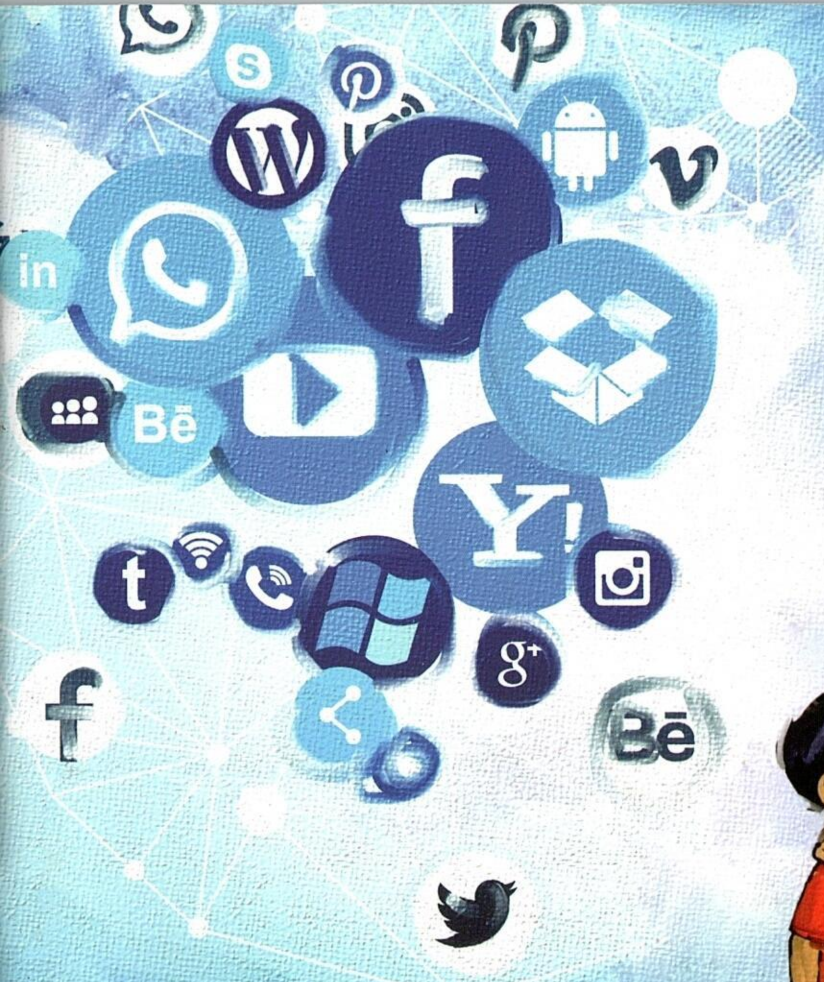
ICT DIVISION
FUTURE IS HERE

ডিজিটাল নিরাপত্তা ও সচেতনতা



ইলেক্ট্রনিক স্বাক্ষর সার্টিফিকেট প্রদানকারী কর্তৃপক্ষের নিয়ন্ত্রক (সিসিএ)-এর কার্যালয়

তথ্য ও যোগাযোগ প্রযুক্তি বিভাগ

ডিজিটাল নিরাপত্তা ও সচেতনতা

সার্বিক নির্দেশনায়
জনাব আবু সাঈদ চৌধুরী
নিয়ন্ত্রক, সিসিএ কার্যালয়

সম্পাদনায়
জনাব হাসিনা বেগম, উপ-নিয়ন্ত্রক (সাবেক)
জনাব শাহিনা পারভীন, উপ-নিয়ন্ত্রক
ড. নাজমা আক্তার, সহকারী নিয়ন্ত্রক
জনাব তানজিলা মেহেনাজ, সহকারী নিয়ন্ত্রক
জনাব নাজনীন আক্তার, সহকারী প্রকৌশলী
জনাব মোঃ খালেদ হোসেন চৌধুরী, আইন কর্মকর্তা
জনাব শামীম আহমেদ ভূঁইয়া, তদন্ত কর্মকর্তা
জনাব মনিরা খাতুন, তদন্ত কর্মকর্তা
জনাব মোঃ বনিআমিন, তদন্ত কর্মকর্তা
জনাব কাজী শোয়েব মোহাম্মদ, সহকারী প্রোগ্রামার
জনাব মোঃ হাসান মুনছুর, সহকারী প্রোগ্রামার
জনাব ফাতেমা খাতুন, সহকারী নিয়ন্ত্রক

প্রকাশনায়
ইলেক্ট্রনিক স্বাক্ষর সার্টিফিকেট প্রদানকারী কর্তৃপক্ষের নিয়ন্ত্রক (সিসিএ)-এর কার্যালয়
প্রথম প্রকাশ: এপ্রিল, ২০১৮
প্রথম সংস্করণ: ডিসেম্বর, ২০২২

প্রচ্ছদ ও অলংকরণ: রাশিদুল হাসান

মুদ্রণ: ঢাকা ট্রেড ইন্টারন্যাশনাল, মোবাইল: ০১৭১১ ২০৪৬২০

কৃতজ্ঞতা স্বীকার

এই নির্দেশিকাটির প্রথম সংস্করণ প্রকাশের ক্ষেত্রে ইলেক্ট্রনিক স্বাক্ষর সার্টিফিকেট প্রদানকারী কর্তৃপক্ষের নিয়ন্ত্রক (সিসিএ)-এর কার্যালয়ের যে সকল কর্মকর্তা সহযোগিতা করেছেন, তাদের সবার প্রতি আমার আন্তরিক কৃতজ্ঞতা। এছাড়া এ নির্দেশিকাটি প্রণয়নে যারা শুরু থেকে শেষ পর্যন্ত সম্পৃক্ত থেকে নিরলসভাবে কাজ করেছেন তাদেরকে সিসিএ কার্যালয়ের পক্ষ থেকে ধন্যবাদ জানাচ্ছি।

নিয়ন্ত্রক
সিসিএ কার্যালয়

সূচী

ভূমিকা ০৪

উদ্দেশ্য ০৬

অনলাইনের সঙ্গে যুক্ত ছাত্র-ছাত্রীরা কীভাবে উপকৃত হচ্ছে ০৭

অনলাইনের সঙ্গে যুক্ত না থাকা ছাত্র-ছাত্রীরা কীভাবে পিছিয়ে পড়ছে ০৮

ডিজিটাল অপরাধ কী ০৯

ডিজিটাল অপরাধ সংঘটনের কারণ ১০

ডিজিটাল অপরাধ কীভাবে সংঘটিত হচ্ছে ১১

কারা ডিজিটাল অপরাধের শিকার হতে পারে ১২

বাংলাদেশে কিশোর-কিশোরীরা উল্লেখযোগ্য যেসব সাইবার অপরাধের শিকার হয় ১৩

কেস স্টাডি ১৪

ডিজিটাল অপরাধের শিকার হলে করণীয় ১৮

অনলাইন নির্যাতন কী ১৯

অনলাইনে নির্যাতনের ধরণ ২০

অনলাইনে নির্যাতনের মাধ্যমগুলো কী কী ২২

কারা এবং কীভাবে অনলাইনে নির্যাতন করে ২৩

অনলাইন নির্যাতনের শিকার হলে কেন শেয়ারিং প্রয়োজন ২৪

অনলাইনে হয়রানি/নির্যাতন থেকে সুরক্ষার উপায় কী ২৫

সামাজিক ট্যাবো বা ভ্রান্ত ধারণা ২৭

ডিজিটাল স্বাক্ষর সম্পর্কিত তথ্য ২৮

ডিজিটাল স্বাক্ষর ব্যবহারের সুবিধা ২৯

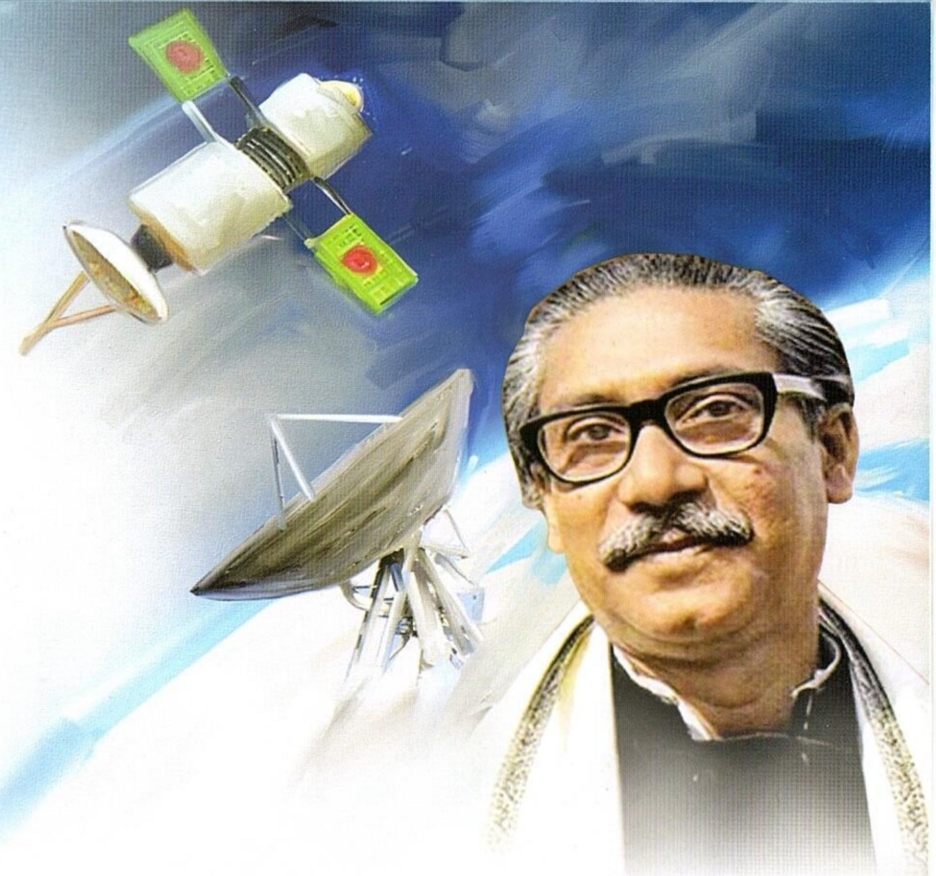
ভূমিকা

সময়ের পরিবর্তনের মধ্য দিয়ে দেশ এগিয়ে চলেছে। দেশে আজ তথ্যপ্রযুক্তির যে বিকাশ ঘটেছে তা একদিনের ইতিহাস নয়। এর পেছনের ইতিহাস দেশের বয়সের প্রায় সমান। জাতির জনক বঙ্গবন্ধু শেখ মুজিবুর রহমান তথ্যপ্রযুক্তির গোড়াপত্তন করেন ১৯৭৫ সালে বেতবুনিয়া ভূ-উপগ্রহ কেন্দ্রটি স্থাপনের মধ্য দিয়ে। এই ভূ-উপগ্রহের মাধ্যমে বিনা তারে সারাবিশ্বের সঙ্গে যোগাযোগ স্থাপিত হয়।

