Cyber awareness

SAIFUL ISLAM

ISLAMIC CYBER SECURITY

সাইবার সিকিউরিটি এবং এর গুরুত্ব

সাইবার সিকিউরিটি কি?

সাইবার সিকিউরিটি হলো প্রযুক্তির গুরুত্বপুর্ন এক অংশ যা নেটওয়ার্ক, ডিভাইস, প্রোগ্রাম, এবং ডাটা কে সুরক্ষা প্রদান, এবং অনাকাঙ্খিত প্রবেশ/এক্সেস থেকে বিরত রাখার জন্য তৈরী করা হয়েছে

সাইবার সিকিউরিটির গুরুত্ব

সাইবার সুরক্ষা গুরুত্বপূর্ণ কারণ সরকার, সামরিক, কর্পোরেট, অর্র্থিক, এবং চিকিত্সা সংস্থা কম্পিউটার এবং অন্যান্য ডিভাইসে অভূতপূর্ব পরিমাণে ডেটা সংগ্রহ, প্রক্রিয়াজাতকরণ এবং সঞ্চয় করে। সেই ডেটার একটি উল্লেখযোগ্য অংশ সংবেদনশীল, আর্থিক তথ্য, ব্যক্তিগত তথ্য বা অন্যান্য ধরণের ডেটা হতে পারে, যার অননুমোদিত অ্যাক্সেস বা প্রকাশ বিরূপ প্রভাব ফেলতে পারে। বিভিন্ন সংস্থা ব্যবসা করার সময় নেটওয়ার্ক এবং অন্যান্য ডিভাইসে সংবেদনশীল ডেটা প্রেরণ করে যেখানে সাইবার সিকিউরিটি সেই তথ্য এবং এটি প্রক্রিয়া করতে বা সঞ্চয় করতে ব্যবহৃত সিস্টেমগুলি সুরক্ষিত করার জন্য শৃঙ্খলা বর্ণনা করে। মার্চ ২০১৩ এর প্রথমদিকে, শীর্ষ গোয়েন্দা কর্মকর্তারা সতর্ক করে দিয়েছিলেন যে

সাইবার আক্রমণ এবং ডিজিটাল গুপ্তচরবৃত্তি জাতীয় সুরক্ষার পক্ষে শীর্ষ হুমকি, এমনকি সন্ত্রাসবাদকেও গ্রহন করে।

সাইবার সিকিউরিটির অন্তর্ভুক্ত বিষয় সমূহ

নেটওয়ার্ক সুরক্ষা

অ্যাপ্লিকেশন সুরক্ষা

এন্ড-পয়েন্ট সুরক্ষা

তথ্য নিরাপত্তা

পরিচয় ব্যবস্থাপনা

ডাটাবেস এবং এর অবকাঠামো সুরক্ষা

ক্লাউড নিরাপত্তা

মুঠো ফোন নিরাপত্তা

যেকোনো বিপর্যয় পুনরুদ্ধার / ব্যবসায় ধারাবাহিকতা পরিকল্পনা

ব্যাবহারকারী সচেতনতা

সাইবার অপরাধের ভয়ঙ্কর গতিপ্রবাহ

এটি সর্বজনবিদিত যে, বিশ্বায়নের কথিত উন্নয়ন পরিমন্ডলে দৃশ্যমান অবকাঠামো ও জীবিকার কৌশল অবলম্বন অনেক ক্ষেত্রে ইতিবাচক পরিবর্তন সাধন করলেও টেকসই জীবনমান প্রতিষ্ঠায় এর প্রভাব কতটুকু অর্থবহ তা গভীর বিশ্লেষণের দাবি রাখে। সংস্কৃতির অসম অগ্রগতির দোলাচলে বস্তুগত সংস্কৃতির পর্যাপ্ত প্রসারমানতায় অবস্তুগত সংস্কৃতি তথা
ঐতিহ্য-কৃষ্টি-মূল্যবোধ-সততা-নৈতিকতা-মানবিকতা ইত্যাদির পরিপুষ্টতা অর্জনে পুরোবিশ্ব যে পিছিয়ে পড়ছে তা বলার অপেক্ষা রাখে না। নিত্যনতুন শোষণ-শাসন প্রক্রিয়া, বৈষম্যের দুর্ভেদ্য প্রাচীর, ধনী-দরিদ্র রাষ্ট্রসমূহের মধ্যে অনধিকার ক্ষমতার প্রয়োগ-বিধিনিষেধের বিভাজন সর্বত্রই উপনিবেশ-সাম্রাজ্যবাদী চরিত্রের অনাকাক্সিক্ষত রূপ পরিগ্রহ করে চলছে। রাষ্ট্র-জনগোষ্ঠীর মধ্যে নানামুখী দূরত্ব কমিয়ে ধরিত্রীকে ছোট-কাছাকাছি নিয়ে আসার পরিকল্পনা যেন ভেস্তে যেতে বসছে। পক্ষান্তরে তথ্যপ্রযুক্তির অপ্রতিরোধ্য অগ্রগতি সামাজিক সুফল ভোগের পরিবর্তে কুফলের হীন অভিপ্রায়ে হচ্ছে পর্যুদস্ত। যথার্থ সতর্কতা ও সংশ্লিষ্ট কর্তৃপক্ষের কার্যকর প্রতিক্রিয়া প্রকৃত অর্থে গুরুত্ব না পেলে বাংলাদেশসহ বিশ্বের ভবিষ্যত অন্ধকারের তলানীতে গিয়ে পৌঁছবে নিঃসন্দেহে তা বলা যায়। বিরাজিত অগ্রগণ্য সঙ্কট হিসেবে সাইবার অপরাধ বা বিপুল

প্রচলিত সাইবার ক্রাইম দ্রুততম সময়ের মধ্যে দুঃসহ পরিবেশ নির্মাণে প্রচ- শক্তিমান। ইন্টারনেটের মাধ্যমে তথ্য চুরি-বিকৃতি, মানি লন্ডারিং, জালিয়াতি, ব্ল্যাকমেল ইত্যাদি কর্মকা-কে সাধারণত সাইবার অপরাধ হিসেবে গণ্য করা হয়। মূলত ইন্টারনেটের মাধ্যমে সংঘটিত সকল ধরনের অপরাধই সাইবার অপরাধের অন্তর্ভুক্ত। সাইবার অপরাধের একেবারে প্রথম পর্যায়ে রয়েছে হ্যাকিং। কম্পিউটার, মোবাইল বা অন্য যে কোন ইলেকট্রনিকস ডিভাইস, সোশ্যাল এ্যাকাউন্ট, বিভিন্ন গুরুত্বপূর্ণ ওয়েবসাইট বা ই-কমার্স ওয়েবসাইটের তথ্য বা ক্রেডিট কার্ডের নম্বর হ্যাকিংয়ের মাধ্যমে প্রতিনিয়ত ব্যাপক ক্ষতির সম্মুখীন হচ্ছে। বিভিন্ন পর্নোসাইটে ভিজিটকারী ব্যক্তির ডিভাইস ক্ষতিকর কম্পিউটার ভাইরাস দিয়ে যে কোন সময় হ্যাকাররা হ্যাক করে ফেলে। মাদক থেকে শুরু করে নারী-শিশু পাচার সবই এখন ইন্টারনেট প্রক্রিয়ায় সংঘটিত হচ্ছে। বিশ্বব্যাপী মাদক ব্যবসায়ীরা অতি গোপনে ওয়েবসাইটের মাধ্যমে মাদকদ্রব্যের ক্রয়-বিক্রয় করে যাচ্ছে। বর্তমানে সাইবার অপরাধের অন্যতম বৃহৎ অনুষঙ্গ হচ্ছে নারী নির্যাতন। মেয়েদের সোশ্যাল মিডিয়া এ্যাকাউন্ট হ্যাক করে ব্যক্তিগত তথ্য-যৌন দৃশ্য প্রকাশের হুমকি বা মেয়েদের ছবি ব্যবহার করে ভুয়া আইডি খোলার মতো সাইবার অপরাধ এখন নিত্যনৈমিত্তিক বিষয়ে পরিণত হয়েছে। এছাড়াও প্রযুক্তির অপব্যহারে আর্টিফিশিয়াল ইন্টেলিজেন্স দিয়ে মেয়েদের ফেস ব্যবহার করে কৃত্রিম যৌন দৃশ্য তৈরি করে ইন্টারনেটে প্রকাশের ফলে লাখ লাখ মেয়ে ক্ষতির সম্মুখীন হওয়ার

পাশাপাশি অনেকেই আত্মহননে উদ্বুদ্ধ হচ্ছে। অনেক ক্ষেত্রে হ্যাকাররা ফোন কল-মেসেজ বা ইমেলের মাধ্যমে আর্থিক লেনদেনের প্ল্যাটফর্ম বা বিভিন্ন কোম্পানি থেকে লক্ষ লক্ষ টাকার লটারীর লোভ দেখিয়ে মানুষকে বোকা বানিয়ে বিশাল অর্থ হাতিয়ে নিচ্ছে। অদক্ষ ইন্টারনেট ব্যবহারকারীরাই সচরাচর সাইবার অপরাধের শিকারে বিপর্যস্ত। প্রতিবছর সারাবিশ্বে সাইবার অপরাধের জন্য শত শত কোটি ডলার ক্ষতি হচ্ছে। কম্পিউটার ইকোনমিক্স জরিপ ২০০৬ অনুযায়ী সারাবিশ্ব ভাইরাসের কারণে ১৩ দশমিক ৩ বিলিয়ন ডলার ক্ষতিগ্রস্ত হয়েছিল। ১৮ জুন ২০২১ প্রকাশিত সাইবার ক্রাইম এ্যাওয়ারনেস ফাউন্ডেশনের প্রতিবেদন সূত্রে জানা যায়, সামাজিক যোগাযোগ মাধ্যম দেশে সংঘটিত সাইবার অপরাধের আখড়ায় পরিণত হয়েছে। এতে সবচেয়ে বেশি আক্রান্ত হচ্ছে ১৮ থেকে ৩০ বছর বয়সী মেয়েরা। ভুক্তভোগীদের মধ্যে ১৮ বছরের কম ১০ দশমিক ৫২ শতাংশ, ১৮ থেকে ৩০ বছরের কম ৭৩ দশমিক ৭১ শতাংশ, ৩০ থেকে ৪৫ বছর ১২ দশমিক ৭৭ শতাংশ এবং ৪৫ বছরের বেশি ৩ শতাংশ। লিঙ্গভিত্তিক পরিসংখ্যানে দেশে সাইবার অপরাধের শিকার ভুক্তভোগীদের ৫১ দশমিক ১৩ শতাংশ নারী এবং ৪৮ দশমিক ৮৭ শতাংশ পুরুষ। অপরাধের ধরন ব্যাখ্যায় প্রতিবেদনে বলা হয়েছে, এ্যাকাউন্ট জাল ও হ্যাক করে তথ্য চুরির মাধ্যমে অনলাইনে সবচেয়ে বেশি অনিরাপদ বাংলাদেশের নারীরা। গড়ে অনলাইনে সামাজিক যোগাযোগ মাধ্যমে ভুয়া এ্যাকাউন্টে অপপ্রচারের শিকার হওয়া ১৪ দশমিক ২৯ শতাংশ

নারীর বিপরীতে পুরুষের সংখ্যা ১২ দশমিক ৭৮ শতাংশ। সামাজিক যোগাযোগ মাধ্যমের আইডি হ্যাকিং/তথ্য চুরির ঘটনা নারী-পুরুষের অনুপাতে পুরুষের অবস্থান দ্বিগুণেরও বেশি। অপরাধের ধরনে তৃতীয় অবস্থানে থাকা ছবি বিকৃতির মাধ্যমে অনলাইনে অপপ্রচারে নারী ও পুরুষের হার যথাক্রমে ১২ দশমিক ০৩ শতাংশ ও ৩ দশমিক ৭৬ শতাংশ। অনলাইনে হুমকিমূলক বার্তা প্রাপ্তির হার নারী ৯ দশমিক ৭৭ শতাংশ এবং পুরুষ ৩ দশমিক ৭৬ শতাংশ। উল্লেখ্য, প্রতিবেদনে আরও বলা হয়েছে, ভুক্তভোগীদের ৩০ শতাংশই জানেন না এর বিরুদ্ধে কিভাবে আইনী ব্যবস্থা গ্রহণ করতে হয় আর বাকিদের মধ্যে ২৫ শতাংশ অভিযোগ করে কোন লাভ হবে না ভেবে আইনশৃঙ্খলা রক্ষাকারী বাহিনীর নিকট অভিযোগ করেন না। ৫ ডিসেম্বর ২০২১ গণমাধ্যম সূত্র অনুযায়ী সাইবার অপরাধের মাত্রা বেড়ে যাওয়ায় ঢাকা মহানগর পুলিশের ৫০টি থানায় পৃথক সাইবার বিভাগ চালু করা হচ্ছে। সম্প্রতি ঢাকা রেঞ্জের প্রতিটি জেলায় এমন উদ্যোগ নেয়া হয়েছে। পুলিশ সদর দফতরের সূত্রমতে শীঘ্রই দেশের সব থানাতে সাইবার অপরাধের জন্য আলাদা বিট গঠন করা হবে। সাইবার অপরাধ নিয়ে উদ্বেগ প্রকাশ করে পুলিশের মহাপরিদর্শক বলেন, গ্রাম পর্যায়েও প্রযুক্তির ছোঁয়া লাগার কারণে সাইবারকেন্দ্রিক অপরাধের মাত্রা দিনকে দিন বেড়েই চলেছে। এজন্য সাইবার নিরাপত্তার বিষয়টি নতুন করে ভাবা হচ্ছে। দেশের সব থানায় সাইবার সংক্রান্ত অপরাধের বিষয়ে মামলা হচ্ছে। এসব মামলার তদন্ত দ্রুত করতে

প্রতিটি থানায় পর্যায়ক্রমে সাইবার বিভাগ চালু করা হবে। অনেকেই প্রযুক্তির কারণে সাইবার অপরাধের শিকার হচ্ছেন। শুধু ব্যক্তি বা সমাজ নয়, রাষ্ট্রও এর বাইরে নয়। গত এক বছরে সামাজিক যোগাযোগ মাধ্যম ব্যবহার করে হয়রানিতে পর্যবসিত হয়েছেন ১৭ হাজারের বেশি নারী। সাইবার অপরাধ বিশেষজ্ঞদের মতে সাইবার অপরাধ নিয়ে গভীরভাবে ভাবার সময় এসেছে। সাইবার অপরাধ সমাধানের জন্য সংশ্লিষ্টদের সক্ষমতা বাড়ানোর কোন বিকল্প নেই। অপরাধ মোকাবেলার সঙ্গে যুগোপযোগী প্রশিক্ষণের ব্যবস্থা করতে হবে। একই সঙ্গে প্রয়োজন সাধারণ মানুষকে সচেতন করার জন্য দেশব্যাপী ইতিবাচক প্রচারণা। ৩ জানুয়ারি ২০২১ ৩৭তম বিসিএস (পুলিশ) ক্যাডারের শিক্ষানবিস সহকারী পুলিশ সুপারদের প্রশিক্ষণ সমাপনী অনুষ্ঠানে দেশের সাইবার অপরাধ দমনে সংশ্লিষ্টদের নির্দেশনা দিয়ে প্রধানমন্ত্রী জননেত্রী শেখ হাসিনা বলেন, 'এখন আধুনিক প্রযুক্তির যুগ। সাইবার ক্রাইম ব্যাপকভাবে বাড়ছে। এটাকে আমাদের দমন করতে হবে। ৯৯৯ নম্বরে ফোন করলে পুলিশ তাৎক্ষণিকভাবে সাহায্য করে যাচ্ছে এবং মানুষের কাছে পৌঁছে যাচ্ছে। প্রযুক্তি ব্যবহারের মাধ্যমে নানা ধরনের অপরাধ সংঘটিত হয়। সেগুলো আমাদের দমন করতে হবে। আরেকটা বিষয় হচ্ছে ফেসবুক, বিভিন্ন ধরনের এ্যাপস দিয়ে সেগুলোর মাধ্যমে অনেক অপরাধ হচ্ছে। বিশেষ করে কিশোর বা উঠতি বয়সের ছেলেমেয়েরা এ ধরনের অপরাধের সঙ্গে জড়িত হচ্ছে। সেখান থেকে তাদের বের করে নিয়ে এসে সুস্থ জীবনে ফিরে আনার ব্যবস্থা নিতে হবে।

সাধারণভাবে গুজব রটানো বা এ ধরনের কাজ যাতে করতে না পারে সেদিকে সজাগ দৃষ্টি দিতে হবে।' ২২ সেপ্টেম্বর ২০২১ গণমাধ্যমে প্রাপ্ত তথ্য অনুসারে ঢাকা সাইবার ট্রাইব্যুনালের দৈনন্দিন কার্যতালিকাসহ মামলার সংশ্লিষ্ট কাগজপত্র পর্যালোচনা করে দেখা যায়, ২০১৩ সাল থেকে ২০২০ সালের সেপ্টেম্বর পর্যন্ত এ ট্রাইব্যুনালে বিচারের জন্য মামলা এসেছে ২ হাজার ৬৬৯টি, যার মধ্যে হ্যাকিং, কম্পিউটার সিস্টেম নষ্ট, কম্পিউটার সোর্স কোড পরিবর্তন, সংরক্ষিত সিস্টেমে প্রবেশ সংক্রান্ত মামলার সংখ্যা মাত্র ১১৩। যা মোট মামলার ৪ দশমিক ২৩ শতাংশ। ট্রাইব্যুনালের সরকারী কৌঁসুলি গণমাধ্যমকে জানান, সাইবার অপরাধের মামলা বেশি হচ্ছে মূলত অনলাইনে মানহানি, মিথ্যা তথ্য, অশ্লীল ছবি ও তথ্য প্রকাশের অভিযোগে। সে তুলনায় হ্যাকিংসহ অন্য গুরুতর অপরাধের মামলা কম এবং সাজাও নগণ্য। তথ্য-যোগাযোগ প্রযুক্তি ও সাইবার অপরাধ বিশেষজ্ঞদের মতে
ফেসবুক-ইমো-লাইকি-টিকটকের মতো সামাজিক গোযাযোগ মাধ্যমের ওয়েবসাইট ও এ্যাপস ব্যবহারকারীর এ্যাকাউন্ট হ্যাকড বেশি হচ্ছে। এসব ঘটনায় করা মামলার আসামিরা বয়সেও তরুণ। পিবিআইয়ের ফরেনসিক বিভাগের প্রধান গণমাধ্যমকে জানান, হ্যাকিংয়ের মামলা বিশ্লেষণে দেখা যাচ্ছে কম বয়সী ছেলেরা ফেসবুক-ইমো-লাইকি ব্যবহারকারীর এ্যাকাউন্ট হ্যাকিংয়ের সঙ্গে জড়িত। আর একাধিক সংঘবদ্ধ চক্র বিকাশ-নগদ-রকেটের মতো আর্থিক সেবাদানকারী প্রতিষ্ঠানের গ্রাহকের এ্যাকাউন্ট এবং এটিএম

