিকতাবিরধী। নিম্নে এরকম কিছু নৈতিকতা তুলেধরা হলঃ

- **সফটওয়্যার পাইরেসি ঃ** সফটওয়্যার পাইরেসি বলতে বোঝায় অবৈধভাবে সফটওয়্যার বা প্রোগ্রামের ব্যবহার, কপি(পুনরুৎপাদন) করা বা ডিস্ট্রিবিউট করা। ওয়ান পিসি লাইসেন্সে একাধিক পিসি চালানো, বেআইনিভাবে বন্ধুদের সাথে শেয়ার বা ভাগাভাগি করা।

❖ **সাইবার অপরাধ ঃ** ইন্টারনেট ব্যবহারকারীর বড় একটি অংশ হলো প্রযুক্তির ই সুবিধাকে কাজে লাগিয়ে বিবিন্ন প্রকার সাইবার অপরাধ করা হচ্ছে। ইন্টারনেটের মাধ্যমে যে অপরাধ সংঘটিত হলে তাকে সাইবার অপরাধ বলে।

❖ **সাইবার আক্রমন** ঃ সাইবার আক্রমন এক ধরনের ইলেকট্রনিক আক্রমণ,যাতে ক্রিমিনালরা ইন্টারনেটের মাধ্যমে কারও সিস্টেমে বিনাঅনুমতিতে প্রবেশ করে ফাইল কিংবা কোনো প্রকার ক্ষতি সাধন করা।

❖ **হ্যাকিংঃ** সাধারণত হ্যাকিং একটি প্রক্রিয়া যার মাধ্যমে কেউ কোন বৈধ অনুমতি ব্যতীত কোন কম্পিউটার বা কম্পিউটার নেটওয়ার্কে প্রবেশ করে। যারা হ্যাকিং করে তারা হচ্ছে হ্যাকার। মোবাইল ফোন, ল্যান্ড ফোন, গাড়ি ট্র্যাকিং, বিভিন্ন ইলেক্ট্রনিক্স ও ডিজিটাল যন্ত্র বৈধ অনুমতি ছাড়া ব্যবহার করলে তা ও হ্যাকিং এর আওতায় পড়ে। হ্যাকাররা সাধারনত এসব ইলেকট্রনিক্স যন্ত্রের ত্রুটি বের করে তা দিয়েই হ্যাক করে। হ্যাকারদের চিহ্নিত করা হয় Hat বা টুপি দিয়ে। তিন প্রকারের হ্যকার রয়েছে।

❖ **স্প্যাম:** ই-মেইল একাউন্টে প্রায়ই কিছু কিছু অচেনা ও অপ্রয়োজনীয় ই-মেইল পাওয়া যায় যা আমাদের বিরক্তি ঘটায়। এই ধরণের ই-মেইলকে সাধারণত স্প্যাম মেইল বলে। যখন কোন ব্যক্তি বা প্রতিষ্ঠান নির্দিষ্ট কোন একটি ইমেইল অ্যাড্রেসে শতশত এমনকি লক্ষ লক্ষ মেইল প্রেরণের মাধ্যমে সার্ভারকে ব্যস্ত বা সার্ভারের পারফর্মেন্সের ক্ষতি করে বা মেমোরি দখল করার এই পদ্ধতিকে স্প্যামিং বলে।

❖ **স্পুফিং:** স্পুফিং শব্দের অর্থ হলো প্রতারনা করা, ধোঁকা দেওয়া। নেটওয়ার্ক সিকিউরিটির ক্ষেত্রে স্পুফিং হলো এমন একটি অবস্থা যেখানে কোন ব্যক্তি বা কোন একটি প্রোগ্রাম মিথ্যা বা ভুল তথ্য উপস্থাপনের মাধ্যমে নেটওয়ার্কে বিভ্রান্ত করে এবং এর সিকিউরিটি সিস্টেমে অনুপ্রবেশ করে অনৈতিকভাবে সুবিধা আদায় করে।

❖ **ফিশিং(Phishing):** ইন্টারনেট ব্যবস্থায় কোনো সুপ্রতিষ্ঠিত ওয়েবসাইট সেজে প্রতারণার মাধ্যমে কারো কাছ থেকে ব্যক্তিগত তথ্য, যেমন ব্যবহারকারী নাম ও পাসওয়ার্ড, ক্রেডিট কার্ডের তথ্য ইত্যাদি সংগ্রহ করাকে ফিশিং বলে। ইমেইল ও ইন্সট্যান্ট মেসেজের মাধ্যমে সাধারণত ফিশিং করা হয়ে থাকে। প্রতারকেরা তাদের শিকারকে কোনোভাবে ধোঁকা দিয়ে তাদের ওয়েবসাইটে নিয়ে যায়। ঐ

ওয়েবসাইটটি সংশ্লিষ্ট ব্যবহারকারীর ইমেইল, ব্যাংক বা ক্রেডিট কার্ডের আসল ওয়েবসাইটের চেহারা নকল করে থাকে। ব্যবহারকারীরা সেটাকে আসল ওয়েবসাইট ভেবে নিজের তথ্য প্রদান করলে সেই তথ্য প্রতারকদের হাতে চলে যায়।

❖ **ভিশিং(Vishing):** মোবাইল, টেলিফোন, ইন্টারনেট ভিত্তিক বিভিন্ন ফোন বা অডিও ব্যবহার করে ফিশিং করাকে ভিশিং বা ভয়েস ফিশিং বলা হয়। যেমনঃ ফোনে লটারী বিজয়ের কথা বলে এবং টাকা পাঠানোর কথা বলে ব্যক্তিগত তথ্য নেওয়া।

❖ **প্লেজিয়ারিজম(Plagiarism):** কোন ব্যাক্তি বা প্রতিষ্ঠানের কোন সাহিত্য, গবেষণা বা সম্পাদনা কর্ম হুবহু নকল বা আংশিক পরিবর্তন করে নিজের নামে প্রকাশ করাই হলো প্লেজিয়ারিজম।

প্রতিষ্ঠানের ক্ষেত্রে সাইবার নৈততিকতা ঃ

❖ প্রতিষ্ঠানের সকল তথ্যের গোপনীয়তা ও বিশ্বস্ততা রক্ষাকরা।
❖ কোনো তথ্যের ভুল উপস্থাপন করা।
❖ অনমোদন ছাড়া চাকুরিদের সম্পদ ব্যবহার করা।
❖ অফিস চলাকালীন সময়ের মধ্যে চ্যাট বা ব্রাউজার করে সময় নষ্ট করা।
❖ ভাইরাস ছড়ানো,স্কামিং ইত্যাদি কর্মকান্ড প্রতিহত করা।

নাগরিকের ক্ষেত্রে সাইবার অপরাধ ঃ

❖ তথ্য প্রযুক্তির মাধ্যমে নিজের দক্ষতা ও জ্ঞান কাজে লাগিয়ে জনগনের সেবা করা।
❖ তথ্যে ও যোগাযোগ প্রযুক্তি আইন ও নীতিমালা মেনে চলা।
❖ জনগনের সমস্যার কারণ হয় এমন বোনো তথ্যের ভুল উপস্থাপন না করা।
❖ ব্যক্তিগত উপার্জনের জন্য অবৈধভাবে তথ্যে প্রযুক্তির ব্যবহার না করা।

ইথিক্যাল হ্যাকিং ঃ

“ইথিক” শব্দের বাংলা অর্থ হচ্ছে “নৈতিক” অর্থাৎ নৈতিক বা বৈধ হ্যাকিং; আর এই হ্যাকিং যারা করে তাদের নীতি রয়েছে, তারা অনৈতিকভাবে কিছু করে না। প্রথমে জানি, একজন হ্যাকারের কাজ কি বা সে কি করে? দেখুন, হ্যাকার যেকোনো সিস্টেমের (কম্পিউটিং/নেটওয়ার্কিং সিস্টেম) ত্রুটি খুঁজে বেড় করার চেষ্টা করে এবং সিস্টেমটির নিরাপত্তা স্তর ভেদ করে মূল সিস্টেমে প্রবেশ করে আর নিয়ন্ত্রন গ্রহন করে। এখন কেউ যদি কোন সিস্টেম থেকে বা যে সফটওয়্যারটির নিরাপত্তা ত্রুটি খোঁজা হচ্ছে সেই কোম্পানি থেকে অনুমতি না নিয়েই সিস্টেমে প্রবেশের চেষ্টা করে তবে এই ধরনের হ্যাকারকে ম্যালিসিয়াস হ্যাকার বা ব্ল্যাক হ্যাট হ্যাকার বলা হবে। ম্যালিসিয়াস হ্যাকার সাধারনত সিস্টেমের রুল এবং সিকিউরিটি ভেঙ্গে ফেলে এবং মূল সিস্টেমের ক্ষতি সাধন করতে পারে।

তো হ্যাকিং বলতে, কোন সিস্টেমের ত্রুটি বা কমতি খুঁজে বেড় করে তাতে প্রবেশ করা। হ্যাকিং হচ্ছে, হ্যাকার কোন সিস্টেম অ্যাডমিন বা সফটওয়্যার কোম্পানি থেকে পারমিশন নেওয়ার পরে সেই সিস্টেমের ত্রুটি চেক করতে আরম্ভ করে। সে যদি সিস্টেমের সিকিউরিটি ব্রেক করেও ফেলে তবে এটা করার জন্য তার সম্পূর্ণ অনুমতি থাকে, সে ম্যালিসিয়াস হ্যাকারের মতো বিনা অনুমতিতে কাজ করে না। একজন এথিক্যাল হ্যাকার অবশ্যই যেকোনো কোম্পানি বা সিস্টেমের প্রাইভেসিকে শ্রদ্ধা জানাবে, এবং অবশ্যই অনুমতি সাপেক্ষেই কাজ করবে। সে কাজ করার পরে, মানে সিস্টেমটি চেক করে যদি কোন ত্রুটি খুঁজে পায় তবে অবশ্যই সেই ত্রুটি সম্পর্কে কোম্পানিকে অবগত করবে এবং সিকিউরিটি প্যাঁচ প্রদান করার মাধ্যমে সিস্টেমটিকে সিকিউর করতে সাহায্য করবে। যে যদি কোন ব্যাকডোর খুঁজে পায় তবে অবশ্যই সেটা সিল করে দেবে যাতে ম্যালিসিয়াস হ্যাকার সেটা দ্বারা প্রবেশ করে সিস্টেমের কোন ক্ষতি সাধন না করতে পারে।

তাছাড়া তিনি সিস্টেমটিতে অনেক প্রকারের অ্যাটাক করবে বিভিন্ন টেকনিক ব্যবহার করে যাতে সিস্টেমটির কোন ত্রুটি থাকলে সেটা সামনে ধরা পড়ে। হ্যাক অ্যাটাক চালানোর পরে যদি সিস্টেমটির ত্রুটি খুঁজে না পাওয়া যায়, তবে এতে কিন্তু এটা নিশ্চিত করে না, সিস্টেমটি

১০০% সিকিউর। কেনোনা ব্যস্তবিকভাবে কোন সিস্টেমই ১০০% সিকিউর নয়, এই জন্যই নিয়মিত সিকিউরিটি চেক করা প্রয়োজনীয়।

ইথিক্যাল হ্যাকিং-এর প্রয়োজনীয়তা ঃ

নিরাপত্তার ক্ষেত্রে ইথিক্যাল হ্যাকিং শেখার প্রয়োজনীয়তা ও তথ্য ও প্রযুক্তিতে এর ব্যবহার বরাবরই সর্বোচ্চ গুরুত্বের সাথে বিবেচনা করা হয়। সাম্প্রতিক সময়ে বিশ্বের অনেক বড় বড় কোম্পানীও নিরাপত্তাজনিত ত্রুটির কারণে বিড়ম্বনার শিকার হয়েছে। ফলাফল স্বরুপ আমরা বলতে পারি যে, বর্তমান সময়ের সবচেয়ে চাহিদা সম্পন্ন পেশার জন্য নিজেকে প্রস্তুত করার উপায় হচ্ছে সাইবার সিকিউরিটি বা ইথিক্যাল হ্যাকিং শেখা।

সাইবার নিরাপত্তা নিয়ে কাজ করতে আগ্রহী হলে অবশ্যই আপনাকে আগে জানতে হবে **হ্যাকাররা কিভাবে হ্যাক করে।** আর ইথিক্যাল হ্যাকিং এর মূল উদ্দেশ্যই থাকে কোন প্রতিষ্ঠানকে সাহায্য করার উদ্দেশ্যে তাদের সিস্টেম হ্যাক করা এবং নিরাপত্তা জনিত ত্রুটি সমূহ সম্পর্কে তাদের অবগত করা। তাছাড়া এই সময়ের যতগুলি পেশাতে সর্বোচ্চ বেতন বা সম্মানি প্রদান করা হয়, তার মধ্যে সাইবার সিকিউরিটি এক্সপার্ট বা একজন ইথিক্যাল হ্যাকারের স্থান অন্যতম।

ডিজিটালাইজেশনের এই যুগে ইন্টারনেট বিশ্বের ভিন্ন ভিন্ন প্রান্তের মানুষগুলোকে কাছে নিয়ে এসেছে। কিন্তু একই সাথে এটি অনলাইনে নিরাপত্তা জনিত অনেক ঝুঁকির সম্ভাবণাও বাড়িয়ে দিয়েছে যা সম্পর্কে এর আগে আমাদের কোন ধারণাই ছিল না।

ইন্টারনেটে লক্ষ লক্ষ এমন সব সফট্ওয়্যার ছড়িয়ে ছিটিয়ে আছে যা ইনষ্টল করলে ব্যবহারকারীর নিরাপত্তা বিঘ্নিত হবেই। তাই নিজেদের নিরাপত্তা নিশ্চিতকরণ সম্পর্কে সবাই কম বেশি উদ্বিঘ্ন থাকে। যার ফলে একজন ইথিক্যাল হ্যাকারের চাহিদা এখন অনলাইনের বাজারে সবচেয়ে বেশি। তাই চলুন জেনে নেওয়া যাক ঠিক কি কি কারণে আপনার ইথিক্যাল হ্যাকিং শেখা প্রয়োজন।

প্রতিটি ওয়েব সাইটের ক্ষেত্রে অবশ্যই ভারনারবেলেটি স্ক্যান করার প্রয়োজনীয়তা রয়েছে। ওয়েব সাইটের ভারনারবেলেটি বা দুর্বলতা সম্পর্কে আগে থেকে সচেতন থাকলে এবং দুর্বলতা গুলো সমাধান করলে,হ্যাকারদের কর্তৃক ওয়েবসাইট ক্ষতিগ্রস্ত হবার ঝুঁকি কমে যায়। অর্থাৎ ভারনারবেলেটি স্ক্যান করার প্রয়োজনীয়তা রয়েছে।