জাতির জনক বঙ্গবন্ধু শেখ মুজিবুর রহমানের আজীবন স্বপ্ন ছিল সুখী-সমৃদ্ধ সোনার বাংলা প্রতিষ্ঠা করা। এ স্বপ্ন পূরণে তথ্য ও যোগাযোগ প্রযুক্তির সর্বাধিক ব্যবহারের মাধ্যমে কৃষক, শ্রমিক ও মেহনতি মানুষকে সমৃদ্ধ করতে সরকার কাজ করছে। এরই অংশ হিসেবে তথ্য-প্রযুক্তির নিরাপদ ব্যবহার ও এর আইনগত বৈধতা নির্ধারণ, অপরাধ ও অপরাধী সনাক্তকরণে ইলেক্ট্রনিক স্বাক্ষর সার্টিফিকেট প্রদানকারী কর্তৃপক্ষের নিয়ন্ত্রক (সিসিএ) এর কার্যালয় নিরলসভাবে কাজ করে যাচ্ছে।

তথ্য ও যোগাযোগ প্রযুক্তির সহজলভ্যতার সুবাদে আজ পুরো বিশ্বের মানুষ খুব সহজেই একে অন্যের সঙ্গে সম্পৃক্ত হতে পারছে। বাংলাদেশের অধিকাংশ মানুষ এখন ইন্টারনেট ব্যবহার করছে।

বর্তমানে আমাদের দেশের মোট জনসংখ্যার প্রায় অর্ধেকই হচ্ছে শিশু ও কিশোর। শিশু ও কিশোর-কিশোরীদের মধ্যে সামাজিক যোগাযোগ মাধ্যম যেমন ইউটিউব, ফেসবুক, হোয়াটসঅ্যাপ, ইমো, ইন্সটাগ্রামসহ নানা চ্যাটিং সাইটগুলো আমাদের দেশে বেশ জনপ্রিয়। প্রতিমুহূর্তে কোথায় কী ঘটছে তার সচিত্র তথ্য শেয়ার হয়ে যাচ্ছে ফেসবুকে, পৌঁছে যাচ্ছে লক্ষ লক্ষ মানুষের কাছে। এসব মাধ্যম ব্যবহারের ফলে পরিচিত-অপরিচিত, বন্ধু থেকে শুরু করে আত্মীয়-স্বজনের গন্ডি পেরিয়ে সবাই একে অপরের খুব কাছাকাছি চলে আসতে পারছে। ভার্চুয়াল এই জগতে মনের ভাব প্রকাশের পাশাপাশি চিন্তা-চেতনা ও জ্ঞান-বিজ্ঞানের নানাদিকে বিচরণ করছে।



ইন্টারনেট হচ্ছে তথ্য ও নানামুখী জ্ঞানের ভান্ডার। ইন্টারনেটের কল্যাণে পুরো বিশ্ব আজ একই সূত্রে গাঁথা। বিশ্বের যে প্রান্তেই থাকুক না কেন কোথায় কী ঘটছে তা মুহূর্তের মধ্যে সবার হাতের মুঠোয় পৌছে যাচ্ছে। এক ক্লিকের মাধ্যমে নানা তথ্য আমাদের সামনে ভেসে উঠছে। ইন্টারনেট আমাদের জন্য খুলে দিচ্ছে নানা সম্ভাবনার দুয়ার। কিন্তু একই সঙ্গে এটাও সত্য যে, ইন্টারনেটের ব্যবহার অনেক সময় বিপদজনক হয়ে উঠতে পারে; বিশেষ করে অপ্রাপ্তবয়স্ক ও মেয়েদের জন্য। এসব বিষয় মাথায় রেখেই সিসিএ কার্যালয় ২০১৭ সাল থেকে এ পর্যন্ত সারাদেশে স্কুল ও কলেজগামী ৯৫,৫৫১ জন কিশোরী ছাত্রীকে হাতে-কলমে ডিজিটাল নিরাপত্তা বিষয়ে প্রশিক্ষণ প্রদান করেছে। তন্মধ্যে কোভিডকালে অনলাইনের মাধ্যমে জুম প্লাটফর্ম ব্যবহার করে ৮ টি বিভাগের ৬৪ টি জেলায় ১৪৮৩ টি বালিকা বিদ্যালয় ও মহিলা মাদ্রাসার ৫০,১৪৪ জন শিক্ষার্থীকে এই প্রশিক্ষণের আওতায় আনা হয়েছে। দেশ-বিদেশে এটি ব্যাপক প্রশংসা অর্জনসহ আন্তর্জাতিক গণমাধ্যমের শিরোনাম হয়েছে। এরই ধারাবাহিকতায় পর্যায়ক্রমে সারাদেশের স্কুল ও কলেজগামী ছাত্র-ছাত্রীদেরকে হাতে-কলমে ডিজিটাল নিরাপত্তা বিষয়ে প্রশিক্ষণ দেয়ার উদ্যোগ নেয়া হয়েছে। আশা করা যায়, এই পুস্তিকাটি স্কুল ও কলেজগামী ছাত্র-ছাত্রীদেরকে ডিজিটাল নিরাপত্তা বিষয়ে সচেতন করতে অত্যন্ত গুরুত্বপূর্ণ ভূমিকা পালন করবে।

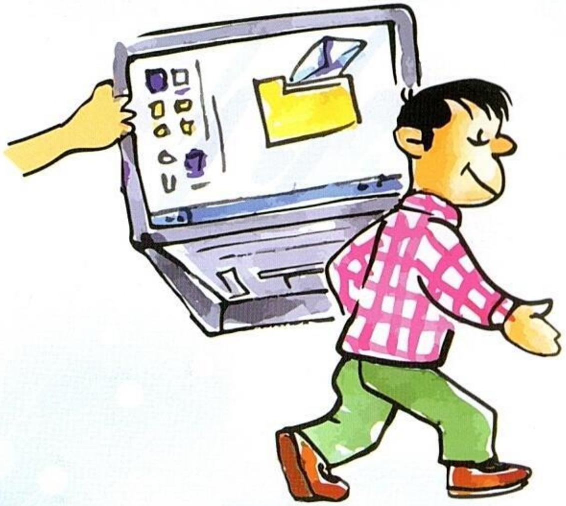
উদ্দেশ্য

- নিরাপদ ইন্টারনেট ব্যবহার সম্পর্কে সচেতনতা বৃদ্ধি করা।
- ইন্টারনেট ব্যবহারের সুফল সম্পর্কে অবগত করা।
- ইন্টারনেট ব্যবহারের নেতিবাচক দিকসমূহ চিহ্নিত করা।
- সচেতনতা বৃদ্ধির মাধ্যমে ইন্টারনেটে নির্যাতনের হার হ্রাস করা।
- ডিজিটাল স্বাক্ষর সম্পর্কে অবগত করা।
- অনলাইনে নির্যাতন/হয়রানির শিকার হলে আইনী প্রতিকার সম্পর্কে অবহিত করা।
- অনলাইন জগতে নিরাপদে বিচরণের কৌশলসমূহ সম্পর্কে ব্যবহারকারীদের প্রাথমিক ধারণা প্রদান।

অনলাইনের সঙ্গে যুক্ত ছাত্র-ছাত্রীরা কীভাবে উপকৃত হচ্ছে

- অবাধ তথ্যের সম্ভারে বিচরণের সুযোগ পাচ্ছে।
- অন্যদের সাথে তথ্য ও ভাবের আদান-প্রদানের মাধ্যমে একে অপরকে সহযোগিতা করতে পারছে।
- বিশ্বের কখন কোথায়, কী ঘটছে সে সম্পর্কে সর্বশেষ তথ্য পাচ্ছে এবং সে বিষয়ে নিজে বিচার-বিশ্লেষণ করতে পারছে।
- নিজের চিন্তা, জ্ঞানের পরিধি, সৃজনশীলতা বৃদ্ধির জন্য প্রয়োজনীয় তথ্য-উপাত্ত সংগ্রহ করতে পারছে।
- ইউটিউব, ভিডিও টিউটোরিয়ালের মাধ্যমে বাস্তব জ্ঞান অর্জনে সক্ষম হচ্ছে।
- বিভিন্ন দেশ, সংস্কৃতি ও বৈচিত্র্য সর্ম্পকে জানতে পারছে যা তার চিন্তা-চেতনার গভীরতা বৃদ্ধিতে সহযোগিতা করছে।
- শিক্ষা উপকরণ, পাঠ্য বই, অনলাইন পত্রিকা, চিকিৎসা, স্বাস্থ্য, খেলাধুলা প্রভৃতি বিষয় সম্পর্কে যাবতীয় তথ্য ইন্টারনেট থেকে পাচ্ছে।
- উচ্চশিক্ষার জন্য বিভিন্ন দেশের স্কলারশীপ সম্পর্কে জানতে পারছে এবং নিজের জীবনে তা কাজে লাগাতে পারছে।
- অনলাইনের মাধ্যমে বিভিন্ন পরীক্ষার ফলাফল ছাত্র-ছাত্রীরা জানতে পারছে।
- নানা রকম ওয়েবসাইট ডিজাইনের জন্য ডিজাইন ও টেমপ্লেট ডাউনলোড করতে পারছে।
- ফেসবুক, ইন্সটাগ্রাম, টুইটার প্রভৃতির মাধ্যমে সামাজিক যোগাযোগ মাধ্যমে যুক্ত হয়ে আত্মীয় ও বন্ধুদের সাথে তথ্য, ছবি ও ভাবের আদান-প্রদান করতে পারছে।
- অনলাইনের মাধ্যমে তথ্য সংগ্রহ করে ছাত্র-ছাত্রীরা তাদের পড়াশোনার প্রস্তুতি ও এসাইনমেন্টের কাজ ভালোভাবে সম্পন্ন করতে পারছে।
- বৈশ্বিক তথ্য প্রযুক্তির সাথে সম্পৃক্ত হয়ে স্মার্ট সিটিজেন হিসেবে নিজেকে গড়ে তোলার সুযোগ পাচ্ছে।