বুথ হ্যাকিংয়ে জড়িত। তিনি আরও বলেন, অভিযুক্ত ব্যক্তিদের মূল কাজ হচ্ছে ব্ল্যাকমেল করা এবং অর্থ হাতিয়ে নেয়া। নিকট অতীতে প্রকাশিত গণমাধ্যম তথ্যে উল্লেখযোগ্য সংখ্যক সাইবার অপরাধ সম্পর্কে জানা যায়। অপরাধগুলোর মধ্যে রয়েছে- শিক্ষা বোর্ডের ওয়েবসাইটে তথ্য জালিয়াতি করে জাল সনদ তৈরি, ব্ল্যাকমেল করে ধর্ষণ এবং এর ভিডিও সামাজিক যোগাযোগ মাধ্যমে ছড়িয়ে দেয়া, ফেসবুক-হোয়াটসঅ্যাপ-মেসেঞ্জার-ইনস্টাগ্রাম-স্কাইপে ভুয়া আইডি খুলে জালিয়াতি ও প্রতারণা, বিভিন্ন অনলাইন পোর্টালে মিথ্যা ও মানহানিকর তথ্য প্রচার, আইডি হ্যাক, ডেবিট-ক্রেডিট কার্ড জালিয়াতি-প্রতারণা, অনলাইনে প্রশ্ন ফাঁস ও জুয়া খেলা ইত্যাদি। আইন করাসহ নানা পদক্ষেপে এমন অপরাধ না কমার পরিবর্তে দিন দিন ভয়ানকরূপ ধারণ করছে। সাইবার সংশ্লিষ্ট সূত্রে জানা যায়, পুলিশের বিভিন্ন ইউনিট, বাংলাদেশ টেলিযোগাযোগ নিয়ন্ত্রণ কমিশন (বিটিআরসি), তথ্য ও যোগাযোগ প্রযুক্তি (আইসিটি) বিভাগের হেল্প ডেস্ক ও ন্যাশনাল টেলিকমিউনিকেশন মনিটরিং সেন্টারে (এনটিএমসি) সাইবার অপরাধ নিয়ে প্রতিদিনই অভিযোগ জমা পড়ছে। ইতোমধ্যে আইজিপি নামে, মন্ত্রীর সহকারী একান্ত সচিব পরিচয়ে প্রতারণা, নারী পুলিশের আপত্তিকর ছবি ছড়ানো, পাত্রী চাই বিজ্ঞাপন দিয়ে প্রতারণা, গৃহবধূকে সংঘবদ্ধ ধর্ষণ করে ভিডিও ছড়িয়ে দেয়া, অনলাইনে জঙ্গীবাদ প্রচার ও জাতীয় সঙ্গীত অবমাননার মতো সাইবার অপরাধের ঘটনায় অনেক অপরাধী গ্রেফতার হয়েছে। ডিএমপি সাইবার সংশ্লিষ্ট তথ্যমতে ডিজিটাল

সিকিউরিটি এ্যাক্ট, পর্নোগ্রাফি আইন, আইসিটি আইন ও টেলিকমিউনিকেশন আইনে সারাদেশে ২০১৫ সালের ৬৩৮টি মামলার বিপরীতে ২০২০ সালে এই সংখ্যা দাঁড়ায় ১৪৫৯টিতে। অধিকাংশ ক্ষেত্রে ভুক্তভোগীরা হয়রানি ও সম্মানের কথা ভেবে এসব বিষয়ে আইনশৃঙ্খলা রক্ষাকারী বাহিনীর কাছে অভিযোগ করে না। সাইবার অপরাধ দমনে সরকার জোরালোভাবে কার্যক্রম শুরু করলেও বিচার ও শাস্তির হার খুবই নগণ্য। এছাড়া স্বচ্ছ ধারণা না থাকা ও প্রতিকার পেতে সময়ক্ষেপণ হওয়ায় আইনের আশ্রয় নিতে অনীহা বেশি। অনেকেই অনলাইনকেন্দ্রিক অপরাধমূলক কর্মকা-প্রতিরোধে বিভিন্ন এ্যাপস বন্ধের প্রয়োজনীয়তার কথা বললেও প্রযুক্তিবিদদের মতে এ্যাপস বন্ধ করা যেমন কঠিন, তেমনি সেগুলো বন্ধ করেও লাভ নেই। তারা সাইবার অপরাধ দমনে পুলিশের সক্ষমতা বাড়ানো এবং প্যারেন্টাল গাইডেন্সের ওপর জোর দেন। ৬ সেপ্টেম্বর ২০২১ সংবাদ সম্মেলনে বিটিআরসির সক্ষমতা তুলে ধরে ডাক ও টেলিযোগাযোগমন্ত্রী বলেন, 'বিটিআরসি শুধু ইউটিউব, ফেসবুকের কোন কনটেন্ট সরানোর অনুরোধ করতে পারে। সেই কনটেন্ট তাদের কমিউনিটি স্ট্যান্ডার্ড পরিপন্থী হলে ফেসবুক কর্তৃপক্ষ তা অপসারণ করে, নয়ত করে না। আইনশৃঙ্খলা রক্ষা বাহিনী বা সরকারের পক্ষে ইন্টারনেট জগতে কোন কিছুর পুরোপুরি নিয়ন্ত্রণ সম্ভব নয়।' এর পূর্বেও অপর সভায় তিনি বলেছিলেন, ডিজিটাল নিরাপত্তা আইন ২০১৮ সালে প্রণয়ন করা হলেও কিছু সীমাবদ্ধতার কারণে ২০২১ সালে এসেও আইনটি অপরাধ দমনে

বিস্তৃত ভূমিকা রাখছে না। আইনের অপপ্রয়োগ মূল সমস্যা হয়ে দাঁড়িয়েছে। এই অবস্থায় আইনের প্রয়োজনীয় সংশোধন করা সম্ভব। সচেতন মহলের ধারণা, উল্লেখ্য তথ্য-উপাত্তের ভিত্তিতে প্রায়োগিক কর্মকৌশল নির্ধারণ ও বাস্তবায়নে ন্যূনতম অবজ্ঞা অদূর ভবিষ্যতে সাইবার অপরাধের গতিপ্রবাহ করোনা অতিমারীর চেয়েও ভয়ঙ্কররূপে আবির্ভূত হওয়ার সমূহ আশঙ্কা রয়েছে।

ড. ইফতেখার উদ্দিন চৌধুরী

লেখক : শিক্ষাবিদ, সাবেক উপাচার্য চট্টগ্রাম বিশ্ববিদ্যালয়

সাইবার অপরাধ

সাইবার অপরাধ ও সাইবার নিরাপত্তা বর্তমান বিশ্বে সর্বাধিক আলোচিত বিষয়। 'উইকিলিকস'-এর প্রতিষ্ঠাতা জুলিয়ান অ্যাসাঞ্জ ও 'সিআইএ'-র তথ্য ফাঁসকারী এডওয়ার্ড স্নোডেনের কল্যাণে বিষয়টি এজেন্ডা হিসেবে বিশ্বরাজনৈতিক পরিমণ্ডলে চলে আসে। তাছাড়া 'পানামা পেপার্স' কেলেংকারি ও 'বাংলাদেশ ব্যাংকের রিজার্ভ চুরি' এতে নতুন মাত্রা যোগ করে। ১২ মে ২০১৭ বিশ্বের ১৫০টি দেশে একযোগে 'র‍্যানসমওয়্যার' দিয়ে ভয়াবহ সাইবার হামলা প্রযুক্তিপ্রেমীদের চরম আতঙ্কে ফেলে দিয়েছে। সাইবার অপরাধ একটি সামাজিক, রাজনৈতিক, অর্থনৈতিক, জাতীয়, বৈশ্বিক ও নৈতিক অপরাধ। বাংলাদেশের মতো তথ্যপ্রযুক্তিতে দ্রুত উন্নয়নশীল দেশের জন্য এটি চরম উদ্বেগের বিষয়।

অপরাধ : সাধারণভাবে অপরাধ বলতে সমাজ কর্তৃক শাস্তিযোগ্য কোনো অন্যায় আচরণকে বুঝায়। সমাজবিজ্ঞানী এমিল ডুর্খেইম মনে করেন, অপরাধ একটি সামাজিক ঘটনা। এটি সমাজ ব্যবস্থার একটি 'স্বাভাবিক' রূপ। যদিও সমাজভেদে তা স্বল্প বা তীব্র মাত্রার হয়ে থাকে। তিনি মনে করেন সমাজে টিকে থাকার জন্য অনেক সময় অপরাধের আশ্রয় নিতে হয়। এটা সমাজ কাঠামোর দুর্বলতার ফল।

সাইবার অপরাধ : তথ্যপ্রযুক্তি বিষয়ক অপরাধ হলো সাইবার অপরাধ। এক্ষেত্রে অপরাধী কোনো ব্যক্তি বা প্রতিষ্ঠানের কম্পিউটারে অনাধিকার প্রবেশ করে ঐ ব্যক্তি বা প্রতিষ্ঠানের তথ্য-উপাত্ত চুরি করে এবং নিজ স্বার্থে তা ব্যবহার করে। এছাড়া ওয়েবসাইটের মাধ্যমে বিকৃত বা অসত্য তথ্য প্রকাশ, অশ্লীল ও কুরুচিপূর্ণ বা ভিডিও প্রকাশ এবং অনুমতি ব্যতীত অন্য কারো মন্তব্য, তথ্য বা ছবি প্রকাশও সাইবার অপরাধ। ফেসবুকে বা কোনো গণমাধ্যমে কাউকে নিয়ে মানহানিকর বা বিভ্রান্তিমূলক কিছু পোস্ট করলে, ছবি বা ভিডিও আপলোড করলে, কারও নামে অ্যাকাউন্ট খুলে ভিভ্রান্তিমূলক পোস্ট দিলে, কোনো স্ট্যাটাস দিলে কিংবা শেয়ার বা লাইক দিলেও সাইবার অপরাধ হতে পারে। কাউকে ইলেকট্রনিক মাধ্যমে হুমকি দিলে, অশালীন কোনো কিছু পাঠালে কিংবা দেশবিরোধী কোনো কিছু করলে তা সাইবার অপরাধ হবে। আবার ইলেকট্রনিক মাধ্যমে হ্যাক করলে, ভাইরাস কিংবা কোনো সিস্টেমে অনধিকার প্রবেশ করলে, অনলাইনে যে কোনো অপরাধমূলক কর্মকাণ্ডে জড়িত হলে তাও সাইবার অপরাধ।

মোদ্দা কথা, ইন্টারনেট অথবা তথ্যপ্রযুক্তি ব্যবহার করে যে কোনো অপরাধ করলে তাকেই সাইবার অপরাধ বলে।

সাইবার অপরাধের মাধ্যম : প্রথমত কম্পিউটার ও ইন্টারনেট

ব্যবহার করে সাইবার অপরাধ করা হয়। বর্তমান কম্পিউটার ও ইন্টানেট হাতের মুঠোয়। এছাড়া ট্যাব, স্মার্টফোন এসব ব্যবহার করে নিমিষে 'বিশ্বভ্রমণ' করা যায়। অ্যাকসেস করা যায় ফেসবুক, টুইটার, ইয়াহু, স্কাইপ, ভাইভার, ইমো, ম্যাসেঞ্জার, হোয়াইটসঅ্যাপে। এছাড়া আছে গুগল, গুগল প্লাস, ডুডুল, লিংকডইন, ইনস্ট্যাগ্রাম, ফ্লিকার, কম্পিউটার ও ক্লাউড। এ মাধ্যমগুলো ব্যবহার করে হ্যাকিং, সাইবার বুনিং, ই-মেইল স্পাম ও ফিশিং, অনলাইন কেলেঙ্কারি ও প্রতারণা, নারী ও শিশুদের বিকৃত ছবি আপলোডসহ, ইলেক্ট্রনিক মানি লন্ডারিং, অপরাধমূলক ষড়যন্ত্রের জন্য পারস্পরিক যোগাযোগ, টেলিযোগাযোগের মাধ্যমে ষড়যন্ত্র, সাইবার সন্ত্রাস, চাঁদাবাজি ইত্যাদি সাইবার অপরাধমূলক কর্মকাণ্ড সংঘটিত হচ্ছে।

সাইবার অপরাধের প্রকারভেদ : বিভিন্ন প্রকার সাইবার অপরাধের মধ্যে নিচের আলোচনায় প্রধান প্রধান কয়েকটি আলোচনা করা হলো

১. সাইবার সন্ত্রাস : সাইবার সন্ত্রাসী হলো সেই ব্যক্তি যে সরকার বা প্রশাসনকে একটি কম্পিউটারভিত্তিক আক্রমণ করে তাঁদের রাজনৈতিক বা সামাজিক উদ্দেশ্য জানতে ভয় প্রদর্শন বা বাধ্য করে। যেমন, নিজেদের দাবী মানতে কর্তৃপক্ষকে বাধ্য করার জন্য ইন্টারনেটে প্রচার করা হলো যে, ছুটির সময় বোমা হামলা হবে,

এটাকে সাইবার সন্ত্রাস হিসেবে বিবেচনা করা যেতে পারে।

২. সাইবার চাঁদাবাজি : সাইবার চাঁদাবাজি তখনই ঘটে যখন একটি ওয়েবসাইট, ই-মেইল, সার্ভার বা কম্পিউটার সিস্টেম ক্ষতিকারণ হ্যাকার দ্বারা বশীভূত হয়রানি পুনরাবৃত্তি হামলার সম্মুখীন হয়। এ হ্যাকাররা হামলা বন্ধ করার জন্য এবং 'সুরক্ষা' প্রদানের প্রস্তাব করার বিনিময়ে অর্থ দাবি করে। ফেডারেল ব্যুরো অফ ইনভেস্টিগেশন অনুযায়ী, সাইবার চাঁদাবাজরা ক্রমবর্ধমানভাবে কর্পোরেট ওয়েবসাইট এবং নেটওয়ার্ক আক্রমণ করছে, তাদের কাজ করার ক্ষমতা পঙ্গু করে দিচ্ছে এবং তাদের সেবা পুনরুদ্ধার করতে অর্থ দাবি করছে।

৩. সাইবার যুদ্ধ : মার্কিন প্রতিরক্ষা বিভাগ দাবি করেছে যে, বেশ কিছু সাম্প্রতিক ঘটনার কারণে ভূ-কৌশলগত গুরুত্ব বিবেচনায় সাইবারস্পেস একটি জাতীয় পর্যায়ের উদ্বেগ হিসেবে আত্মপ্রকাশ করেছে। ২০০৭ সালে এস্তোনিয়ার পরিকাঠামোতে রাশিয়ান হ্যাকার দ্বারা হামলা এর অন্তর্ভুক্ত। ২০০৮ এর আগস্টে রাশিয়া আবার জর্জিয়ার বিরুদ্ধে একটি সমন্বিত ও সুসংগত কথিত সাইবার আক্রমণ চালায়। ভয়ের বিষয় এই যে, এ ধরনের আক্রমণ ভবিষ্যতে জাতি-রাষ্ট্রের মধ্যে সমস্যা সৃষ্টি করতে পারে, সাইবারস্পেসের ধারণা বদলে দিতে পারে এবং যুদ্ধপরিস্থিতির উদ্ভব ঘটাতে পারে।

সাইবার অপরাধ ও বিশ্ব : ১২ মে ২০১৭ বিশ্বজুড়ে একযোগে বড় ধরনের সাইবার হামলার ঘটনা ঘটে। র‍্যানসমওয়্যারহামলায় আক্রান্ত হয় সাইবার জগৎ। এর মাধ্যমে বাংলাদেশসহ বিশ্বের ১৫০টি দেশের কম্পিউটার ব্যবস্থায় হানা দেয় হ্যাকাররা। বিশ্বব্যাপী এ সাইবার হামলায় তিন লক্ষাধিক কম্পিউটার আক্রান্ত হয়। এরূপ বিশ্বব্যাপী আলোচিত আরো কয়েকটি সাইবার হামলার বর্ণনা নিচে দেওয়া হলো।

১. উইকিলিকস : উইকিলিকস-এর মাধ্যমে যে তথ্যগুলো প্রকাশিত হয়েছে তা পৃথিবীর ইতিহাসে সবচেয়ে ভয়ানক সাইবার অপরাধ হিসেবে কুখ্যাতি লাভ করে। বিভিন্ন দেশের প্রায় ৩ থেকে ৪ লাখ গোপন তারবার্তা প্রকাশ করা হয় উইকিলিকসের মাধ্যমে। যার ফলে বিশ্বব্যাপী আন্তঃরাষ্ট্রিক সম্পর্ক, বাণিজ্যিক সম্পর্ক ও রাজনৈতিক সম্পর্কের মধ্যে ব্যাপক প্রভাব পড়ে। উইকিলিকসের প্রতিষ্ঠাতা জুলিয়ান অ্যাসাঞ্জ সাইবার অপরাধের দায়ে অভিযুক্ত হয়ে যুক্তরাজ্যে ইকুয়েডরের দূতাবাসে বন্দী জীবনযাপন করছেন।

২. মার্কিন গোয়েন্দা কর্মকর্তা এডওয়ার্ড স্নোডেন : মার্কিন গোয়েন্দা

সংস্থা সিআইএ কর্মকর্তা এডওয়ার্ড স্নোডেন 'সিআইএ' যে বিশ্বব্যাপী গুরুত্বপূর্ণ ব্যক্তিদের ফোনে আড়ি পাতে সে খবর ফাঁস করে দিয়ে আলোড়ন সৃষ্টি করে। তিনিও সাইবার অপরাধে অভিযুক্ত হয়ে বর্তমান রাশিয়া অবস্থান করছেন।

৩. পানামা পেপার্স : ৩ এপ্রিল ২০১৬ ওয়াশিংটনভিত্তিক ইন্টারন্যাশনাল কনসোর্টিয়াম অব ইনভেস্টিগেটিভ জার্নালিস্ট (ICIJ) গোপন সম্পদধারীদের আইনি সহায়তা ও সেবাদানকারী পানামার প্রতিষ্ঠান মোস্যাক ফনসেকার ১ কোটি ১৫ লাখ নথি ফাঁস করে। একে বলা হচ্ছে Crime of the Century বা শতাব্দী সেরা অপরাধ। এ যাবতকালের সবচেয়ে বড় তথ্য ফাঁসের ঘটনা পানামা পেপারস কেলেঙ্কারির ফলে আইসল্যান্ডের প্রধানমন্ত্রী সিগমুন্ড গুনলাগসন ৫ এপ্রিল ২০১৬ ব্যাপক বিক্ষোভ ও জনদাবির মুখে পদত্যাগ করেন। ২৮ জুলাই ২০১৭ সুপ্রিম কোর্টের রায়ে প্রধানমন্ত্রী পদে অযোগ্য ঘোষণা ও পদত্যাগের শিকার হন পাকিস্তানের মিয়া মোহাম্মদ নওয়াজ শরীফ।

৪. CIH : ১৯৮৬ সালের ২৬ এপ্রিল এ ভাইরাস প্রথম আঘাত করে, যার ফলে চেরনোবিলে মর্মান্তিক তেজস্ক্রিয় দুর্ঘটনা ঘটে। এজন্য এ তারিখে আঘাতকারী CIH-কে চেরনোবিল ভাইরাস বলে। এছাড়া এ ভাইরাস ২৬ এপ্রিল ১৯৯৯ বিশ্বব্যাপী কম্পিউটারে ব্যাপক

বিপর্যয় সৃষ্টি করে।

৫. হিলারি ক্লিনটনের ই-মেইল হ্যাক : বিশ্ব মোড়ল মার্কিন যুক্তরাষ্ট্রের সাবেক পররাষ্ট্রমন্ত্রী ও সদ্য অনুষ্ঠিত প্রেসিডেন্ট নির্বাচনে বিজিত প্রার্থী হিলারি ক্লিনটনের ই-মেইল ফাঁসের ঘটনায় সাইবার নিরাপত্তা ভোটের রাজনীতিতে নতুন ইস্যু হিসেবে অভির্ভূত হয়েছে।

সাইবার অপরাধ ও বাংলাদেশ : বর্তমান বিশ্বঅর্থনীতিতে বাংলাদেশ সুদৃঢ় অবস্থানে থাকলেও এটি একটি তৃতীয় বিশ্বের উন্নয়নশীল দেশ যার ফলে তথ্য ও প্রযুক্তিখাতে এখনো পরিপক্ব হয়ে ওঠেনি এবং অধিকাংশ ক্ষেত্রে বৈদেশিক সফ্টওয়্যার এর উপর নির্ভরশীল হওয়ার ঘন ঘন সাইবার হামলার স্বীকার হচ্ছে।

নিম্নে কয়েকটি সাইবার হামলার আলোচনা দেওয়া হলো –

বাংলাদেশ ব্যাংকের রিজার্ভ চুরি : যুক্তরাষ্ট্রের ফেডারেল রিজার্ভ ব্যাংকে গচ্ছিত রাখা বাংলাদেশ ব্যাংকের বৈদেশিক মুদ্রার রিজার্ভ থেকে ১০১ মিলিয়ন ডলার বা ১০ কোটি ১০ লাখ ডলার অর্থ ৫ ফেব্রুয়ারি ২০১৬ হ্যাকিংয়ের মাধ্যমে চুরি হয়ে যাওয়ার ঘটনা ঘটে। এ ঘটনার কারণে বাংলাদেশ ব্যাংকের গভর্নরকে পদত্যাগ করতে