ইথিক্যাল হ্যাকিং-এর বিভিন্ন দিক সমূহ ঃ

- নেটওয়ার্কে নিরাপত্তা ব্যবস্থা দেখতে সিস্টেমে প্রবেশ করতে পারবে কিন্তু কোনো ক্ষতি বা কোনো ফাইল সংগ্রহ করতে পারবে না ।
- প্রতিষ্ঠানের সিকিউরিটি রক্ষার খাতিরে তাদের উপস্থিতিতে বা তাদেও অনুমতি সাপেক্ষে সিকিউরিটি রক্ষার কাজ করতে পারবে ।
- সিকিউরিটিতে আঘাত করে এমন কোনো তথ্যে কোথাও প্রচার করা যাবে না । ইথিক্যাল হ্যাকারদের কাজ সাইটের সিকিউরিটির সমস্যা বের করা এবং অ্যাডমিনকে জানানো ।

সাইবার নিরাপত্তা সম্পর্কে বাংলাদেশের বিভিন্ন আইন ঃ

- ডিজিটাল নিরাপত্তা আইন ২০১৮ – শিরোনামের সাইবার অপরাধ দমন আইনটিতে মোট ৪৮টি ধারা আছে। এর মধ্যে ১৭ থেকে ৪৮ ধারায় বিভন্ন অপরাধ ও শাস্তির বিধান রয়েছে। প্রধানমন্ত্রী শেখ হাসিনার সভাপতিত্বে মন্ত্রিসভা এই আইনের খসড়ায় চূড়ান্ত অনুমোদন দেয়ার ফলে, সংসদে এই আইন পাসে আর কোনো বাধা থাকলো না। তথ্য-প্রযুক্তি আইনের ৫৭ ধারাসহ আরো কিছু ধারা ব্যাপক সমালোচনার মুখে পড়ায়, ঐ আইনের ৫৪, ৫৫, ৫৬, ৫৭ ও ৬৬ ধারা বাতিলে করার অনুমোদন দিয়েছে মন্ত্রিসভা।

- নতুন আইনের ১ থেকে ১৬ ধারায় ডিজিটালের সংজ্ঞা, ডিজিটাল ফরেন্সিক ল্যাব, এমার্জেন্সি রেসপন্স টিম গঠন, প্রধানমন্ত্রীর নেতৃত্বে ১১ সদস্যের একটি ডিজিটাল নিরাপত্তা কাউন্সিল গঠনের কথা বলা হয়েছে।

- ডিজিটাল আইনের ৩২ ধারায় বলা হয়েছে, সরকারি, আধাসরকারি, স্বায়ত্তশাসিত প্রতিষ্ঠানে কেউ যদি বেআইনিভাবে প্রবেশ করে কোনো ধরনের তথ্য-উপাত্ত, যে কোনো ধরনের ইলেকট্রনিক্স যন্ত্রপাতি দিয়ে গোপনে রেকর্ড করে, তাহলে সেটা গুপ্তচরবৃত্তির অপরাধ হবে এবং এ অপরাধে সেই ব্যক্তি ১৪ বছর কারাদণ্ড ও ২০ লাখ টাকা জরিমানা বা উভয় দণ্ডে দণ্ডিত হবেন।

- ২৮ ধারায় বলা হয়েছে, কেউ যদি ধর্মীয় বোধ ও অনুভূতিতে আঘাত_করে, তাহলে তার ১০ বছরের জেল ও ২০ লাখ টাকা জরিমানা হবে।

- ২৯ ধারায় বলা হয়েছে, কেউ মানহানিকর কোনো তথ্য দিলে সেই ব্যক্তির তিন বছরের জেল ও পাঁচ লাখ টাকা জরিমানা বা উভয় দণ্ডে দণ্ডিত হবে।

সাইবার অপরাধ সম্পর্কে বাংলাদেশের বিভিন্ন আইন ঃ-

- তথ্য ও যোগাযোগ প্রযুক্তি আইন, ২০০৬ (সংশোধিত ২০১৩)-এর ৫৪ থেকে ৬৭ নম্বর ধারায় অপরাধের দণ্ড সংক্রান্ত বিষয় উল্লেখ করা হয়েছে। আইন পর্যালোচনা করে দেখা গেছে, আইনের ৫৪ ধারায় বলা হয়েছে, কম্পিউটার বা কম্পিউটার সিস্টেম ইত্যাদির ক্ষতি, অনিষ্ট সাধন যেমন ই-মেইল পাঠানো, ভাইরাস ছড়ানো, সিস্টেমে অনধিকার প্রবেশ বা সিস্টেমের ক্ষতি করা ইত্যাদি অপরাধ করলে সর্বোচ্চ ১৪ বছর ও সর্বনিম্ন সাত বছর কারাদণ্ড বা সর্বোচ্চ ১০ লাখ টাকা পর্যন্ত জরিমানা হতে পারে। আইনের এই বিধান অনুযায়ী উভয় (কারাদণ্ড ও অর্থদণ্ড) প্রদানের বিধানও রয়েছে। আইনের ৫৫ নম্বর ধারায় বলা হয়েছে, কম্পিউটারের সোর্স কোড পরিবর্তন সংক্রান্ত অপরাধের কথা। এখানে বলা হয়েছে, কম্পিউটারের সোর্স কোড পরিবর্তন সংক্রান্ত অপরাধ করলে সর্বোচ্চ তিন বছর কারাদণ্ড অথবা সর্বোচ্চ তিন লাখ টাকা অর্থদণ্ড বা উভয় দণ্ড হতে পারে।

- ৫৬ ধারায় বলা হয়েছে, কেউ যদি ক্ষতি করার উদ্দেশে এমন কোনো কাজ করেন, যার ফলে কোনো কম্পিউটার রিসোর্সের কোনো তথ্য বিনাশ, বাতিল বা পরিবর্তিত হয় বা এর উপযোগিতা হ্রাস পায় অথবা কোনো কম্পিউটার, সার্ভার, নেটওয়ার্ক বা কোনো ইলেকট্রনিক সিস্টেমে অবৈধভাবে প্রবেশ

করেন, তবে এটি হবে হ্যাকিং অপরাধ, যার শাস্তি সর্বোচ্চ ১৪ বছর কারাদণ্ড এবং সর্বনিম্ন ৭ বছর কারাদণ্ড বা ১ কোটি টাকা পর্যন্ত জরিমানা।

❖ ৫৭ ধারায় বলা হয়েছে, কোনো ব্যক্তি যদি ইচ্ছাকৃতভাবে ওয়েবসাইটে বা অন্য কোনো ইলেকট্রনিক বিন্যাসে কোনো মিথ্যা বা অশ্লীল কিছু প্রকাশ বা সম্প্রচার করে, যার দ্বারা মানহানি ঘটে, আইনশৃঙ্খলার অবনতি হয় অথবা রাষ্ট্র বা ব্যক্তির ভাবমূর্তি ক্ষুণ্ন হয়, তাহলে এগুলো হবে অপরাধ। এর শাস্তি সর্বোচ্চ ১৪ বছর কারাদণ্ড এবং সর্বনিম্ন ৭ বছর কারাদণ্ড এবং ১ কোটি টাকা পর্যন্ত জরিমানা। উভয় (কারাদণ্ড ও অর্থদণ্ড) দণ্ড দেওয়ার বিধানও এই আইনে রয়েছে। উল্লেখ্য, তীব্র সমালোচনা ও বিতর্কের পর এই ধারাটি আইনে বাদ দেওয়ার উদ্যোগ গ্রহণ করেছে সরকার। তবে একই ধরনের একটি ধারা ডিজিটাল নিরাপত্তা নামে নতুন একটি আইনে সংযুক্তির চেষ্টাও চলছে বলে জানা গেছে।

❖ আইনের ৫৮ ধারায় লাইসেন্স সমর্পণে ব্যর্থতার দায়ে সর্বোচ্চ ছয় মাস কারাদণ্ড ও সর্বোচ্চ ১০ হাজার টাকা অর্থদণ্ড অথবা উভয় দণ্ডে দণ্ডিত হবে বলে উল্লেখ রয়েছে। আইনের ৫৯ ধারায় বলা হয়েছে, ‘এই আইন বা এর বিধি বা প্রবিধান প্রতিপালন নিশ্চিত করার প্রয়োজনে নিয়ন্ত্রক, আদেশ দিয়ে বা কোনো সার্টিফিকেট প্রদানকারী কর্তৃপক্ষ বা উহার কোনো কর্মচারীকে আদেশে উল্লিখিত মতে কোনো বিষয়ে ব্যবস্থা গ্রহণ করতে বা কোনো কার্য করা হতে বিরত থাকতে নির্দেশ দিলে কোনো ব্যক্তি যদি ওই নির্দেশ লঙ্ঘন করেন, তাহা হলে ওই লঙ্ঘন একটি অপরাধ হবে। এই অপরাধে সর্বোচ্চ ১ বছর কারাদণ্ড বা ১ লাখ টাকা জরিমানা অথবা উভয় দণ্ডে দণ্ডিত করার বিধান রয়েছে এই আইনে।’

❖ আইনের ৬০ নম্বর ধারায় জরুরি পরিস্থিতিতে নিয়ন্ত্রকের নির্দেশ অমান্যে সর্বোচ্চ ৫ বছর কারাদণ্ড অথবা ৫ লাখ টাকা পর্যন্ত জরিমানা অথবা উভয় দণ্ডের বিধান রয়েছে। আইনের ৬১ ধারায় সংরক্ষিত সিস্টেমে প্রবেশের অপরাধে সর্বোচ্চ ১৪ বছর কারাদণ্ড অথবা ১০ লাখ টাকা অর্থদণ্ড অথবা উভয় দণ্ডের বিধান রয়েছে। আইনের ৬২ ধারায় সর্বোচ্চ ২ বছর কারাদণ্ড বা দুই লাখ

টাকা অর্থদণ্ড বা উভয় দণ্ডের কথা বলা হয়েছে লাইসেন্স বা সার্টিফিকেট প্রাপ্তিতে মিথ্যা প্রতিনিধিত্ব বা তথ্য গোপন সংক্রান্ত অপরাধে।

- আইনের ৬৩ ধারায় গোপনীয়তা প্রকাশ সংক্রান্ত অপরাধে সর্বোচ্চ দুই বছর কারাদণ্ড বা দুই লাখ টাকা অর্থদণ্ড অথবা উভয় দণ্ড প্রদানের কথা বলা হয়েছে। ৬৪ ধারায় সর্বোচ্চ দুই বছর কারাদণ্ড বা দুই লাখ টাকা অর্থদণ্ড অথবা উভয় দণ্ড প্রদানের কথা বলা হয়েছে ভুয়া ইলেকট্রনিক স্বাক্ষর সার্টিফিকেট প্রকাশ সংক্রান্ত অপরাধে। ৬৫ ধারায় বলা হয়েছে, প্রতারণার উদ্দেশে ইলেকট্রনিক স্বাক্ষর সার্টিফিকেট প্রকাশ সংক্রান্ত অপরাধে সর্বোচ্চ দুই বছর কারাদণ্ড বা দুই লাখ টাকা অর্থদণ্ড অথবা উভয় দণ্ড প্রদানের কথা বলা হয়েছে।

- আইনের ৬৬ ধারায় বলা হয়েছে, ‘কারও কম্পিউটার ব্যবহারের মাধ্যমে অপরাধ সংঘটিত হলে, অপরাধকারী যে দণ্ডে দণ্ডিত হবেন, ইচ্ছাকৃতভাবে অপরাধে সহায়তার জন্য কম্পিউটারের মালিকও সমান সাজা পাবেন। ৬৭ ধারায় বলা হয়েছে, কোনো কোম্পানি কর্তৃক এই আইনের অধীনে থাকা কোনো অপরাধ সংঘটিত হলে ওই অপরাধের সঙ্গে প্রত্যক্ষ সংশ্লিষ্টতা রয়েছে কোম্পানির এমন প্রত্যেক পরিচালক, ম্যানেজার, সচিব, অংশীদার, কর্মকর্তা এবং কর্মচারী উক্ত অপরাধ সংঘটিত করেছেন বলে গণ্য হবে। তবে ওই অপরাধ কোনো ব্যক্তির অজ্ঞাতসারে সংঘটিত হয়েছে প্রমাণ হলে অথবা ওই ব্যক্তি অপরাধ রোধ করতে যথাসাধ্য চেষ্টা করেছেন প্রমাণ হলে তিনি অভিযোগ থেকে অব্যাহতি পাবেন।

জব নং ঃ ০১

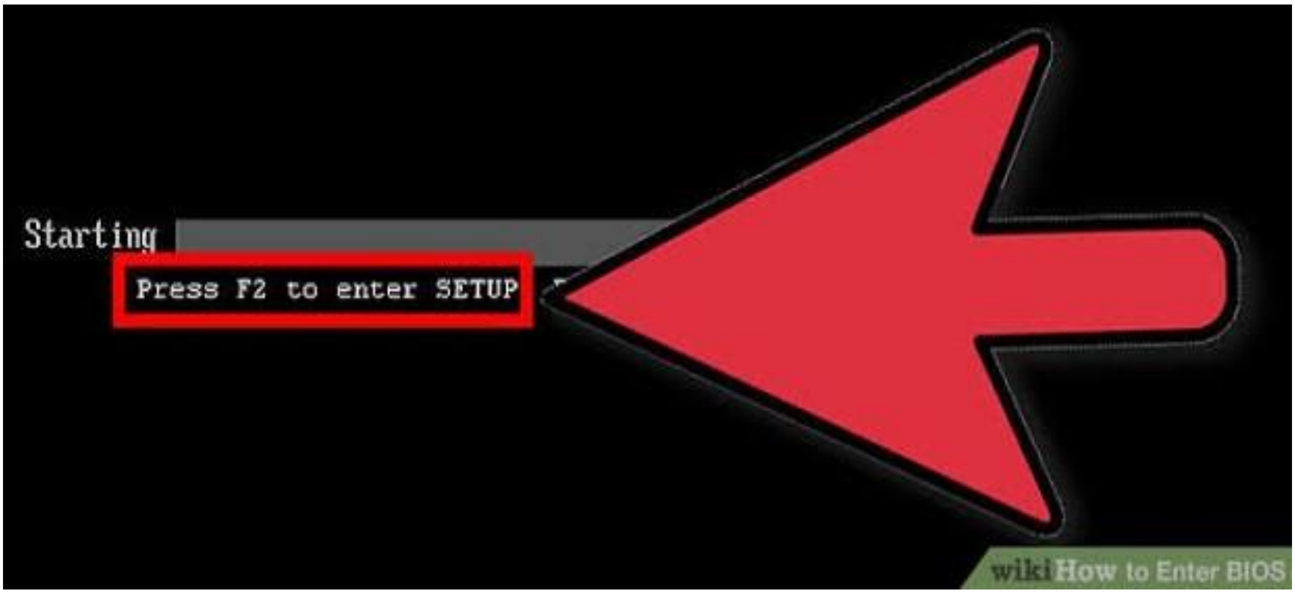
জবের নাম ঃ কম্পিউটার সিস্টেম এবং বিভিন্ন ফাইলগুলোতে যেমন-মাইক্রোসফট ওয়ার্ড, মাইক্রোসফট এক্সেল ইত্যাদিতে পাসওয়ার্ড প্রয়োগ করা।