অনলাইনের সঙ্গে যুক্ত না থাকা ছাত্র-ছাত্রীরা কীভাবে পিছিয়ে পড়ছে



- অবাধ তথ্যের ভান্ডারে বিচরণ করতে পারছে না।
- তথ্য আদান-প্রদানের সুবিধা থেকে পিছিয়ে পড়ছে।
- উচ্চশিক্ষার সুযোগসমূহ সম্পর্কে জানতে পারছে না।
- তাদের চিন্তা-চেতনা এবং জ্ঞানের পরিধি সংকীর্ণ থেকে যাচ্ছে।
- সৃষ্টিশীল কোনো কাজে নিজেকে পরিপূর্ণভাবে উপস্থাপন করতে পারছে না;
- বিশ্বের কখন কোথায় কী ঘটছে ও বিভিন্ন দেশের সংস্কৃতি এবং চর্চা সম্পর্কে সর্বশেষ তথ্য পাচ্ছে না এবং সে অনুযায়ী নিজের বিচার বিশ্লেষণ ক্ষমতা প্রয়োগ করতে পারছে না।
- বিভিন্ন শিক্ষা উপকরণ, পাঠ্যবই, অনলাইন পত্রিকা, চিকিৎসা, স্বাস্থ্য, খেলাধুলা প্রভৃতি সম্পর্কে পর্যাপ্ত তথ্য পাচ্ছে না।
- অনলাইনে নানা রকম লেনদেন ও কেনাকাটার সুবিধা হতে বঞ্চিত হচ্ছে।
- দরখাস্ত জমা দেওয়ার ক্ষেত্রে সশরীরে অফিসে হাজির হতে হচ্ছে।
- দেশের যেকোনো স্থান হতে নিরাপদে লেনদেন করা সম্ভব হচ্ছে না।

ডিজিটাল অপরাধ কী?

ডিজিটাল অপরাধ হলো এমন একটি অপরাধ যা কম্পিউটার এবং কম্পিউটার সংশ্লিষ্ট নেটওয়ার্কের সাথে জড়িত। সাধারণত কোনো কম্পিউটার বা ইলেক্ট্রনিক ডিভাইসের মাধ্যমে ডিজিটাল অপরাধ সংঘটিত হতে পারে। আধুনিক টেলিযোগাযোগ নেটওয়ার্ক, যেমন ইন্টারনেট এবং মোবাইল ফোন ব্যবহার করে অপরাধ করার মানসিকতা নিয়ে কোনো ব্যক্তি বা ব্যক্তিবর্গের বিরুদ্ধে ইচ্ছাকৃতভাবে সম্মানহানী কিংবা সরাসরি বা পরোক্ষভাবে শারীরিক বা মানসিক ক্ষতিসাধন করার মাধ্যমে এ অপরাধ সংঘটিত হতে পারে। কোনো ব্যক্তি বা কম্পিউটার নিজেই উক্ত অপরাধের লক্ষ্যবস্তু হতে পারে। এ ধরনের অপরাধ ব্যক্তি থেকে শুরু করে জাতীয় নিরাপত্তা ও আর্থিক ব্যবস্থাপনার জন্য হুমকি হয়ে উঠতে পারে। এছাড়া আইনগতভাবে বা আইন বহির্ভূতভাবে বিশেষ তথ্যসমূহ বাধাপ্রাপ্ত বা প্রকাশিত হলে গোপনীয়তা লঙ্ঘন হয় বিধায় এসব অপরাধ অনেক বড় ক্ষতির কারণ হতে পারে।

এক কথায়, কম্পিউটার ও কম্পিউটার প্রযুক্তি ব্যবহার করে দেশের প্রচলিত আইনের ব্যত্যয় ঘটিয়ে যে অপরাধ সংগঠিত হয় তাকে ডিজিটাল অপরাধ বলা হয়।

ডিজিটাল অপরাধ সংঘটনের কারণ

বিভিন্ন কারণে ডিজিটাল অপরাধ সংঘটিত হতে পারে। নিম্নোক্ত কারণসমূহ ডিজিটাল অপরাধ সংঘটনের জন্য সহায়ক বলে বিবেচিত হয়-

- কম্পিউটার ও তথ্যপ্রযুক্তি ব্যবহারকারীদের অসচেতনতা, অসতর্কতা ও অদক্ষতা।
- অপরাধীর প্রযুক্তি বিষয়ে দক্ষতা।
- গতানুগতিক পদ্ধতিতে অপরাধ সংঘটনের সুযোগ ও ক্ষেত্র কমে যাওয়া।
- সমাজে কম্পিউটার ও তথ্যপ্রযুক্তির ব্যাপক বিস্তার।
- এ ধরণের অপরাধের ক্ষেত্রে ঝুঁকি কম থাকা বা না থাকা।
- অপরাধীর বিরুদ্ধে আইনগত ব্যবস্থা গ্রহণে জটিলতা।
- প্রচুর আর্থিক লাভের (Monetary Gain) সম্ভাবনা।
- ডিজিটাল অপরাধকে সংজ্ঞায়িত করার ক্ষেত্রে ডিজিটাল অপরাধ সংক্রান্ত আইনের অপর্যাপ্ততা।
- ডিজিটাল আইন সম্পর্কে পর্যাপ্ত জ্ঞানের অভাব।
- প্রকৃত অপরাধী নির্ণয়ে সমস্যা।
- অপরাধের নতুন নতুন কৌশল উদ্ভাবন ও আইন প্রয়োগকারী সংস্থার দুর্বলতা।

এছাড়াও কিছু কিছু ডিজিটাল অপরাধের ক্ষেত্রে ক্ষতিগ্রস্ত ব্যক্তির আইনি ব্যবস্থা গ্রহণে অনাগ্রহ ইত্যাদি ডিজিটাল অপরাধ সংঘটনের অন্যতম প্রধান কারণ।

ডিজিটাল অপরাধ কিভাবে সংঘটিত হচ্ছে

- অবৈধ, অশ্লীল, আপত্তিকর ছবি বা ভিডিও প্রচার, হয়রানি এবং হুমকি প্রদানের মাধ্যমে;
- হ্যাকিং, কপিরাইটের লঙ্ঘন এবং শিশু পর্নোগ্রাফি তৈরির মাধ্যমে;
- ইন্টারনেট ও মোবাইল ফোন ব্যবহার করে কোনো নারী বা শিশুর শারীরিক বা মানসিক ক্ষতিসাধনের মাধ্যমে;
- স্কুল বা কলেজে মজা করার জন্য কিংবা ইচ্ছাকৃতভাবে কাউকে কষ্ট দিতে অনলাইনে হয়রানি করে। অনেক সময় বিষয়টি মজার পর্যায়ে না থেকে অনেক ভয়ঙ্কর রূপ ধারণ করতে পারে;
- বিভিন্ন সামাজিক যোগাযোগ মাধ্যম বা নিউজ পোর্টাল বা ই-মেইল ব্যবহার করে কোনো জাতি, ধর্ম, বর্ণ, লিঙ্গ ইত্যাদি সম্পর্কে বিভিন্ন আক্রমণাত্মক ও অশ্লীল ভাষায় গালিগালাজ, উষ্কানিমূলক বা ঘৃণাযুক্ত এবং অবমাননাকর বক্তব্য প্রচারের মাধ্যমে ডিজিটাল হয়রানি সংঘটিত হতে পারে;
- কম্পিউটার সিস্টেম ব্যবহার করে ব্যাংক জালিয়াতি, কার্ড জালিয়াতি, পরিচয় প্রতারণা এবং তথ্য চুরির মাধ্যমে;
- র‍্যানসমওয়্যার বা ডিজিটাল চাঁদাবাজির মাধ্যমে। এক্ষেত্রে হ্যাকাররা কোনো ওয়েবসাইট, ই-মেইল সার্ভার বা কম্পিউটার সিস্টেমকে নিয়ন্ত্রণের মাধ্যমে উক্ত ডিজিটাল হামলা বন্ধ ও সুরক্ষা প্রদানের বিনিময়ে অর্থ দাবি করে থাকে;
- আইনগত বা আইনবহির্ভূতভাবে বিশেষ তথ্যসমূহ বাধাপ্রাপ্ত বা প্রকাশিত হয়ে গোপনীয়তা লঙ্ঘনের মাধ্যমে;
- ফিশিং, স্ক্যাম এবং স্প্যাম ছড়ানোর মাধ্যমে;
- ইন্টারনেটের বিভিন্ন ডাকসাইটে সাংকেতিক মেসেজিং সিস্টেম ব্যবহার করে মাদক ক্রয়-বিক্রয় এর মাধ্যমে;
- মোবাইল ফোনের মাধ্যমে।

এ ধরনের আক্রমণ ভবিষ্যতে জাতি-রাষ্ট্রের মধ্যে সমস্যা সৃষ্টি করতে পারে, ডিজিটাল ওয়ার্ল্ডের ধারণা বদলে দিতে পারে এবং যুদ্ধ পরিস্থিতির উদ্ভব ঘটাতে পারে।