হয়।

এটিএম, ডেবিট, ক্রেডিট কার্ড জালিয়াতি : ২০১৬ সালে বাংলাদেশের বেসরকারি ব্যাংকের পাইরেসি করা এটিএম, ডেবিট কার্ড, ক্রেডিট কার্ড ব্যবহার করে এটিএম বুথ থেকে প্রচুর অর্থ লুটের ঘটনা ঘটে। এ ঘটনার জের ধরে ৪ মার্চ ২০১৬ পুলিশ ১৪ ব্যক্তিকে আটক করে তাদের মধ্যে ১২ জন ছিল বিদেশি নাগরিক যারা বিশ্বের বিভিন্ন দেশে সাইবার অপরাধের সাথে জড়িত।

বাংলাদেশে সংঘটিত আরও কয়েকটি সাইবার অপরাধ : ২০১২ সালে ফেসবুকে গুজব ছড়িয়ে কক্সবাজারে বৌদ্ধ সম্প্রদায়ের ওপর হামলা করা হয়। সম্প্রতি কে বা কারা পূর্ণিমা শীলের ফেসবুক অ্যাকাউন্ট হ্যাক করে তার ছবি ও টেলিফোন নম্বর দিয়ে তার নামে পর্নোগ্রাফির ফেসবুক পেজ খোলে। কয়েকদিন আগে ফেসবুকে ইসলাম অবমাননার গুজব রটিয়ে ব্রাহ্মণবাড়িয়ার নাসিরনগরে হিন্দু সম্প্রদায়ের ওপর হামলা করা হয়। তা ছাড়া ফটোশপের মাধ্যমে এর ছবি ওর সঙ্গে জড়িয়ে দেওয়া ঘটনা ক্রমাগত ঘটছে। এমনকি ২০০৮ সালের দিকে র‍্যাবেরওয়েবসাইট হ্যাক করা হয়। এসব ঘটনা আমাদের সাইবার নিরাপত্তাকে প্রশ্নবিদ্ধ করে।

সাইবার অপরাধ প্রতিরোধের উপায় : বাংলাদেশে যেভাবে সাইবার অপরাধ বৃদ্ধি পাচ্ছে তার লাগাম টেনে না ধরা গেলে নিকট ভবিষ্যতে তা আরও ভয়ানক আকার ধারণ করতে পারে। নিচে প্রতিকারের উপায়গুলো নিয়ে আলোচনা করা হলো :

- ঢাকা মেট্রোপলিটন পুলিশে 'কাউন্টার টেরোজিম ও ট্রান্সন্যাশনাল ক্রাইম ইউনিট' গঠন করা হয়েছে, যা সাইবার অপরাধের বিষয়গুলো দেখছে। তবে পুলিশ সাইবার অপরাধ বিষয়ক নতুন ইউনিট খোলা প্রয়োজন। যার কাজ হবে সাইবার অপরাধের সাথে সংশ্লিষ্ট আইনগুলোকে যথাযথ প্রয়োগ করা।

তথ্য ও যোগাযোগপ্রযুক্তি আইন, ২০০৬ (সংশোধিত ২০১৩)-এর ৫৪, ৫৬, ৫৭ ধারা অনুযায়ী বর্তমানে সাইবার অপরাধ সংক্রান্ত মামলার রায় দেওয়া হয়। কিন্তু ৫৭ ধারা নিয়ে জনমনে প্রশ্ন আছে যে, এ ধারায় মানুষের বাক-স্বাধীনতাকে অবহেলা করা হয়েছে। তাই ৫৭ ধারাকে সংশোধন করে সময়ের উপযোগী করে আইন তৈরি করা প্রয়োজন।

- কেবল আইন তৈরি করে নয়, আইন প্রয়োগের সঙ্গে সঙ্গে শিক্ষার পরিবর্তন আনতে হবে। ঢাকা ও চট্টগ্রাম বিশ্ববিদ্যালয়ে ক্রিমিনোলজি

এবং মাওলানা ভাসানী বিজ্ঞান ও প্রযুক্তি বিশ্ববিদ্যালয়ে ক্রিমিনোলজি ও পুলিশ বিভাগ রয়েছে। যুগের সঙ্গে তাল মিলিয়ে আরও দুয়েকটি বিশ্ববিদ্যালয়ে ক্রিমিনোলজি বিভাগ চালু করে সাইবার অপরাধ ও নিরাপত্তা বিষয়ে পর্যাপ্ত গবেষণার সুযোগ সৃষ্টি করা প্রয়োজন।

- ব্যাংকে দেশীয় সফ্টওয়ার ব্যবহার করা উচিত যাতে বর্তমান সময়ে ঘটে যাওয়া ঘটনাগুলোর পুনরাবৃত্তি এড়ানো যায়।

- সাইবার অপরাধ সংঘটিত হলে সাথে সাথে ব্যবস্থা নিতে হবে যাতে ভবিষ্যতে আর এরকম ঘটনা না ঘটতে পারে।

- আইন শৃঙ্খলা বাহিনী এবং প্রযুক্তি বিশেষজ্ঞ ব্যক্তিদেরকে নিয়ে টার্সফোর্স গঠন করতে হবে, যাতে তারা সাইবার নিরাপত্তার উপর সার্বক্ষণিক নজর রাখতে পারে।

- আধুনিক প্রযুক্তির ব্যবহার নিশ্চিত করতে হবে এবং আমাদের এন্টিভাইরাস ও সিকিউরিটি সফ্টওয়্যার সবসময় হালনাগাদ রাখতে পারে।

গবেষণায় দেখা গেছে ৭০/৮০ ভাগ সাইবার অপরাধের সাথে জড়িত থাকে অফিসিয়াল কর্মকরর্তা। এক্ষেত্রে সকল অফিস, ব্যাংক, বীমা প্রতিষ্ঠানে নজরদারি বাড়ানো উচিত যাতে অসৎ কর্মকর্তাদেরকে চিহ্নিত করা যথাযথ আইনের অধীনে এনে শাস্তির ব্যবস্থা করা যায়।

উপসংহার : 'পে-পাল' বাংলাদেশে এসেছে। নিকট ভবিষ্যতে আসবে 'ইবে', 'আমাজন', 'আলিবাবা'। তাই অনলাইন বিপণনে আর্থিক ব্যবস্থাপনার নিরাপত্তা নিশ্চিত করতে হবে। যুগোপযোগী ও যথাযথ আইন প্রণয়ন করে সাইবার নিরাপত্তা বাড়ানো উচিত। শিক্ষার্থীদের সাইবার ইথিক্স শেখানো উচিত। যাতে পূর্ণিমাশীলদের বাকিটা জীবন নির্বিঘ্নে; অভিজিৎরা তাদের চিন্তা-চেতনা নিয়ে বেঁচে থাকতে পারে, রাজকোষ ও জনতার অর্থ নিরাপদ হয়। নিশ্চিত হয় ডিজিটাল বাংলাদেশের নিরাপত্তা।

আঠারো থেকে ত্রিশ বছর বয়সীদের ৮০ শতাংশের বেশি সাইবার অপরাধের শিকার। সবচেয়ে বেশি আক্রান্ত নারীরা। সাইবার ক্রাইম অ্যাওয়ারনেসের জরিপে এ তথ্য উঠে এসেছে।

সাইবার অপরাধের মধ্যে রয়েছে ছবি বিকৃত করে অপপ্রচার, পর্নোগ্রাফি কনটেন্ট, সামাজিক মাধ্যমে অপপ্রচার এবং অনলাইনে-ফোনে মেসেজ পাঠিয়ে হুমকি দিয়ে মানসিক হয়রানি। ব্যক্তিকেন্দ্রে এই গবেষণা করা হলেও প্রতিষ্ঠানগুলো সাইবার অপরাধের আওতার বাইরে নয়। আইনি কাঠামো শক্তিশালী না হওয়ায় এ প্রবনতা কমছে না বলে অভিমত বিশ্লষকদের। সাইবার অপরাধীরা প্রতিদিনই তাদের ধরণ বদলাচ্ছে। তুলনামূলকভাবে বাড়ছে না পুলিশের সংখ্যা। তাই সচেতনতার বিকল্প নেই বলে জানানো হয় অনুষ্ঠানে।

হয়রানির শিকারের পর ভুক্তভোগীদের মাত্র ২৬ দশমিক ৬ শতাংশ আইনশৃঙ্খলা বাহিনীর কাছে গেছে। এছাড়া আইনের আশ্রয় নেওয়া ভুক্তভোগীদের মাত্র ৭ দশমিক ৪ শতাংশ আশানুরূপ ফল পেয়েছেন বলে জানিয়েছেন। লোকলজ্জার ভয়সহ বিভিন্ন কারণে অপরাধের বিষয়ে ভুক্তভোগীরা কোথাও অভিযোগ করেন না। সার্বিক পরিস্থিতিতে সাইবার অপরাধ নিয়ন্ত্রণে ব্যাপকভাবে। সচেতনতামূলক কার্যক্রমসহ আটটি সুপারিশ তুলে ধরা হয় গবেষণা প্রতিবেদনে।

জরিপে ২০২১ সালের ১৫ ফেব্রুয়ারি থেকে ২০২২ সালের ২ মার্চ পর্যন্ত ব্যক্তি পর্যায়ে ভুক্তভোগী ১৯৯ জনকে ১৮টি প্রশ্ন করা হয়। সেই মতামতের ভিত্তিতে এ বছরের গবেষণা প্রতিবেদন তৈরি করা হয়।

উপরের গবেষণা প্রতিবেদটি ব্যক্তি পর্যায়ে করা হয়েছে। সব তথ্য কিন্তু পাওয়া যায় না। যেমন, ব্যাংকের অ্যাকাউন্ট হ্যাক হলে আইন অনুযায়ী সরকার তথ্য দিতে বাধ্য। কিন্তু এটি দেশে এখনও পর্যন্ত প্রতিষ্ঠিত করতে পারা যায়নি। প্রকৃত তথ্য জানা গেলে আরও ভালো করে বলতে পারা যেত, কেন সাইবার অপরাধ বাড়ছে!

অপরাধের ধরন:

ভুক্তভোগীদের বেশির ভাগই সাইবার বুলিংয়ের শিকার। এর মধ্যে রয়েছে ছবি বিকৃত করে অপপ্রচার, পর্নোগ্রাফি কনটেন্ট, সামাজিক মাধ্যমে অপপ্রচার এবং অনলাইনে ফোনে মেসেজ পাঠিয়ে হুমকি দিয়ে মানসিক হয়রানি। এবারের জরিপে সাইবার বুলিংয়ের শিকার হওয়া ভুক্তভোগী কিছুটা বেড়ে ৫০ দশমিক ২৭ শতাংশ হয়েছে, যা গতবারের প্রতিবেদনে ছিল ৫০ দশমিক ১৬ শতাংশ।

এবার দেশে সাইবার অপরাধের মধ্যে আশঙ্কাজনকভাবে বেড়েছে

সামাজিক মাধ্যমসহ অন্যান্য অনলাইন অ্যাকাউন্ট হ্যাকিং বা তথ্য চুরি। এছাড়াও সামাজিক যোগাযোগ মাধ্যম ব্যাবহার করে অপপ্রচার চালানো এবং অনলাইনে পণ্য কিনতে গিয়ে প্রতারণার শিকার ভুক্তভোগীর সংখ্যা চোখে পড়ার মতো।

এবারের জরিপে সাইবার অপরাধের তুলনামূলক পরিসংখ্যান বিশ্লেষণ করে দেখা গেছে, প্রথম স্থানে রয়েছে সামাজিক যোগাযোগ মাধ্যমসহ অন্যান্য অনলাইন একাউন্ট হ্যাকিংয়ের ঘটনা, যার হার ২৩ দশমিক ৭৯ শতাংশ। ২০২১ সালের প্রতিবেদনে এই হার ছিল ২৮ দশমিক ৩১ শতাংশ, যা এবারের তুলনায় ৪ দশমিক ৫২ শতাংশ বেশি। তবে চিন্তার বিষয় এই যে, গতবারের প্রতিবেদনে সামাজিক যোগাযোগ মাধ্যমে অপপ্রচারের ঘটনা ছিল ১৬ দশমিক ৩১ শতাংশ। কিন্তু এবার তা বেড়ে গিয়ে দাঁড়ায় ১৮ দশমিক ৬৭ শতাংশ, যা গতবারের তুলনায় ২ দশমিক ৩৬ শতাংশ বেশি। এছাড়াও যৌন হয়রানিমূলক একান্ত ব্যক্তিগত মুহূর্তের ছবি/ভিডিও (পর্নোগ্রাফি) ব্যাবহার করে হয়রানি এবং ফটোশপে ভুক্তভোগীর ছবি বিকৃত করে হয়রানির ঘটনা উদ্বেগজনক হারে বেড়েছে। যৌন হয়রানিমূলক একান্ত ব্যক্তিগত মুহূর্তের ছবি/ভিডিও (পর্নোগ্রাফি) ব্যাবহার করে হয়রানির পরিমাণ গতবার ৭ দশমিক ৬৯ শতাংশ ছিল। কিন্তু সেটা এবার বেড়ে গিয়ে দাঁড়ায় ৯ দশমিক ৩৪ শতাংশে এবং ফটোশপে ভুক্তভোগীর ছবি বিকৃত করে হয়রানির ঘটনা গতবারের প্রতিবেদনে ৫ দশমিক ৮৫ শতাংশ পাওয়া গেলেও এবার

তা ১ দশমিক ৮ শতাংশ বেড়ে গিয়ে দাঁড়ায় ৬ দশমিক ৯৩ শতাংশ।

করোনা মহামারির কারণে বিশাল সংখ্যক মানুষ অনলাইনে কেনাকাটায় অভ্যস্ত হয়ে যাওয়ার কারণে অনলাইনে পণ্য কিনতে গিয়ে প্রতারণার শিকার ভুক্তভোগীর সংখ্যা বিপুল হারে বেড়ে গেছে। জরিপ অনুযায়ী প্রায় ১৫ দশমিক ৬ শতাংশ মানুষ অনলাইনে পণ্য কিনতে গিয়ে প্রতারণার শিকার হয়েছেন।

করোনা পরিস্থিতি:

করোনাভাইরাসে সৃষ্ট পরিস্থিতির আগের বছরগুলোর এবং পরের বছরের গবেষণা প্রতিবেদনে পাওয়া তথ্য অনুযায়ী সর্বোচ্চ সংঘটিত অপরাধগুলোর তুলনামূলক বিশ্লেষণ করলে দেখা যায়, উল্লেখযোগ্য হারে বিগত চার বছর ধরে সামাজিক যোগাযোগ মাধ্যমে অপ্রপ্রচার কমলেও গত বছর এই ধরনের অপরাধের প্রবণতা আবারো বাড়তে শুরু করেছে। ফটোশপে ছবি বিকৃতির ঘটনাও নতুন করে বাড়ছে। সবচেয়ে শঙ্কার জায়গা তৈরি হয়েছে অনলাইন কেনাকাটায়। ই-কমার্স খাতে চার বছরে ধারাবাহিক অপরাধ বৃদ্ধির হার প্রায় দ্বিগুণ।

ভুক্তভোগীদের বয়স:

ভুক্তভোগীদের মধ্যে বেশির ভাগের বয়স ১৮-৩০ বছর এবং এই হার ৮০ দশমিক ৯০ শতাংশ। দ্বিতীয় স্থানে রয়েছে ১৮ বছরের কম বয়সী ভুক্তভোগী এবং এই ভুক্তভোগীদের হার ১৩ দশমিক ৫৭ শতাংশ। তৃতীয় স্থানে রয়েছে ৩১-৪৫ বছর বয়সের ভুক্তভোগী যাদের হার ৫ দশমিক ৩ শতাংশ এবং সর্বশেষ অবস্থান করছে ৪৫ বছরের ঊর্ধ্বের ভুক্তভোগী, যার হার শূন্য দশমিক ৫০ শতাংশ। ১৮-৩০ বছর এবং ১৮-এর চেয়ে কম বয়সের ভুক্তভোগীরা সামাজিক যোগাযোগ মাধ্যমে আইডি হ্যাকিং বা তথ্য চুরির মতো সাইবার অপরাধের শিকার হয়েছেন বেশি। আরেকটি আশঙ্কাজনক ব্যাপার হচ্ছে ১৮ বছরের কম বয়সী ভুক্তভোগীদের বৃদ্ধির হার গত বছরের তুলনায় ৪ দশমিক ৬৪ শতাংশ বেশি এসেছে এবারের জরিপে।

জেন্ডারভিত্তিক অপরাধ:

তথ্য-উপাত্ত বিশ্লেষণ করে পরিলক্ষিত হয়েছে, নারী ও পুরুষের মধ্য সাইবার অপরাধে আক্রান্ত হওয়ার মাত্রায় ভিন্নতা রয়েছে। পুরুষের তুলনায় নারীরা সাইবার অপরাধের শিকার বেশি হয়েছেন। সাইবার অপরাধের ভুক্তভোগীদের জেন্ডারভিত্তিক পার্থক্য করলে দেখা যায়, ভুক্তভোগীদের মধ্য পুরুষের সংখ্যা ৪৩ দশমিক ২২ শতাংশ এবং নারীদের সংখ্যা ৫৬ দশমিক ৭৮ শতাংশ। এছাড়াও পুরুষের

তুলনায় নারীরা সামাজিক যোগাযোগ মাধ্যমে হয়রানি এবং পর্নোগ্রাফির শিকার বেশি হয়েছেন। অন্যদিকে নারীদের তুলনায় পুরুষরা মোবাইল ব্যাংকিং/এটিএম কার্ড হ্যাকিংয়ের শিকার বেশি হয়েছেন এবং অনলাইনে পণ্য কিনতে গিয়ে পুরুষদের তুলনায় নারীরা বেশি প্রতারণার শিকার হয়েছেন।

সংবাদ সম্মেলনে বলা হয়, ভুক্তভোগীদের মধ্যে তথ্যপ্রযুক্তিবিষয়ক আইন সম্পর্কে জানেন ৪৩ দশমিক ২২ শতাংশ। বাকি ৫৬ দশমিক ৭৮ শতাংশ ভুক্তভোগীর দেশে বিদ্যমান আইন সম্পর্কে কোনো ধারণা নেই। গত বছরের সঙ্গে তুলনা করলে দেখা যায় যে ভুক্তভোগীদের মধ্যে গত বছরের তুলনায় এই বছর ২১ দশমিক ৭ শতাংশ কম ভুক্তভোগী তথ্যপ্রযুক্তিবিষয়ক আইন সম্পর্কে জানেন।

আইনের আশ্রয় নেওয়ার প্রবণতা কম:

১৯৯ জন ভুক্তভোগীদের মধ্যে মাত্র ৫৩ জন সমস্যা নিয়ে আইনশৃঙ্খলা বাহিনীতে অভিযোগ করেছেন। এটা মোট ভুক্তভোগীর মাত্র ২৬ দশমিক ৬ শতাংশ, যা ২০২১ এর পরিসংখানের তুলনায় মাত্র ৫ দশমিক ১৭ শতাংশ বেশি। সমস্যা নিয়ে পুরুষ অভিযোগকারীর ১৫ দশমিক ৫৮ শতাংশ আইনশৃঙ্খলারক্ষাকারী বাহিনীর দ্বারস্থ হয়েছেন এবং ২৭ দশমিক ৬৪ শতাংশ হননি। পরিসংখ্যানে এও লক্ষণীয় যে, পুরুষ অভিযোগকারীদের তুলনাই

নারী অভিযোগকারীর সংখ্যা তুলনামূলক কম। নারী ভুক্তভোগীদের মধ্যে মাত্র ১১ দশমিক ৬ শতাংশ সমস্যা নিয়ে আইনশৃঙ্খলা বাহিনীর দ্বারস্থ হয়েছেন এবং ৪৫ দশমিক ৭৩ শতাংশ আইনের আশ্রয় নিতে অনীহা প্রকাশ করেছেন।

