বাংলাদেশের সুবর্ণজয়ন্তী Bangladesh 50

ICT DIVISION FUTURE IS HERE

DIGITAL SECURITY AGENCY

মুজিব শতবর্ষ MUJIB 100

ডিজিটাল নিরাপত্তা বিষয়ক

কল সেন্টার পরিচালনা

স্ট্যান্ডার্ড অপারেটিং প্রসিডিউর

Standard Operating Procedure (SOP)

ডিজিটাল নিরাপত্তা এজেন্সি

তথ্য ও যোগাযোগ প্রযুক্তি বিভাগ

ডিজিটাল নিরাপত্তা এজেন্সি

ডিজিটাল নিরাপত্তা বিষয়ক কল সেন্টারের

স্ট্যান্ডার্ড অপারেটিং প্রসিডিউর (Standard Operating Procedure)

উপদেষ্টা

জনাব মোঃ খায়রুল আমীন, মহাপরিচালক (অতিরিক্ত সচিব), ডিজিটাল নিরাপত্তা এজেন্সি

নির্দেশনা

জনাব মোঃ আবদুস সাত্তার সরকার, পরিচালক (প্রশাসন ও অর্থ) (যুগ্মসচিব), ডিজিটাল নিরাপত্তা এজেন্সি
জনাব তারেক এম বরকতউল্লাহ, পরিচালক (অপারেশন), ডিজিটাল নিরাপত্তা এজেন্সি

সহযোগিতা

জনাব মু. ইকরামুল ইসলাম, উপপরিচালক (প্রশাসন), ডিজিটাল নিরাপত্তা এজেন্সি
জনাব মোহাম্মদ আনোয়ার হোসেন, উপপরিচালক (অপারেশন), ডিজিটাল নিরাপত্তা এজেন্সি
জনাব মোছাঃ ফারজানা খান তমা, সহকারী পরিচালক (প্রশিক্ষণ), ডিজিটাল নিরাপত্তা এজেন্সি
জনাব যুথিকা মজুমদার, সহকারী পরিচালক (প্রশাসন), ডিজিটাল নিরাপত্তা এজেন্সি
জনাব মোঃ নাঈম খান, সহকারী পরিচালক (পরিকল্পনা ও উন্নয়ন), ডিজিটাল নিরাপত্তা এজেন্সি
জনাব উত্তরা শতদ্রু প্রাচী, সহকারী পরিচালক (বাজেট), ডিজিটাল নিরাপত্তা এজেন্সি
জনাব মোঃ সোহেল রানা, সহকারী পরিচালক (সেবা), ডিজিটাল নিরাপত্তা এজেন্সি
জনাব নাবিল আহমেদ খান, আইন কর্মকর্তা, সার্ট টিম
জনাব মোঃ রেজাউল ইসলাম, কোয়ালিটি অ্যাসিওরেন্স ম্যানেজার, সার্ট টিম
জনাব রেজাউর রহমান, ইনসিডেন্ট হ্যান্ডলার, সার্ট টিম
জনাব মোহাম্মদ মাকছুদুল আলম, ইনসিডেন্ট হ্যান্ডলার, সার্ট টিম
জনাব মো: সামিউল ইসলাম, ইনসিডেন্ট হ্যান্ডলার অ্যাসোসিয়েট, সার্ট টিম