কারা ডিজিটাল অপরাধের শিকার হতে পারে

- যেকোনো বয়সের নারী বা পুরুষ ডিজিটাল অপরাধের শিকার হতে পারে। তবে কম বয়সী বিশেষত স্কুল বা কলেজগামী শিক্ষার্থীরাই বেশিরভাগ ক্ষেত্রে এ ধরণের অপরাধের শিকার হয়ে থাকে। এসব অপরাধের বেশিরভাগই আবার সামাজিক যোগাযোগ মাধ্যম ব্যবহার করে সংঘটিত হয়। শিশুরাও বিভিন্নভাবে বিশেষত শিশু পর্নোগ্রাফির মাধ্যমে ডিজিটাল অপরাধের শিকার হচ্ছে। এছাড়া পূর্ণবয়স্ক ব্যক্তিগণও এ ধরণের অপরাধের শিকার হতে পারেন।
- ব্যক্তির পাশাপাশি বিভিন্ন প্রতিষ্ঠানসমূহ বিশেষত আর্থিক প্রতিষ্ঠানসমূহ ডিজিটাল হামলার শিকার হতে পারে। এর ফলে এসব প্রতিষ্ঠানকে বিরাট অঙ্কের আর্থিক ক্ষতির সম্মুখীন হতে হয়। বাংলাদেশ ব্যাংকের অ্যাকাউন্ট হ্যাকিং হলো এর সবচেয়ে বড় উদাহরণ। ২০১৬ সালের ৪ ফেব্রুয়ারি বাংলাদেশ ব্যাংকের অ্যাকাউন্ট হ্যাক করার মাধ্যমে হ্যাকাররা প্রায় আটশত আশি কোটি টাকা হাতিয়ে নিয়ে যায় যার ক্ষুদ্র একটি অংশ এ পর্যন্ত উদ্ধার করা সম্ভব হয়েছে।
- যেকেনো রাষ্ট্র সাইবার হামলার শিকার হতে পারে; এমনকি পুরো বিশ্ব এক সাথে সাইবার হামলার শিকার হতে পারে। যেমন: চেরনোবিল, আই লাভ ইউ, স্টর্ম ওয়ার্ম প্রভৃতি ভাইরাস এর ফলে পুরো বিশ্বের লক্ষ লক্ষ কম্পিউটার আক্রমনের শিকার হয় এবং এর ফলে বিলিয়ন ডলারের ক্ষয়-ক্ষতি সাধিত হয়।

বাংলাদেশে কিশোর-কিশোরীরা উল্লেখযোগ্য যেসব সাইবার অপরাধের শিকার হয়

- ব্যক্তিগত ছবি, ভিডিও ছড়িয়ে দেওয়া, ছড়িয়ে দেওয়ার হুমকি প্রদান বা ছড়িয়ে দেওয়ার হুমকি দিয়ে অর্থ আদায়;
- ফেসবুক বা সামাজিক যোগাযোগ মাধ্যমের আইডি হ্যাক করা;
- অনলাইন বা ডিজিটাল মাধ্যমে ব্ল্যাকমেইলিং;
- সুপার ইম্পোজ ছবি;
- অন্যের ছবি দিয়ে আপত্তিকর কন্টেন্ট বা ফেক আইডি তৈরি;
- সাইবার বুলিং;
- অনুমতি ব্যতীত ফোন নম্বর ছড়িয়ে দেওয়া;
- হয়রানিমূলক এসএমএস, মেইল বা লিংক পাঠানো।

কেস স্টাডি

এক

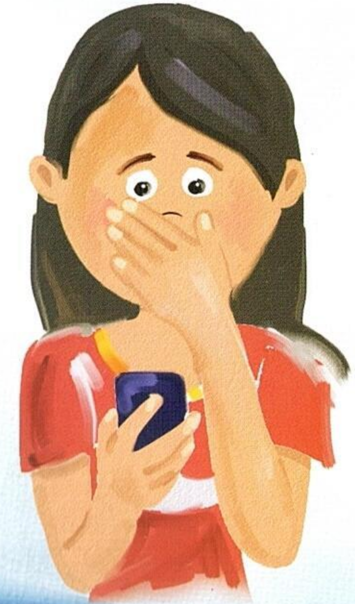
তিন্নি আহ্‌ছানউল্লাহ বিজ্ঞান ও প্রযুক্তি বিশ্ববিদ্যালয়ে পড়ে। একবার ওয়েব সাইট ডিজাইনের জন্য বিভিন্ন বিশ্ববিদ্যালয়ের ছাত্র-ছাত্রীদের কাছ থেকে ডিজাইন জমা দেওয়ার কথা বলা হয়। তিন্নি দিনরাত পরিশ্রম করে ইন্টারনেট থেকে বিভিন্ন দৃষ্টিনন্দন ডিজাইন ও টেমপ্লেট নামিয়ে ওয়েব সাইটটির ফ্রন্ট-এন্ড ও ব্যাক-এন্ড ডিজাইন করে। এক্ষেত্রে ইন্টারনেট তিন্নিকে প্রচুর সহযোগিতা করেছে। বিভিন্ন স্কুল, কলেজ ও বিশ্ববিদ্যালয়ের মধ্যে ওয়েবসাইট ডিজাইন প্রতিযোগিতায় তিন্নির তৈরি করা ওয়েবসাইটটি শ্রেষ্ঠ ওয়েবসাইট এর পুরস্কার অর্জন করে। পরবর্তীতে তার ডিজাইনকৃত ওয়েবসাইটটি যুক্তরাষ্ট্রের এক ওয়েবসাইট ডিজাইন প্রতিযোগিতায় অংশগ্রহণ করে এবং প্রথম স্থান অধিকার করে। এর ফলে সে বাংলাদেশের জন্য সুনাম ও গৌরব বয়ে এনেছে। এ উপলক্ষে বিশ্ববিদ্যালয়ের পক্ষ থেকে তাকে সংবর্ধনা দেয়া হয়েছে। ইন্টারনেটের সঠিক ব্যবহারের মাধ্যমে তিন্নি তার জীবন পরিবর্তন করতে পেরেছে। আমাদের সকলের উচিত তিন্নির মতো ইন্টারনেটের নিরাপদ ও সঠিক ব্যবহারের মাধ্যমে নিজেদের জীবনের মানোন্নয়নে ইন্টারনেটকে কাজে লাগানো।

দুই

মাধবী ভিকারুন্নেসা স্কুলে নবম শ্রেণির একজন মেধাবী ছাত্রী। সে পড়াশুনার পাশাপাশি অন্যান্য সহশিক্ষা কার্যক্রমে সক্রিয়ভাবে অংশগ্রহণ করতো। স্কুলের শিক্ষকরা তাকে তার আচার-ব্যবহার এবং মেধার কারণে খুবই স্নেহ করতেন। তার বাবা-মা তাকে নিয়ে গর্ববোধ করতেন। স্কুলে যাওয়া আসার পথে মামুন নামের একটি ছেলে তাকে উত্যক্ত করতো। বিষয়টি মাধবী তার বাবা-মাকে জানায়। মাধবীর বাবা-মা ছেলেটির অভিভাবককে বিষয়টি জানলে তারা ছেলেটিকে বকাঝকা করেন। এতে ছেলেটি মাধবীর উপর ক্ষিপ্ত হয়।

মাধবী সামাজিক যোগাযোগ মাধ্যম ফেসবুক ব্যবহার করতো। সে ফেসবুকে নিজের, পরিবার ও বন্ধুদের ছবি আপলোড করতো। কিন্তু ব্যক্তিগত ছবির প্রাইভেসির বিষয়ে সে সচেতন ছিল না। ফেসবুকে আপলোড করা তার ছবিগুলোর প্রাইভেসি সেটিংস পাবলিক করা ছিল। ফলে মামুন ফেসবুক থেকে সহজেই মাধবীর ছবি সংগ্রহ করে এবং ছবিগুলো এডিট করে নিজের ছবির সাথে যুক্ত করে সামাজিক যোগাযোগ মাধ্যমে ছড়িয়ে দেয়। ফলে মামুনের সাথে মাধবীর সম্পর্ক আছে এরকম একটি ভুল ধারণা সামাজিক পরিমণ্ডলে ছড়িয়ে পড়ে। এতে মাধবীর বাবা-মাও তাকে ভুল বোঝে। ফলে মাধবী মানসিক ভাবে বিপর্যস্ত হয়ে পড়ে এবং তার লেখাপড়া ব্যাহত হয়।