অভিযোগের পর আশানুরূপ ফল:

অভিযোগকারীদের মধ্যে মাত্র ৭ দশমিক ৪ শতাংশ আইনশৃঙ্খলা বাহিনীর দ্বারস্থ হয়ে আশানুরূপ ফল পেয়েছেন এবং ৫৫ দশমিক ২৭ শতাংশ ভুক্তভোগী অভিযোগের পর প্রত্যাশা অনুযায়ী ফল পাননি। অভিযোগের পর প্রত্যাশিত ফল পাওয়ায় পুরুষ এবং নারীভেদে ভিন্নতা রয়েছে। অভিযোগের পর আশানুরূপ ফল পাওয়ার ক্ষেত্রে যেখানে পুরুষের সংখ্যা ৮ জন বা ৪ দশমিক ২ শতাংশ, সেখানে নারীর সংখ্যা মাত্র ৬ জন বা ৩ দশমিক ২ শতাংশ। অন্যদিকে আশানুরূপ ফল না পাওয়া নারীদের সংখ্যা ২৮ দশমিক ৬৪ শতাংশ, যেদিকে পুরুষের সংখ্যা ২৬ দশমিক ৬৩ শতাংশ।

২০২১ সালের প্রতিবেদনে দেখা যায়, অভিযোগের পর আশানুরূপ ফল পেয়েছেন মোট ভুক্তভোগীর ২২ দশমিক ২২ শতাংশ, যা ২০২২ সালের পরিসংখ্যানের তুলনায় ১৫ দশমিক ১৮ শতাংশ বেশি। অর্থাৎ এবারের প্রতিবেদনে প্রতাশিত ফল পাওয়ার পরিমাণ অনেকাংশে কমেছে।

যেসব কারণে ভুক্তভোগীরা আইনের আশ্রয় নিতে চান না:

প্রাপ্ত উপাত্তগুলোকে বিশ্লেষণের মাধ্যমে ভুক্তভোগীদের আইনি ব্যাবস্থা না নেওয়ার কারণের মধ্যে ভিন্নতা দেখা গেছে। বিষয়টিকে গোপন রাখতে আইনি ব্যবস্থা নেননি সর্বোচ্চ ২১ শতাংশ ভুক্তভোগী। এছাড়া ১৭ শতাংশ ভুক্তভোগী সামাজিক ভাবমূর্তি রক্ষার জন্য, ১৭ শতাংশ আইনি ব্যবস্থা নিয়ে উল্টো হয়রানি পোহাতে হবে, ১৭ শতাংশ অভিযোগ, করেও কোনো লাভ হবে না ভেবে কোনো বাবস্থা নেননি। অভিযুক্ত ব্যক্তি প্রভাবশালী হওয়ায় কোনো পদক্ষেপ নেননি ৭ শতাংশ ভুক্তভোগী। অন্যদিকে ২ শতাংশ ভুক্তভোগী ব্যবস্থা গ্রহণের প্রয়োজন আছে, তা মনেই করেননি।

সাইবার বুলিং

সাইবার বুলিং কী এবং এটি কীভাবে প্রতিরোধ করা যায়?

“সাইবার বুলিয়িং সম্পর্কে তোমরা কী জানতে চাও?” বিশ্বজুড়ে তরুণদেরকে আমরা এই প্রশ্নটি করেছিলাম। এই প্রশ্নের উত্তরে আমরা হাজার রকমের প্রতিক্রিয়া পেয়েছি।

আমরা ইউনিসেফের বিশেষজ্ঞ এবং আন্তর্জাতিক সাইবার বুলিয়িং ও শিশু সুরক্ষা বিশেষজ্ঞদের একত্রিত করে প্রশ্নের উত্তর দিতে ও অনলাইন বুলিং প্রতিরোধের উপায়গুলো সম্পর্কে কিশোর-কিশোরীদেরকে পরামর্শ দিতে ফেসবুক, ইনস্টাগ্রাম ও টুইটারের সাথে জোটবদ্ধ হয়েছি।

সাইবার বুলিং কী?

ডিজিটাল প্রযুক্তি ব্যবহার করে হয়রানি করার নামই সাইবার বুলিয়িং। এটি সামাজিক মিডিয়া, মেসেজিং প্ল্যাটফর্ম, গেমিং প্ল্যাটফর্ম এবং মোবাইল ফোনে ঘটতে পারে। এক্ষেত্রে যাদেরকে

টার্গেট করা হয় তাদেরকে ভয় দেখানো, রাগিয়ে দেওয়া, লজ্জা দেওয়া বা বিব্রত করার জন্য বার বার এরূপ আচরণ করা হয়। উদাহরণ হিসাবে বলা যায়:

সামাজিক মাধ্যমে কারো সম্পর্কে মিথ্যা তথ্য ছড়িয়ে দেওয়া বা বিব্রতকর অথবা অবমাননাকর ছবি পোস্ট করা, মেসেজিং প্ল্যাটফর্মের মাধ্যমে ক্ষতিকর মেসেজ দেওয়া বা হুমকি দেওয়া, অন্যের ছদ্মবেশ ধারণ করে তার পক্ষে আর একজনকে ম্যাসেজ পাঠানো, মুখোমুখি বুলিয়িং এবং সাইবার বুলিয়িং প্রায়শই একে অপরের পাশাপাশি ঘটতে পারে। তবে, সাইবার বুলিয়িং একটি ডিজিটাল পদচিহ্ন রেখে যায়। এই ডিজিটাল পদচিহ্ন এমন একটি রেকর্ড যা কার্যকর প্রমাণ হিসাবে কাজ করতে পারে এবং অপব্যবহার বন্ধে সহায়তা করতে প্রমাণ সরবরাহ করতে পারে।

আপনি যদি নিজের সুরক্ষা অথবা অনলাইনে আপনার সাথে ঘটেছিল এমন কোন কিছু সম্পর্কে উদ্বিগ্ন হন, আপনার বিশ্বস্ত কোনো একজন প্রাপ্তবয়স্ক ব্যক্তির সাথে জরুরি ভিত্তিতে কথা বলুন।

১। অনলাইনে কি আমাকে বুলিয়িং করা হচ্ছে? রসিকতা এবং বুলিংয়ের মধ্যকার পার্থক্য কীভাবে নির্ণয় করা সম্ভব?

বন্ধুরা সবাই একে অপরের সাথে রসিকতা করে। কিন্তু, অনলাইনে কেউ আপনার সাথে রসিকতা করছে, নাকি আপনাকে কষ্ট দেওয়ার চেষ্টা করছে কখনও কখনও এটি বলা খুব কঠিন হয়ে পড়ে। কখনও কখনও তারা 'কেবল মজা করেছে' বা 'এটিকে এত গুরুত্ব দেয়ার কোন কারণ নেই' এমনটা বলে হাসাহাসি করবে।

তবে আপনি যদি কষ্ট পান বা আপনি যদি মনে করেন যে, অন্যরা আপনাকে নিয়ে হাসাহাসি বা তামাশা করছে, তাহলে বুঝতে হবে রসিকতার মাত্রা ছাড়িয়ে গেছে। যে ব্যক্তি আপনাকে নিয়ে রসিকতা করছে তাকে থামতে বলার পরেও যদি সেটা চালিয়ে যেতে থাকে এবং আপনি এতে বিরক্ত হন, তবে তা বুলিংয়ের পর্যায়ে পড়ে।

এছাড়াও, যখন অনলাইনে বুলিয়িং ঘটে, তখন এটি অপরিচিত সহ বহু মানুষের অযাচিত মনোযোগ আকর্ষণ করতে পারে। যেখানেই এটি ঘটুক না কেন, আপনি যদি এটিতে ভাল বোধ না করেন, তাহলে এটির বিরুদ্ধে আপনার সোচ্চার হওয়া উচিত।

আপনি যদি ভাল বোধ না করেন এবং এটি যদি বন্ধ না হয়, তাহলে আপনার সাহায্যের প্রয়োজন। এর জন্য আপনি কল করতে পারেন। সাইবার বুলিয়িং বন্ধ করা মানে কেবল বুলিয়িং না করাই

নয় বরং অনলাইনে ও বাস্তব জীবনে প্রত্যেকেরই যে শ্রদ্ধা পাওয়ার অধিকার রয়েছে তাকে স্বীকৃতি দেওয়া।

২। সাইবার বুলিয়িং এর প্রতিক্রিয়া হিসাবে কী হতে পারে?

বুলিয়িং যখন অনলাইনে সংঘটিত হয়, তখন এমন মনে হয় যে নিজের বাড়ির ভেতর সহ সর্বত্র আপনি আক্রমনের শিকার হচ্ছেন। এ সময় মনে হতে পারে যে, এ থেকে আপনার পালানোর কোনো পথ নেই। এর প্রভাব দীর্ঘ সময় ধরে থাকতে পারে এবং এটি একজন ব্যক্তিকে বিভিন্নভাবে প্রভাবিত করতে পারে। এগুলো হলো:

মানসিকভাবে – এ সময় বিরক্ত বোধ হয়, বিব্রত লাগে, নিজেকে বোকা মনে হয়, এমনকি নিজের উপর রাগ হয়

আবেগগতভাবে - লজ্জা বোধ হয় বা নিজের পছন্দের জিনিসের প্রতি আগ্রহ হারিয়ে ফেলা এমন বোধ হয়

শারীরিকভাবে –ক্লান্ত বোধ হয় (ঘুম না হওয়া), বা পেটের ব্যথা এবং মাথা ব্যথার মতো লক্ষণগুলো দেখা যায়

আপনাকে কেউ উপহাস করছে বা অন্যের দ্বারা আপনি হয়রানির শিকার হচ্ছেন আপনার এমন অনুভূতি আপনাকে অন্যের সাথে কথা বলতে বা কোনো সমস্যা সমাধান করার প্রচেষ্টাকে বাধাগ্রস্ত করতে পারে। বিশেষ বিশেষ ক্ষেত্রে, সাইবার বুলিংয়ের ফলে কখনও

কখনও মানুষ তার নিজের জীবনকে বিলিয়ে দিতেও দ্বিধা করে না।

সাইবার বুলিয়িং আমাদেরকে বিভিন্ন নেতিবাচকভাবে প্রভাবিত করতে পারে। তবে, এগুলো সমাধান করা যেতে পারে এবং মানুষ তার আত্মবিশ্বাস এবং স্বাস্থ্য ফিরে পেতে পারে।

৩। আমি সাইবার বুলিংয়ের শিকার হচ্ছি, কিন্তু আমি আমার বাবা-মায়ের সাথে এ বিষয়ে কথা বলতে ভয় পাচ্ছি।আমি কীভাবে তাদেরকে এটা জানাতে পারি?

আপনি যদি সাইবার বুলিংয়ের শিকার হন, সেক্ষেত্রে সবচেয়ে গুরুত্বপূর্ণ যে পদক্ষেপটি আপনি গ্রহণ করতে পারেন সেটা হলো আপনি নিরাপদ বোধ করেন এমন কোনও বিশ্বস্ত প্রাপ্তবয়স্ক ব্যক্তির সাথে কথা বলা।

মা-বাবার সাথে কথা বলা সবার পক্ষে সহজ নয়। তবে এমন কিছু বিষয় রয়েছে যা আপনাকে আপনার বাবা-মার সাথে কথোপকথনে সহায়তা করতে পারে। যে সময়ে আপনার বাবা-মায়ের পুরো মনোযোগ পাবেন বলে মনে করেন ঠিক সে সময়কে তাদের সাথে কথা বলার জন্য নির্ধারণ করুন। আপনার জন্য সমস্যাটি কতটা

মারাত্মক তাদেরকে সে বিষয়টি বুঝিয়ে বলুন। মনে রাখবেন, তারা আপনার মতো প্রযুক্তি-বান্ধব নাও হতে পারে। সুতরাং কী ঘটছে তা বুঝতে আপনার তাদেরকে সাহায্য করার প্রয়োজন হতে পারে।

তাদের কাছে আপনার প্রশ্নের তাৎক্ষণিক উত্তর নাও থাকতে পারে। তবে তারা আপনাকে সহায়তা করতে উদ্যোগী হবেন এবং তাদের সাথে মিলে আপনি একটি সমাধান খুঁজে পেতে পারেন। দুই চোখের চেয়ে চার চোখ সবসময় ভালো! আপনি কী করবেন সে সম্পর্কে এখনও নিশ্চিত না হলে, বিশ্বস্ত অন্য কারও কাছে যাওয়ার বিষয়টি সবসময় বিবেচনা করুন। আপনার আশেপাশে প্রায়শই এমন অনেক মানুষ আছে যারা আপনাকে অনেক ভালবাসে এবং আপনি যতটা প্রত্যাশা করেন না, তার চেয়েও অনেক বেশি সহায়তা করতে চায়।

৪। আমার যেসব বন্ধু সাইবার বুলিংয়ের বিষয়টি রিপোর্ট করতে চায় না, তাদেরকে সাইবার বুলিংয়ের বিষয়টি রিপোর্ট করতে আমি কীভাবে সহায়তা করতে পারি?

যে কোনও ব্যক্তি সাইবার বুলিংয়ের শিকার হতে পারেন। আপনি চেনেন এমন কারও সাথে এমনটি ঘটতে দেখলে তাকে সহযোগিতা করার চেষ্টা করুন।

আপনার বন্ধুর কথা শোনা জরুরী। সাইবার বুলিংয়ের শিকার হলেও কেন তারা বিষয়টি রিপোর্ট করতে চান না? তারা বিষয়টি নিয়ে কি ভাবছে? কোন কিছু যে আনুষ্ঠানিকভাবে জানানোর প্রয়োজন নেই, এই বিষয়টি তাদেরকে জানান। তবে সাহায্য করতে পারেন এমন কারও সাথে কথা বলা অত্যন্ত গুরুত্বপূর্ণ।

মনে রাখবেন, আপনার বন্ধু হয়তো ভেঙ্গে পড়েছে। তার প্রতি সদয় হন। তারা কী বলতে পারে এবং কাকে বলতে পারে তাদের মাধ্যমেই তাদেরকে ভাবতে সহায়তা করুন। তারা রিপোর্ট করার সিদ্ধান্ত নিলে তাদের সংগ দেওয়ার প্রস্তাব দিন। আপনি যে তাদের প্রয়োজনে আছেন এবং তাদেরকে সহায়তা করতে চান সে বিষয়টি তাদেরকে মনে করিয়ে দেওয়া হলো সবচেয়ে গুরুত্বপূর্ণ বিষয়।

আপনার বন্ধুটি যদি এখনও ঘটনাটি সম্পর্কে রিপোর্ট করতে না চান, তবে পরিস্থিতি মোকাবেলায় তাকে সহযোগিতা করতে পারে এমন একজন বিশ্বস্ত প্রাপ্তবয়স্ককে খুঁজে দিতে সহায়তা করুন। মনে রাখবেন, বিশেষ কিছু পরিস্থিতিতে সাইবার বুলিংয়ের পরিণতি প্রাণঘাতী হতে পারে।

কোনো কিছু না করলে সেই ব্যক্তির অনুভূতি এমন পারে যে, প্রত্যেকেই তার বিপক্ষে অবস্থান করছে বা কেউ তাকে পাত্তা দিচ্ছে না।

যে কেউ সাইবার বুলিংয়ের শিকার হতে পারেন।

৫। কেউ যদি আমাকে অনলাইনে বুলিয়িং করে তবে আমি কার সাথে কথা বলব? এক্ষেত্রে রিপোর্টিং গুরুত্বপূর্ণ কেন?

আপনি বুলিংয়ের শিকার হচ্ছেন এমনটি মনে করলে, প্রথম পদক্ষেপটি হলো আপনার বাবা-মা, পরিবারের ঘনিষ্ঠ সদস্য বা অন্য কোনও বিশ্বস্ত প্রাপ্তবয়স্ক ব্যক্তির কাছ থেকে সাহায্য নেওয়া।

আপনার স্কুলে আপনি কাউন্সেলর, খেলাধূলার প্রশিক্ষক বা আপনার প্রিয় শিক্ষকের সাথে যোগাযোগ করতে পারেন। তবে আপনি যদি নিজের পরিচিত কারও সাথে কথা বলতে স্বাচ্ছন্দ্য বোধ না করেন, তখন একজন পেশাদার কাউন্সেলরের সাথে কথা বলার জন্য আপনার দেশের একটি হেল্পলাইন অনুসন্ধান করুন।

সামাজিক প্লাটফর্মে যদি বুলিয়িং ঘটে থাকে, সেক্ষেত্রে যিনি বুলিয়িং করছেন তাকে ব্লক করে দেওয়ার বিষয়টি বিবেচনা করুন এবং তাদের এই আচরণ সম্পর্কে আনুষ্ঠানিকভাবে প্ল্যাটফর্মে জানান। সামাজিক মাধ্যম সংস্থাগুলো তাদের ব্যবহারকারীদের সুরক্ষিত রাখার ক্ষেত্রে দায়বদ্ধ।

কী ঘটছে তা দেখানোর জন্য সামাজিক মাধ্যমের পোস্টগুলোর টেক্সট মেসেজ এবং স্ক্রিনশট প্রমাণ হিসাবে কাজ করতে পারে।

বুলিয়িং বন্ধ করার জন্য অবশ্যই এটিকে সনাক্ত করা দরকার এবং বুলিংয়ের বিষয়টি রিপোর্ট করা অত্যন্ত গুরত্বপূর্ণ। যারা বুলিয়িং করে তাদের সেই আচরণটি যে একেবারেই অগ্রহণযোগ্য সে বিষয়টি বুলিকে জানাতে এটি সহায়তা করতে পারে।

আপনি যদি তাৎক্ষণিকভাবে কোনো বিপদে পড়েন, তখন দেশের পুলিশ বা জরুরি সেবা সংস্থাসমূহের সাথে যোগাযোগ করা উচিত।

বুলিয়িং বন্ধ করার জন্য অবশ্যই এটি সনাক্ত করা দরকার এবং বুলিংয়ের বিষয়টি রিপোর্ট করা অত্যন্ত গুরত্বপূর্ণ ।

৬। ইন্টারনেট ব্যবহারের সুযোগ না হারিয়ে কীভাবে আমরা সাইবার বুলিয়িং বন্ধ করব?

অনলাইনের অনেক সুবিধা রয়েছে। কিন্তু জীবনে অনেক কিছুর মতো এখানেও কিছু ঝুঁকি থাকে যা প্রতিরোধ করা প্রয়োজন হয়ে পড়ে।

আপনি যদি সাইবার বুলিংয়ের শিকার হন, নিজেকে পুনরায় ফিরিয়ে আনার জন্য আপনাকে কিছু সময়ের জন্য কিছু অ্যাপ মুছে ফেলতে হতে পারে বা অফলাইনে থাকতে হতে পারে। তবে, ইন্টারনেট থেকে বিচ্ছিন্ন থাকা দীর্ঘমেয়াদী কোনো সমাধান নয়। আপনি তো কোনো ভুল করেন নি। তাহলে কেন আপনি অসুবিধা ভোগ করবেন? যারা বুলিয়িং করে এটি তাদেরকে ভুল সংকেতও দিতে পারে। পক্ষান্তরে এটি তাদেরকে গ্রহণযোগ্য নয় এমন আচরণ চালিয়ে যেতে উৎসাহিত করতে পারে।

সাইবার বুলিয়িং বন্ধ হোক- এটা আমরা সবাই চাই।এ কারনে সাইবার বুলিংয়ের বিষয়টি রিপোর্ট করা অত্যন্ত গুরত্বপূর্ণ। কিন্তু আমরা যে ইন্টারনেট সিস্থাচার ব্যবহার রীতি অনুসরণ করি তা বুলিয়িং বন্ধে সবসময় সহায়তা করে না। অন্যকে আঘাত করতে পারে এমন বিষয়গুলো শেয়ার করা বা বলার ক্ষেত্রে আমাদের

চিন্তাভাবনা করা উচিত। অনলাইন এবং বাস্তব জীবনে আমাদের একে অপরের প্রতি সদয় হওয়া প্রয়োজন। এটা আমাদের সকলের জন্যই সমান প্রয়োজ্য!