প্রকাশকাল

অক্টোবর ২০২১

প্রকাশনা

ডিজিটাল নিরাপত্তা এজেন্সি

মুখবন্ধ

মো: খায়রুল আমীন
মহাপরিচালক (অতিরিক্ত সচিব)
ডিজিটাল নিরাপত্তা এজেন্সি

মাননীয় প্রধানমন্ত্রী ঘোষিত 'ডিজিটাল বাংলাদেশ' উদ্যোগের এক যুগের পথ পরিক্রমায় আমাদের দেশ বিভিন্ন ক্ষেত্রে উল্লেখযোগ্য সাফল্য অর্জন করেছে। অধিকাংশ সরকারি সেবাসমূহ জনগণের দোরগোড়ায় পৌঁছে দেয়া সম্ভব হয়েছে, প্রান্তিক পর্যায় পর্যন্ত ফাইবার অপটিক/ব্রডব্যান্ড কানেক্টিভিটি স্থাপন করা হয়েছে; বিপুল সংখ্যক তরুণ জনগোষ্ঠী তথ্য ও যোগাযোগ প্রযুক্তি বিষয়ে উচ্চ শিক্ষা অর্জন করছে এবং তথ্য প্রযুক্তি খাতের ব্যবসা প্রসারণের জন্য প্রণোদনা প্রদানসহ স্থাপন করা হয়েছে বিভিন্ন টেকনোলজি পার্ক। এ কার্যক্রম পরিচালনা করতে গিয়ে তৈরি হয়েছে বিপুল তথ্য ভান্ডার, সংরক্ষণ করা হয়েছে অনেক গোপনীয় ও সংবেদনশীল তথ্য-উপাত্ত এবং তৈরি করা হয়েছে প্রয়োজনীয় অবকাঠামো। 'ডিজিটাল বাংলাদেশ'-এর অর্জনসমূহকে টেকসই করা এবং 'রূপকল্প ২০৪১' অনুসারে বাংলাদেশকে একটি উন্নত সমৃদ্ধ রাষ্ট্রে পরিণত করতে হলে প্রয়োজন তা সঠিকভাবে রক্ষণাবেক্ষণ ও নিরাপত্তা প্রদান করা।

ডিজিটাল নিরাপত্তা নিশ্চিতকরণ এবং ডিজিটাল মাধ্যমে সংঘটিত অপরাধ শনাক্তকরণ, প্রতিরোধ, দমন, বিচার ও আনুষঙ্গিক কার্যক্রম গ্রহণের লক্ষ্যে সরকার 'ডিজিটাল নিরাপত্তা আইন ২০১৮' প্রণয়ন করেছে। সামগ্রিক ডিজিটাল নিরাপত্তা সংক্রান্ত কার্যক্রম পরিচালনার নিমিত্ত উক্ত আইনের বিধান অনুসারে সরকার 'ডিজিটাল নিরাপত্তা এজেন্সি' গঠন করেছে। প্রধানমন্ত্রীর তথ্য ও যোগাযোগ প্রযুক্তি বিষয়ক মাননীয় উপদেষ্টা জনাব সজীব ওয়াজেদ -এর দিক-নির্দেশনাদ, তথ্য ও যোগাযোগ প্রযুক্তি বিভাগের মাননীয় প্রতিমন্ত্রী জনাব জুনাইদ আহ্‌মেদ পলক এমপি-র গতিশীল নেতৃত্ব এবং এ বিভাগের সম্মানিত সিনিয়র সচিব জনাব এন এম জিয়াউল আলম পিএএ -এর তত্ত্বাবধানে দেশের সাইবার স্পেসকে নিরাপদ রাখা এবং জনগণের মধ্যে সাইবার সচেতনতা সৃষ্টির লক্ষ্যে 'ডিজিটাল নিরাপত্তা এজেন্সি' নিরলসভাবে কাজ করে যাচ্ছে।