তিন



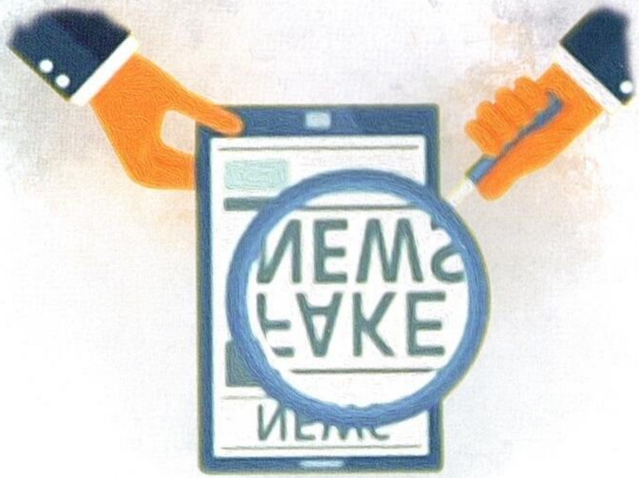
ঐশী রংপুর কারমাইকেল কলেজে ১ম বর্ষে পড়ে। তার মা তাকে মাসিক খরচ বাবদ ৮০০০ টাকা পাঠায়। সে কলেজ শেষ করে সবেমাত্র বাসায় ফিরেছে। হঠাৎ তার মোবাইলে একটি অপরিচিত নম্বর থেকে কল আসে। ফোনের অপর প্রান্তের ব্যক্তিটি খুবই বিনয়ের সাথে তাকে জানায় যে তার নম্বর থেকে ঐশীর বিকাশ নম্বরে ভুল করে কিছু টাকা চলে গেছে। সে গরিব মানুষ। টাকাগুলো ফেরত পেলে তার খুব উপকার হতো। ঐশী তখন নিজের একাউন্ট ব্যালেন্স চেক করে দেখে যে ওর একাউন্ট ব্যালেন্স আগের মতোই আছে এবং সে ওই ব্যক্তিকে জানায় যে তার বিকাশ একাউন্টে নতুন করে কোনো টাকা আসেনি। কিন্তু ফোনের অপর প্রান্তে থাকা ব্যক্তি আগের মতোই বলেন যে তার একাউন্ট থেকে টাকাটা গেছে। হয়তো নেটওয়ার্কে কোনো সমস্যা থাকতে পারে কিন্তু টাকাটা অবশ্যই গেছে। টাকা ফেরত না পেলে সে অনেক বড় বিপদে পড়ে যাবে। এর কিছুক্ষণ পরেই ঐশীর মোবাইলে একটি ম্যাসেজ আসে। ঠিক একই সময় ওই ব্যক্তি আবার ঐশীকে ফোন করে আরও একবার ম্যাসেজ চেক করে দেখতে অনুরোধ করেন। ঐশী দেখে যে সত্যি সত্যিই একটি ম্যাসেজ এসেছে এবং ম্যাসেজটি পড়ে দেখে যে তার একাউন্টে ৬০০০ টাকা যোগ হয়েছে। ঐশীর মনে ওই ব্যক্তির জন্য দয়া হয় এবং দেরী না করে ঐ ব্যক্তির নম্বরে ৬০০০ টাকা পাঠিয়ে দেয়। টাকাটা পাঠানোর পরে ঐশী নিজের একাউন্ট চেক করে দেখে যে তার বিকাশ একাউন্টে আসলে কোনো টাকাই যোগ হয়নি বরং তাঁর বিকাশ একাউন্টে থাকা ৮০০০ টাকার পরিবর্তে সেখানে মাত্র ২০০০ টাকা রয়েছে। ঐশী ঘাবড়ে গিয়ে দ্রুত সেই ম্যাসেজ চেক করে। কিন্তু ম্যাসেজ তো ঠিকই আছে! ভালো করে দেখার পর ঐশী দেখতে পায় যে ঐ ম্যাসেজে bkash এর বদলে bkesh লেখা রয়েছে। bkash এর a এর পরিবর্তে e ব্যবহার করে তাকে ম্যাসেজটি পাঠানো হয়েছে। তখন ঐশী আবার ওই ব্যক্তিকে কল করেন কিন্তু ঐ নম্বরটি ততক্ষণে বন্ধ হয়ে গিয়েছে। ঐশীর আর বুঝতে বাকি থাকে না যে সে প্রতারণার শিকার হয়েছে।

চার

বর্তমানে ফেসবুক প্লাটফর্ম গুজবের একটি বড় জায়গায় পরিণত হয়েছে। সত্য ঘটনার চেয়ে গুজবই যেনো ফেসবুকে বেশি ভাইরাল হয়। আর এই গুজবকে কেন্দ্র করেই বাংলাদেশে অনেক অঘটন ঘটছে। ২০১৯ সালের অক্টোবরে একটি কথিত ফেসবুক ম্যাসেজকে কেন্দ্র করে হিন্দুদের বাড়িঘরে হামলা হয় এবং সংঘর্ষে চারজন নিহত হয়। কিন্তু যে ব্যক্তি ফেসবুকে ম্যাসেজ দিয়েছে বলে দাবি করা হয়েছে তার ফেসবুক আইডিটি পূর্বেই হ্যাক হয়। আর ওই হ্যাক হওয়া আইডি থেকে অন্যকেউ উদ্দেশ্যমূলকভাবে ধর্মীয় অবমাননার ম্যাসেজ দিয়ে তার স্ক্রিনশট ছড়িয়ে দেয়। শুধু ভোলাতেই নয়, ব্রাহ্মণবাড়িয়া, রংপুর, রামু - এসব জায়গাতেও ফেসবুকে গুজব ছড়িয়ে সংখ্যালঘুদের ওপর হামলা চালানো হয়েছে ।

২০১৮ সালের সেপ্টেম্বরে পদ্মা সেতুর নির্মাণ কাজে মানুষের কাটা মাথা লাগবে বলে সারাদেশে একটি গুজব ছড়িয়ে পড়ে। আর এই গুজবকে কেন্দ্র করে ঢাকা ও ঢাকার বাইরে 'ছেলে ধরা' সন্দেহে মানুষকে পিটিয়ে হত্যার মতো ঘটনাও ঘটেছে।

তাই ফেসবুকে বা অন্য কোনো সামাজিক যোগাযোগ মাধ্যমে কিছু শেয়ার করার আগে জেনে বুঝে শেয়ার করুন। নিজে সচেতন হোন, অন্যকে সচেতন করুন।



ডিজিটাল অপরাধের শিকার হলে করণীয়

শুধু ঐশীর সাথেই নয়, কিছু সংঘবদ্ধ চক্র এই প্রক্রিয়ায় যেসব মোবাইল নম্বরে লেনদেন হয় সেসব নম্বরকেই টার্গেট করে থাকে। এভাবে প্রতিনিয়ত বিকাশ ও বিভিন্ন মোবাইল ব্যাংকিং কোম্পানির নাম ব্যবহার করে সাধারণ জনগণের সাথে প্রতারণা করে যাচ্ছে যা থেকে অনেক শিক্ষিত মানুষ পর্যন্ত রেহাই পাননি। এইসব প্রতারণা থেকে বাঁচতে হলে নিম্নবর্ণিত নির্দেশনাসমূহ মেনে চলা উচিত-

১. নিজের মোবাইল ব্যাংকিং একাউন্টের পিন নম্বর ও একাউন্ট ব্যালেন্স অপরকে জানাবেন না।

২. ফোনে অপরিচিত কেউ যদি আপনাকে ভুল করে টাকা পাঠানোর কথা বলে টাকা ফেরত চায় তাহলে তাকে টাকা ফেরত পাঠাবেন না। কোনো ম্যাসেজ দ্বারা প্রভাবিত হয়ে কাউকে টাকা ফেরত পাঠাবেন না। সেক্ষেত্রে আগে মূল একাউন্ট ব্যালেন্স চেক করুন।

৩. কখনও লটারি জেতার কথা শুনে কোনো টাকা-পয়সা লেনদেন করবেন না।

৪. ফোনে কখনও কারো কথায় বা কারো নির্দেশনায় কোনো নম্বরে ডায়াল করবেন না বা ব্যক্তিগত তথ্য প্রদান করবেন না বা টাকা পাঠাবেন না।

আপনি বা আপনার কাছের কেউ এই ধরনের কোনো পরিস্থিতির মুখোমুখি হলে যতদ্রুত সম্ভব নিকটস্থ থানায় রিপোর্ট করুন অথবা সিসিএ কার্যালয়ের কন্যাকথা ওয়েবপোর্টালে (www.konnakotha.cca.gov.bd) রেজিস্ট্রেশন করে আপনার অভিযোগ জানান। নিজে সচেতন হোন,

অন্যকে সচেতন করুন।

অনলাইন নির্যাতন কী

অনলাইনে নির্যাতন বলতে ই-মেইল, সামাজিক যোগাযোগ মাধ্যম তথা ইন্টারনেট ব্যবহার করে কোনো ব্যক্তির সাথে যোগাযোগ স্থাপন করে অশালীন কথা-বার্তা, ছবি কিংবা ভিডিও প্রদান করা, আবেগঘন সম্পর্ক স্থাপন করে নানা অনৈতিক কাজে নিয়োজিত করা, বিবিধ পরিস্থিতির সুযোগ নিয়ে কিংবা অর্থ বা কোনো উপহার প্রদানের মাধ্যমে তাদের নানা অশালীন অঙ্গভঙ্গি কিংবা আচরণে প্ররোচিত করা ইত্যাদিকে বোঝানো হয়। অধিকাংশ সময় অপরিচিত ব্যক্তির দ্বারা এই ধরণের হয়রানি সংঘটিত হলেও কিছু কিছু ক্ষেত্রে পরিচিত ব্যক্তিগণও এরুপ হয়রানি করে থাকে। আবার অনেক সময় দেখা যায় অনৈতিক সম্পর্ক স্থাপনের কিছু স্থিরচিত্র কিংবা ভিডিওচিত্র ধারণ করে অনলাইন জগতে ছেড়ে দেওয়া হয়। একইভাবে এসকল ধারণকৃত ভিডিও সংরক্ষণ করে ভুক্তভোগীকে ভয় দেখিয়ে পুনরায় তার সাথে অনৈতিক সম্পর্ক করতে বাধ্য করা হয়। এছাড়াও অনেক সময় ধারণকৃত ভিডিও বাণিজ্যিকভাবে ক্রয়-বিক্রয়ের মাধ্যমে আর্থিক সুবিধা গ্রহণ করা হয়। এভাবে কোনো ব্যক্তি অনলাইনে নির্যাতনের শিকার হয়ে থাকে।

অনলাইনে নির্যাতনের ধরণ

বিভিন্ন ধরণের তথ্য ও যোগাযোগ প্রযুক্তির (যেমন কম্পিউটার, ল্যাপটপ, মোবাইল, ট্যাব ইত্যাদি) মাধ্যমে নানাভাবে কোনো ব্যক্তি অনলাইন নির্যাতনের শিকার হতে পারেন। যেমন ঃ-