অন্যকে আঘাত করতে পারে এমন যে বিষয়গুলো আমরা শেয়ার করি বা বলি সে সম্পর্কে আমাদের চিন্তাভাবনা করা উচিত।

৭। আমার ব্যক্তিগত তথ্যাদি ব্যবহার করে সামাজিক মাধ্যমে আমাকে হেনস্তা বা অপমান করা হলে আমি কীভাবে প্রতিরোধ করতে পারি?

অনলাইনে কোনো কিছু পোস্ট করা বা শেয়ার করার আগে অন্তঃত দু'বার ভাবুন। এটি চিরকাল অনলাইনে থাকতে পারে এবং পরে আপনার ক্ষতি করতে ব্যবহৃত হতে পারে। আপনার ঠিকানা, টেলিফোন নম্বর বা আপনার স্কুলের নামের মতো ব্যক্তিগত বিবরণ দেবেন না। আপনার প্রিয় সামাজিক মিডিয়া অ্যাপের প্রাইভেসি সেটিংস সম্পর্কে জানুন। বেশ কিছু পদক্ষেপের মধ্যে এখানে কয়েকটি পদক্ষেপ রয়েছে। এগুলোর মধ্যে আপনি কয়েকটি নিতে পারেন।

কে আপনার প্রোফাইল দেখতে পাবে, কে আপনাকে সরাসরি মেসেজ পাঠাতে পারবে বা কে আপনার পোস্টগুলোতে মন্তব্য করতে পারবে আপনার অ্যাকাউন্টের প্রাইভেসি সেটিংসকে সমন্বয় করার মাধ্যমে সে সম্পর্কে আপনি সিদ্ধান্ত নিতে পারেন।

আপনি ক্ষতিকারক মন্তব্য, মেসেজ এবং ফটো সম্পর্কে রিপোর্ট করতে এবং সেগুলো সরিয়ে নিতে অনুরোধ করতে পারেন।

আনফ্রেন্ড করা ছাড়াও, আপনার প্রোফাইল দেখতে বা আপনার সাথে যোগাযোগ করা আটকাতে আপনি মানুষজনকে সম্পূর্ণরূপে ব্লক করতে পারেন।

সম্পূর্ণরূপে ব্লক না করে কেবলমাত্র নির্দিষ্ট কিছু মানুষ যেন মন্তব্য করতে পারে সে বিষয়টিও আপনি বিবেচনা করতে পারেন।

আপনি আপনার প্রোফাইলে থাকা পোস্টগুলি মুছতে পারেন বা নির্দিষ্ট কিছু মানুষজন থেকে এগুলো আড়াল করে রাখতে পারেন।

আপনার পছন্দের বেশিরভাগ সামাজিক মাধ্যমে ব্লক, রেসট্রিক্ট বা রিপোর্ট করার বিষয়টি মানুষজনকে জানানো হয় না।

৮। সাইবার বুলিংয়ের জন্য কি কোনও শাস্তি রয়েছে?

বেশিরভাগ স্কুল বুলিয়িং বেশ গুরুত্বের সাথে বিবেচনা করে এবং এর বিরুদ্ধে ব্যবস্থা নেবে। অন্য কোনো শিক্ষার্থীর দ্বারা আপনি যদি বুলিংয়ের শিকার হন, তবে আপনার স্কুলে তা রিপোর্ট করুন।

বুলিয়িং ও সাইবার বুলিয়িং সহ যে কোনও ধরণের সহিংসতার শিকার হচ্ছেন এমন মানুষের ন্যায়বিচার পাবার এবং অপরাধীকে জবাবদিহিতার আওতায় আনার অধিকার রয়েছে।

বুলিংয়ের, বিশেষত সাইবার বুলিংয়ের, বিরুদ্ধে যে সব আইন রয়েছে সেগুলো অপেক্ষাকৃত নতুন এবং এখনও সব জায়গায় এই আইনের অস্তিত্ব ও প্রয়োগ চোখে পড়ে না। এ কারণে সাইবার বুলিদের শাস্তি দেওয়ার জন্য অনেক দেশ অন্যান্য প্রাসঙ্গিক আইন যেমন, হয়রানির বিরুদ্ধে আইন-কে ব্যবহার করে।

সাইবার বুলিংয়ের বিরুদ্ধে সুনির্দিষ্ট আইন রয়েছে এমন দেশগুলোতে ইচ্ছাকৃতভাবে গুরুতর মানসিক সমস্যা সৃষ্টি করে এমন অনলাইন আচরণকে অপরাধমূলক কর্মকান্ড হিসাবে দেখা হয়। এসব দেশগুলোর মধ্যে কিছু দেশে সাইবার বুলিংয়ের শিকার হচ্ছেন এমন

মানুষজন সুরক্ষা চাইতে পারেন, নির্দিষ্ট ব্যক্তির সাথে যোগাযোগ করা বন্ধ করতে পারেন এবং অস্থায়ীভাবে বা স্থায়ীভাবে সাইবার বুলিংয়ের জন্য সেই ব্যক্তির ব্যবহৃত বৈদ্যুতিক ডিভাইসের ব্যবহারকে বন্ধ করতে পারেন।

তবে বুলিদের আচরণ পরিবর্তন করার জন্য সব সময় শাস্তি যে সবচেয়ে কার্যকর উপায় নয় সে বিষয়টি মনে রাখা জরুরী। সবচেয়ে ভাল উপায় হলো ক্ষতি পুষিয়ে নেওয়া এবং সম্পর্কের উন্নতির দিকে মনোনিবেশ করা।

৯। অনলাইন বুলিয়িং এবং হয়রানির বিষয়ে ইন্টারনেট সেবাদানকারী সংস্থাগুলো কোনো চিন্তা করে না বলে মনে হয়।তাদেরকে কি দায়বদ্ধতার মধ্যে আনা হচ্ছে?

ইন্টারনেট সেবাদানকারী সংস্থাগুলো অনলাইন বুলিংয়ের বিষয়ে ক্রমশ মনোযোগ দিচ্ছে।

তাদের অনেকেই অনলাইন বুলিয়িং থেকে রক্ষার পদ্ধতি বের করছে। এছাড়াও, তাদের অনেকেই নতুন টুলস, নির্দেশিকা এবং অনলাইন গালাগাল সম্পর্কে রিপোর্ট করার মাধ্যমে তাদের

ব্যবহারকারীদের আরও সুরক্ষিত করার উপায় বের করছে।

কিন্তু, এটা সত্য যে, এর চেয়েও বেশি কিছু করা দরকার। প্রতিদিন অসংখ্য তরুণ সাইবার বুলিংয়ের শিকার হচ্ছে। এদের মধ্যে অনেকেই মারাত্মক রকমের অনলাইন নির্যাতনের শিকার হচ্ছে। সাইবার বুলিংয়ের ফলস্বরূপ অনেকেই নিজের জীবন পর্যন্ত দিয়ে দিচ্ছে।

তাদের শিশু এবং তরুণ ব্যবহারকারী সহ সকল অনলাইন ব্যবহারকারীকে সুরক্ষার ব্যাপারে প্রযুক্তি সংস্থাগুলোর একটি দায়িত্ব রয়েছে।

যখন তারা এই দায়িত্বগুলো পালন করে না, তখন আমাদের সকলের উচিত তাদেরকে জবাবদিহিতার আওতায় নিয়ে আসা।

১০। শিশুদের বা তরুণদের জন্য অনলাইনে বুলিয়িং প্রতিরোধী কোনও টুলস রয়েছে কি?

প্রতিটি সামাজিক মিডিয়া প্ল্যাটফর্ম তাদের ব্যবহারীদের জন্য কিছু

টুলস (পর্যাপ্ত টুলস নিচে দেখুন) সরবরাহ করে। এসব টুলস আপনাকে আপনার পোস্টে মন্তব্য করা বা আপনার পোস্ট দেখা বা বন্ধু হিসাবে কারা নিজেরাই স্বয়ংক্রিয়ভাবে সংযুক্ত হতে পারে এবং বুলিংয়ের ঘটনাগুলো রিপোর্ট করতে পারে সেগুলো বন্ধ করার অনুমতি দেয়। এদের মধ্যে অনেকে সাইবার বুলিয়িং ব্লক করতে, মিউট করতে বা রিপোর্ট করতে নিঃশব্দ বা কিছু সহজ পদক্ষেপ গ্রহণ করে। এগুলো খুঁজে বের করতে আমরা আপনাকে উৎসাহিত করি।

ঝুঁকি এবং অনলাইনে নিরাপদে থাকার উপায় সম্পর্কে শিখতে শিশু, বাবা-মা এবং শিক্ষকদের জন্য সামাজিক মিডিয়া সংস্থাগুলো শিক্ষামূলক টুলস এবং গাইডেন্স প্রদান করে।

এছাড়াও, সাইবার বুলিংয়ের বিরুদ্ধে প্রতিরক্ষার প্রথম পদক্ষেপ আপনিই নিতে পারেন। আপনার কমিউনিটিতে কোথায় সাইবার বুলিং হয় এবং সাইবার বুলিং প্রতিরোধের বিভিন্ন উপায় যেমন, কথা বলা, বুলিকে খুঁজে বের করা, বিশ্বস্ত প্রাপ্তবয়স্কদের কাছে যাওয়া বা এই ইস্যুতে সচেতনতা সৃষ্টির কৌশল সম্পর্কে ভাবুন। এমনকি সদয় আচরণের মতো একটি সাধারণ কাজ আরও অনেক দূর পর্যন্ত যেতে পারে।

আপনি যদি আপনার নিরাপত্তা সম্পর্কে উদ্বিগ্ন হন বা অনলাইনে যদি কিছু ঘটে থাকে, তবে জরুরি ভিত্তিতে আপনার বিশ্বস্ত কারও সাথে কথা বলুন। পৃথিবীর অনেক দেশে একটি বিশেষ হেল্পলাইন চালু রয়েছে যেখানে আপনি বিনামূল্যে কল করতে পারেন এবং কারও সাথে পরিচয় গোপন রেখে কথা বলতে পারেন। আপনার দেশে সহায়তা পেতে চাইল্ড হেল্পলাইন দেখুন।

সাইবার বুলিংয়ের বিরুদ্ধে সুরক্ষার প্রথম পদক্ষেপটি আপনিই নিতে পারেন।

সাইবার ক্রাইম:
সচেতনতার বিকল্প নেই

ইন্টারনেটের মাধ্যমে হয়রানি ক্রমেই বাড়ছে। তুলনামূলক নারীরা সাইবার ক্রাইমের শিকার বেশি হচ্ছে। ব্যক্তিপর্যায় থেকে শুরু করে আর্থিক প্রতিষ্ঠান। কেউ সাইবার আক্রমণ থেকে রক্ষা পাচ্ছে না। তথ্যপ্রযুক্তির সঠিক ব্যবহার না জানা, আইনের যথাযথ প্রয়োগের অভাব এবং এই আইন সম্পর্কে না জানার কারণে এ ধরনের অপরাধে ভুক্তভোগির সংখ্যা বাড়ছে।

'সাইবার অপরাধ' বলতে ইন্টারনেট ব্যবহার করে যে অপরাধ করা হয়, তাকেই বোঝানো হয়। তথ্য চুরি, তথ্য বিকৃতি, প্রতারণা, ব্ল্যাকমেইল, অর্থ চুরি ইত্যাদি তথ্যপ্রযুক্তির মাধ্যমে করা হলে সেগুলোকে সাধারণ ভাষায় সাইবার অপরাধ বলা হয়। সাইবার অপরাধ মূলত কম্পিউটারে ব্যবহৃত কর্মকাণ্ড, যার নেটওয়ার্ক ব্যবহার করে বিশ্বব্যাপী অপরাধ পরিচালিত করে থাকে অপরাধিরা।

দেশে যে ধরনের সাইবার অপরাধ ঘটছে, তার মধ্যে রয়েছে- ই-মেইলে হুমকি, আইন প্রয়োগকারী সংস্থার ওয়েবসাইট হ্যাক,

বিভিন্ন প্রতিষ্ঠান-ব্যক্তির ওয়েবসাইট হ্যাক বা তথ্যচুরি, বিভিন্ন সামাজিক যোগাযোগ মাধ্যমে হুমকি দেয়া, নাজেহাল করা ও অপপ্রচার ব্যাপকভাবে বেড়ে গেছে। প্রচলিত সাইবার অপরাধের মধ্যে আছে ফ্রড কিংবা প্রতারণা, ক্রেডিট কার্ডের নাম্বার চুরি, ব্ল্যাকমেইল ,পর্নোগ্রাফি, হয়রানি, অনলাইনের মাধ্যমে মাদক পাচার/ব্যবসায় প্রভৃতি। আবার জাল সার্টিফিকেট তৈরি, জাল টাকা বা জাল পাসপোর্ট, বিভিন্ন প্রকার দলিল-দস্তাবেজ কম্পিউটারের মাধ্যমে তৈরির ঘটনা অহরহ উদ্‌ঘাটিত হচ্ছে।

যেভাবে সাইবার আক্রমণ

ইন্টারনেটের মাধ্যমে কম্পিউটার, নেটওয়ার্ক অবকাঠামোকে সরাসরি আক্রমণ এবং ব্যক্তি ও জাতীয় নিরাপত্তা ব্যতয় ঘটানোর মাধ্যমে সাইবার অপরাধ ঘটতে পারে।

ভাইরাস আক্রমণ। ব্যক্তি, প্রতিষ্ঠান বা রাষ্ট্রীয় ওয়েবসাইট হ্যাকিং (বেদখল)। ম্যালওয়্যার স্পামিং বা জাঙ্ক মেইল; এটি সম্পূর্ণই মেইল ভিত্তিক। ভুয়া আইডি/ই-মেইল অ্যাড্রেস ব্যবহার করে নাম-ঠিকানা, ক্রেডিট কার্ড নাম্বার এমনকি ফোন নাম্বার নিয়ে মিষ্টি কথায় ভোলাতে চেষ্টা করবে অপরাধী চক্র। ফাঁদে পা দিলেই বিপদ! স্প্যাম ফোল্ডারে এমন মেইল প্রায়ই আসে। সাইবার হয়রানি-ইমেইল বা ব্লগ বা ওয়েবসাইট ব্যবহার করে হুমকি দেয়া, ব্যক্তির

নামে মিথ্যাচার/অপপ্রচার,নারী অবমাননা, যৌন হয়রানি।

এছাড়াও ফিশিং- লগইন/অ্যাকসেস তথ্যচুরি, বিশেষত ই-কমার্স, ই-ব্যাংকিং সাইটগুলো ফিশারিদের লক্ষ্যবস্তু হয়ে থাকে। অর্থ আত্মসাৎ-ইন্টারনেট থেকে তথ্যচুরি করে ব্যাংকের এক অ্যাকাউন্ট থেকে অন্য অ্যাকাউন্টে অর্থ স্থানান্তর একটি উদাহরণ। সাইবার মাদক ব্যবসায়-আইনশৃঙ্খলা রক্ষা বাহিনীকে ফাঁকি দিতে ইদানীং ইন্টারনেট ব্যবহার করে মাদক ব্যবসার প্রবণতা বেড়েছে। পাইরেসি- সদ্য প্রকাশিত গান ও সিনেমার এমপিথ্রি বা মুভি ফাইল ইন্টারনেটে শেয়ার হয়ে যাচ্ছে। ইন্টেলেকচুয়াল প্রপার্টি- ব্লগ ও ওয়েবসাইট থেকে কোনো লেখা ও ফটোগ্রাফি সহজেই কপি-পেস্ট করে নিজের নামে চালিয়ে দেয়ার প্রবনতা বেড়েছে সাইবার কমিউনিটিতে। পর্নোগ্রাফি- শিশু পর্নোগ্রাফি ইন্টারনেটে ভয়ঙ্করভাবে বেড়েছে। ব্যক্তিগত তথ্য-পরিচয়-ছবি চুরি ও ইন্টারনেটর অপব্যবহার বেড়েছে। হ্যাকিং- বাংলাদেশেও ওয়েবসাইট হ্যাকিং ব্যাপকভাবে বেড়েছে। ক্র্যাকিং- ক্র্যাকিং হলো গুরুত্বপূর্ণ তথ্য কিংবা ক্রেডিট কার্ড নাম্বার চুরি করে গোপনে অনলাইন ব্যাংক থেকে ডলার চুরি করা ।

তথ্যপ্রযুক্তি আইন

ইংল্যান্ড বিশ্বে প্রথম সাইবার আইন প্রণেতা হিসেবে তৈরি করে

কম্পিউটার মিসইউজ অ্যাক্ট ১৯৯০। ই-অপরাধ প্রতিরোধে ২০০৮ সালে জাতীয় ই-অপরাধ ইউনিটও গঠন করা হয়। ভারতেও তৈরি হয় তথ্যপ্রযুক্তি আইন ২০০০। বাংলাদেশে ২০০৬ সালে তথ্যপ্রযুক্তি ও যোগাযোগ আইন তৈরি হয় এবং পরে এ আইন সংশোধন করা হয় ।

এ আইনের ৫৭ ধারায় বলা হয়েছে, যদি কোনো ব্যক্তি ইচ্ছে করে ওয়েবসাইট বা অন্য কোনো ইলেকট্রনিক বিন্যাসে এমন কিছু প্রকাশ বা সম্প্রচার করেন, যা মিথ্যা ও অশ্লীল বা সংশ্লিষ্ট অবস্থা বিবেচনায় কেউ পড়লে বা শুনলে নীতিভ্রষ্ট বা অসৎ হতে উদ্বুদ্ধ হতে পারে বা যার মাধ্যমে মানহানি ঘটে, আইনশৃঙ্খলার ঘটে বা ঘটার সম্ভাবনা সৃষ্টি হয়, রাষ্ট্র বা ব্যক্তির ভাবমূর্তি ক্ষুণ্ন হয় বা ধর্মীয় অনুভূতিতে আঘাত করে বা করতে পারে এ ধরনের তথ্যাদির মাধ্যমে কোনো ব্যক্তি বা সংগঠনের বিরুদ্ধে উস্কানি দেয়া হয়, তাহলে তার এই কাজ অপরাধ হিসেবে গণ্য হবে। কোনো ব্যক্তি এ ধরনের অপরাধ করলে তিনি অনাধিক ১০ বছর কারাদণ্ডে দণ্ডিত হতে পারেন এবং অনাধিক এককোটি টাকা অর্থদণ্ডে দণ্ডিত হতে পারেন।

সচেতনতা

আমাদের দেশে আইন থাকলেও আইনি অব্যবস্থাপনা নিয়ে জনসাধারণের মধ্যে চাপা ক্ষোভ রয়েছে। বর্তমানে আমাদের দেশে

ইন্টারনেট ব্যবহারকারির সংখ্যা দিনদিন বাড়ছে। তার সঙ্গে পাল্লা দিয়ে বাড়ছে সাইবার অপরাধও। ইন্টারনেট ব্যবহারকারিদের বেশিরভাগেরই তথ্যপ্রযুক্তি আইন সম্পর্কে কোনো ধারণা নেই। তাই বুঝে হোক বা না বুঝে হোক সাইবার অপরাধে জড়িয়ে পড়ছে। যারা সাইবার অপরাধের শিকার, তারাও সঠিক আইনি ব্যবস্থা নিতে জানেন না। আবার অনেকে থানায় গেলেও ফল পান না। কারণ অনেক পুলিশ কর্মকর্তাই জানেন না এ ধরনের অভিযোগ পেলে তার ঠিক কী করা উচিত। তাই এই আইন সম্পর্কে সচেতনতা বৃদ্ধিতে আইনের প্রচার বাড়াতে হবে ও প্রয়োগ নিশ্চিত করতে হবে। একইসঙ্গে তথ্যপ্রযুক্তির ব্যবহারে আপনাকে খুব সচেতন হতে হবে। যেমন আপনি যদি ইমেইল, ফেসবুক কিংবা কোনো অনলাইন অ্যাকাউন্টের নিরাপত্তার বিষয়গুলো ঠিকভাবে সেটিং করতে পারেন দুনিয়ার যতো বড় ক্রিমিনাল হোক আপনার অ্যাকউন্টের ক্ষতি করতে পারবে না।

সাইবার ক্রাইম কি?