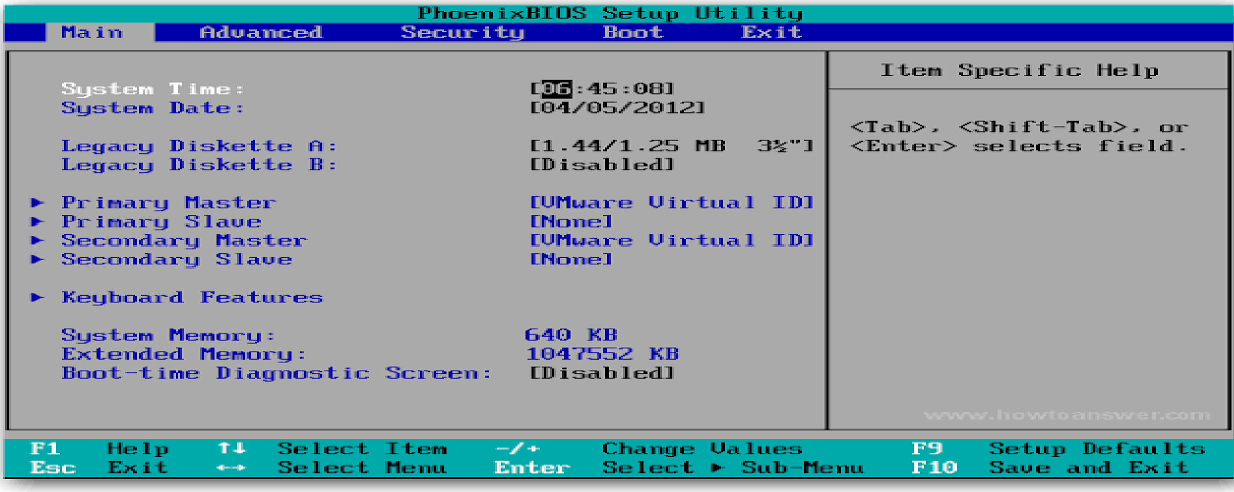
উদ্দেশ্য ঃ কম্পিউটার সিস্টেম এবং বিভিন্ন ফাইলগুলোতে পাসওয়ার্ড প্রদান করার মাধ্যমে কম্পিউটারের সাধারন নিরাপত্তা বৃদ্ধি করা।

যন্তপাতি ঃ কম্পিউটার সিস্টেম এবং বিভিন্ন অ্যাপ্লিকেশন সফটওয়্যার(যেমন- মাইক্রোসফট ওয়ার্ড, মাইক্রোসফট এক্সেল ইত্যাদি)।

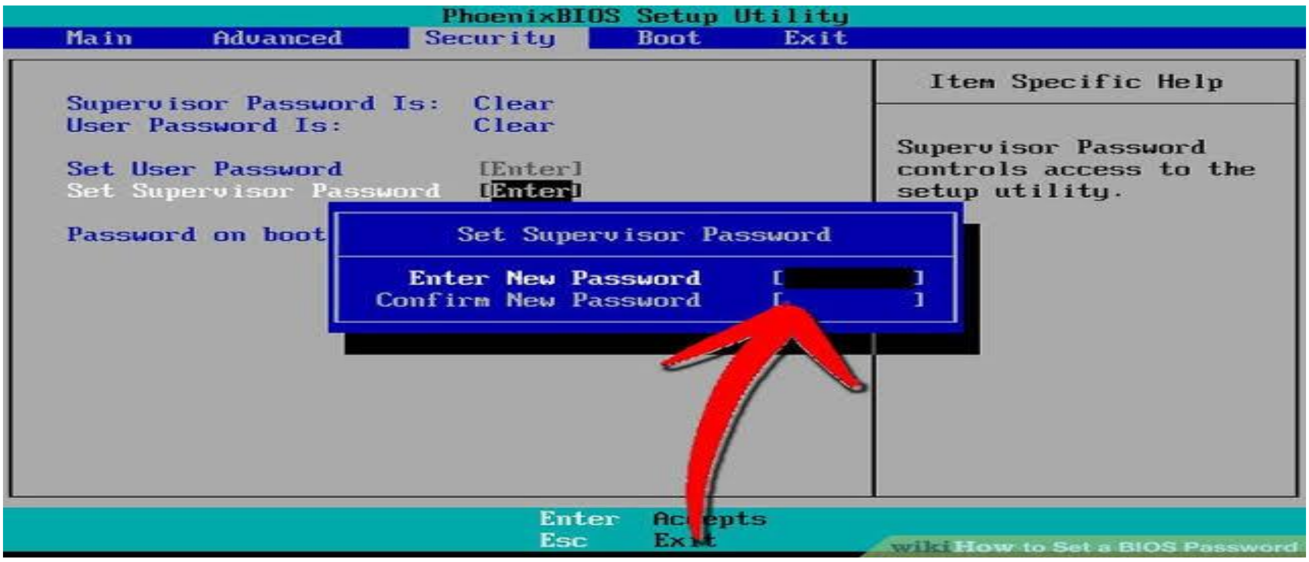
বর্ণনা ঃ নিম্নে একটি কম্পিউটার সিস্টেমে এবং বিভিন্ন ফাইলে পাসওয়ার্ড প্রয়োগ করার পদ্ধতি বণৃনা করা হল ঃ-

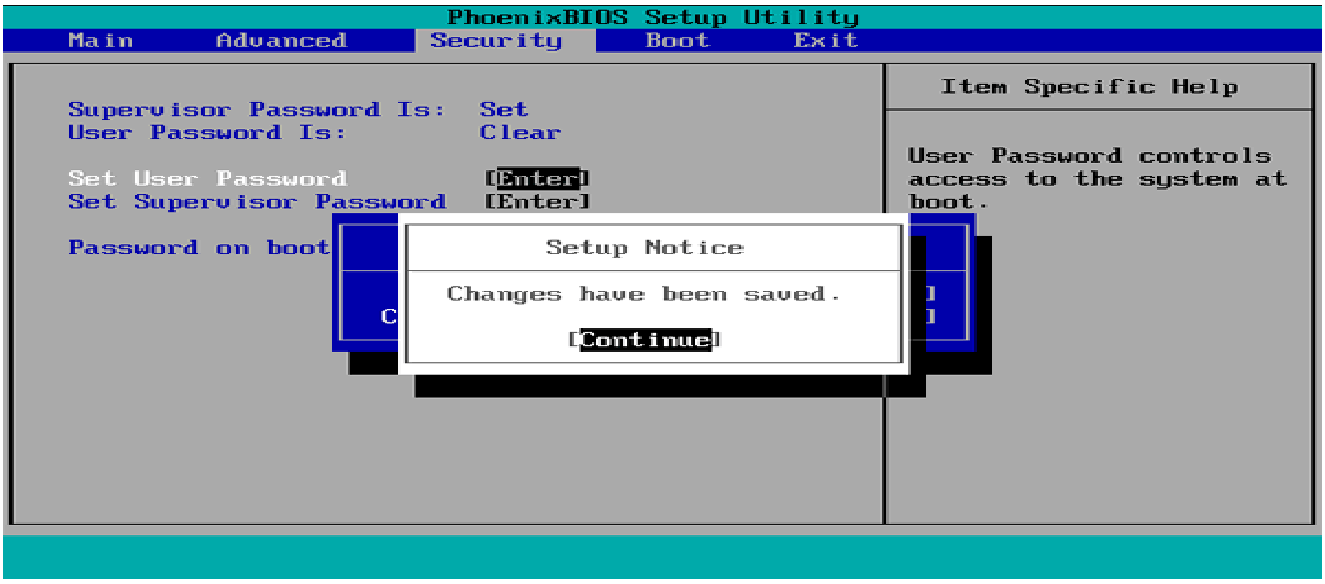
- **একটি কম্পিউটার চালু করে এর BIOS সেটআপ এ-প্রবেশ করবে ঃ-** BIOS তে যাওয়ার জন্য কম্পিউটার চালু হওয়ার সময় কী-বোর্ডেও একটি নির্দিষ্ট বাটন চাপতে হবে। এই বাটনটি বিভিন্ন মাদারবোর্ড-এ বিভিন্ন রকম হয়। মাদারবোর্ড-এ যে বাটন চাপতে হবে সেটি জানার জন্য মাদারবোর্ড ম্যানুয়েল অথবা ইন্টারনেট সার্চ করা যেতে পারে।





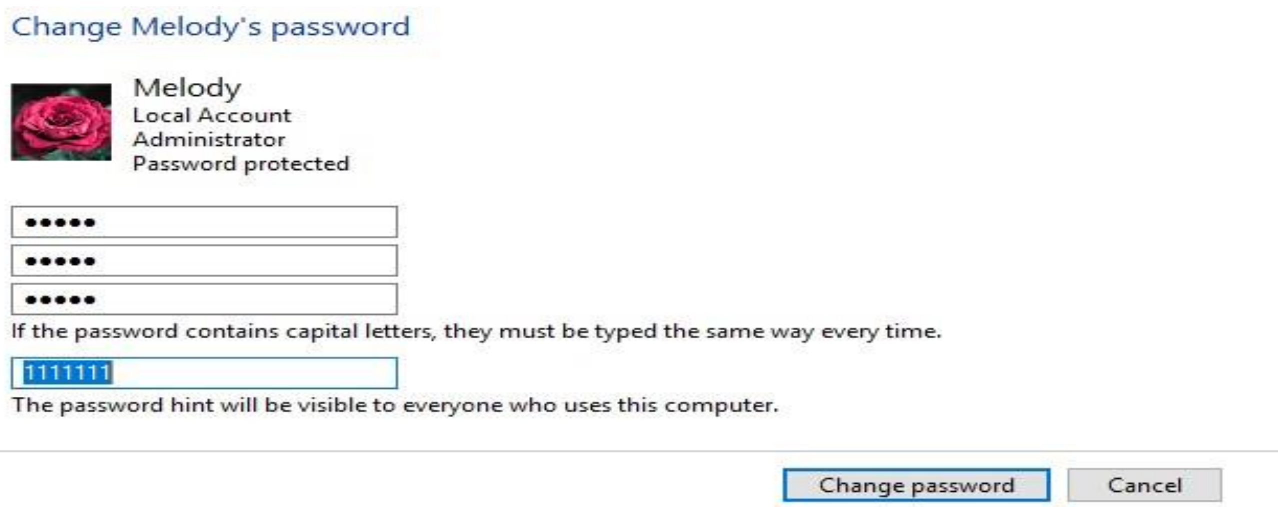
❖ **BIOS সিকিউরিটিতে পাসওয়ার্ড প্রদান ঃ** BIOS সিকিউরিটিতে পাসওয়ার্ড প্রদান করার জন্য নিম্নের চিত্র অনুসরন করতে হবে।



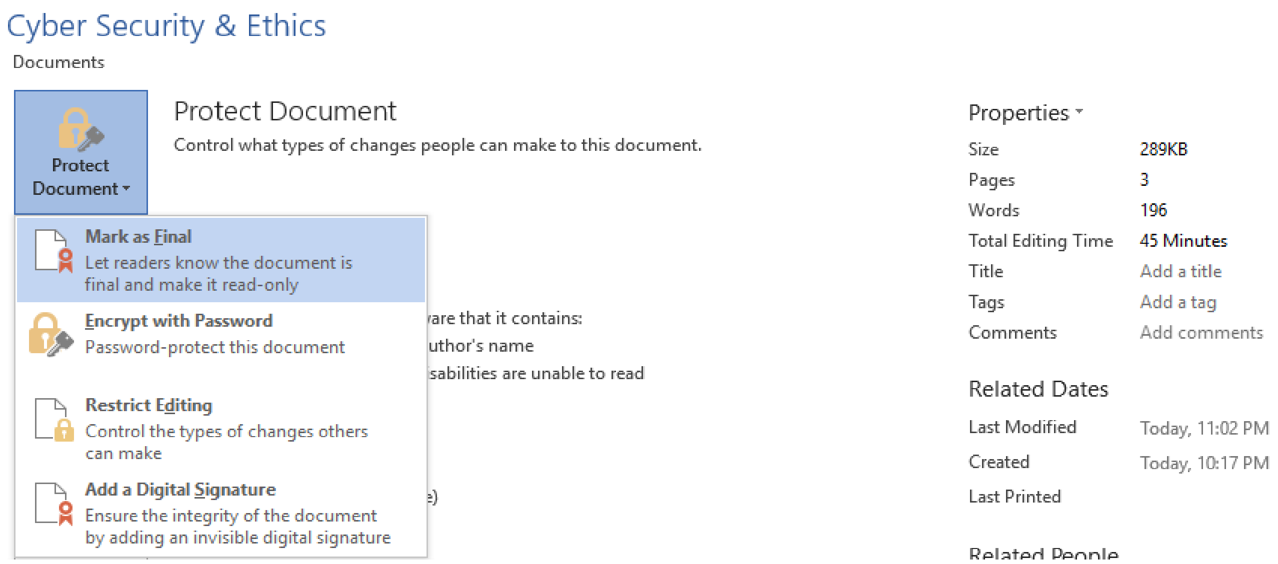


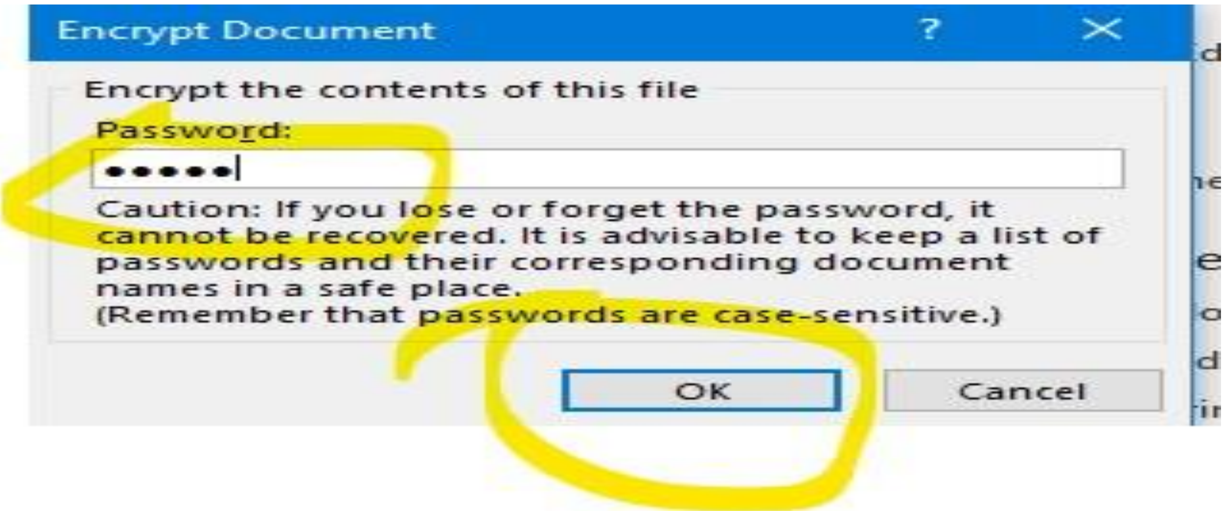
❖ পুনরায় কম্পিউটার চালু করে কন্টোল প্যানেল হতে পাসওয়ার্ড প্রদান ঃ পুনরায় কম্পিউটার চালু করে কন্টোল প্যানেল হতে পাসওয়ার্ড প্রদানের জন্য প্রথমে কম্পিউটার চালু করে কন্টোল প্যানেলে যেতে হবে।