সরকারি কার্যক্রমের পাশাপাশি বেসরকারি খাত এবং দেশের বিপুল জনগোষ্ঠী দৈনন্দিন কার্যক্রম ও সেবার জন্য ডিজিটাল মাধ্যমের ওপর নির্ভরশীল। অন্তর্জাল ও সামাজিক যোগাযোগ মাধ্যমের ব্যাপক ব্যবহারের ফলে একদিকে যেমন পারস্পরিক যোগাযোগ রক্ষা, বিভিন্ন সৃজনশীল কার্যক্রম পরিচালনা, শিক্ষা ও চিকিৎসাসহ প্রয়োজনীয় সেবা প্রদানের ক্ষেত্রে অবারিত সুযোগ সৃষ্টি হচ্ছে; অপরদিকে এর অপব্যবহারের মাধ্যমে কোনো কোনো ক্ষেত্রে সাইবার অপরাধ সংঘটন, মিথ্যা সংবাদ ও গুজব প্রচার, হিংসা ও বিদ্বেষমূলক বক্তব্য প্রদানের মাধ্যমে সামাজিক অসন্তোষও সৃষ্টি করা হচ্ছে। সাইবার অপরাধ প্রতিরোধ এবং জনসাধারণকে বিশেষ করে কিশোর-কিশোরীদেরকে এর অভিঘাত থেকে রক্ষা করার নিমিত্ত পরামর্শ ও সহযোগিতা প্রদানের জন্য ডিজিটাল নিরাপত্তা এজেন্সি 'কল সেন্টার' স্থাপন করেছে। উক্ত কল সেন্টারে যাতে পেশাদারিত্বের সাথে সেবা গ্রহীতাদেরকে সেবা প্রদান করা হয়, সে লক্ষ্যে এই 'স্ট্যান্ডার্ড অপারেটিং প্রসিডিউর' (SOP) প্রস্তুত করা হয়েছে।

আমি আশাকরি SOP-টি অনুসরণের মাধ্যমে কল সেন্টারে কলকারী সেবা প্রার্থীদের দক্ষতার সাথে আর্ন্তজাতিক মানের ২৪/৭ সেবা প্রদান করা সম্ভব হবে। SOP প্রণয়নে ডিজিটাল নিরাপত্তা এজেন্সি ও বিজিডি ই-গভ সার্ট টিম সহ অন্যান্য সদস্যরা যে নিরলস পরিশ্রম করেছেন সে জন্য তাদেরকে আন্তরিক ধন্যবাদ জানাচ্ছি। বিশেষ করে জনাব মু. ইকরামুল ইসলাম, উপ-পরিচালক, ডিজিটাল নিরাপত্তা এজেন্সি- তা চূড়ান্তকরণে যে কঠোর প্ররিশ্রম করেছেন, সে জন্য তাকে ধন্যবাদ দিয়ে খাটো করতে চাই না। পরিশেষে এই SOP টি সঠিকভাবে অনুসরণের মাধ্যমে জনগণকে পেশাদারিত্বের সাথে মানসম্মত সেবা প্রদানের জন্য সংশ্লিষ্ট সকলের সহযোগিতা কামনা করছি।

(মো: খায়রুল আমীন)

সূচিপত্র

সম্ভাষণ (Greetings)..১

কল সেন্টার অপারেটর কর্তৃক অনুসরনীয় উত্তম চর্চাসমূহ.. ২

করনীয়:..২

বর্জনীয়:..২

অধ্যায়-১: ডিজিটাল ডিভাইসের নিরাপদ ব্যবহার.. ৩

প্রশ্ন ১। কিভাবে শক্তিশালী পাসওয়ার্ড সেট করা যায়? ৩

প্রশ্ন ২। আমার পাসওয়ার্ড কিভাবে নিরাপদে সংরক্ষণ করতে পারি?... ৩

প্রশ্ন ৩। কিভাবে এলার্ট নোটিফিকেশন ব্যবহার করা যায়?.. ৩

প্রশ্ন ৪। নতুন ব্যবহারকারী তার ডিভাইস সুরক্ষিত রাখতে কি কি করবেন? ৪

প্রশ্ন ৫। পার্সোনাল কম্পিউটার সুরক্ষার ক্ষেত্রে করণীয় কি? ৪

প্রশ্ন ৬। ডিজিটাল ডিভাইস/ কম্পিউটার সিস্টেমে পাসওয়ার্ড হ্যাক করে/বেআইনি প্রবেশ রোধে কি করণীয়?..৪

প্রশ্ন ৭। কিভাবে নিরাপদে ইউএসবি পেনড্রাইভ ব্যবহার করতে পারি? ৪

প্রশ্ন ৮। আমার ডকুমেন্ট/সফটওয়্যার/কম্পিউটার খুলতে পারছি না। অথবা আমি ভাইরাস/ ম্যালওয়্যার দ্বারা আক্রান্ত হয়েছি। এখন কি করতে পারি? ৫