সাইবার ক্রাইম সম্পর্কে বিস্তারিত জানুন!

আজ আমরা সাইবার ক্রাইম কি? সাইবার ক্রাইম সম্পর্কে বিস্তারিত জানার চেষ্টা করব।

বর্তমানে কম-বেশি সবাই কোন না কোন ভাবে ইন্টারনেটের সাথে যুক্ত। আর ইন্টারনেটের সাথে যুক্ত সবাই মোটামোটি সাইবার ক্রাইম শব্দটির সাথে পরিচিত। বর্তমান সময়ে বাংলাদেশে অনেক সাইবার ক্রাইম সংগঠিত হচ্ছে। শুধু বাংলাদেশেই না, বিশ্বের প্রতিটি দেশে-ই সাইবার ক্রাইমের খবর পাওয়া যাচ্ছে। বর্তমান সময়ের ক্রাইম গুলোর মধ্যে সাইবার ক্রাইম একটা ভীতিজনক শব্দে পরিণত হয়েছে।

প্রতিদিন লক্ষ লক্ষ লোক সাইবার ক্রাইমের শিকার হচ্ছেন। মূলত এই ক্রাইমের টার্গেট হচ্ছেন যেসকল ইন্টারনেট ব্যহারকারী ইন্টারনেট ব্যবহারে দক্ষ নয়।

সাইবার ক্রাইম

বিশ্বব্যাপী প্রতি বছর সাইবার ক্রাইমের জন্য শত শত কোটি ডলার ক্ষতি হচ্ছ। ২006 সালে কম্পিউটার ইকোনোমিক্স জরিপ অনুযায়ী ভাইরাসের কারণে ১৩.৩ বিলিয়ন ডলার ক্ষতিগ্রস্ত হয়েছিল সারাবিশ্ব।

সাইবার ক্রাইম কোন নতুন অপরাধ নয়। ইন্টারনেটের মাধ্যমে তথ্য চুরি, তথ্য বিকৃতি, মানি লন্ডারিং, জালিয়াতি, ব্ল্যাকমেইল ইত্যাদির মতো অপরাধ গুলো করা হলে তা সাইবার ক্রাইম হিসেবে বিবেচনা করা হয়।

সাইবার ক্রাইম কি?

ইন্টারনেটের মাধ্যমে সংঘটিত সকল ধরনের অপরাধই সাইবার ক্রাইমের অন্তর্ভুক্ত। মূলত, সাইবার ক্রাইম হচ্ছে এমন একটি অপরাধ, যাতে প্রধানত কম্পিউটার বা অন্য কোন ইলেক্ট্রনিক যন্ত্র ব্যবহৃত হয় এবং অপরাধীরা ইন্টারনেট ব্যবহার করে বিশ্বব্যাপী অপরাধগুলো করে।

সাইবার ক্রাইমকে চার ভাগে ভাগ করা হয়েছে।

ইনসাইডারস

হ্যাকার

ভাইরাস রাইটারস এবং

ক্রিমিনাল গ্রুপ।

বিভিন্ন প্রকার সাইবার ক্রাইম

১. হ্যাকিং

সাইবার ক্রাইমের প্রথমেই আসে হ্যাকিং। হ্যাকিং এবং হ্যাকার শব্দ দুটির সাথে আমরা সবাই মোটামোটি পরিচিত। সাধারণত হ্যাকিং মানে হচ্ছে কারো অনুমতি ব্যতিত তার ইলেকট্রনিক ডিভাইসের কন্ট্রোল নেওয়া বা তার ক্ষতি করা। আর যারা হ্যাকিং-এর এসব কাজগুলো করে থাকেন তাদেরকে হ্যাকার বলা হয়।

আরো পড়ুন- হ্যাকিং থেকে আপনার এন্ড্রয়েড ফোনকে নিরাপদ রাখুন সহজ ৫ উপায়ে!

একজন হ্যাকার আপনার কম্পিউটার, মোবাইল বা অন্য যেকোন ইলেকট্রনিক ডিভাইস ভাইরাস বিস্তার করে আপনার গুরুত্বপূর্ণ যেকোন তথ্য আুরি বা নষ্ট করে দিতে পারে। তাছাড়া হ্যাকাররা আপনার সোসাল একাউন্ট হ্যাক করে আপনার যেকোন ক্ষতি করতে পারে। আবার অনেক হ্যাকার বিভিন্ন গুরুত্বপূর্ণ ওয়েবসাইট বা ই-কমার্স ওয়েবসাইটের তথ্য বা ক্রেডিট কার্ডের নম্বর হ্যাক করে আপনাকে ব্যাপক ক্ষতির মুখে ফেলতে পারে। কয়েক প্রকারের হ্যাকিং আছে। তার মধ্যে ব্লাক হ্যাট হ্যাকিং সবচেয়ে ক্ষতিকর। ব্লাক হ্যাট হ্যাকাররা তাদের টার্গেটদের বিরাট ক্ষতির মুখে ফেলে।

২. পর্নোগ্রাফি

পর্নোগ্রাফির মাধ্যমে অনেকেই হ্যাকারদের কবলে পড়ে। বেশির ভাগ পর্ণ সাইটগুলোতেই ক্ষতিকর কম্পিউটার ভাইরাস থাকে। যেকোন সময় হ্যাকাররা পর্ণসাইটে ভিজিটকারী ব্যক্তির ডিভাইস হ্যাক করে নিতে পারে।

তাছাড়া অনেক সাইট পপ-আপ এড সো করে আবার অনেক সাইট কখনো কখনো ইমেইল এড্রেস চেয়ে থাকে। এই সকল কাজের মাধ্যমে বা যারা এসকল সাইট থেকে ভিডিও ডাউনলোড দেয়, তারা না জেনে অনেক সময় ভিডিওর সাথে হ্যাকারদের তৈরি করা অনেক ভাইরাস ফাইল ডাউনলোড করে নিতে পারে। এসকল

ফাইলের মাধ্যমে হ্যাকাররা ডিভাইসের কন্ট্রোল নিজেদের কাছে নিয়ে নিতে পারে। ফলে তারা ব্যাপক ক্ষতির মুখে পড়তে পারে।

৩. ড্রাগ ব্যবসা

ইন্টারনেটের মাধ্যমে এখন কি না হয়? মাদক থেকে শুরু করে নারী-শিশু পাচার সবই এখন ইন্টারনেটের মাধ্যমে হয়। ড্রাগ ব্যবসায়ীরা তাদের ওয়েবসাইটের মাধ্যমে মাদকদ্রব্যের ক্রয়, বিক্রয় ইত্যাদি কাজগুলো বিশ্বব্যাপী করে যাচ্ছে। যা মারাত্মক সাইবার ক্রাইম। তারা গোপনে এসকল কাজ করে যাচ্ছে।

৪. নারীর নির্যাতন

সাইবার ক্রাইমের আরেকটা বড় ইস্যু হচ্ছে নারী নির্যাতন। শত শত নারী প্রতিনিয়ত সাইবার ক্রাইমের শিকার হচ্ছেন। এখানে অভিনেত্রী থেকে শুরু করে একটা সাধারণ মেয়েও বাদ যাচ্ছে না। ইন্টারনেট ব্যবহারের দক্ষতার অভাব বা সাইবার ক্রাইম সম্পর্কে ভাল ধারণা না থাকায় অনেকেই সাইবার ক্রাইমের শিকার হয়। মেয়েদের সোসাল মিডিয়া একাউন্ট হ্যাক করে ব্যক্তিগত তথ্য প্রকাশ করা, যৌণ দৃশ্য প্রকাশ করা বা প্রকাশ করার হুমকি দেওয়া কিংবা মেয়েদের ছবি ব্যবহার করে ফেইক একাউন্ট খোলার মতো সাইবার

ক্রাইম প্রায়ই সংঘটিত হচ্ছে।

তাছাড়া প্রযুক্তির উন্নয়নের ফলে অনেকেই এর অপব্যবহার করে আর্টিফিশিয়াল ইন্টেলিজেন্সের মাধ্যমে মেয়েদের ফেইস ব্যবহার করে কৃত্রিম যৌন দৃশ্য তৈরি করে ইন্টারনেটে প্রকাশ করছে। ফলে লক্ষ লক্ষ মেয়ে ক্ষতির সম্মুখীন হচ্ছে আবার অনেকেই আত্মহত্যার পথ বেঁচে নিচ্ছে।

আবার পর্নোগ্রাফি সাইটগুলোতে অনেক মেয়ের ছবি পাওয়া যাচ্ছে, যেগুলো তাদের সোসাল মিডিয়া একাউন্ট থেকে নিয়ে এসকল পর্নোগ্রাফি সাইটে প্রকাশ করা হচ্ছে। ফলে তাতেও অনেকেই নানা-মুখী সমস্যার শিকার হচ্ছে। আর এসকল অপরাধের মাত্রা দিন দিন বেড়েই চলছে।

৫. স্প্যামিং এবং জাঙ্ক মেইল

সাধারণ মানুষদের ঠকানোর একটি কার্যকরী উপায় হলো এটি। বিভিন্ন সময় অনেক মানুষকে বিভিন্ন ফেইক অফিস নম্বর থেকে ফোন করে বলা হয় আমি বিকাশ থেকে বা এমুক কোম্পানি থেকে বলছি, আপনি লক্ষ টাকা লটারি জিতেছেন। এর মাধ্যমে তারা মানুষকে বোকা বানিয়ে তাদের বিভিন্ন একাউন্ট নম্বর হাতিয়ে নেয়।

ফলে লটারির লোভে পড়ে অনেকে বিশাল আর্থিক ক্ষতির সম্মুখীন হয়।

তাছাড়া এমন আরো অনেক সমস্যার কথা বলে বা বিভিন্ন লোভ দেখিয়ে ব্যবহারকারীর ব্যক্তিগত তথ্য, ঠিকানা, পাসওয়ার্ড, একাউন্ট নম্বর নিয়ে নেয়। এই কাজ গুলো হ্যাকাররা সাধারণত ফোন কলের মাধ্যমে করে থাকে আবার অনেক সময় মেসেজ বা ইমেইলের মাধ্যমেও করে থাকে।

সাইবার ক্রাইম নিয়ন্ত্রণে আইন

উন্নত দেশগুলোর মতো বাংলাদেশেও সাইবার ক্রাইম সংঘটিত হয়ে আসছে। উন্নত বিশ্বের সাইবার ক্রাইম বেশি হওয়ায় সাইবার ক্রাইমকে অপরাধের তালিকায় শীর্ষে রাখা হয়েছে। ফলে সাইবার ক্রাইম নিয়ন্ত্রণে নতুন নতুন আইন প্রণয়ন করা হয়েছে। বাংলাদেশেও সাইবার ক্রাইম নিয়ন্ত্রণের জন্য একাধিক আইন প্রণয়ন করা হয়েছে। তথ্য ও যোগাযোগ প্রযুক্তি আইন ২০০৬ তে এ সংক্রান্ত বিষয়ে বিস্তারিত নির্দেশনা দেওয়া আছে।

তথ্য ও যোগাযোগ প্রযুক্তি আইনের ৫৬ ধারায় বলা আছে–

“যদি কোনো ব্যক্তি জনসাধারণের বা কোনো ব্যক্তির ক্ষতি করার

উদ্দেশ্যে বা ক্ষতি হবে মর্মে জানা সত্ত্বেও এমন কোনো কাজ করেন, যার ফলে কোনো কম্পিউটার রিসোর্সের কোনো তথ্যবিনাশ, বাতিল বা পরিবর্তিত হয় বা তার মূল্য বা উপযোগিতা হ্রাস পায় বা অন্য কোনোভাবে একে ক্ষতিগ্রস্ত করে| এমন কোনো কম্পিউটার সার্ভার, কম্পিউটার নেটওয়ার্ক বা অন্য কোনো ইলেকট্রনিক সিস্টেমে অবৈধভাবে প্রবেশ করার মাধ্যমে এর ক্ষতিসাধন করেন, কিন্তু তিনি মালিক বা দখলদার নন, তাহলে তাঁর এই কাজ হবে একটি হ্যাকিং অপরাধ| কোনো ব্যক্তি হ্যাকিং অপরাধ করলে তিনি অনূর্ধ্ব ১০ বছর কারাদণ্ডে দণ্ডিত হবেন | এক কোটি টাকা অর্থদণ্ডে দণ্ডিত হতে পারেন বা উভয়দণ্ড দেওয়া যেতে পারে |”

তথ্যপ্রযুক্তি আইনের ৫৭ ধারায় বলা আছে–

“যদি কোনো ব্যক্তি ইচ্ছাকৃতভাবে ওয়েবসাইটে বা অন্য কোনো ইলেকট্রনিক বিন্যাসে এমন কিছু প্রকাশ বা সম্প্রচার করেন যা মিথ্যা ও অশ্লীল বা সংশ্লিষ্ট অবস্থা বিবেচনায় কেউ পড়লে বা শুনলে নীতিভ্রষ্ট বা অসৎ হতে উদ্বুদ্ধ হতে পারে বা যার দ্বারা মানহানি ঘটে, আইনশৃঙ্খলার অবনতি ঘটে বা ঘটার সম্ভাবনা সৃষ্টি হয়, রাষ্ট্র বা ব্যক্তির ভাবমূর্তি ক্ষুণ্ন হয় বা ধর্মীয় অনুভূতিতে আঘাত করে বা করতে পারে বা এ ধরনের তথ্যাদির মাধ্যমে কোনো ব্যক্তি বা সংগঠনের বিরুদ্ধে উস্কানি প্রদান করা হয়, তাহলে তার এই কাজ অপরাধ বলে গণ্য হবে |”

সর্বোপরি বলা যায়, সাইবার ক্রাইম একটি মারাত্মক অপরাধ। যা দেশ ও সমাজের জন্য ক্ষতিকর। আমরা সবাই সাইবার ক্রাইম থেকে বিরত থাকবো এবং অন্যকেও সাইবার অপরাধ সম্পর্কে সচেতন করবো। সাইবার ক্রাইমের কবলে পড়লে যেমন ক্ষতির সম্মুখীন হতে হবে তেমনি সাইবার অপরাধ করেও কেউ রেহাই পাবে না। তাই সাইবার ক্রাইম সম্পর্কে আমাদের সবারই সচেতন থাকতে হবে। আর অবশ্যই এমন জগ্ন অপরাধ থেকে আমরা সবাই বিরত থাকবো।

আজ এই পর্যন্তই। আশা করি সাইবার ক্রাইম কি? সাইবার ক্রাইম সম্পর্কে বিস্তারিত জানুন! নিয়ে লেখা এই আর্টিকেলটি আপনার ভাল লীছে। বন্ধু-বান্ধবদের মধ্যে যারা সাইবার ক্রাইম সম্পর্কে এখনো সচেতন নয় অবশ্যই তাদের কাছে শেয়ার করবেন। ভাল থাকবে, সুস্থ থাকবেন। ধন্যবাদ।

সাইবার ক্রাইম মানে কি ?

এবং, এই ইন্টারনেটের যুগে আমরা আমাদের জীবনের প্রায় অনেক বেশি পরিমানের সময় “online” থেকেই খরচ করি।

তবে, ইন্টারনেট এতো মজার এবং সবাইর প্রিয় হওয়ার কারণ কিন্তু প্রচুর রয়েছে।

নতুন নতুন খবর অনেক তাড়াতাড়ি বিভিন্ন ওয়েবসাইটের মাধ্যমে পেয়ে যাওয়া, যেকোনো জায়গার থেকে আমাদের প্রিয়জনের সাথে কথা, চ্যাটিং এবং video call এর মাধ্যমে যোগাযোগ, ইন্টারনেটের মাধ্যমে অনলাইন কেনাকাটা করা, যেকোনো বিষয়ে সঠিক তথ্য গ্রহণ, মনোরঞ্জনের জন্য ভিডিও দেখা, অনলাইন গেম খেলা এবং online bill payment এর মতো প্রায় সব ধরণের কাজ আজ ইন্টারনেটের মাধ্যমে অনেক সহজে করে নেয়াটা সম্ভব হয়ে দাঁড়িয়েছে।

সত্যি বললে, internet আমাদের জন্য এক অবদান বলে আমি মনে করি।

কেবল, এক দিনের জন্য সম্পূর্ণ ইন্টারনেট নাই হয়ে গেলেই, সাধারণ জনজীবনে অনেক প্রভাব পড়তে পারে।

এখন, যেখানে কম্পিউটার এবং ইন্টারনেটের এতটা ভালো গুন্ বা লাভ রয়েছে, সেখানে ইন্টারনেটের সাথে এক অনেক ক্ষতিকারক বিষয় জড়িয়ে রয়েছে।

সেটা হলো, "সাইবার ক্রাইম (cyber crime)" বা "সাইবার অপরাধ".

ইন্টারনেটে যেকোনো সময়, কোটি কোটি লোকেরা সক্রিয় থাকেন এবং তারা নিজের মোবাইল বা কম্পিউটারে ইন্টারনেট ব্যবহার কোরে বিভিন্ন website বা application ব্যবহার করেন।

এই ক্ষেত্রে, এমন অনেক ব্যাক্তি রয়েছে যারা কম্পিউটার এবং ইন্টারনেট ব্যবহার করে ইন্টারনেটে সক্রিয় থাকা এই "online traffic" বা "online internet users" দেড় থেকে বিভিন্ন অবৈধ (illegal) মাধ্যমে তাদের personal information চুরি করা, ঠকানো (cheating), ঠকিয়ে টাকা আদায় এবং আরো অন্যান্য অপরাধ করেন।

এভাবেই, একটি মোবাইল, কম্পিউটার এবং ইন্টারনেটের মাধ্যমে অনলাইন লোকেদের ঠকানো, privacy ও data চুরি করা বা data misuse করার অপরাধ গুলোকেই বলা হয় সাইবার ক্রাইম বা সাইবার অপরাধ।

এবং, যারা এই ধরণের cyber crime করেন, তাদের cybercriminals বলা হয়।

ইন্টারনেটে বিভিন্ন রকমের সাইবার ক্রাইম এর প্রকার রয়েছে। মানে, অনলাইনে বিভিন্ন অবৈধ মাধ্যমে cyber criminal গুলি আপনাকে ঠকাতে পারে।

আপনি যদি ইন্টারনেট ব্যবহার করার সময় সতর্ক না থাকেন, তাহলে হতে পারে "তাদের পরের শিকার আপনি".

সাইবার ক্রাইম কাকে বলে ? (What Is Cyber Crime in Bangla)

সাইবার ক্রাইম, সাইবার অপরাধ বা কম্পিউটার অপরাধ, এমন যেকোনো ধরণের অপরাধ, যেখানে একটি কম্পিউটার

(computer), নেটওয়ার্ক (internet) বা ইন্টারনেট সংযুক্ত ডিভাইস (device) অপরাধের সাধন (object) হিসেবে ব্যবহার করা হয়।

একটি কম্পিউটার বা ইন্টারনেট ব্যবহার করে যদি কারো ব্যক্তিগত তথ্যের অবৈধ ব্যবহার, copyright infringement, ঠকানো, personal data চুরি, hacking, phishing, spamming বা privacy theft এবং এগুলির মতো অপরাধ করা হয়, তাহলে একে বলা হয় “cybercrime” .