❖



❖ **একটি এমএস ওয়ার্ড ফাইল তৈরী করা এবং এটি খোলা ও সম্পাদান করার জন্য একটি পাসওয়ার্ড দিয়ে সংরক্ষন করা ঃ** প্রথমে এমএস ওয়ার্ড চালু করে নিম্নোক্ত চিত্রের মতো ফাইল মেনু অপশনে ক্লিক করতে হবে।





সবশেষে ফাইলটি সেভ করতে হবে। তারপর থেকে ফাইলটির মাঝে যাই লেখা হক না কেন ফাইলটি চালু এবং সম্পাদনার জন্য সেই পাসওয়ার্ডটি প্রদান করতে হবে।

- **এমএস এক্সেল এবং এমএস অ্যাক্সেস ফাইল তৈরী করা এবং এটি খোলা ও সম্পাদান করার জন্য একটি পাসওয়ার্ড দিয়ে সংরক্ষন করা ঃ** এমএস ওয়ার্ডয়ের মতই ধাপ অনুসরন করে এমএস এক্সেল এবং এমএস অ্যাক্সেস ফইলেও খোলা ও সম্পাদান করার জন্য একটি পাসওয়ার্ড দিয়ে সংরক্ষন করা যায়।

মন্তব্য ঃ এ অধ্যায়ে আমরা শিখলাম কীভাবে কম্পিউটারের BIOS সিস্টেমে পাসওয়ার্ড প্রদান করতে হয়। আমরা আরও শিখলাম কীভাবে এমএস ওয়ার্ড এমএস এক্সেল এবং এমএস অ্যাক্সেস ফাইলে পাসওয়ার্ড প্রদান করে ফাইল নিরাপদ রাখতে হয়।

----------o----------

জব নং ঃ ০২

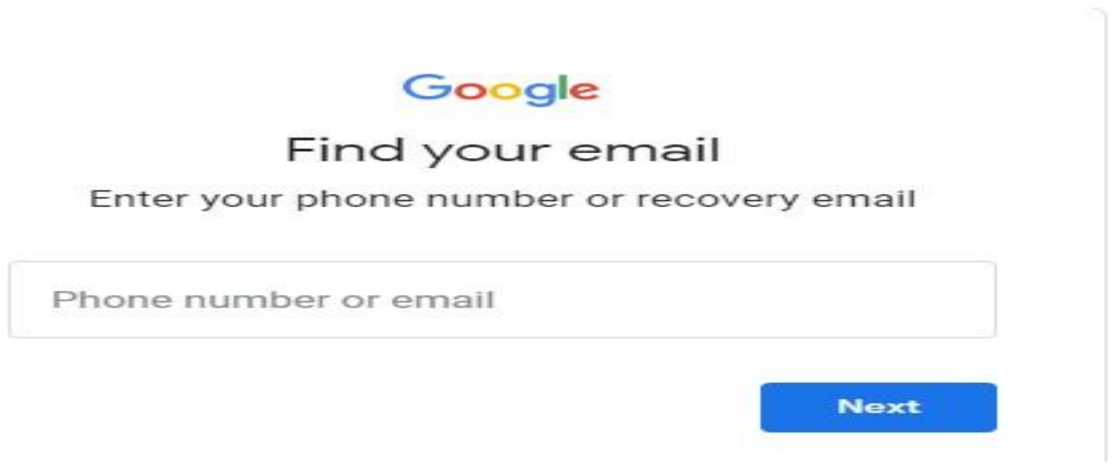
জবের নাম ঃ একটি ই-মেইলের ভুলে যাওয়া পাসওয়ার্ড পুনরুদ্ধার করা।

উদ্দেশ্য ঃ ই-মেইলের ভুলে যাওয়া পাসওয়ার্ড পুনরুদ্ধার করণ।

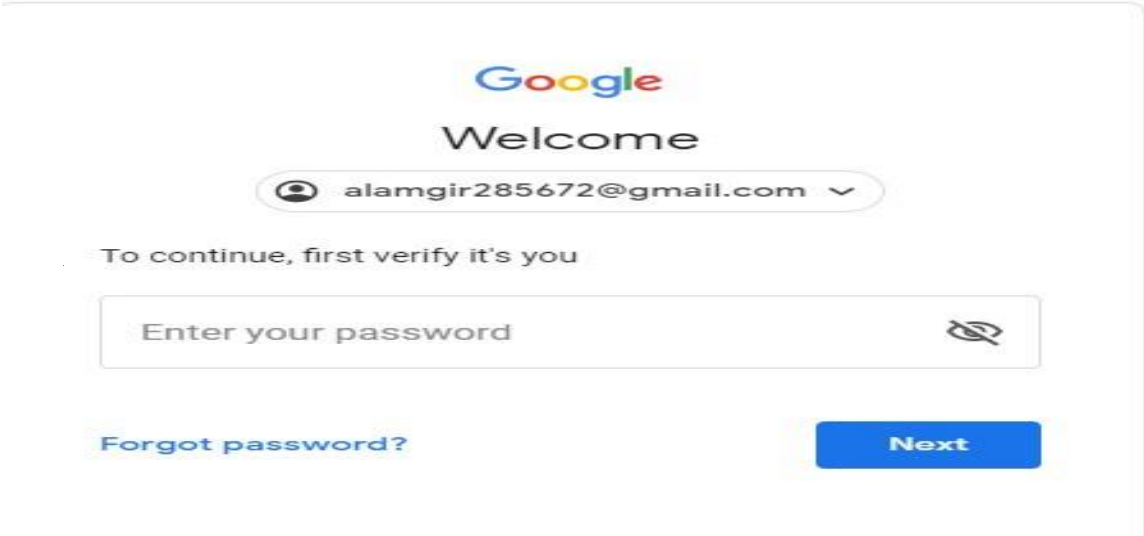
যন্তপাতি ঃ কম্পিউটার সিস্টেম, একটি ই-মেইল অ্যাকাউন্ট।

বর্ণনা ঃ নিম্নে একটি ই-মেইলের ভুলে যাওয়া পাসওয়ার্ড পুনরুদ্ধার করার পদ্ধতি বর্ণনা করা হলো ঃ-

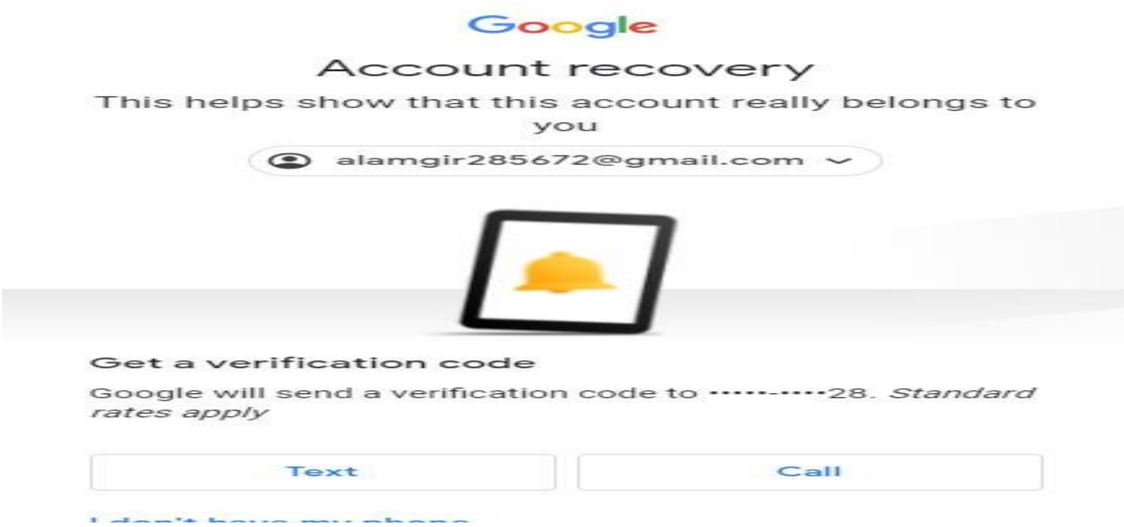
- **কম্পিউটার চালু করে একটি ব্রাউজার খোলা এবং জি-মেইল,ইয়াহু প্রোভাইডারে যাওয়া ঃ** ই-মেইল অ্যাকাউন্ট পাসওয়ার্ড পুনরুদ্ধারের জন্য প্রথমে কম্পিউটার চালু করে একটি ব্রাউজার ওপেন করতে হবে। তারপর https://accounts.google.com/signin/v2/usernamerecover লিংক-এ প্রবেশ করতে হবে-



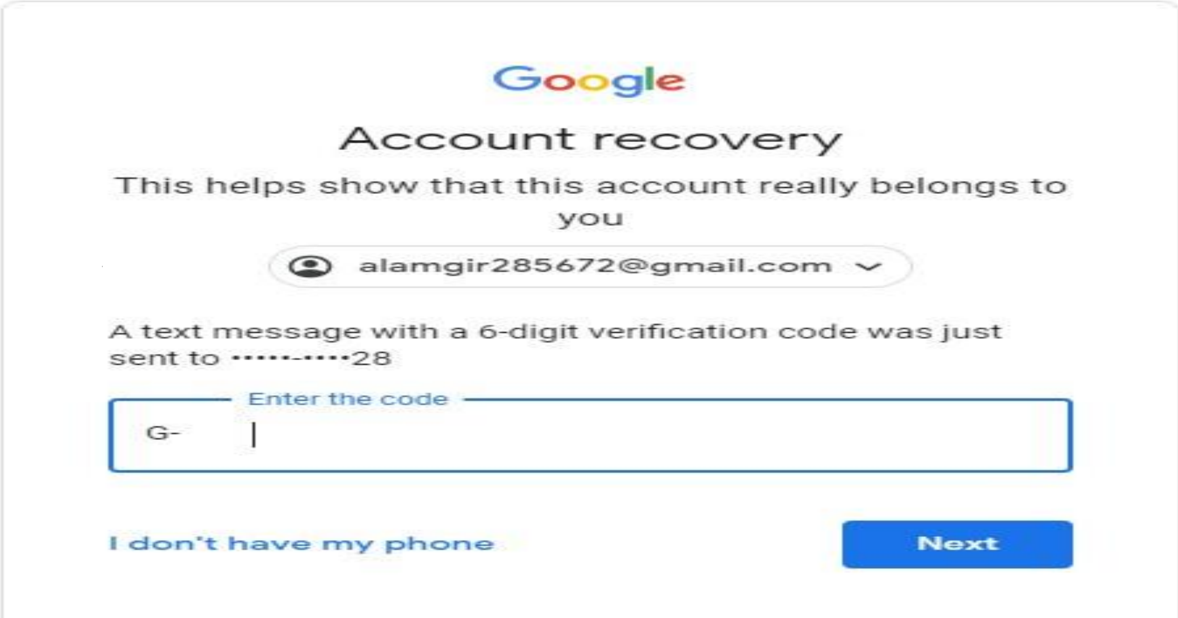
- **বিভিন্ন তথ্য প্রাদান করে ভুলে যাওয়া পাসওয়ার্ড পুনরুদ্ধারের চেষ্টা করা ঃ** এবার যে জি-মেইলের পাসওয়ার্ড পুনরুদ্ধার করা হবে সেটি ইউজার আডিতে দিতে হবে।

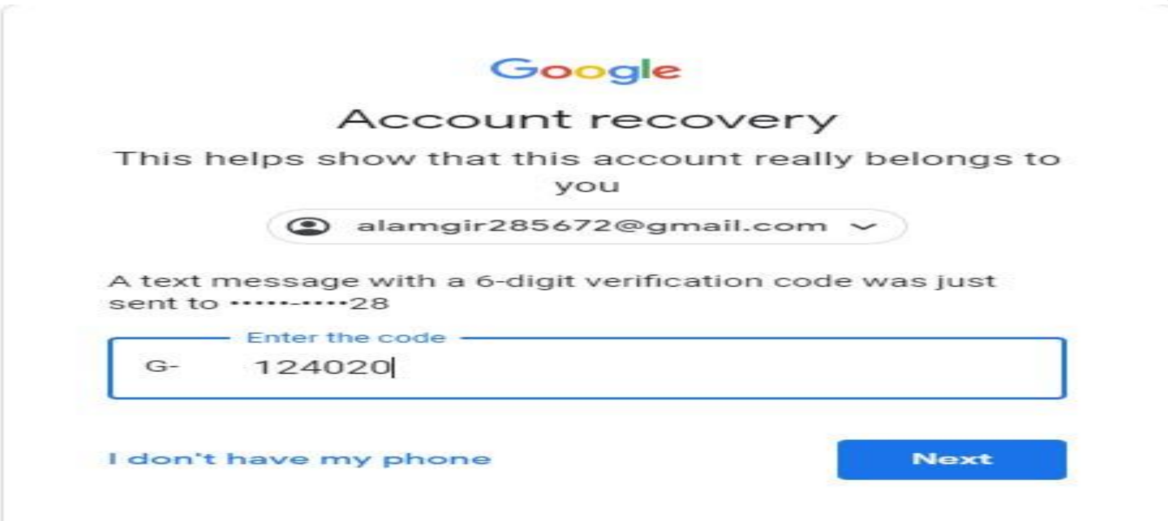


ইউজার আইডি দিয়ে “পরবর্তী” ধাপে গেলে পাসওয়ার্ড পুনরুদ্ধারের বিভিন্ন অপশন আসবে। সুবিধানুযায়ী যে কোনো অপশন সিলেক্ট করার জন্য “অন্য ভাবে চেষ্টা করুন” অপশনটিকে ক্লিক করতে হবে।

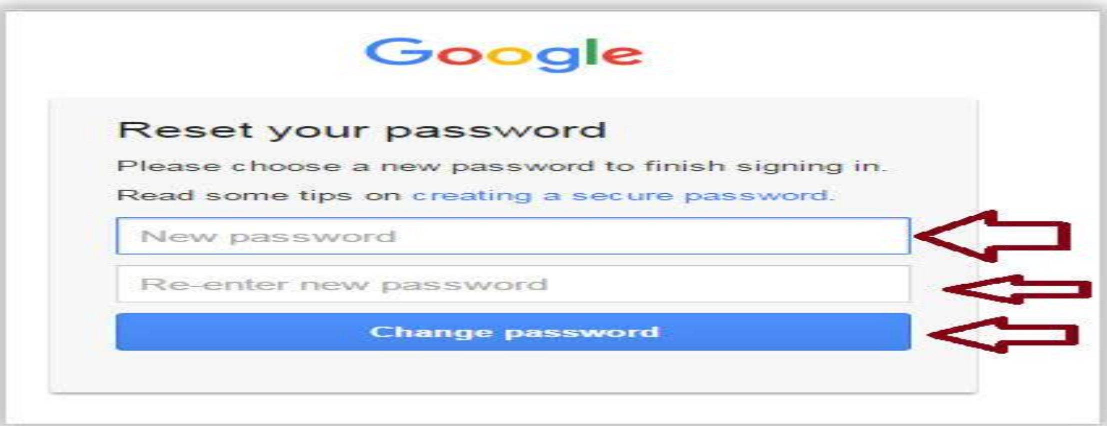


সুবিধামতো অপশন সিলেক্ট করার পর অ্যাকাউন্ট তৈরী করার সময় যে মুঠোফোনের নম্বর দেয়া ছিল,সেই মুঠোফোনের নম্বরটি এখানে প্রবেশ করাতে হবে। তারপর মুঠোফোনে একটি কোড আসবে এবং সেই কোড নিম্নে চিত্রের মতো প্রবেশ করালে পাসওয়ার্ড তৈরী করার অপশন পাওয়া যাবে।