প্রশ্ন ৯। ডিজিটাল ডিভাইস/কম্পিউটার সিস্টেম হতে কোনো তথ্য উপাত্ত সংগ্রহ/স্থানান্তর রোধে কি করণীয়?..৫

প্রশ্ন ১০। আমার মোবাইলে আমার ব্যক্তিগত ছবি ছিলো। আমি কারো সাথে এটা শেয়ার করি নি। এটা কিভাবে সোশ্যাল মিডিয়াতে/ফেসবুকে ছড়িয়ে গেলো?.. ৬

প্রশ্ন ১১। পাবলিক ওয়াই-ফাই ব্যবহারের বিষয়ে কি কি সতর্কতা অবলম্বন করা প্রয়োজন?.......................৭

প্রশ্ন ১২। পার্সোনাল ওয়াইফাই পার্শ্ববর্তী অন্য কেউ ব্যবহার করলে করণীয় কি?..................................৭

অধ্যায়-২: নিরাপদ ইন্টারনেট ব্যবহার ৮

প্রশ্ন ১৩। ফিশিং ও স্পুফিং কি? ৮

প্রশ্ন ১৪। আমাকে অযাচিতভাবে বিজ্ঞাপন মেইল/এসএমএস প্রেরণ করা হয়েছে। সেক্ষেত্রে করণীয় কি? ৮

প্রশ্ন ১৫। সন্দেহজনক ইমেইল/মেসেজ কিভাবে চিহ্নিত করব?... ৮

প্রশ্ন ১৬। জিমেইল/ফেসবুক একাউন্টে প্রমাণীকরণ ধাপ (authentication step) কিভাবে যোগ করব? ...৯

প্রশ্ন ১৭। জিমেইল/ফেসবুক একাউন্ট পুনরুদ্ধার..৯

প্রশ্ন ১৮। আমি একটি সন্দেহজনক ইমেল বা বার্তা পেয়েছি। / আমি অচেনা কারো কাছ থেকে একটি সংযুক্তি সহ একটি ইমেল পেয়েছি। আমার কি করা উচিত? ১০

প্রশ্ন ১৯। নিরাপদে ইন্টারনেট ব্যবহারের জন্য আমি কি করতে পারি? ১০

প্রশ্ন ২০। নকল ওয়েবসাইট কিভাবে চিনতে পারব? ১০

প্রশ্ন ২১। সন্দেহজনক লিংক ব্যবহারের ক্ষেত্রে কি ধরণের সতর্কতা অবলম্বন করা উচিত? ১১

প্রশ্ন ২২। আমার ইন্টারনেট সার্ভিস প্রদানকারীর কাছ থেকে আমার পাসওয়ার্ড চাওয়ার একটি বার্তা পাই। তারা বলে আমার একাউন্ট ঠিক করার জন্য তাদের দরকার। আমার কি পাসওয়ার্ড তাদের দেওয়া উচিত হবে? ... ১১

প্রশ্ন ২৩। আমি ফেসবুক, ইউটিউব বা কোনো সোশ্যাল মিডিয়ায় একটি পোস্ট দেখেছি, যেখানে অংশগ্রহণকারীরা সন্ত্রাস, জিহাদ এবং এরকম কিছু নিয়ে আলোচনা করেছে। আমার কি করা উচিৎ? ১১

অধ্যায়-৩: হ্যাকিং/পরিচয় চুরি/র‍্যানসমওয়্যার... ১২

প্রশ্ন ২৪। অনলাইনে হুমকি বা পরিচয় চুরির শিকার হলে কি করব? ১২

প্রশ্ন ২৫। আমি পরিচয় চুরির শিকার হয়েছি এবং ইতিমধ্যে হ্যাকারদের যোগাযোগের উত্তর দিয়েছি/কথামতো কাজ করেছি। এখন কি করনীয়? ১২

প্রশ্ন ২৬। আমার পরিচয় চুরি (identity theft) কিভাবে প্রতিরোধ করব? ১২

প্রশ্ন ২৭। আমার হ্যাক হওয়া একাউন্ট পুনরুদ্ধার করেছি। এখন আমার কি করা প্রয়োজন? ১৩