Cybercrime কে computer-oriented crime বলেও বোঝা যেতে পারে।

কারণ, এই ধরণের অপরাধে একটি computer device অবশই ব্যবহার করা হয়।

এই ধরণের অপরাধ বেশিরভাগ ক্ষেত্রে, সহজে লাভ আয়ের উদ্দেশ্যে এবং ডাটা চুরির করার উদ্দেশ্যে করা দেখা গেছে।

তবে, কারণ যাই হোক না কেন, আজ ইন্টারনেটে এই ধরণের অপরাধ অনেক বেশি পরিমানে হচ্ছে।

তাই, যেকোনো রকমের সাইবার ক্রাইম থেকে নিজেকে বাঁচিয়ে রাখার চেষ্টা রাখুন।

কম্পিউটার ক্রাইম, অনেক রকমের হতে পারে।

যেমন, কম্পিউটারের মাধ্যমে তথ্য চুরি করা, তথ্যর ভুল ব্যবহার করা, কারো ব্যক্তিগত তথ্য অন্যকে দিয়ে দেয়া, অনুমতি ছাড়া তথ্য নষ্ট করা এবং আরো অনেক রয়েছে।

আবার cyber crime অনেক রকমের হতে পারে।

যেমন, email spam (ইমেইলের মাধ্যমে ঠকানো), hacking, phishing, virus এর মাধ্যমে, অনলাইন যেকোনো ব্যক্তির ব্যক্তিগত তথ্য অনুমতি ছাড়া চুরি করা এবং আরো রয়েছে।

সাইবার ক্রাইম এর ক্ষেত্রে, আপনার ব্যাঙ্ক একাউন্টের তথ্য গ্রহণ করা, ডেবিট কার্ডের (debit card) অবৈধ ব্যবহার, net banking password চুরি ও অবৈধ ব্যবহার এবং ব্যক্তির bank সাথে জড়িত তথ্য চুরি করা, এবং এই ধরণের ঠকবাজি সবচেয়ে বেশি পরিমানে করা হয়।

তাহলে বন্ধুরা, বুঝলেনতো "সাইবার ক্রাইম কাকে বলে" (What Is Cyber Crime in Bangla) ?

যা আমি ওপরেই বললাম, সাইবার ক্রাইম এর প্রকার অনেক। মানে, ইন্টারনেট এবং কম্পিউটারের ব্যবহার করে অনেক রকমের অবৈধ কাজ বা অপরাধ করা হয়। তবে, অনেক বছর আগে, cybercrime বললে, কেবল "hacking" কেই বলা হতো। কারণ, আজ থেকে অনেক বছর আগে, প্রযুক্তি (technology) এতোটা উন্নত কখনোই ছিলোনা। তাছাড়া, ইন্টারনেট বা কম্পিউটার ডিভাইসের ব্যবহার আজকের তুলনায় অনেক বেশি কম ছিল। তবে, আজ প্রযুক্তি (technology) অনেক উন্নত হয়ে যাওয়ার সাথে সাথে, কম্পিউটার এবং ইন্টারনেটের ব্যবহার হাজার গুনে বেড়ে গেছে। এবং, এর সাথে সাথে বিভিন্ন রকমের আলাদা আলাদা সাইবার ক্রাইম এর প্রকার সাইবার অপরাধীরা খুঁজে বের করেছেন।

আজকের সময়ে, বিভিন্ন business বা company গুলি cyber security র ক্ষেত্রে অনেক বেশি পরিমানে টাকা খরচ করেন।

সাইবার সিকিউরিটির (cyber security) মাধ্যমে, তারা বিভিন্ন সাইবার ক্রাইম গুলির থেকে নিজের business বা company কে অনেক ক্ষেত্রে বাঁচিয়ে রাখতে পারেন।

তাহলে চলুন, নিচে আমরা কিছু cybercrime এর প্রকারের বিষয়ে জেনেনেই।

৮ টি অধিক বেশি পরিমানে হওয়া সাইবার ক্রাইমের প্রকার

নিচে বিভিন্ন রকমের সাইবার ক্রাইম এর ব্যাপারে আমি বলেছি।

১. Cyber Fraud

Cyber fraud মানে হলো এমন এক রকমের অপরাধ যেটা ইন্টারনেটে বা ইন্টারনেটের মাধ্যমে করা হয়।

এই ধরণের অপরাধের ক্ষেত্রে, অপরাধীরা লোকেদের বিভিন্ন ব্যক্তিগত (personal) তথ্য (data) যেমন, business secrets, personal photos, personal information গুলিকে চুরি, পরবর্তন বা নষ্ট (destroy) করতে পারে।

বেশিরভাগ ক্ষেত্রে, এই ধরণের সাইবার অপরাধ (cyber fraud) করা হয়, অবৈধ ভাবে লাভ (profit) আয় করার উদ্দেশ্যে।

২. Hacking

হ্যাকিং (hacking) অনেক বেশি পরিমানে হওয়া সাইবার ক্রাইম, যার বেপারে অনেক কম লোকেরাই জানেন।

হে, আমি জানি যে আপনি “hacking” বিষয়টি নিয়ে অল্প হলেও জ্ঞান রাখেন। তবে, হতে পারে আপনার কম্পিউটার, মোবাইল বা নেটওয়ার্ক ও বর্তমানে হ্যাক করা হয়েছে, কিন্তু আপনি সেটা জানেননা।হতে পারে।

হ্যাকিং এর ক্ষেত্রে, সাইবার অপরাধীরা একটি ওয়েবসাইট,

কম্পিউটার, সিস্টেম (computer) বা নেটওয়ার্ক (network) এর ফাঙ্কশনে (function), সম্পূর্ণ বা অংশিক ভাবে নিয়ন্ত্রণ (control) অর্জন করে ফেলে।

এভাবে, নিয়ন্ত্রণ অর্জন করার পর তারা সেই সিস্টেম, কম্পিউটার বা নেটওয়ার্কের ব্যবহার করে বিভিন্ন অবৈধ (illegal) কাজ করে নিতে পারেন।

তাছাড়া, হ্যাক করা ওয়েবসাইট, সিস্টেম বা নেটওয়ার্কে থাকা বিভিন্ন জরুরি ও ব্যক্তিগত তথ্য (information) জেনে নিতে পারে।

বেশিরভাগ ক্ষেত্রে, হ্যাকার (hacker) গুলি corporate এবং Government accounts ও website গুলিকে হ্যাক করা দেখা গেছে।

হ্যাকিং করার এমনিতে বিভিন্ন আলাদা আলাদা নিয়ম এবং প্রক্রিয়া রয়েছে, যেগুলির ব্যাপারে আমার এবং আপনার মতো সাধারণ লোকেদের কাছে নেই।

৩. Identity theft

Identity theft এক ধরণের একটি নির্দিষ্ট রকমের cybercrime, যেখানে ব্যাক্তির ব্যক্তিগত তথ্য চুরি করা হয়।

এই ব্যক্তিগত তথ্যের মধ্যে বেশিরভাগ ক্ষেত্রে, account passwords, ব্যাঙ্ক একাউন্ট এর তথ্য, credit ও debit card এর তথ্য এবং এই ধরণের জরুরি এবং গোপনীয় তথ্য গুলি চুরি করা হয়।

এই ধরণের অপরাধীরা আপনার একাউন্টে থাকা টাকা গুলিও চুরি করে নিতে পারে।

৪. Scamming

বিভিন্ন রকমে scamming করা যেতে পারে বা করা হয়।

যেকোনো অবৈধ মাধ্যমে টাকা আয়ের উদ্দেশ্যে একজন ব্যক্তি বা সংগঠনের দ্বারা, লোকেদের ঠকানোকে স্ক্যামিং (scamming) বলা যেতে পারে।

আপনারা হয়তো নিজেদের ইমেইলে বা মোবাইলের sms বক্সে একটি মেসেজ (message) অনেক সময় দেখেছেন, যেখানে বলা হয় যে, আপনাকে কোনো একটি কোম্পানির থেকে অনেক ভারী সংখ্যায় টাকা, লটারি (lottary) বা পুরস্কার (prize) হিসেবে দেয়া হচ্ছে।

এবং, সেই ভারী সংখ্যার টাকার জন্য আপনার একটি processing amount বা fees তাদের ব্যাঙ্ক একাউন্টে দিয়ে দিতে হবে। এবং, তারপর তারা আপনাকে সেই ভারী সংখ্যার টাকা দিয়ে দিবে।

এখন, আপনি এবং আমি জানি যে, এই ধরণের মেসেজ (sms) লোক ঠকিয়ে টাকা আয় করার জন্য পাঠানো হয়।

কিন্তু, অনেক লোক রয়েছে, যারা এই ধরণের মেসেজ গুলি সত্যি বলে ভাবেন এবং অধিক টাকার লোভে তাদেরকে সেই processing amount money বা fees দিয়ে দেন।

কিন্তু টাকা দেয়ার পর, কিছুই হয়না এবং কিছু সময় পর টাকা দেওয়া লোকেরা বুঝতে পারেন যে, তাদেরকে ঠকানো হয়েছে।

এভাবে, বিভিন্ন মাধ্যমে লোকেদের ঠকিয়ে টাকা আদায় করাকেই বলা হয় “scamming”.

অনলাইন ইন্টারনেটে এভাবে scam করে টাকা আদায় করার অনেক প্রক্রিয়া রয়েছে।

যেমন,

Charity fraud – ইন্টারনেটে বিভিন্ন ওয়েবসাইটে বা আপনার ইমেইলের বক্সে দান (charity) দেয়ার জন্য বলা হবে।

Fake price – যা আমি ওপরে বললাম, অধিক ভারী পরিমানে টাকার পুরস্কার বা লটারির লোভ দেখিয়ে ঠকানো।

Gambling fraud .

Online gift cards.

ব্যাঙ্ক লোন দেয়ার নাম দিয়ে।

Make money online scams – ইন্টারনেটে অনেক এমন ওয়েবসাইট রয়েছে, যারা আপনাকে অনলাইন টাকা আয় করার লোভ দেখিয়ে ঠকিয়ে দিবে।

Job offer scams – চাকরি দেয়ার লোভ দেখিয়ে ঠকানো।

Phishing website scam – ইন্টারনেটে বিভিন্ন ধরণের ওয়েবসাইট রয়েছে যেগুলি original নয় এবং লোক ঠকানোর উদ্দেশ্যে বিভিন্ন original website গুলির প্রতিলিপি (duplicate) তৈরি করা হয়। তাই, যেকোনো ওয়েবসাইটে গিয়ে নিজের personal information & data দেয়ার আগে বা অনলাইন পেমেন্ট করার আগে, ভালো করে যাচাই করে নিবেন।

৫. Computer virus

অনেক অপরাধীরা কম্পিউটার ভাইরাস (computer virus) এর সাহায্য নিয়ে, বিভিন্ন কম্পিউটার সিস্টেম গুলিতে ঢুকে পড়ে।

তারপর, এই ভাইরাস গুলির সাহায্যে, কম্পিউটার থেকে অবৈধ ভাবে ব্যক্তিগত এবং আর্থিক তথ্য চুরি করাটা বেশির ভাগ ক্ষেত্রে দেখা গেছে।

তাছাড়া, অনেক অভিজ্ঞতা এবং জ্ঞান থাকা programs রা কম্পিউটার সিস্টেম ও নেটওয়ার্ক গুলিতে বিভিন্ন রকমের viruses, malware এবং Trojan পাঠিয়ে, সম্পূর্ণ সিস্টেম (system) সংক্রমিত (infect) বা নষ্ট করে দিতে পারে।

বেশিরভাগ ক্ষেত্রে, এই ধরণের virus গুলি internet এবং removable device থেকে আপনার network বা computer system গুলিতে ঢুকে যেতে পারে।

৬. Ransomware

এইটা এক রকমের malware-virus attack যেখানে অপরাধীরা আপনার কম্পিউটার নেটওয়ার্কে ঢুকে সেখানে থাকা জরুরি files গুলি এনক্রিপ্ট (encrypt) করে রাখে।

মানে, আপনার জরুরি ফাইল গুলিকে কিছু কোড (code) ব্যবহার করে লক (lock) করে রাখা হয়। ফলে, আপনি আপনার সিস্টেমে থাকা জরুরি files গুলি আর খুলতে পারেননা। এই ধরণের ransomware attack করে file ও system লক করার পর, অপরাধীরা ব্যাক্তির কাছে কিছু টাকার চাহিদা করেন। টাকা দিয়ে দেওয়ার পর, lock করা file বা system গুলি আবার খুলে দেয়া হয়।

৭. Phishing

Phishing এক ধরণের সাইবার অপরাধ, যেখানে অপরাধীরা

একটি বৈধ কোম্পানি বা organization হিসেবে নিজেকে দেখানোর চেষ্টা করে।

এই ধরণের প্রক্রিয়া ব্যবহার করে অপরাধীরা, আপনার personal data & information, আর্থিক তথ্য, bank details এবং credit & debit card details নিয়ে নিতে পারে।

এই প্রক্রিয়াতে, বেশিরভাগ ক্ষেত্রে আপনাকে হাজার হাজার ইমেইল (email) পাঠানো হয়, যেখানে অনেক নকল (fake) ওয়েবসাইটের লিংক দেয়া থাকে। এবং, আপনাকে এভাবে সাজিয়ে ইমেইল করা হবে, আপনি ভাববেন যে ইমেইল কোনো আসল ওয়েবসাইট বা কোম্পানির থেকে পাঠানো হয়েছে। ফলে, অনেক সহজে যেকোনো ব্যাক্তি এই সাইবার ক্রাইম এর শিকার হয়ে যায় এবং তারা তাদের গোপনীয় তথ্য দিয়ে দেয়।

৮. Software Piracy

ইন্টারনেটে এমন অনেক ওয়েবসাইট বা এপ্লিকেশন রয়েছে যেগুলি অবৈধ ভাবে original software বা original file গুলিকে অনলাইনে বিতরণ করে।

এভাবে original software, application, movies, videos, images, songs গুলিকে অবৈধ ভাবে অনলাইন বিতরণ করাকে বলা হয় “online piracy “.

এই ধরণের online piracy র ফলে, software company এবং developers দেড় অনেক বেশি পরিমানে আর্থিক ক্ষতির অভিমুখ হতে হয়।

কারণ, তাদের content, software বা movies ইন্টারনেটের মাধ্যমে লোকেরা ফ্রীতেই কোনো অফিসিয়াল অনুমতি ছাড়া ডাউনলোড করে ব্যবহার করছেন।

Original software বা অন্য যেকোনো original file এভাবে অবৈধ ভাবে বিতরণ করাটা যেরকম একটি অপরাধ, ঠিক সেভাবেই pirated software বা pirated files ব্যবহার করাটাও কিন্তু একটি অপরাধ।

তাই, ইন্টারনেট থেকে কোনো রকমের pirated software বা file ডাউনলোড ও ব্যবহার করবেননা।

কেবল, official website থেকে তাদের অনুমতি নিয়েই যেকোনো ফাইল ডাউনলোড ও ব্যবহার করার পরামর্শ আমি আপনাদের দিবো।

সাইবার সিকিউরিটি কি ? (What Is Cyber Security in Bangla)

সাইবার সিকিউরিটি (cybersecurity) মানে হলো এমন একটি প্রক্রিয়া, যেখানে বিভিন্ন আধুনিক প্রযুক্তির (technology) মাধ্যম, প্রক্রিয়া (process) এবং চর্চার ব্যবহার করে, computer device, data, network এবং program গুলিকে cyber attack, cybercrime এবং অবৈধ ব্যবহার থেকে সুরক্ষিত করে রাখা হয়।

সোজা ভাবে বললে, computer, device বা network গুলিকে cybercrime থেকে বাঁচিয়ে রাখার প্রক্রিয়াটিকেই বলা হয় সাইবার সিকিউরিটি।

Cybersecurity কে computer security এবং

information technology security (IT Security) বলেও বলা যেতে পারে।

সাইবার সিকিউরিটির প্রক্রিয়ার ব্যবহার করে কম্পিউটার বা নেটওয়ার্ক গুলিতে এতো করা ভাবে সুরক্ষা দিয়ে রাখা হয় যে বাইরের সাইবার অপরাধীরা সেই সিস্টেম (system) বা নেটওয়ার্কে (network) সহজে প্রবেশ করতে পারেনা।

Cyber security র সেবা প্রদান করা অনেক ভালো ভালো কোম্পানি বা organization রয়েছে, যারা কিছু টাকা নিয়ে অন্যান্য কোম্পানি বা organization গুলির computer ও network গুলিকে নিরাপত্তা প্রদান করে যেকোনো ধরণের সাইবার ক্রাইম বা cyber attack থেকে।

তাহলে বুঝলেনতো, “সাইবার সিকিউরিটি মানে কি“.

নিজেকে সাইবার ক্রাইম থেকে কিভাবে বাঁচিয়ে রাখবেন ?

সাইবার ফ্রড (cyber fraud), যেকোনো ব্যাক্তির সাথেই হতে পারে।

বেশিরভাগ ক্ষেত্রে, আমার এবং আপনার মতো সাধারণ জনসাধারণের সাথে অনেক রকমের online fraud বা scamming করার চেষ্টা করা হয়।

তাছাড়া, ইন্টারনেট এবং অনলাইন প্রযুক্তির ব্যবহার ও উন্নয়ন যতটা বেশি হচ্ছে, ততটাই বেশি পরিমানে এই ধরণের সাইবার ক্রাইমের ভয় ও বেড়ে যাচ্ছে।

তাই, নিচে আমি এমন কিছু টিপস বা সমাধান দিব, যেগুলি মেনে চললে, ইন্টারনেটের মাধ্যমে হওয়া সাইবার ক্রাইম গুলির থেকে নিজেকে অনেক ক্ষেত্রে বাঁচিয়ে রাখতে পারবেন।

Tips to protect yourself from cybercrime

নিজের কম্পিউটার ডিভাইস এবং নেটওয়ার্ক গুলিকে সাইবার ক্রাইম থেকে সম্পূর্ণ ভাবে সুরক্ষতি করে রাখার তেমন কোনো শক্ত এবং দ্রুত নিয়ম (hard & fast rules) থাকতে পারেনা।

তবে হে, নিচে দেয়া টিপস বা পরামর্শ গুলি মেনে চললে, আপনি আপনার কম্পিউটার ডিভাইস ও নেটওয়ার্ক গুলিকে যুক্তিসঙ্গতভাবে নিরাপদ করে রাখতে পারবেন।

নিজের কম্পিউটার ও মোবাইলে কেবল genuine বা original software এবং application ইনস্টল করবেন।

ইন্টারনেটে কোনো ধরণের অবিস্বস্ত ওয়েবসাইট থেকে কোনো রকমের ফাইল ডাউনলোড করবেননা।

যদি আপনি একটি android mobile ব্যবহার করছেন, তাহলে কেবল Google play store থেকেই apps download করবেন।

অবিস্বস্ত ওয়েবসাইট, apps এবং social profile গুলিতে নিজের mobile number এবং কোনো ধরণের তথ্য দিবেননা।

আপনার ইমেইল একাউন্টে আশা যেকোনো রকমের পুরস্কার, উপহার বা লটারির ইমেইল গুলিকে সাথে সাথে ডিলিট করে দিবেন। এই ধরণের ইমেইল আপনাকে লোভ দেখিয়ে ঠকানোর

জন্য পাঠানো হয়।

অপ্রয়োজনীয় এবং অবিস্বস্ত application মোবাইলে ইনস্টল করবেননা। অনেক অবিস্বস্ত apps রয়েছে যেগুলি আপনার মোবাইলের file manager, camera, sms inbox, location এবং আরো অন্যান্য তথ্য আপনার অনুমতি ছাড়া গ্রহণ করতে পারে।

নিজের মোবাইল বা কম্পিউটার অন্য ব্যাক্তিকে ব্যবহার করতে দিলে, আপনি অবশই চোখ রাখবেন। অনেক বেশি সময়ের জন্য আপনার device কাওকে ব্যবহার করতে দিবেননা।

আমরা যখন ঘরের বাইরে থাকি, তখন যেকোনো জায়গায় open wifi connection পেয়েগেলে অনেক খুশি হয়ে যাই। কিন্তু সাবধান, এই ধরণের password ছাড়া wifi connection বেশিরভাগ ক্ষেত্রে হ্যাকিং (hacking) এর উদ্দেশ্যে open রাখা হয়। আপনি সেই open wifi নেটওয়ার্কে connect করার সাথে সাথে আপনার ডিভাইস হ্যাক হয়ে যেতে পারে।

যেকোনো computer cafe, office computer বা public কম্পিউটার থেকে online banking বা banking transactions করবেননা।

নিজের মোবাইল বা কম্পিউটার থেকে banking transaction করার পর, online banking passwords বা debit

card details কখনো সেভ (save) করে রাখবেননা।

নিজের পুরোনো কম্পিউটার বা মোবাইল বিক্রি করার আগে অবশই সম্পূর্ণ ডিভাইস ফরম্যাট (format) করে নিবেন। এতে, আপনার ব্যক্তিগত সব ধরণের তথ্য ডিলিট হয়ে যাবে।