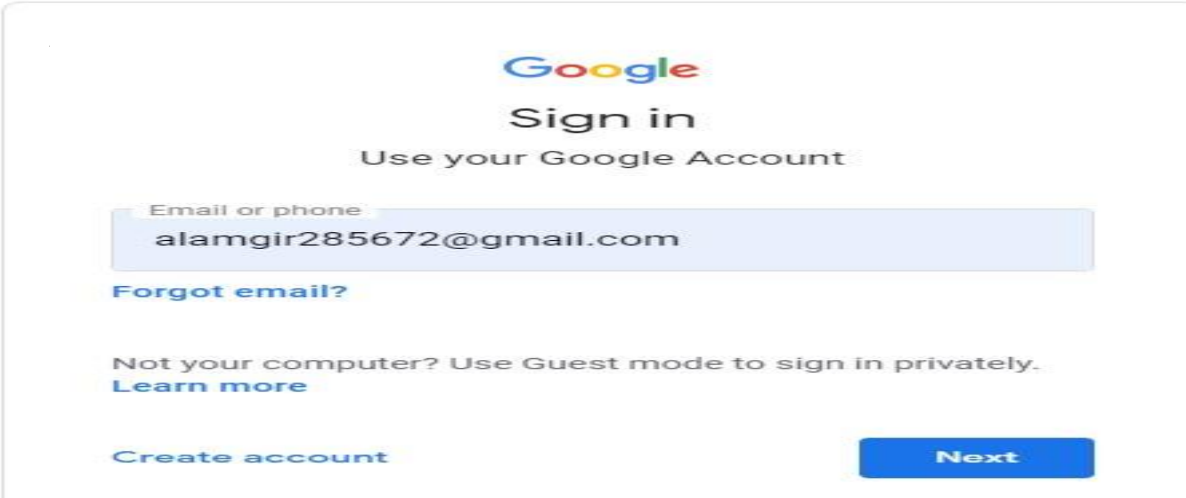




নতুন পাসওয়ার্ড প্রদান করে সাবমিট করলে পাসওয়ার্ড পুনরুদ্ধার প্রক্রিয়া সম্পন্ন হবে।



❖ **নতুন পাসওয়ার্ডের মাধ্যমে ই-মেইল লগইন করা ঃ** পাসওয়ার্ড পরিবর্তন করার পর https://accounts.google.com/signin/ লিংকে প্রবেশ করে জি-মেইল ইউজার আইডি এবং নতুন পাসওয়ার্ড দ্বারা লগইন করা যাবে।



মন্তব্য ঃ একটি ই-মেইলের ভুলে যাওয়া পাসওয়ার্ড পুনরুদ্ধার করা শিখলাম এবং এটি সম্পর্কে বাস্তব জ্ঞান অর্জন করলাম।

-----------o----------

জব নংঃ ০৩

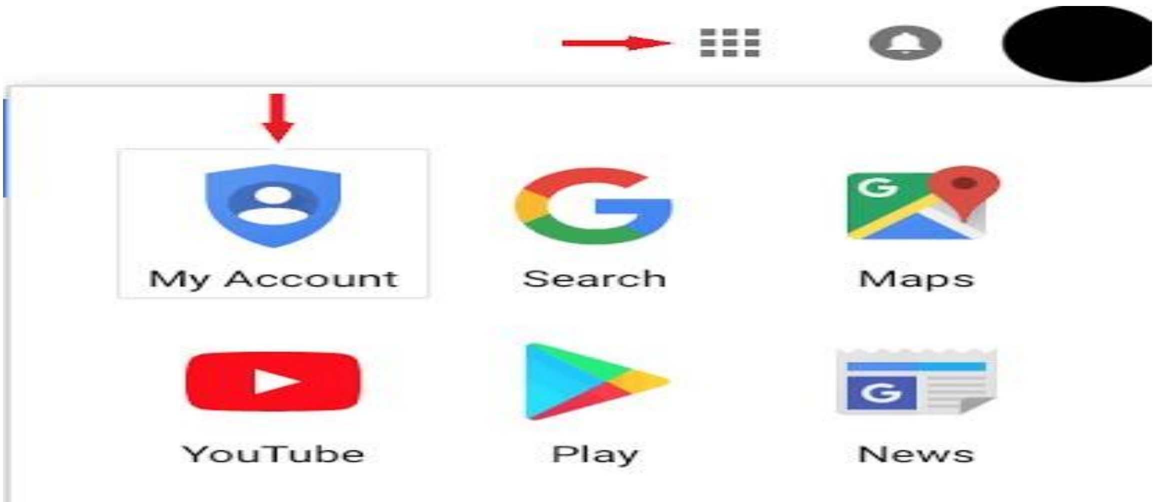
জবের নাম ঃ ই-মেইলে বিবিন্ন সিকিউরিটি স্টেপ প্রয়োগ করা।

উদ্দেশ্য ঃ ই-মেইলে নিরাপত্তা বৃদ্ধি করার জন্য বিবিন্ন সিকিউরিটি স্টেপ প্রয়োগ করা।

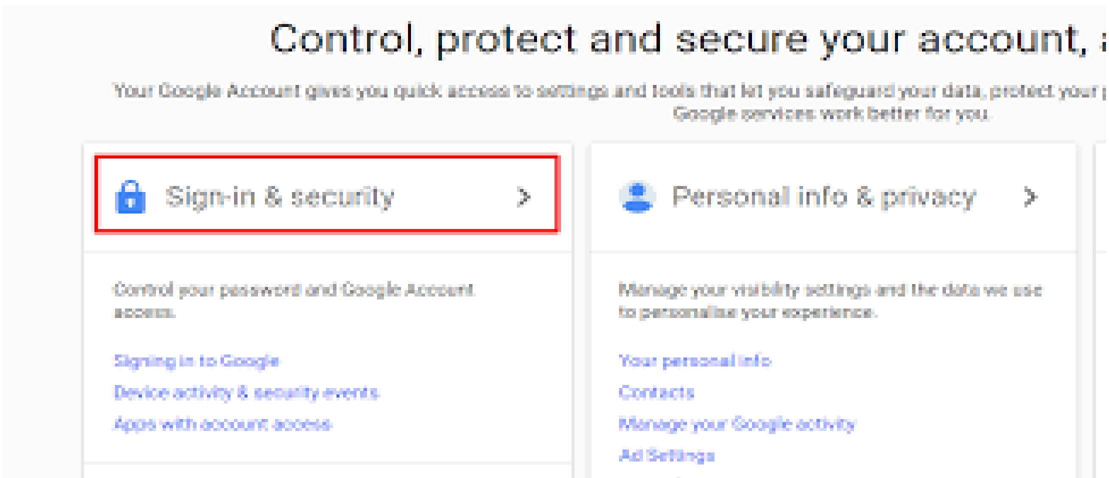
যন্তপাতি ঃ কম্পিউটার সিস্টেম, একটি ই-মেইল অ্যাকাউন্ট।

বর্ণনা ঃ ই-মেইলে নিরাপত্তা বৃদ্ধি করার জন্য ই-মেইলে বিবিন্ন সিকিউরিটি স্টেপ প্রয়োগ করার পদ্ধতি নিম্নে বর্ণনা করা হলো ঃ

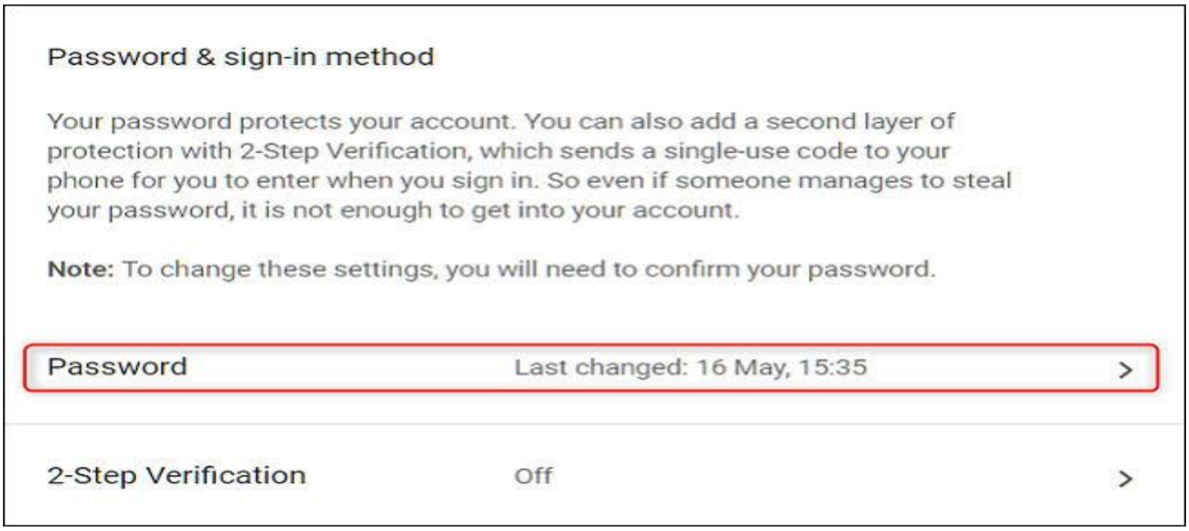
❖ **ই-মেইল চালু করা ঃ** ই-মেইল অ্যাকাউন্ট চালু করার জন্য https://accounts.google.com/signin/ লিংকে প্রবেশ করে জি-মেইল আইডি এবং পাসওয়ার্ড দ্বারা লগইন করতে হবে।



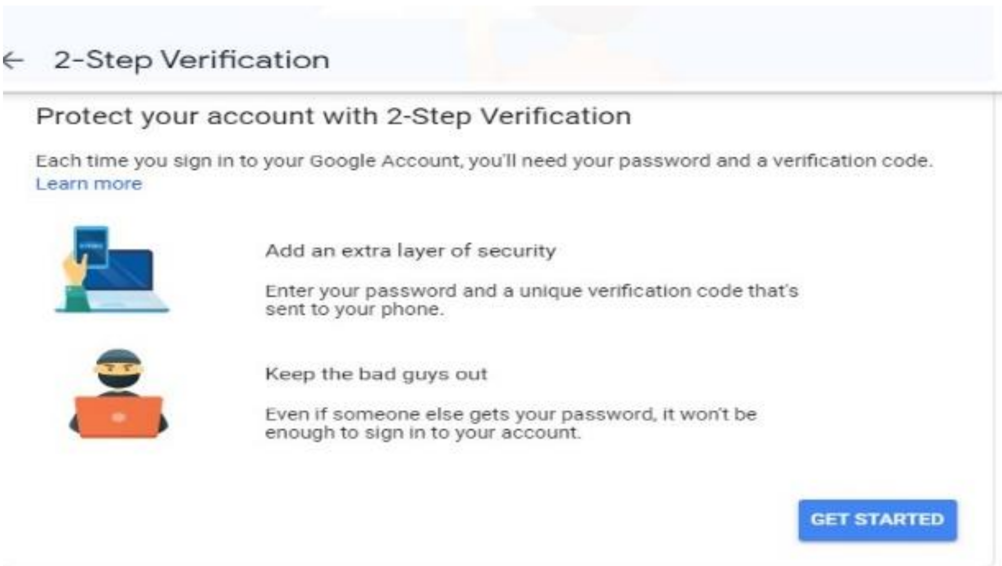
সেখান থেকে “My Account” এ ক্লিক করে সেটিংস-এ প্রবেশ করতে হবে।



❖ **মোবাইল নম্বও বা অন্যান্য ই-মেইল অ্যাড্রেস প্রদান করে দুই ধাপ নিরাপত্তি প্রয়োগ করা ঃ** দুই ধাপ নিরাপত্তা যাচাইকরণ প্রক্রিয়া চালু করার জন্য প্রথমে উপরের চিত্রে“ Sign-in and Security ” এর মাঝে ক্লিক করতে হবে।



তারপর “step-2 verification” অপশনে ক্লিক করতে হবে।



তারপর নিম্নের চিত্রানুযায়ী কার্যক্রম সম্পন্ন করতে হবে।

← 2-Step Verification

Let's set up your phone

What phone number do you want to use?

+880 1794-011664

Google will only use this number for account security.
Don't use a Google Voice number.
Message and data rates may apply.

How do you want to get codes?

Text message   Phone call

Don't want to use text message or voice call?

Choose another option

Step 1 of 3   NEXT

← 2-Step Verification

Confirm that it works

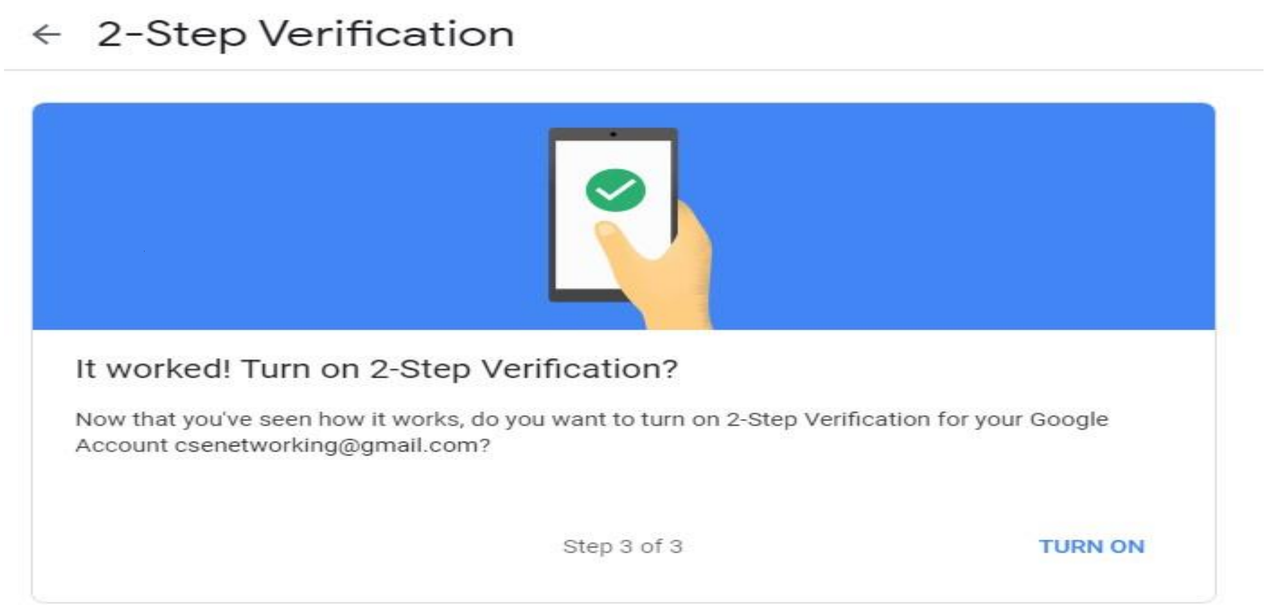
Google just sent a text message with a verification code to **01794-011664**.