- প্রতারণার মাধ্যমে ওয়েবক্যামের সাহায্যে ধারণকৃত কোনো ব্যক্তির অশ্লীল চিত্র অনলাইনে প্রচার এবং তার বিনিময়ে অর্থ উপার্জন;
- যখন কোনো ব্যক্তি ইলেকট্রনিক যোগাযোগ মাধ্যমে অন্যজনকে হুমকি বা ভীতিমূলক বার্তা প্রদান করে তখন তাকে ডিজিটাল হয়রানি (Bullying) বলে। ডিজিটাল হয়রানির মাধ্যমে অল্পবয়সী ছেলে-মেয়েরা নির্যাতনের শিকার হতে পারে।
- অনেক সময় অল্পবয়সী ছেলে-মেয়েরা কোনো বল প্রয়োগের মাধ্যমে বা সম্পূর্ণ নিজের ইচ্ছায় অশ্লীল ছবি বা ভিডিও ধারণ করে থাকে তাকে সেক্সটিং (Sexting) বলে। এই ছবিগুলো তারা তাদের ছেলে বা মেয়ে বন্ধুকে পাঠায়। কিছুদিন পর তাদের সম্পর্ক ভেঙ্গে গেলে এই ছবিগুলো ইন্টারনেটে ছড়িয়ে পড়তে পারে। অল্পবয়সী ছেলে-মেয়েদের প্রতি আকৃষ্ট ব্যক্তিরা তা সংগ্রহ ও বিক্রি করতে পারে যা তাদের বর্তমান ও ভবিষ্যৎ বিকাশের ক্ষেত্রে ভয়াবহ হুমকি হিসাবে দেখা দিতে পারে। আমাদের দেশে প্রায়শই এ ধরণের ঘটনা ঘটছে।
- অল্পবয়সী ছেলে-মেয়েরা প্রতারণামূলকভাবে ধারণকৃত অশ্লীল ছবির কারণে নানাভাবে নির্যাতনের শিকার হচ্ছে। প্রতারকরা এই ছবিগুলো পরবর্তীতে তাদের বন্ধু, পরিবার বা বৃহৎ পরিসরে (অনলাইন) বিতরণ করার হুমকি দিয়ে তাদের সাথে অনৈতিক সম্পর্ক স্থাপন বা টাকা প্রদানে বাধ্য করতে পারে। এই ধরনের আচরণকে সেক্সটরশন (Sextortion) বলা হয়।
- গ্রুমিং (Grooming) এর মাধ্যমেও অনলাইনে অল্পবয়সী ছেলে-মেয়েরা নির্যাতনের শিকার হতে পারে। যখন কেনো বয়স্ক ব্যক্তি বন্ধুত্বপূর্ণ, উৎসাহব্যঞ্জক অথবা কূট-কৌশলের মাধ্যমে এসব ছেলে-মেয়েকে অনৈতিক কার্যকলাপে জড়িয়ে পড়তে বাধ্য করে তখন তাকে গ্রুমিং বলে। এধরনের অনেক গ্রুমিং এর ঘটনা ইন্টারনেট বিশেষত ফেসবুক এর মাধ্যমে ঘটে থাকে। পরে তারা সরাসরি দেখা করতে আসে এবং গ্রুমিং এর অংশ হিসেবে এসব ছেলে-মেয়েদের অশ্লীল কোনো বস্তু বা ছবি দেখতে প্ররোচিত করে। অশ্লীলতাকে সাধারণ বিষয় হিসেবে তাদের কাছে উপস্থাপন করাই এর মূল উদ্দেশ্য।

- অনেক সময় অল্পবয়সী ছেলে-মেয়েদের বিশেষভাবে প্রাধান্য দিয়ে অথবা অর্থ, উপহার, খাদ্য, চাকুরী ইত্যাদি দেওয়ার মাধ্যমে নির্যাতন করা হতে পারে। এক্ষেত্রে তাদের নির্যাতনের ভিডিও বা ছবির দৃশ্য দেখতেও অপরাধীরা বাধ্য করে থাকে। কোন অল্পবয়সী ছেলে-মেয়ে অনৈতিক সম্পর্ক স্থাপনে অস্বীকৃতি জানালে অপরাধীরা তাকে অশ্লীল কথা বলে, অনেক ক্ষেত্রে তাকে বা তার পরিবারের সদস্যদের শারীরিক নির্যাতন করে অনৈতিক কাজে অংশগ্রহণ করতে বাধ্য করে।

- অনেক সময় সামাজিক যোগাযোগ মাধ্যম (ফেসবুক, টুইটার ইত্যাদি) দ্বারাও এ ধরণের নির্যাতন হতে পারে, যেমন কারো নামে ফেসবুক মিথ্যা একাউন্ট খুলে তাকে নানাভাবে হয়রানি করা বা কারো একাউন্ট, পাসওয়ার্ড বা তথ্য হ্যাক করার মাধ্যমে হয়রানি করা। আবার অজ্ঞাত ব্যক্তির সাথে চ্যাটিং করার মধ্য দিয়েও অল্পবয়সী ছেলে-মেয়েরা অনলাইনে নির্যাতনের শিকার হতে পারে।

অনলাইনে নির্যাতনের মাধ্যমগুলো কী কী

মানুষের দৈনন্দিন কার্যক্রম অনলাইন নির্ভরশীল। তথ্য ও যোগাযোগ প্রযুক্তি সামগ্রী সহজলভ্য হওয়ায় বিভিন্ন সামাজিক যোগাযোগ মাধ্যম ব্যবহার করে অনেক সময় নিজের অজান্তেই কিছু ভুল করে থাকি, যেমন:

- অনলাইনে অশ্লীলতা সম্পর্কিত কন্টেন্ট দেখা ও পড়া;
- কাউকে ভয় দেখানো/হুমকি দেওয়া;
- আইডি হ্যাক করা, ভাইরাস ছড়ানো;
- ফাঁদে ফেলা, হয়রানি করে পর্নোগ্রাফি তৈরি করা;
- পছন্দের বিষয় খুঁজতে গিয়ে কিছু নিষিদ্ধ সাইটে প্রবেশ করা এবং লোভ দেখিয়ে (আকর্ষণীয় ছবি, ওয়াল পেপার, আর্থিক অনুদান, চাকরি, লটারি পুরস্কার) বিভিন্ন লিংকে প্রবেশ করানো ইত্যাদি।

কারা এবং কীভাবে অনলাইনে নির্যাতন করে

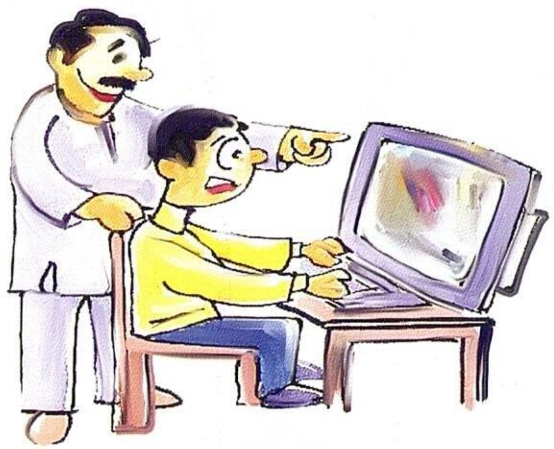
আত্মীয় কিংবা অনাত্মীয় যেকোনো ব্যক্তিই নির্যাতনকারী হতে পারে। শিশু-কিশোর, প্রাপ্তবয়স্ক এমনকি বয়স্ক ব্যক্তিও নির্যাতনকারী হতে পারে। এদের মধ্যে সহপাঠী, খেলার সাথী, শিক্ষক, শিক্ষা প্রতিষ্ঠানে কর্মরত কর্তাব্যক্তিগণ, ধর্মীয় গুরু, প্রতিবেশী, কর্মস্থলে উর্ধ্বতন ব্যক্তি যে কেউই হতে পারে। এছাড়া মানসিকভাবে অসুস্থ এক ধরনের ব্যক্তি আছেন যারা অল্পবয়সী ছেলে-মেয়েদের প্রতি অনৈতিক আগ্রহ বোধ করে তারাও বিভিন্ন সময়ে নির্যাতন করে থাকে। নির্যাতনকারীরা নিম্নোক্তভাবে নির্যাতন করে থাকে-

- ইন্টারনেটে (ফেসবুক, টুইটার প্রভৃতি) ভালো ব্যবহার করে ও অমায়িক আচরণের মাধ্যমে বিশ্বস্ততার সম্পর্ক গড়ে তোলে;
- অনলাইনে কোনো কিছুর প্রলোভন দেখিয়ে যেমন: উপহার, টাকা, চকলেট ইত্যাদি;
- নতুন কোনো সিনেমা দেখানোর অজুহাতে পর্নোগ্রাফি দেখিয়ে;
- ফাঁদে ফেলে বা প্রলোভন দেখিয়ে যেমন: কাজ বা চাকুরী দিবে বলে;
- অনলাইনে ভিডিও শেয়ারিং করে শরীরের বিভিন্ন অঙ্গ-প্রতঙ্গ চেনানোর মাধ্যমে;
- নিজের শরীরের বিশেষ অঙ্গ প্রদর্শনের মাধ্যমে;
- ফোনে বা বিভিন্ন সামাজিক মাধ্যমে অশ্লীল বিষয় নিয়ে কথা বলে বা ছবি শেয়ার করে।

অনলাইন নির্যাতনের শিকার হলে কেন শেয়ারিং প্রয়োজন

কোনো ব্যক্তি অনলাইনে বা সরাসরি যেকোনো ধরনের নির্যাতনের শিকার হলে তা সংশ্লিষ্ট ব্যক্তির ওপর চরম মানসিক আঘাত হানে। এরূপ ঘটনা থেকে মুক্তির জন্য এবং মানসিক যন্ত্রণা লাঘবের জন্য বিষয়টি নিয়ে শেয়ারিং খুবই গুরুত্বপূর্ণ। ঠিক একইভাবে বিষয়টি কোনো ব্যক্তির সাথে শেয়ার করা প্রয়োজন তা নির্বাচন করাও অত্যন্ত গুরুত্বপূর্ণ। কারণ শেয়ার করার পূর্বে যার সাথে শেয়ার করা হবে সেই ব্যক্তি কতটা নিরাপদ তা ভালোভাবে বিবেচনা করে নেওয়াটা জরুরি। অন্যের সাথে নিজের নির্যাতনের অভিজ্ঞতা বর্ণনা করা কঠিন এবং খুবই সাহসী কাজ। চুপ করে থাকাটা ভয়ঙ্কর এবং নিরাময়ের পথে বাধা তৈরি করে। একইভাবে কোনো অল্পবয়সী ছেলে-মেয়ের সাথে ঘটে যাওয়া নির্যাতনও অভিভাবক বা শিক্ষকের সাথে শেয়ার করা আবশ্যক। কেননা এরুপ যন্ত্রণার মধ্যে থাকলে তাদের পূর্ণ বিকাশ বাধাপ্রাপ্ত হয়। এছাড়া এরূপ শেয়ারিং নিম্নোক্ত ক্ষেত্রেও তাদের সহযোগিতা করে-