প্রশ্ন ২৮। আমার একাউন্ট হ্যাক/লক করে আমার কাছে টাকা চাইছে। এমন র‍্যানসমওয়্যার নোট পেলে কি করবেন? কম্পিউটার আনলক করার জন্য মুক্তিপণ দেওয়া কি উচিৎ হবে? ১৩

প্রশ্ন ২৯। র‍্যানসামওয়্যার আক্রমণ করে আমার ডিভাইসের ডাটা নষ্ট করে দেওয়া হয়েছে। এক্ষেত্রে করণীয় কি? ১৪

প্রশ্ন ৩০। এসএমএস এর মাধ্যমে আমার কাছে একটি লিংক আসে। লিংকে ক্লিক করার পরই আমার জিমেইল আইডি হ্যাক হয়ে যায়। আমার করণীয় কি? ১৪

অধ্যায়-৪: ফোন হারিয়ে গেলে করণীয়.. ১৫

প্রশ্ন ৩১। এন্ড্রয়েড ফোন হারিয়ে গেলে কি করণীয়? ১৫

প্রশ্ন ৩২। আইফোন ফোন হারিয়ে গেলে কি করণীয়? ১৬

প্রশ্ন ৩৩। Android মোবাইল সুরক্ষিত রাখতে করণীয়? ১৮

প্রশ্ন ৩৪। ল্যাপটপ এ গুরত্বপূর্ণ অ্যাপ্লিকেশন অটো কারেক্ট/ পাসওয়ার্ড সেভ হয়ে থাকে। কিভাবে অটো কারেক্ট বন্ধ করা যায়? ১৯

অধ্যায়-৫: ব্যাংক/ফিনান্সিয়াল সার্ভিস সংক্রান্ত... ২০

প্রশ্ন ৩৫। আমি সন্দেহ করছি যে আমার ব্যাংক/বিকাশ/নগদ একাউন্টের তথ্য চুরি হয়েছে। এখন কি করব?.২০

প্রশ্ন ৩৬। মোবাইল ব্যাংকিং ও এটিএম কার্ড প্রতারণা এড়াতে করণীয়?..২০

প্রশ্ন ৩৭। বিকাশে অ্যাকাউন্ট রিকভার করার জন্য কোড চেয়েছিলো। কোড দেয়ার পরে আমার অ্যাকাউন্টে টাকা নাই। কি করতে পারি? ২০

অধ্যায়-৬: মানহানী এবং সাইবার বুলিং...২১

প্রশ্ন ৩৮। আমি মানহানীর শিকার হলে কি করব? ২১

প্রশ্ন ৩৯। কিভাবে একটি সাইবার হুমকি বা সাইবার অপরাধ রিপোর্ট করবেন?.................................২১

প্রশ্ন ৪০। বিভিন্ন আইডি এবং গ্রুপের মাধ্যমে আমার নামে অপ-প্রচার চালানো হচ্ছে। এগুলো বন্ধ করতে আমার করণীয় কি?..২১

প্রশ্ন ৪১। যদি কেউ আমাকে অনলাইনে উত্ত্যক্ত করে তাহলে আমার কার সাথে কথা বলা উচিত? ২১

প্রশ্ন ৪২। আমি সাইবার বুলিংয়ের সম্মুখীন হচ্ছি, কিন্তু আমি আমার বাবা-মায়ের সাথে এটি সম্পর্কে কথা বলতে ভয় পাই। আমি কিভাবে তাদের কাছে যেতে পারি? ২২

প্রশ্ন ৪৩। কিভাবে আমি আমার বন্ধুদের সাইবার বুলিংয়ের একটি মামলা রিপোর্ট করতে সাহায্য করতে পারি, বিশেষ করে যদি তারা এটি করতে না চায়?..২২

প্রশ্ন ৪৪। ইন্টারনেটে অ্যাক্সেস বন্ধ না করে আমরা কীভাবে সাইবার বুলিং বন্ধ করব? ২২