Enter the code

934940

Didn't get it? Resend

BACK   Step 2 of 3   NEXT



মন্তব্য ঃ এই অধ্যায়ে আমরা শিখলাম কীভাবে দুই ধাপ মোবাইল কোড যাচাইকরণ-এর মাধ্যমে ই-মেইল এর নিরাপত্তা বৃদ্ধি।

----------o---------

জব নং ঃ ০৪

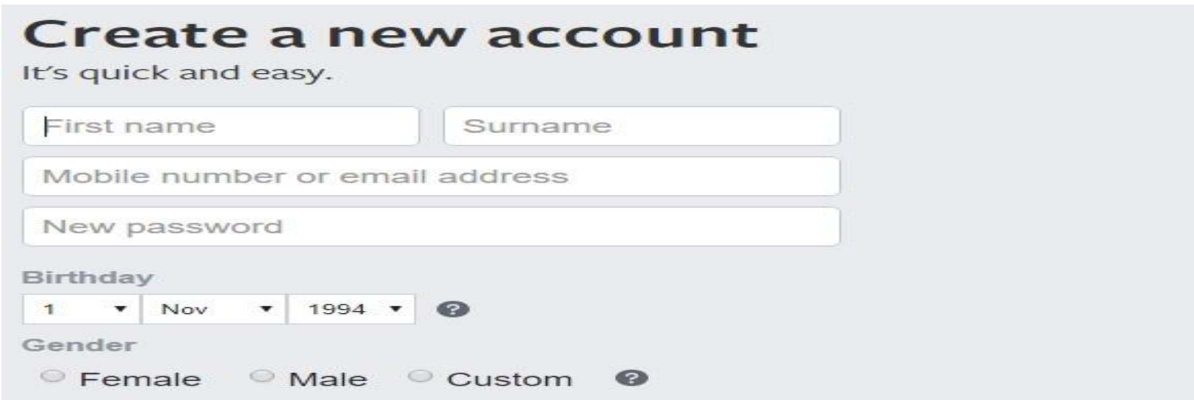
জবের নাম ঃ সামাজিক মিডিয়া হিসাবে ফেসবুক লগইন-এর বিভিন্ন নিরাপত্তা পদক্ষেপ গ্রয়োগ করা।

উদ্দেশ্য ঃ সামাজিক মিডিয়া ফেসবুক-এর নিরাপত্তা বৃদ্ধি করার জন্য এর বিভিন্ন নিরাপত্তা ধাপ প্রয়োগ করা।

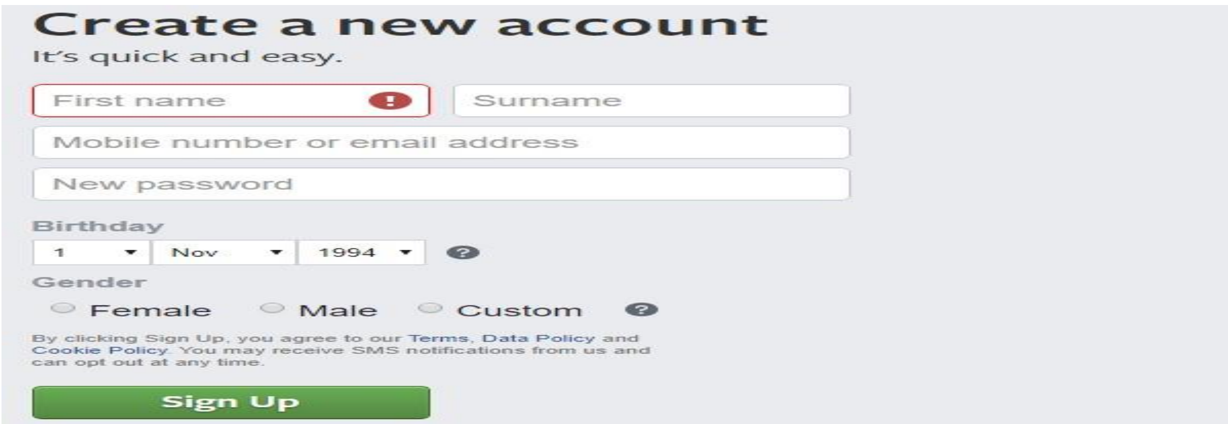
যন্তপাতি ঃ কম্পিউটার সিস্টেম,একটি মেইল অ্যাকাউন্ট।

বর্ণনা ঃ নিম্নে ফেসবুক-এর নিরাপত্তা বৃদ্ধি করার জন্য এর বিভিন্ন নিরাপত্তা ধাপ প্রয়োগ করার পদ্ধতি বর্ণনা করা হল ঃ

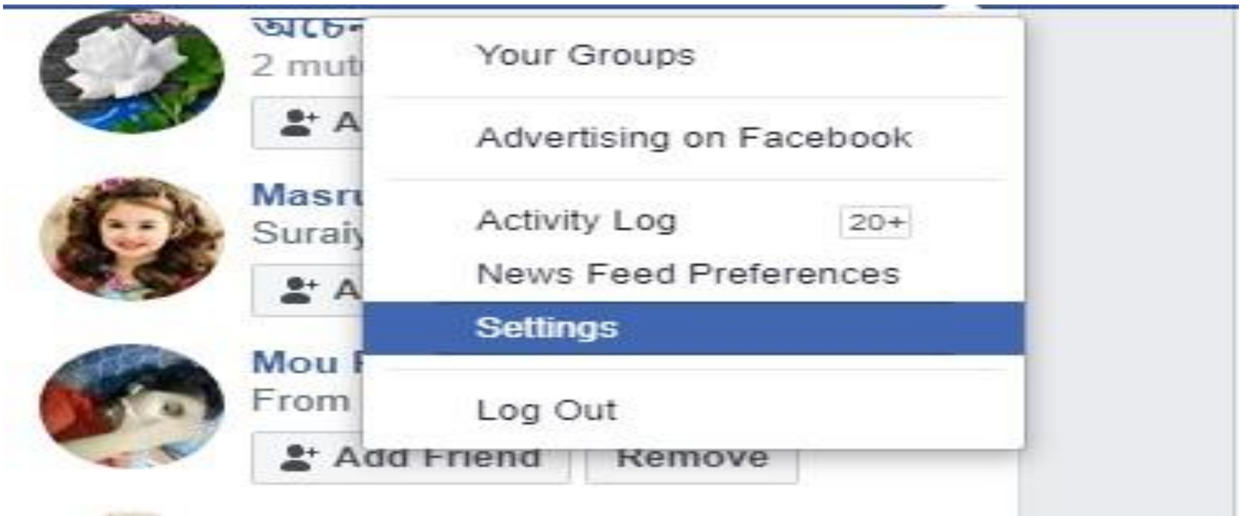
- ফেসবুক অ্যাকাউন্ট খোলার জন্য প্রথমে লিংক-এ প্রবেশ করতে হবে। উক্ত লিংকে প্রবেশ করলে নিম্নের ইন্টারফেস আসবে।



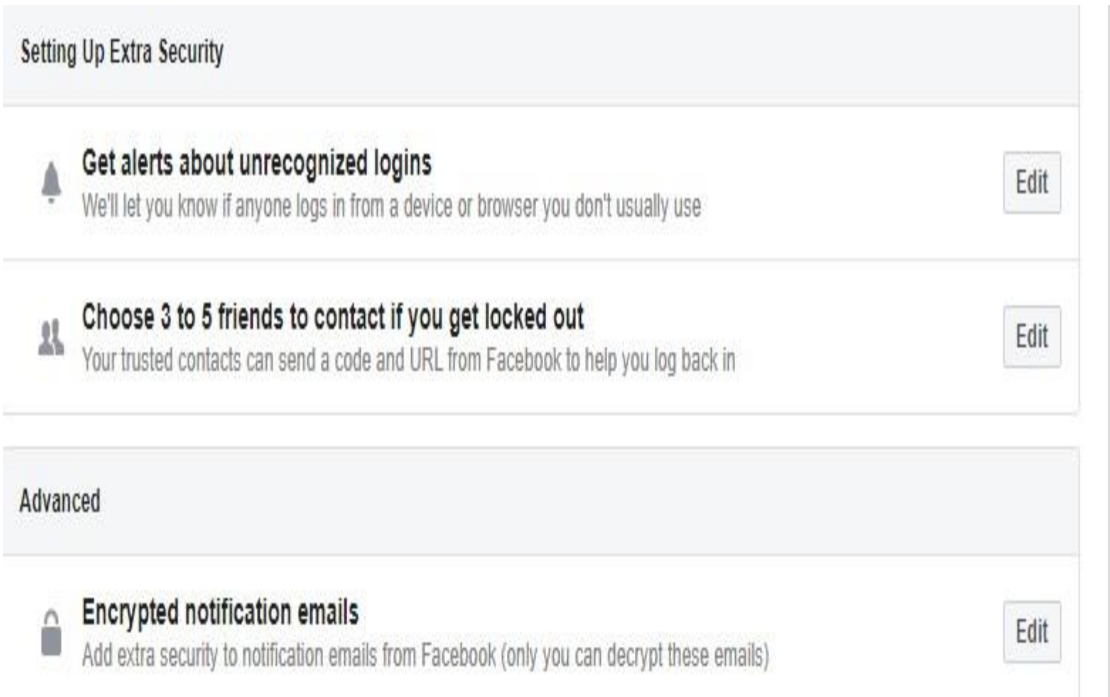
উপরের ইন্টারফেস সবগুলো তথ্য সঠিকভাবে পূরন করে নিম্নের চিত্রের মতো সাবমিট করতে হবে।

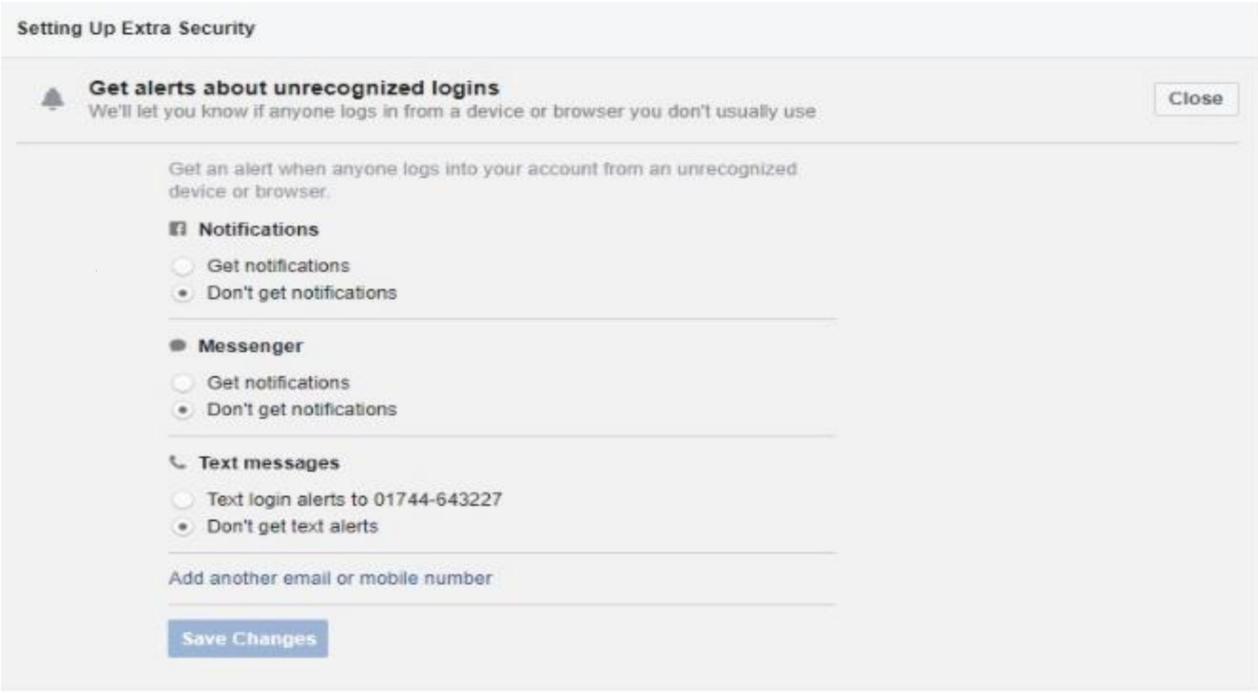


❖ **সেটিংস-এ যাওয়া ঃ** ফেসবুক অ্যাকাউন্ট খোলার পর সবার উপরে ডান দিকে সেটিংস অপশনে ক্লিক করতে হবে।,যা নিম্নে দেয়া হলো ঃ-

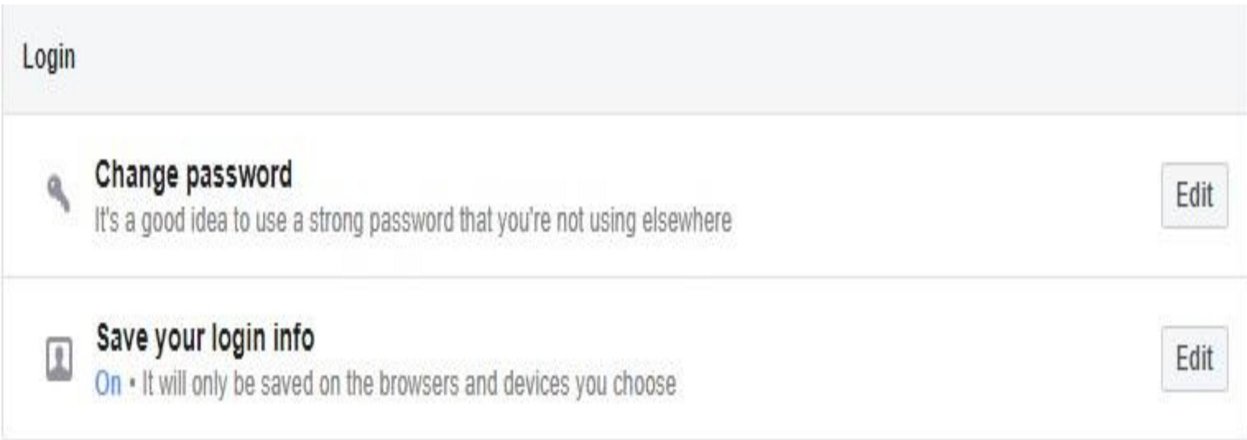


❖ **মোবাইল নম্বর এবং ই-মেইল ঠিকানা ব্যবহার করে বিভিন্ন নিরাপত্তা পদক্ষেপ প্রয়োগ করা ঃ** উপরে উল্লেখিত সেটিংস অপশনে ক্লিক কারর পর নিম্নের মতো ইন্টারফেস আসবে। এবং " Login Alerts"এ ক্লিক করতে হবে।





❖ **নিরাপত্তা পদক্ষেপ প্রয়োগকরে ফেসবুক পাসওয়ার্ড পরিবর্তন করার চেষ্টা ঃ** সেটিংস থেকে " Security and Login" অপশনে ক্লিক করার মাধ্যমে বিভিন্ন পদক্ষেপ ব্যবহার করে পাসওয়ার্ড পরিবর্তন করা যায়।