মোবাইলে ডাউনলোড করা প্রায় ৯০% এপস আপনার gallery বা file manager এ প্রবেশ করার অনুমতি চায়। এবং, আমরা সকলে কিছু না ভেবেই সেই এপস গুলিকে অনুমতি দিয়ে দেই। তাই, নিজের মোবাইলে কোনো রকমের ব্যক্তিগত ছবি (personal pictures) রাখবেননা।

নিজের কম্পিউটার এবং wifi connection গুলিতে পাসওয়ার্ড অবশই দিয়ে রাখবেন।

ব্যক্তিগত ফাইল এবং ছবি গুলিকে একটি external hard drive এ রাখার চেষ্টা করুন। এবং external hard drive পাসওয়ার্ড দিয়ে লক করে রাখুন।

নিজের কম্পিউটারে অরিজিনাল OS (operating system) তাদের অফিসিয়াল ওয়েবসাইট থেকে ডাউনলোড করে ব্যবহার করবেন।

নিজের social media account password, email account password এবং online banking password সময়ে সময়ে পরিবর্তন করতে থাকবেন।

কম্পিউটার এবং মোবাইলে একটি ভালো antivirus এবং internet protector সফ্টওয়ার অবশই ব্যবহার করবেন।

ইন্টারনেট মানে কি ? কিভাবে কাজ করে

তাহলে বন্ধুরা, ওপরে আমি বলা নিয়ম গুলি মেনে চললে, আপনি নিজেকে সাইবার ক্রাইমের শিকার হওয়ার থেকে বাঁচিয়ে রাখতে পারবেন।

মনে রাখবেন, ইন্টারনেট মানে হলো একটি নেটওয়ার্ক (network) এবং এই নেটওয়ার্ক বিশ্বের হাজার কোটি কম্পিউটারের সাথে সংযুক্ত হয়ে রয়েছে।

তাই, যখন আপনিও আপনার মোবাইল অথবা কম্পিউটারে ইন্টারনেট ব্যবহার করেন, তখন সেই হাজার কোটি কম্পিউটারের সাথে সংযুক্ত হয়ে যান।

এবং, যদি আপনি কিছু জরুরি সতর্কতা মেনে না চলেন, তাহলে কিছু অবৈধ প্রক্রিয়া বা প্রযুক্তির ব্যবহার করে সাইবার অপরাধীরা আপনার কম্পিউটারে এই ইন্টারনেট নেটওয়ার্কের মাধ্যমে প্রবেশ করতে পারে।

শেষ কথা,

আজকের এই ইন্টারনেটের যুগে সাইবার ক্রাইম এবং এর থেকে নিরাপদ থাকার বিষয় গুলি নিয়ে আমাদের প্রত্যেকের অল্প হলেও মন দেয়া উচিত। ইন্টারনেটে এবং কম্পিউটার ডিভাইস এর মাধ্যমে কখন কে কাকে ঠকিয়ে দিতে পারে, তার ধারণাও আপনি করতে পারবেননা।

তাই, এই আর্টিকেলে আমি আপনাদের সম্পূর্ণ ভাবে বুঝিয়ে বলেছি যে, "সাইবার ক্রাইম কি" (What is cyber crime), "সাইবার ক্রাইম এর বিভিন্ন প্রকার গুলি কি কি", "সাইবার সিকিউরিটি কাকে বলে" এবং শেষে "নিজেকে সাইবার ক্রাইম থেকে নিরাপদ রাখার কিছু উপায় ও পরামর্শ".

আশা করছি আমার এই আর্টিকেল আপনাদের প্রচুর কাজে আসবে।

যে কোন প্রকার সাইবার ক্রাইম যথাযথ কর্তৃপক্ষকে জানানোর পদ্ধতি, যোগাযোগের ঠিকানা, মোবাইল নম্বর

সাইবার ক্রাইম কী?

কম্পিউটার, নেটওয়ার্ক বা অনলাইন প্ল্যাটফর্ম ব্যবহার করে বেআইনীভাবে করা অপরাধকে সাইবার ক্রাইম বলা হয়।

ধরুন, আপনি বা আপনার পরিচিত কেউ সাইবার ক্রাইমের শিকার হলেন। এখন আপনি অপরাধীর বিরুদ্ধে ব্যবস্থা নিতে চাচ্ছেন। কিন্তু কীভাবে নিবেন? আমাদের দেশে সাইবার অপরাধের শিকার বেশিরভাগ ভিক্টিমই অপরাধীদের আইনের আওতায় আনে না বা আনতে পারে না। নারী-পুরুষ উভয়েরই সাইবার সিকিউরিটি আইন সম্পর্কে জানাশোনা কম থাকায় এবং আইনের সহযোগিতা নেবার মাধ্যম না জানায় অভিযোগ করছে না বেশিরভাগই। ফলে অপরাধীরা পার পেয়ে যায় এবং নতুন করে এ ধরনের অপরাধ করতে উদ্বুদ্ধ হয়। তাই এর প্রতিকারে অপরাধ সংঘটনের পর এ বিষয়ে যথাযথ কর্তৃপক্ষের কাছে অভিযোগ জানানো দরকার। চলুন দেখা যাক, কেউ অপরাধের শিকার হলে কীভাবে যথাযথ কর্তৃপক্ষের কাছে অভিযোগ জানাতে পারবেন।

কোথায় অভিযোগ করবেন?

অভিযোগ জানানোর জন্য নিম্নোক্ত উপায়ে পুলিশের সঙ্গে যোগাযোগ করতে পারবেন –

প্রাথমিকভাবে আপনার নিকটস্থ থানায় অভিযোগ করতে পারেন।

'Police Cyber Support for Women PCSW' নামক ফেসবুক পেইজে (https://www.facebook.com/PCSW.PHQ) মেসেজ দিয়ে অভিযোগ জানাতে পারেন।

cybersupport.women@police.gov.bd বা cyberhelp@dmp.gov.bd - এই দুইটি ঠিকানায় ইমেইল পাঠিয়ে যোগাযোগ করতে পারেন।

পুলিশ সদর দফতরের ০১৩২০০০০৮৮৮ নম্বরে ফোন করে অভিযোগ জানাতে পারেন।

হটলাইন নম্বর ৯৯৯ এ ফোন করেও অভিযোগ করা যাবে।

সরাসরি কথা বলার প্রয়োজনবোধ করলে চলে আসতে পারেন ডিএমপি-র কাউন্টার টেরোরিজম ডিভিশনের Cyber Crime Unit অফিসে। কথা বলতে পারেন দায়িত্বরত কর্মকর্তার সাথে এই নাম্বারে - ০১৭৬৯৬৯১৫২২। ঠিকানা : ঢাকা মেট্রোপলিটন পুলিশ

হেডকোয়ার্টার্স, ৩৬, শহীদ ক্যাপ্টেন মনসুর আলী স্মরণী, রমনা, ঢাকা - ১০০০।

কিভাবে অভিযোগ করবেন?

সাইবার অপরাধের শিকার হলে যত দ্রুত সম্ভব অভিযোগ জানানো উচিত। অভিযোগ জানানোর জন্য নিম্নের প্রক্রিয়া অনুসরণ করতে পারেন -

অভিযোগ করার ক্ষেত্রে আপনার অভিযোগের স্বপক্ষে কিছু প্রমাণাদি প্রয়োজন। যেমন - সংশ্লিষ্ট আলামতের স্ক্রীনশট, লিংক, অডিও/ভিডিও ফাইল অথবা রিলেটেড ডকুমেন্টস।

স্ক্রীনশট সংগ্রহের ক্ষেত্রে খেয়াল রাখতে হবে যেন Address Bar - এর URL টি দৃশ্যমান হয়।

ই-মেইল এর মাধ্যমে অভিযোগ জানাতে চাইলে এসব প্রমাণাদি সংযুক্ত (অ্যাটাচ) করে আপলোড করতে পারেন।

প্রয়োজনে Cyber Crime Unit - এর অফিসারদের নিকট থেকে প্রয়োজনীয় পরামর্শ গ্রহণ করতে পারেন যা আপনার আইনগত ব্যবস্থা গ্রহণের সহায়ক হতে পারে।

সাইবার নিরাপত্তার গুরুত্বে সরকারি ২৯টি প্রতিষ্ঠানকে সিআইআই ঘোষণা

সাইবার নিরাপত্তার গুরুত্ব বিবেচনায় সরকারি ২৯টি প্রতিষ্ঠানকে জনগুরুত্বপূর্ণ তথ্য পরিকাঠামো (ক্রিটিকাল ইনফরমেশন ইনফ্রাস্ট্রাকচার) বা সিআইআই হিসেবে ঘোষণা করা হয়েছে।

ডিজিটাল নিরাপত্তা আইনের বিধান অনুযায়ী এসব প্রতিষ্ঠানের তালিকা করা হয়েছে। সরকারের তথ্য ও যোগাযোগ প্রযুক্তি বিভাগ সম্প্রতি এ সংক্রান্ত প্রজ্ঞাপন জারি করেছে। উপসচিব সুফিয়া আক্তার রুমি সই করা প্রজ্ঞাপনটি রবিবার (৩ অক্টোবর) গেজেট আকারে প্রকাশিত হয়।

সিআইআই ঘোষিত প্রতিষ্ঠানগুলো হলো- রাষ্ট্রপতির কার্যালয়, প্রধানমন্ত্রীর কার্যালয়, বাংলাদেশ ব্যাংক, জাতীয় রাজস্ব বোর্ড, বাংলাদেশ ডাটা সেন্টার কোম্পানি লিমিটেড, সেতু বিভাগ, ইমিগ্রেশন ও পাসপোর্ট অধিদফতর, জাতীয় ডাটা সেন্টার, বাংলাদেশ কম্পিউটার কাউন্সিল, বাংলাদেশ টেলিযোগাযোগ নিয়ন্ত্রণ কমিশন, জাতীয় পরিচয় নিবন্ধন অনুবিভাগ, নির্বাচন কমিশন সচিবালয়, সেন্ট্রাল প্রকিউরমেন্ট টেকনিক্যাল ইউনিট, সোনালী

ব্যাংক লিমিটেড, অগ্রণী ব্যাংক লিমিটেড, জনতা ব্যাংক লিমিটেড, রূপালী ব্যাংক লিমিটেড, রূপপুর পারমাণবিক বিদ্যুৎ কেন্দ্র স্থাপন প্রকল্প, বিমান বাংলাদেশ এয়ারলাইন্স, ইমিগ্রেশন-বাংলাদেশ পুলিশ, বাংলাদেশ টেলিকমিউনিকেশন কোম্পানি লিমিটেড (বিটিসিএল), বাংলাদেশ বিদ্যুৎ উন্নয়ন বোর্ড, পাওয়ার গ্রিড কোম্পানি অব বাংলাদেশ, তিতাস গ্যাস ট্রান্সমিশন অ্যান্ড ডিস্ট্রিবিউশন কোম্পানি লিমিটেড, সেন্ট্রাল ডিপজিটরি বাংলাদেশ লিমিটেড, বঙ্গবন্ধু স্যাটেলাইট কোম্পানি লিমিটেড, বাংলাদেশ সিকিউরিটিজ অ্যান্ড এক্সচেঞ্জ কমিশন, সিভিল এভিয়েশন অথোরিটি বাংলাদেশ, রেজিস্ট্রার জেনারেলের কার্যালয়, জন্ম ও মৃত্যু নিবন্ধন, ঢাকা স্টক এক্সচেঞ্জ লিমিটেড এবং চট্টগ্রাম স্টক এক্সচেঞ্জ।

ডিজিটাল নিরাপত্তা আইন-২০১৮-এর ১৫ ধারার বিধান মতে এসব সরকারি প্রতিষ্ঠানকে সিআইআই ঘোষণা করা হয়। আইনের ওই ধারায় বলা আছে, এই আইনের উদ্দেশ্য পূরণকল্পে সরকার সরকারি গেজেটে প্রজ্ঞাপন দ্বারা কোনও কম্পিউটার সিস্টেম, নেটওয়ার্ক বা তথ্য পরিকাঠামোকে গুরুত্বপূর্ণ তথ্য পরিকাঠামো হিসাবে ঘোষণা করতে পারবে।

০৩ অক্টোবর ২০২২, ২০:০৭

রেজিস্টার্ড নং ডি এ-১

বাংলাদেশ গেজেট

অতিরিক্ত সংখ্যা

কর্তৃপক্ষ কর্তৃক প্রকাশিত

রবিবার, অক্টোবর ২, ২০২২

গণপ্রজাতন্ত্রী বাংলাদেশ সরকার

ডাক, টেলিযোগাযোগ ও তথ্যপ্রযুক্তি মন্ত্রণালয়

তথ্য ও যোগাযোগ প্রযুক্তি বিভাগ

পলিসি শাখা

প্রজ্ঞাপন

তারিখ : ৬ আশ্বিন ১৪২৯/২১ সেপ্টেম্বর ২০২২

নং **৫৬.০০.০০০০.০৬১.২২.০০৯.২০.১২০**—ডিজিটাল নিরাপত্তা আইন ২০১৮ এর ধারা ১৫ অনুসারে নিম্নোক্ত ২৯টি প্রতিষ্ঠানসমূহকে গুরুত্বপূর্ণ তথ্য পরিকাঠামো (Critical Information Infrastructure-CII) হিসেবে ঘোষণা করা হলো। ইহা সর্বসাধারণের জ্ঞাতার্থে প্রকাশ করা হলো।

ক্রমিক	প্রতিষ্ঠানের নাম
১	রাষ্ট্রপতির কার্যালয়
২	প্রধানমন্ত্রীর কার্যালয়
৩	বাংলাদেশ ব্যাংক
৪	জাতীয় রাজস্ব বোর্ড
৫	বাংলাদেশ ডাটা সেন্টার কোম্পানি লিমিটেড
৬	সেতু বিভাগ
৭	ইমিগ্রেশন ও পাসপোর্ট অধিদপ্তর
৮	জাতীয় ডাটা সেন্টার, বাংলাদেশ কম্পিউটার কাউন্সিল
৯	বাংলাদেশ টেলিযোগাযোগ নিয়ন্ত্রণ কমিশন
১০	জাতীয় পরিচয় নিবন্ধন অনুবিভাগ, নির্বাচন কমিশন সচিবালয়
১১	সেন্ট্রাল প্রকিউরমেন্ট টেকনিক্যাল ইউনিট

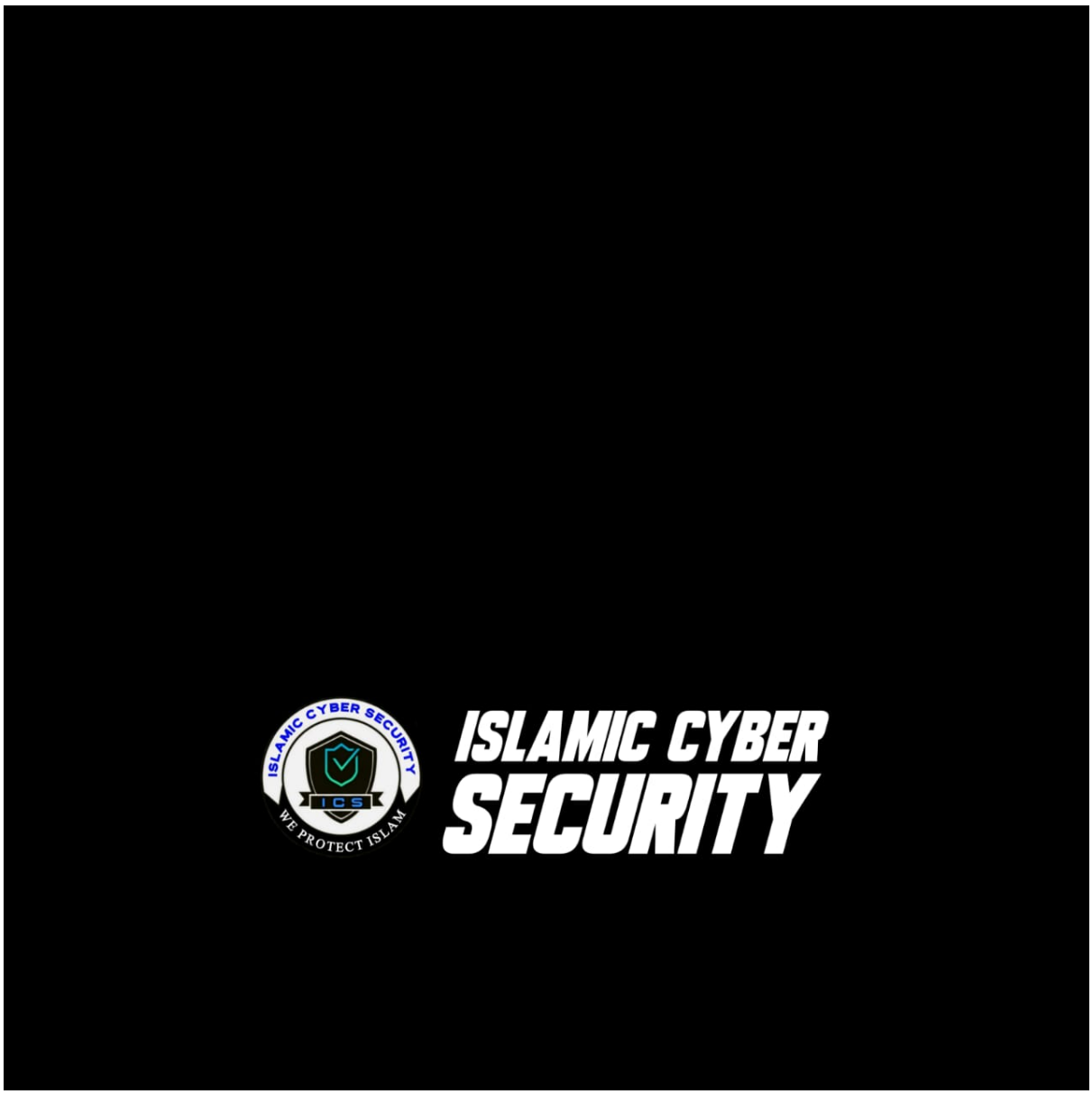
(১৫৯১৯)

মূল্য : টাকা ৪.০০

ক্রমিক	প্রতিষ্ঠানের নাম
১২	সোনালী ব্যাংক লিমিটেড
১৩	অগ্রণী ব্যাংক লিমিটেড
১৪	জনতা ব্যাংক লিমিটেড
১৫	রূপালী ব্যাংক লিমিটেড
১৬	রূপপুর পারমাণবিক বিদ্যুৎ কেন্দ্র স্থাপন প্রকল্প
১৭	বিমান বাংলাদেশ এয়ারলাইন্স
১৮	ইমিগ্রেশন, বাংলাদেশ পুলিশ
১৯	বাংলাদেশ টেলিকমিউনিকেশন কোম্পানি লিমিটেড (BTCL)
২০	বাংলাদেশ বিদ্যুৎ উন্নয়ন বোর্ড
২১	পাওয়ার গ্রীড কোম্পানী অব বাংলাদেশ
২২	তিতাস গ্যাস ট্রান্সমিশন এন্ড ডিস্ট্রিবিউশন কোম্পানী লিমিটেড
২৩	সেন্ট্রাল ডিপজিটরি বাংলাদেশ লিমিটেড
২৪	বঙ্গবন্ধু স্যাটেলাইট কোম্পানী লিমিটেড
২৫	বাংলাদেশ সিকিউরিটিজ অ্যান্ড এক্সচেঞ্জ কমিশন
২৬	সিভিল এভিয়েশন অথোরিটি বাংলাদেশ
২৭	রেজিস্ট্রার জেনারেলের কার্যালয়, জন্ম ও মৃত্যু নিবন্ধন
২৮	ঢাকা স্টক এক্সচেঞ্জ লিমিটেড
২৯	চট্টগ্রাম স্টক এক্সচেঞ্জ

রাষ্ট্রপতির আদেশক্রমে

সুফিয়া আক্তার রুমী
উপসচিব (অতিরিক্ত দায়িত্ব)।


ISLAMIC CYBER SECURITY
ICS
WE PROTECT ISLAM
ISLAMIC CYBER
SECURITY