- এটা নিজেকে রক্ষার প্রথম পদক্ষেপ;
- নিজেকে নিরাপদ রাখে ও নিরাপত্তা নিশ্চিত করে;
- নিজের কষ্ট, রাগ, ভয় থেকে তৈরি খারাপ অনুভূতিগুলো দূর হয়। ব্যক্তি তার নিজস্ব ক্ষমতাকে অনুধাবন করতে পারে যা আত্মসম্মানবোধ বৃদ্ধিতে সাহায্য করে;
- ঘটনার পরিপ্রেক্ষিতে যে শারীরিক ও মানসিক প্রভাব পড়ে তার দীর্ঘমেয়াদি ক্ষতিকর প্রভাব থেকে নিজেকে রক্ষা করতে পারে;
- পরিস্থিতির পরিপ্রেক্ষিতে উদ্ভূত মানসিক চাপ এবং এর ফলে সৃষ্ট সমস্যা মোকাবেলায় সাহায্য করে;
- অন্যের সাথে নেতিবাচক অনুভূতিগুলো শেয়ার করার মাধ্যমে সে নিজের সম্পর্কে সচেতন হয় যা তাকে ঘটনার ক্ষতিকর প্রভাব থেকে রক্ষা করে;
- পরিবারের অন্যরা সচেতন হতে পারে।



অনলাইনে হয়রানি / নির্যাতন থেকে সুরক্ষার উপায় কী

প্রযুক্তিগত উৎকর্ষ বৃদ্ধির সাথে সাথে মানুষের জীবনমান যেমন সহজ হয়েছে তেমনিভাবে নানা ধরনের বিড়ম্বনার শিকার হতে হচ্ছে। প্রযুক্তি সম্পর্কিত বিষয়ের সাথে শিশু ও কিশোর-কিশোরীরা বেশি ব্রাউজার নিরাপত্তা জড়িত থাকে। বেশিরভাগ সময়ে তারা বিভিন্ন শিক্ষামূলক ও গেমস সাইটগুলোতে প্রবেশ করে। তাই নিরাপদে ইন্টারনেট ব্যবহারের জন্য নিম্নোক্ত বিষয়গুলো বিবেচনায় নেওয়া যেতে পারে-

কম্পিউটারের নিরাপত্তা

- কম্পিউটারে এন্টিভাইরাস (Antivirus) ব্যবহার করুন।
- নিজের কম্পিউটারের পাসওয়ার্ড অন্য কাউকে দেওয়া থেকে বিরত থাকুন।
- নিরাপদ/নিরাপত্তামূলক সফটওয়্যার ব্যবহার করুন।

ই-মেইল নিরাপত্তা

- একাউন্ট রিসেট বা আপগ্রেড করার জন্য কোনো লিংকে ক্লিক করবেন না।
- শক্তিশালী পাসওয়ার্ড ব্যবহার করুন এবং সর্বোচ্চ ০৩ (তিন) মাসের মধ্যে পাসওয়ার্ড পরিবর্তন করুন।
- নিরাপদ পাসওয়ার্ড বিশেষ করে পাসওয়ার্ডের সাথে কমপক্ষে ১টি বিশেষ চিহ্ন (@, # ইত্যাদি) ব্যবহার করুন।
- ই-মেইল বা মেসেজের মাধ্যমে কেউ টাকা দিতে চাইলে অথবা লটারি বা পুরস্কার জেতার কথা বললে বিশ্বাস করবেন না।
- ই-মেইলে তথ্য আদান-প্রদানে ডিজিটাল স্বাক্ষর ব্যবহার করুন।

ব্রাউজার নিরাপত্তা

- আপনার ব্রাউজার নিয়মিত আপডেট করুন।
- কোনো ওয়েবসাইটে লগইন করার আগে ওয়েব এড্রেস যাচাই করে নিন।
- অনলাইন একাউন্টে লগইন করার সময় ওয়েব এড্রেস https/Secure কিনা যাচাই করুন। এ ক্ষেত্রে http এর পরে s থাকলে সেই ওয়েবসাইটটি নিরাপদ এবং http এর পর যদি s না থাকে তবে সেই সাইটটি অনিরাপদ হিসেবে বিবেচিত হবে।
- আপনার অনলাইন একাউন্টে প্রয়োজনে One Time Password (OTP)/ Two Factor Authentication সিস্টেম চালু করে নিন।
- ইন্টারনেট ব্যবহারের সময় নতুন অপশন এলে ভেবে-চিন্তে সেগুলোতে প্রবেশ করুন।
- যে সকল গেমস ইন্টারনেট সংযোগ ছাড়াই খেলা যায় সেগুলো খেলার সময় ইন্টারনেট সংযোগ বন্ধ করে রাখুন।
- শুধু শিক্ষামূলক ও নির্ভরযোগ্য সাইটগুলো ব্যবহার করুন।
- ব্রাউজারের কিছু অপশন প্রয়োজনে নিষ্ক্রিয়/সক্রিয় করে রাখুন; যেমনঃ popup block, site block ইত্যাদি।

সামাজিক যোগাযোগ মাধ্যমের নিরাপত্তা

- ফেসবুক এবং অন্যান্য সোশ্যাল মিডিয়ার নিরাপত্তা সেটিংস নিয়মিত যাচাই করুন।
- আপনার সোশ্যাল মিডিয়া একাউন্টের ই-মেইল/এসএমএস নোটিফিকেশন চালু করে নিন।
- কোনো পোস্ট প্রকাশ করার আগে কে পোস্টটি দেখতে পারে তা যাচাই করে নিন।
- অধিকতর নিরাপত্তার জন্য আপনার সোশ্যাল মিডিয়ার একাউন্টে মোবাইল নম্বর নিবন্ধন করুন।
- আপনার একাউন্টে টু ফ্যাক্টর অথেনটিকেশন (Authentication) সিস্টেম চালু রাখুন।
- অনলাইনে অপরিচিত কারো সাথে বন্ধুত্ব করার ক্ষেত্রে সতর্ক থাকুন।
- যত কাছেরই হোক না কেন, কারো অনুরোধে ওয়েব ক্যামেরা বা মোবাইল ফোনের ক্যামেরার সামনে কোনো ধরনের শারীরিক অঙ্গ-ভঙ্গি কিংবা অঙ্গ প্রদর্শন করা থেকে বিরত থাকুন।
- নিজের ব্যক্তিগত তথ্য, ছবি ও ভিডিওচিত্র শেয়ার করা থেকে বিরত থাকুন।
- অনলাইনে কেউ উত্ত্যক্ত করলে বা সন্দেহজনক আচরণ করলে তা বাবা-মাকে জানান। বাবা-মার সাথে বন্ধুত্বপূর্ণ সম্পর্ক বজায় রাখুন যাতে তাদের সাথে সবকিছু শেয়ার করা যায় এবং প্রয়োজনে সহযোগিতা পাওয়া যায়।

ওয়াইফাই নেটওয়ার্ক ব্যবহারে সতর্কতা

- পাবলিক প্লেসে ফ্রি ওয়াইফাই নেটওয়ার্ক ব্যবহার করা থেকে বিরত থাকুন।
- অনলাইন আর্থিক লেনদেন করার ক্ষেত্রে ফ্রি ওয়াইফাই নেটওয়ার্ক ব্যবহার করা থেকে বিরত থাকুন।

সামাজিক ট্যাবো বা ভ্রান্ত ধারণা

ট্যাবো হচ্ছে সামাজিকভাবে নিষিদ্ধ কিছু বিষয় যার ভিত্তি কিছু ভ্রান্ত ধারণা ও প্রচলিত বিশ্বাস যেগুলো সত্য নাও হতে পারে। শিশু নির্যাতন নিয়ে আমাদের সমাজে বেশ কিছু সামাজিক ট্যাবো রয়েছে। এসব ট্যাবো সমাজে নির্যাতন প্রতিহত করার পথে বাধার সৃষ্টি করে। প্রচলিত ট্যাবোসমূহ হলো-

অনলাইনে নির্যাতন/হয়রানির বিষয় প্রমাণ করতে গেলে কী কী বিষয়ে সতর্ক হওয়া প্রয়োজন

যেকোনো অনলাইন মাধ্যমে নির্যাতন/হয়রানির বিষয় প্রমাণের প্রয়োজনে নিম্নোক্ত বিষয়গুলো বিবেচনায় নিতে হবে-

- হার্ডকপি রাখতে হবে।
- URL সহ স্ক্রিনশট প্রিন্ট করে রাখতে হবে।
- বিষয়গুলো সংরক্ষণ করে রাখা যেতে পারে।
- বিভিন্ন ওয়েব অ্যাড্রেস (URL), ফেসবুক আইডি, ই-মেইল আইডি ও তারিখ সংরক্ষণ করতে হবে।
- যত বেশি সম্ভব প্রমাণ রাখতে হবে (এসএমএস, ভয়েস রেকর্ড, অশ্লীল মন্তব্য ইত্যাদি)।