মন্তব্য ঃ এই অধ্যায়ে আমরা শিখলাম কীভাবে ফেসবুক অ্যাকাউন্ট খোলা এবং নিরাপত্তা বৃদ্ধি করা যায়।

-----------o-----------

জব নংঃ ০৫

জবের নাম ঃ অ্যান্টিভাইরাস সফটওয়্যার ইনস্টল করা এবং সফটওয়্যার দিয়ে কম্পিউটার সিস্টেম স্ক্যান করা।

উদ্দেশ্য ঃ কম্পিউটার সিস্টেমকে ভাইরাস,ম্যালওয়্যার ইত্যাদি থেকে নিরাপদ রাখার জন্য কম্পিউটারে একটি অ্যান্টিভাইরাস সফটওয়্যার ইনস্টল করা কম্পিউটার সিস্টেম স্ক্যান করা।

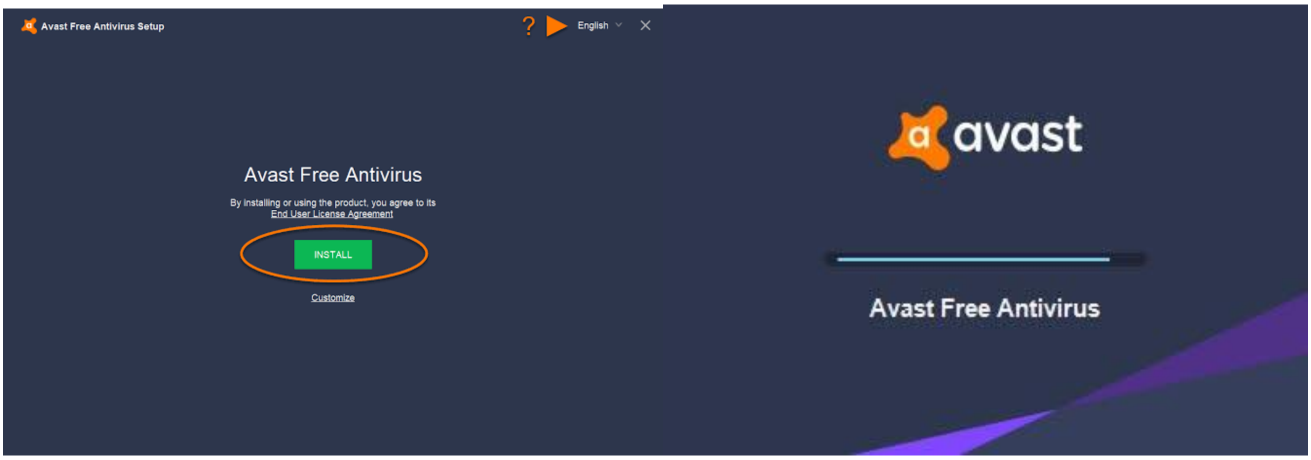
যন্তপাতি ঃ কম্পিউটার সিস্টেম, অ্যান্টিভাইরাস সফটওয়্যার।

বর্ণনা ঃ নিম্নে অ্যান্টিভাইরাস সফটওয়্যার ইনস্টল করা এবং সফটওয়্যার দিয়ে কম্পিউটার সিস্টেম স্ক্যান করার পদ্ধতি নিম্নে দেয়অ হলোঃ-

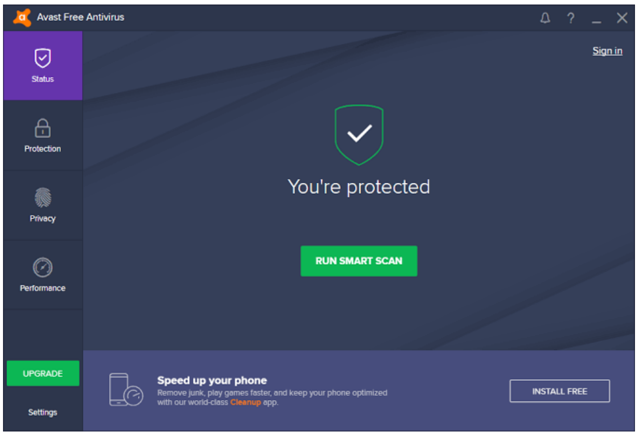
- ❖ **কম্পিউটার চালু করা ঃ** অ্যান্টিভাইরাস সফটওয়্যার ইনস্টল করার জন্য প্রথমে কম্পিউটারটি চালু করতে হবে।
- ❖ **ওয়েব ব্রাউজার ব্যবহার করে ফ্রিতে অ্যাভাস্ট,অ্যাভিয়া ইত্যাদি অ্যান্টিভাইরাস সফটওয়্যার ডাউনলোড করা ঃ** কম্পিউটার চালু করার পর ফ্রিতে অ্যাভাস্ট অ্যান্টিভাইরাস সফটওয়্যার ডাউনলোড করার জন্য প্রথমে যেতে হবে অ্যাভাস্ট অফিসিয়াল পেজে।

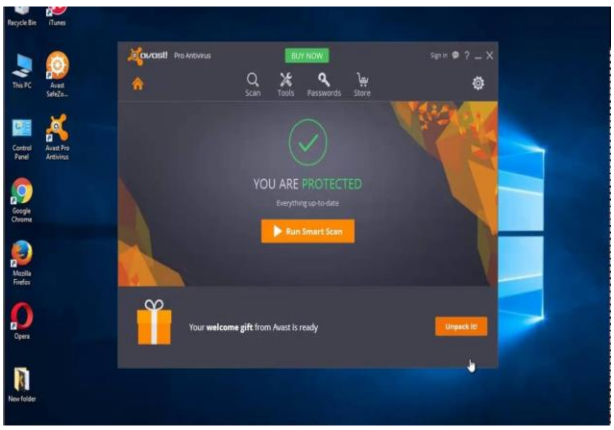
সেখান থেকে “ FREE DOWNLOAD FOR PC”অপশনে ক্লিক করে সফটওয়্যারটি ডাউনলোড করতে হবে।

❖ **অ্যান্টিভাইরাস সফটওয়্যার ইনস্টল করা ঃ** অ্যান্টিভাইরাস সফটওয়্যার ডাউনলোড করার পর, সফটওয়্যারটির ফাইলের মাঝে ডাবল ক্লিক করতে হবে ঃ তারপর নিম্নের উইন্ড আসবে।



❖ **অ্যান্টিভাইরাস সফটওয়্যারের মাধ্যমে স্কান করা ঃ** অ্যান্টিভাইরাস সফটওয়্যার সঠিক ভাবে ইনস্টল করার পর নিম্নের ইন্টারফেস আসবে। সেখান থেকে স্কান অপশনে ক্লিক করে কম্পিউটার সিস্টেমকে স্কান করতে হবে।





মন্তব্য ঃ এই অধ্যায়ে আমরা শিখলাম কীভাবে অ্যান্টিভাইরাস সফটওয়্যার ইনস্টল করা যায় এবং অ্যান্টিভাইরাস সফটওয়্যার দিয়ে কম্পিউটার সিস্টেমকে স্কান করে এর নিরাপত্তা বৃদ্ধি করা যায়।

জব নং ঃ ০৬

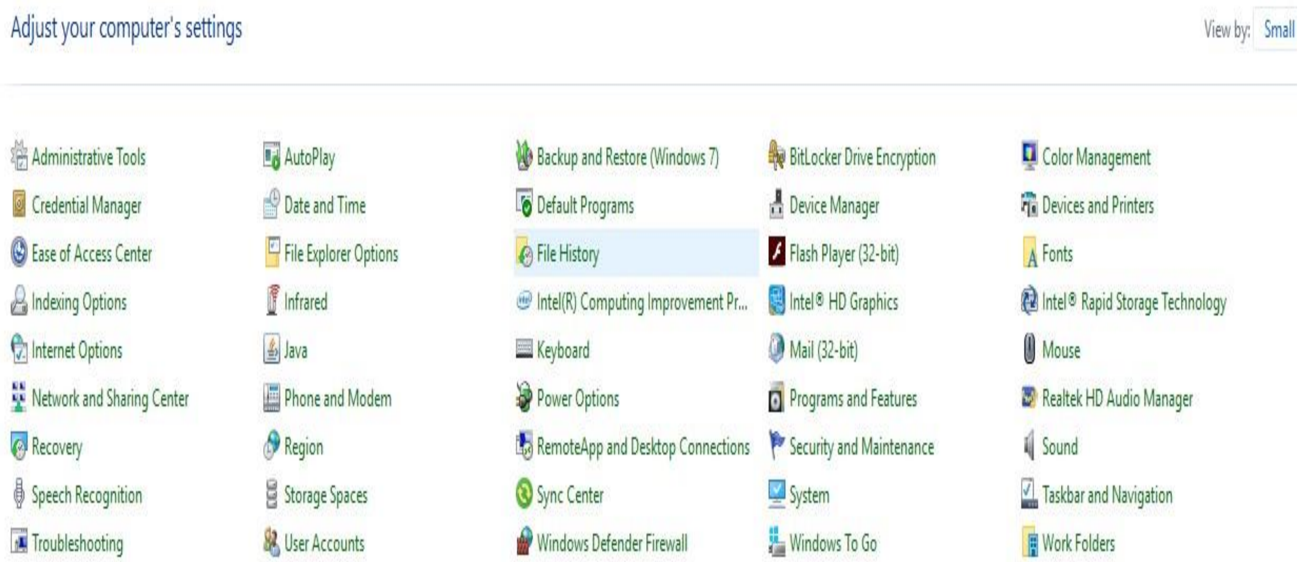
জবের নাম ঃ একটি কম্পিউটার সিস্টেমে ফায়ারওয়াল ইনস্টল করা এবং অনুপ্রবেশকারী থেকে কম্পিউটার সিস্টেমকে প্রতিরোধ করা।

উদ্দেশ্য ঃ কম্পিউটার সিস্টেমে অনুপ্রবেশকারী থেকে কম্পিউটার সিস্টেমকে নিরাপদ রাখার জন্য ফায়ারওয়াল ইনস্টল করা।

যন্ত্রপাতি ঃ কম্পিউটার সিস্টেম।

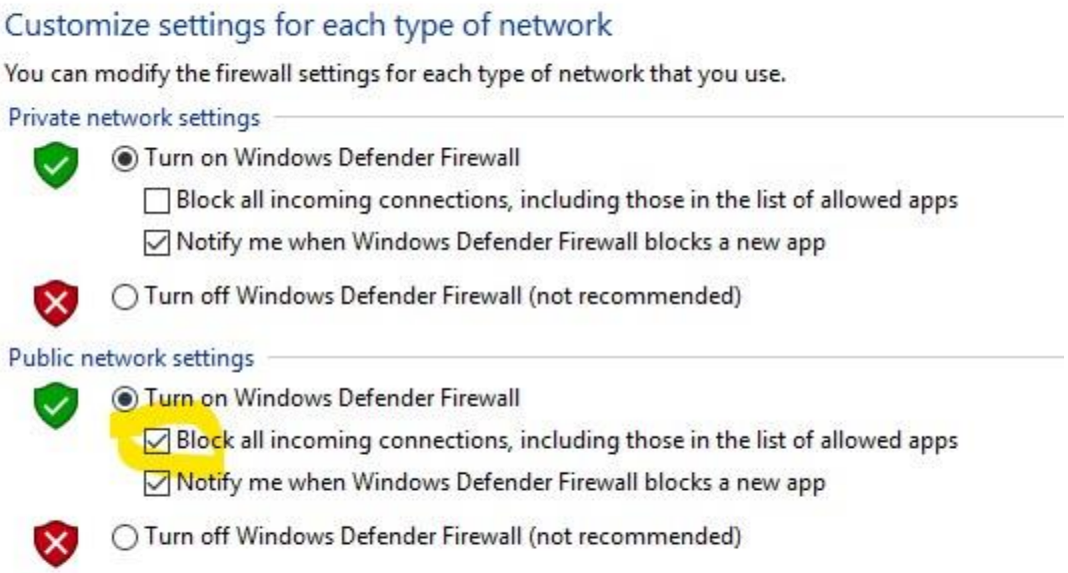
বর্ণনা ঃ নিম্নে একটি কম্পিউটার সিস্টেমে ফায়ারওয়াল ইনস্টল করা এবং অনুপ্রবেশকারী থেকে কম্পিউটার সিস্টেমকে প্রতিরোধ করার পদ্ধতি বর্ণনা করা হলো ঃ-

- **কম্পিউটার চালু করা ঃ** কম্পিউটার সিস্টেমে ফায়ারওয়াল ইনস্টল করার জন্য প্রথমে কম্পিউটারটি চালু করতে হবে।
- **কন্টোল প্যানেল থেকে উইন্ডোজ ফায়ারওয়াল দিয়ে পিসিকে সুরক্ষা প্রদান ঃ** কম্পিউটার চালু করার পর কম্পিউটার সিস্টেমে ফায়ারওয়াল চালু করার জন্য প্রথমে কম্পিউটারের কন্টোল প্যানেল যেতে হবে।



তারপর ধাপে ধাপে নিম্নের চিত্রের মতো ফায়ারওয়াল চালু/বন্ধ করতে হবে।

" ON/OFF" অপশনে ক্লিক করে ফায়ারওয়াল চালু কিংবা বন্ধ করতে হবে। সাথে " BLOCK"অপশনে ক্লিক করে বিভিন্ন ইননকামিং ব্লক করেও রাখা যায়।



মন্তব্য ঃ এই অধ্যায়ে আমরা শিখলাম কীভাবে একটি কম্পিউটার সিস্টেমে ফায়ারওয়াল চালু কিংবা বন্ধ করা যায় এবং নিরাপত্তা বৃদ্ধি করা যায়।

------------o-----------

জব নং ঃ ০৭

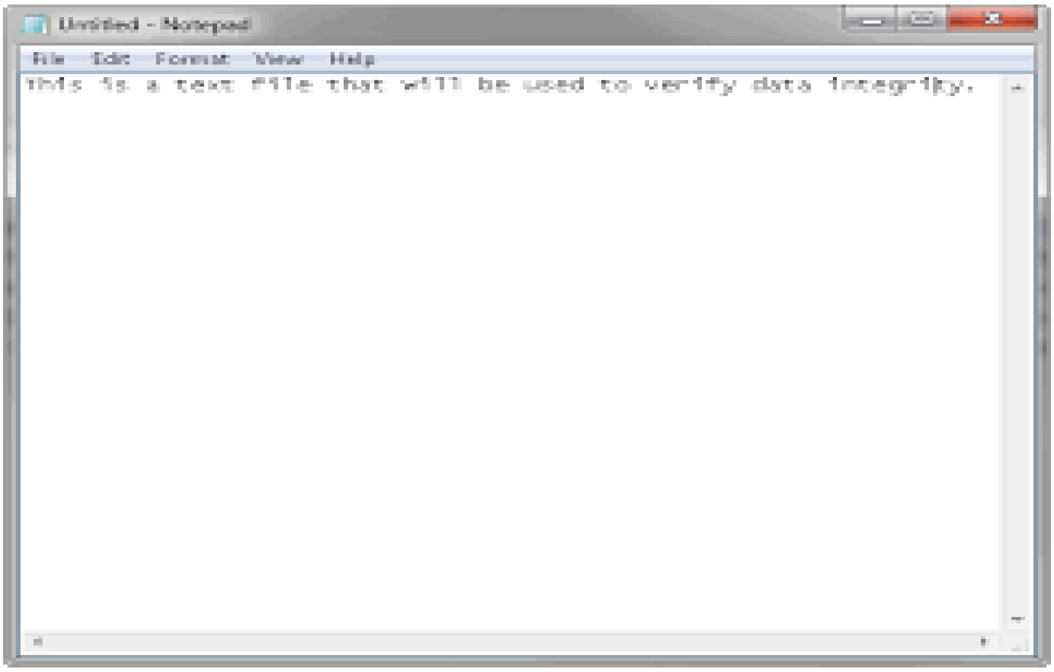
জবের নাম ঃ Hashcalc প্রোগ্রামের মাধ্যমে ডাটা অখন্ডতা যাচাই করার জন্য একটি হ্যাসিং প্রোগ্রাম ব্যবহার করা।