ডিজিটাল স্বাক্ষর সম্পর্কিত তথ্য

ইলেক্ট্রনিক স্বাক্ষরের বিশ্বব্যাপী পরীক্ষিত ও স্বীকৃত প্রযুক্তি হল ডিজটাল স্বাক্ষর। ইহা ডিজিটাল বার্তা বা দলিলের সত্যতা যাচাই এর একটি পদ্ধতি। একটি বৈধ ডিজিটাল স্বাক্ষর সম্বলিত বার্তা বা দলিল দেখে প্রাপক বুঝতে পারবেন যে, বার্তাটি যিনি পাঠিয়েছেন সেটি পাঠানোর তার একক কর্তৃত্ব রয়েছে (authentication), বার্তাটি পাঠানোর পর প্রেরক অস্বীকার করতে পারবে না (non-repudiation), বার্তাটি পথিমধ্যে কোনো ধরনের পরিবর্তন হয়নি (integrity) এবং বার্তাটির গোপনীয়তা নিশ্চিত হয়েছে (confidentiality)। অর্থাৎ ইলেক্ট্রনিক/ডিজিটাল স্বাক্ষর ব্যবহার করে তথ্যের অবিকৃত আদান-প্রদান, তথ্য প্রদানকারী ও গ্রহণকারীর পরিচিতি প্রতিপাদন এর পাশাপাশি তথ্যের গোপনীয়তা নিশ্চিত করা সম্ভব।

ডিজিটাল স্বাক্ষর ব্যবহারের সুবিধা

- অনলাইনে তথ্য বিনিময়ের ক্ষেত্রে কোনো তথ্যের বিকৃতি ও জালিয়াতি রোধ করা যায়;
- ডিজিটাল স্বাক্ষরের আইনগত বৈধতা এবং সাক্ষ্যগত মূল্য নিশ্চিত করা হয়েছে;
- আইনে ডিজিটাল স্বাক্ষরকে হাতে লেখা স্বাক্ষরের সমান বৈধতা দেওয়া হয়েছে;
- ডিজিটাল স্বাক্ষর এর মাধ্যমে স্বাক্ষরদাতার পরিচয় যাচাই করার সুযোগ রয়েছে;
- ডিজিটাল স্বাক্ষর ব্যবহারের মাধ্যমে অনলাইনে তথ্য বিনিময়ের ক্ষেত্রে স্বাক্ষরকারী ব্যক্তি বা প্রতিষ্ঠানের পরিচিতি নিশ্চিত করা যায় বিধায় তা যেকোনো সাইবার অপরাধের শনাক্তকরণ ও তদন্তে কার্যকর ভূমিকা রাখে;
- ডিজিটাল স্বাক্ষর ব্যবহার করলে TCV (Time, Cost, Visit) যৌক্তিকভাবে কমিয়ে আনা সম্ভব;
- পেপারলেস অফিস বাস্তবায়নে ডিজিটাল স্বাক্ষরের প্রয়োজনীয়তা অনস্বীকার্য;
- ডিজিটাল স্বাক্ষরের ব্যাপক প্রচলন সবুজ অর্থনীতি (গ্রীন ইকোনমি) নিশ্চিতকরণে ভূমিকা রাখবে।

কোথায় জানাবেন?

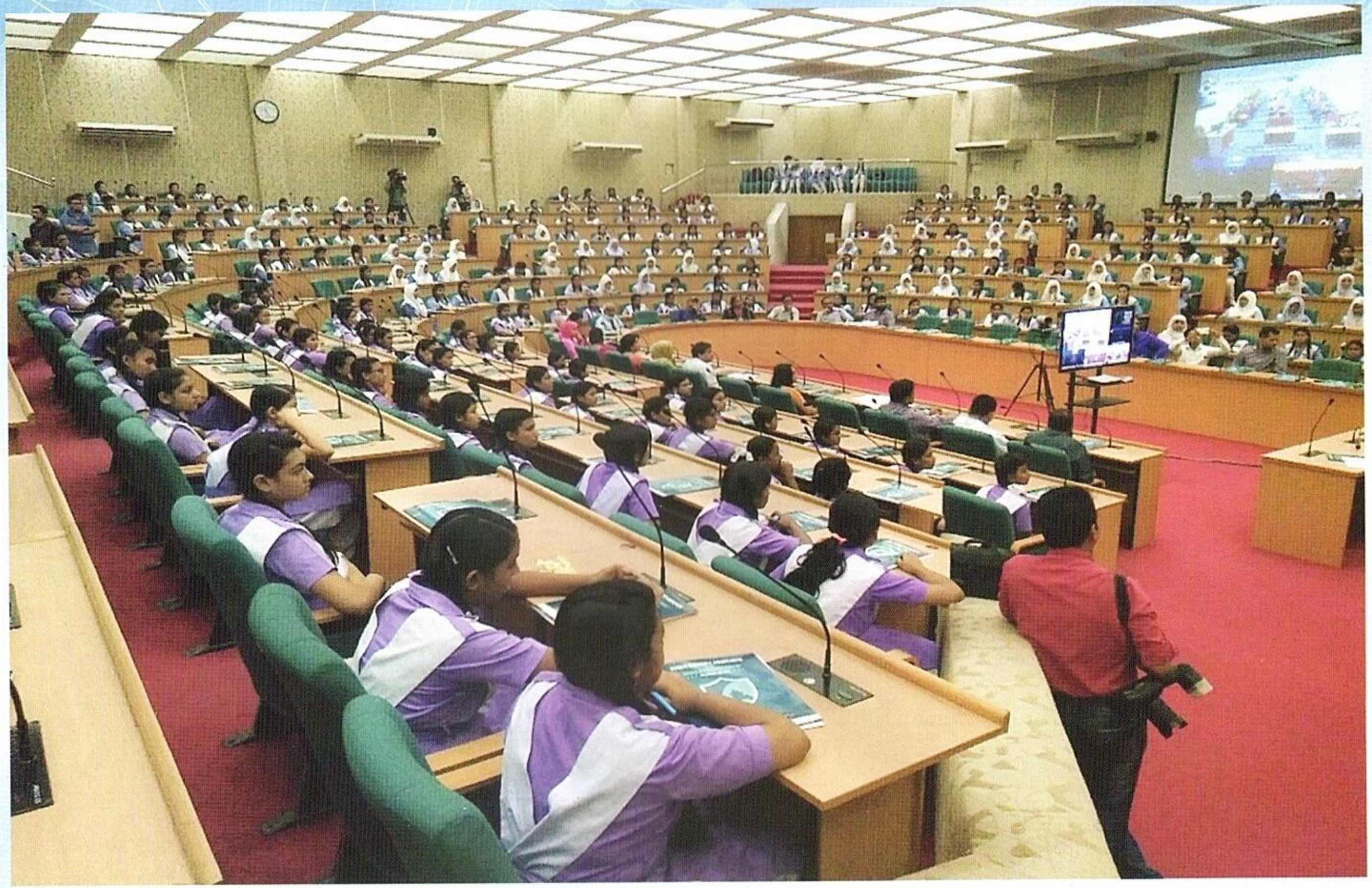
- নিকটস্থ থানায় যোগাযোগ করতে হবে।
- Police cyber support for women (PCSW) নামে ফেসবুক পেজে (www.facebook.com/PCSW.PHQ) মেসেজ দিয়ে অভিযোগ জানাতে হবে।
- cybersupport.women@police.gov.bd এই ঠিকানায় মেইল করা যাবে।
- পুলিশ সদর দফতরের ০১৩২০০০০৮৮৮ নম্বরে ফোন করে অভিযোগ করা যাবে।
- হটলাইন নম্বর ৯৯৯ এ ফোন করেও অভিযোগ করা যাবে।
- হেল্পলাইন ৩৩৩ কলসেন্টারে ফোন করে বাল্যবিবাহ প্রতিরোধসহ সাইবার অপরাধ বিষয়ে যোগাযোগ করা যাবে।
- সিসিএ কার্যালয়ের ফেসবুক পেজ অথবা কন্যাকথা ওয়েবসাইট www.konnakotha.cca.gov.bd -এ মেসেজ দিয়ে সাইবার সিকিউরিটি বিষয়ক যেকোনো পরামর্শের জন্য যোগাযোগ করা যাবে।

CCA
ইলেক্ট্রনিক স্বাক্ষর সার্টিফিকেট প্রদানকারী কর্তৃপক্ষের নিয়ন্ত্রক-এর কার্যালয়

http://www.cca.gov.bd

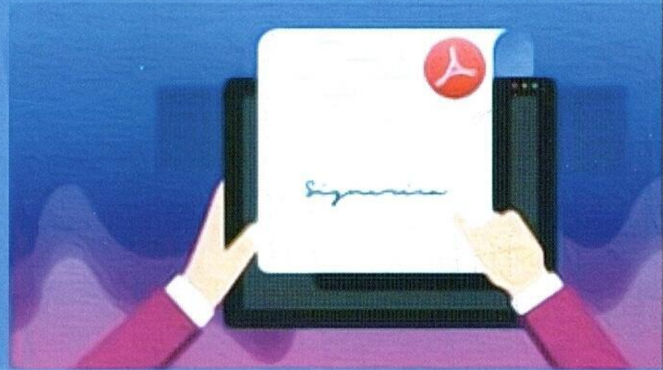
ইলেক্ট্রনিক স্বাক্ষর সার্টিফিকেট প্রদানকারী কর্তৃপক্ষের নিয়ন্ত্রক (সিসিএ)-এর কার্যালয়

তথ্য ও যোগাযোগ প্রযুক্তি বিভাগ



Cyber Security Awareness for Women Empowerment শীর্ষক সচেতনতামূলক ওয়ার্কশপ-২০১৭ সালের উদ্বোধনী অনুষ্ঠানের চিত্র।

মাইবার অপরাধ রোধে
ডিজিটাল স্বাক্ষর ব্যবহার করুন



ডিজিটাল স্বাক্ষর ব্যবহার করুন
ডিজিটাল জগতে সুরক্ষিত থাকুন

"সচেতনতাই নিরাপত্তার চাবি"

ইলেক্ট্রনিক স্বাক্ষর সার্টিফিকেট প্রদানকারী কর্তৃপক্ষের নিয়ন্ত্রক (সিসিএ)-এর কার্যালয়

তথ্য ও যোগাযোগ প্রযুক্তি বিভাগ

ই-১৪/এক্স, আইসিটি টাওয়ার, আগারগাঁও, ঢাকা- ১২০৭

ফোন: +৮৮-০২-৫৫০০৬৮১৯, ফ্যাক্স: +৮৮-০২-৮১৮১৭১১

ই-মেইল: info@cca.gov.bd, ওয়েব: www.cca.gov.bd