উদ্দেশ্য ঃ ডাটা অখন্ডতা যাচাই করার জন্য একটি হ্যাসিং প্রোগ্রাম ব্যবহার করা।

যন্তপাতি ঃ কম্পিউটার সিস্টেম,হ্যাশিং প্রোগ্রাম।

বর্ণনা ঃ নিম্নে একটি কম্পিউটার সিস্টেমে Hashcalc প্রোগ্রামের মাধ্যমে ডাটা অখন্ডতা যাচাই করার জন্য একটি হ্যাসিং প্রোগ্রাম ব্যবহার করার পদ্ধতি বণৃনা করা হল ঃ-

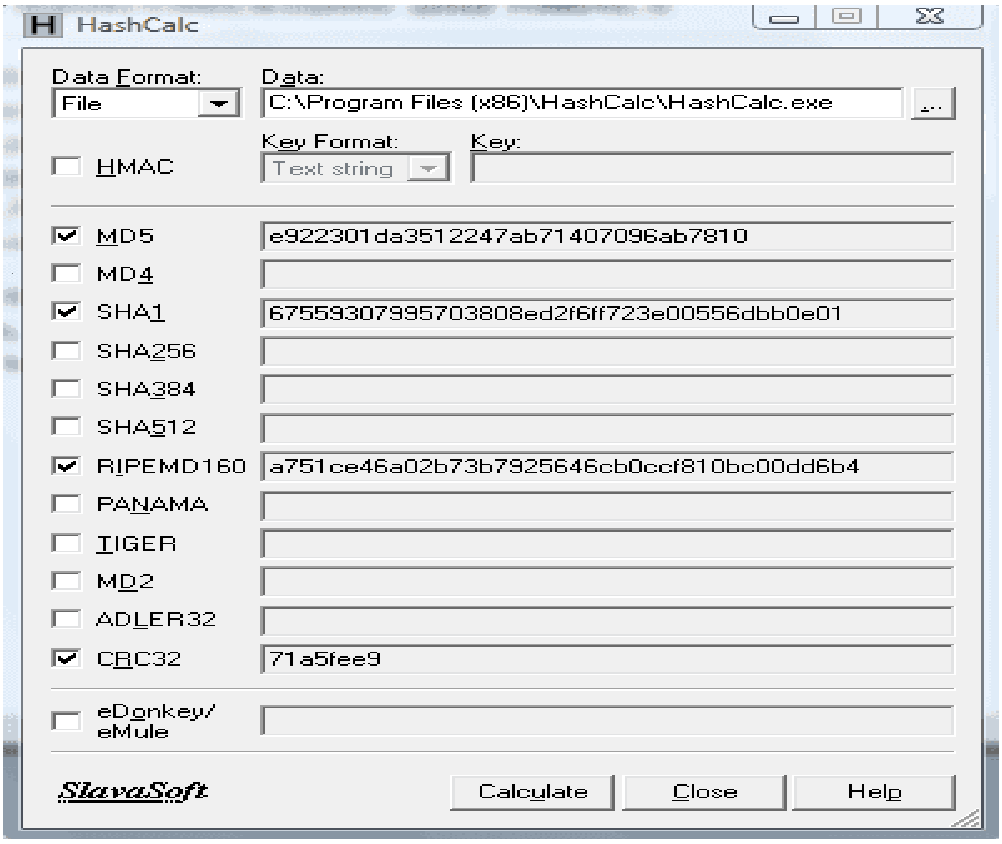
- ❖ **কম্পিউটার চালু করা ঃ** ডাটা অখন্ডতা যাচাই করার জন্য প্রথমে কম্পিউটারটি চালু করতে হবে।
- ❖ **একটি টেক্সট ফাইল তৈরী করা ঃ** একটি টেক্সট ফাইল তৈরী করার জন্য প্রথমে কম্পিউটার নোটপ্যাড ওপেন করতে হবে।তারপর সেখানে কিছু লিখে সেটি ডেস্কটপে সেইভ করতে হবে। সেইভ করার সময় এক্সটেনশন অবশ্যই .txt হতে হবে।



❖ **ওয়েবসাইট থেকে Hashcalc ডাউনলোড করে ইনস্টল করা ঃ** Hashcalc ডাউনলোড করার জন্য https://softradar.com/hashcalc/ লিংকে প্রবেশ করতে হবে ঃ-

ডাউনলোড হবার পর সফটওয়্যারটি ইনস্টল করতে হবে।

ইনস্টল করার পর সফটওয়্যারটি ইনস্টল নিম্নের চিত্রের ন্যায় হবে ঃ



- **Hash.txt ফাইলের হ্যাশ গণনা করা ঃ**
  Data Format: File
  Data: Click the…button next to the data filed, navigate to the desktop the choose the Hash.txt file.
  Uncheck HMAC
  Uncheck all hash types except MD5

- **Hash.txt ফাইলটিতে পরিবর্তন করা ঃ** ডেক্সটপ সেভ করা Hash.txt ফাইলটি ওপেন করে সেখানে কোনো পরিবর্তন করতে হবে।

- **Hash.txt ফাইলের নতুন হ্যাস গণনা করা ঃ** পুনরায় অপশনে ক্লিক করতে হবে। তাহলে পরিবর্তন হলে সেটি বুঝা যাবে।

মন্তব্য ঃ এই অধ্যায়ে আমরা শিখলাম কীভাবে Hashcalc প্রোগ্রামের মাধ্যমে ডাটা অখন্ডতা যাচাই করা যায়।

জব নং ঃ ০৮

জবের নাম ঃ WinZip ব্যবহার করে ই-মেইলের মাধ্যমে গোপনীয় তথ্য পাঠানো।

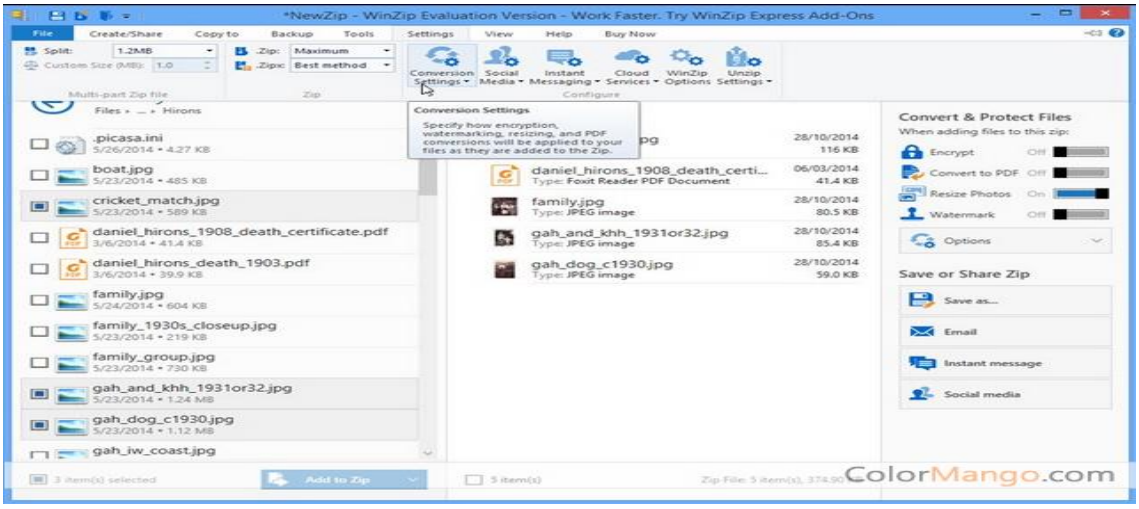
উদ্দেশ্য ঃ WinZip ব্যবহার করে ই-মেইলের মাধ্যমে গোপনীয় তথ্য পাঠানো এ জবের মূল উদ্দেশ্য।

যন্তপাতি ঃ কম্পিউটার সিস্টেম, WinZip সফটওয়্যার।

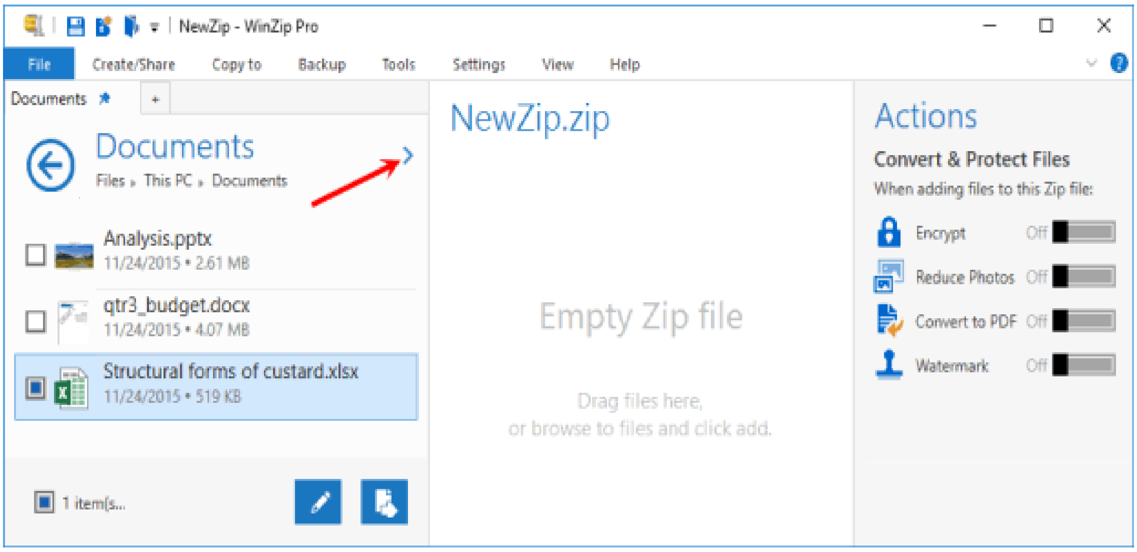
বর্ণনা ঃ নিম্নে WinZip ব্যবহার করে ই-মেইলের মাধ্যমে গোপনীয় তথ্য পাঠানোর পদ্ধতি বর্ণনা করা হল ঃ

- ❖ **কম্পিউটার চালু করা ঃ** প্রথমে কম্পিউটারটি চালু করতে হবে।

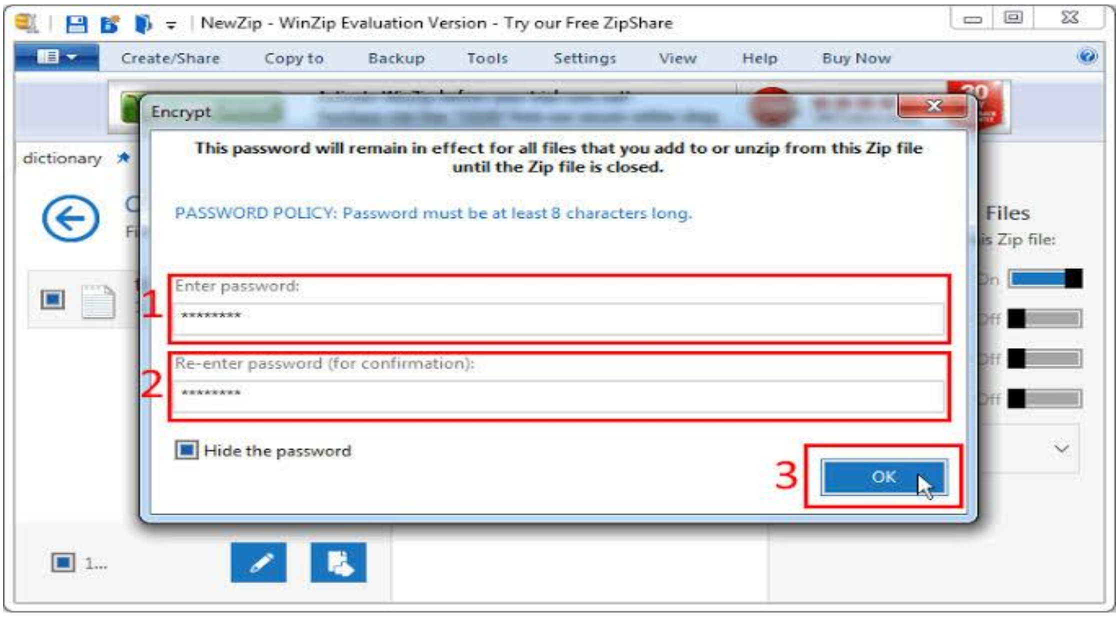
- ❖ **Confidential Document.docx নামের একটি এমএস ওয়ার্ড ফাইল তৈরী করা এবং WinZip দ্বারা একটি শক্তিশালী পাসওয়ার্ড দিয়ে ফাইলটি এনক্রিপ্ট করা ঃ** কম্পিউটারটি চালু করার পর এমএস ওয়ার্ড চালু করতে হবে। এমএস ওয়ার্ড চালু করার পর সেখানে থেকে ফাইলটি Confidential Document.docx নামে ডেস্কটপ-এ সেইভ করতে হবে। তারপর WinZip সফটওয়্যারটি ইনস্টল করে ওপেন করতে হবে।ওপেন করার পর ডান দিকে "Encrypt" অপশনটি চালু করতে হবে।



তারপর নিম্নের চিত্রের মতো ফাইলটি WinZip সফটওয়্যার ড্রাগ অ্যান্ড ড্রপ করতে হবে।



তারপর Encrypt পাসওয়ার্ড দিত হবে।



❖ **বন্ধুর কাছে এনক্রিপ্ট করা ফাইলটি ই-মেইল করা ঃ** জি-মেইল লগইন করে এনক্রিপ্ট করা ফাইলটি ই-মেইল করতে হবে এবং এনক্রিপ্ট পাসওয়ার্ড বলে দিতে হবে।

❖ **ফাইলটি পাসওয়ার্ড দ্বরা ওপেন ঃ** সকশেষে WinZip সফটওয়্যারের মাধ্যমে পুনরায় এমএস ফাইলটি পাসওয়ার্ড ব্যবহার করে ওপেন করতে হবে।

মন্তব্য ঃ এই অধ্যায়ে আমরা শিখলাম কীভাবে WinZip ব্যবহার করে ই-মেইলের মাধ্যমে গোপনীয় তথ্য পাঠানো যায়।

----------------------o----------------------