প্রশ্ন ৪৫। সোশ্যাল ওয়েবে উত্যক্তের শিকার হচ্ছি। এই পরিস্থিতিতে কি করতে পারি? ২৩

অধ্যায়-৭: সোশ্যাল মিডিয়ার নিরাপদ ব্যবহার...২৪

প্রশ্ন ৪৬। ফেসবুকে আমার নাম ও ছবি ব্যবহার করে ফেইক আইডি তৈরি করা হয়েছে। এটা কিভাবে বন্ধ করবো? ২৪

প্রশ্ন ৪৭। আমার ফেসবুক আইডি হ্যাকড হয়েছে। আমি ঢুকতে পারছি না। এখন কিভাবে আইডি উদ্ধার করবো? ২৪

প্রশ্ন ৪৮। হোয়াটস অ্যাপে অপরিচিত নম্বর থেকে কল করে অশালীন ভাষায় মন্তব্য ও কুরুচিপূর্ণ কথাবার্তা বলা হচ্ছে এবং কল কেটে দেয়ার সাথে সাথে বিভিন্ন অশ্লীল ছবি এবং ভিডিও পাঠাচ্ছে। আমার করণীয় কি?.....২৫

প্রশ্ন ৪৯। কিভাবে আমি আমার ব্যক্তিগত তথ্যকে সোশ্যাল মিডিয়ায় পরিচয় চুরি বা অপমান করার জন্য ব্যবহার করা থেকে বিরত রাখব?.. ২৬

৫০। হ্যাকার একটি সোশ্যাল সাইটের প্রোফাইল হ্যাক করেছে, এখন টাকা দাবি করছে। যদি ভিকটিম টাকা না দেয় তাহলে হ্যাকার তার প্রোফাইল থেকে অশ্লীল জিনিস ছড়াবে। এই পরিস্থিতিতে আমি কি করব? ২৬

প্রশ্ন ৫১। কেউ কেউ সর্বদা আমার ছবিতে মন্তব্য করছে এবং ব্যক্তিগত / পাবলিক গ্রুপে হয়রানিমূলক মন্তব্য পোস্ট করছে। আমি কি করতে পারি?.. ২৬

প্রশ্ন ৫২। আমার এক বন্ধু ইচ্ছাকৃতভাবে আমার কিছু তথ্য সামাজিক যোগাযোগ মাধ্যমে প্রকাশ করেছে। এই বিষয়ে আমার কাকে রিপোর্ট করা উচিত এবং রিপোর্ট করার উপায় কী? ২৭

প্রশ্ন ৫৩। আমি অনলাইনে আছি এবং সোশ্যাল মিডিয়া/ চ্যাটরুমে অপরিচিত এক ব্যাক্তির সাথে চ্যাট করি। তাকে কি আমার ঠিকানা বা ফোন নম্বর দেওয়া ঠিক হবে যাতে আমরা একত্রিত হতে পারি?..................২৭

প্রশ্ন ৫৪। আপনি যদি সোশ্যাল মিডিয়ায় কিছু পোস্ট করেন, তাহলে কে তা দেখতে পাবে? ২৭

প্রশ্ন ৫৫। আমি অনলাইনে কাদের কাছ থেকে ফ্রেন্ড রিকোয়েস্ট গ্রহণ করব?....................................২৭

প্রশ্ন ৫৬। আমি একজন ব্যক্তির কাছ থেকে একটি নতুন বন্ধু অনুরোধ পেয়েছি যার প্রোফাইল ছবি নেই, কিন্তু আমি আমার ক্লাসে এই নামে একজন সহপাঠী আছে । আমার কি ফ্রেন্ড রিকুয়েস্ট গ্রহন করা উচিত ?...............২৭

প্রশ্ন ৫৭। আমি সোশ্যাল মিডিয়ায় কি ধরনের কন্টেন্ট পোস্ট করব?.. ২৮

প্রশ্ন ৫৮। সোশ্যাল মিডিয়া কীভাবে মানসিক স্বাস্থ্যের উপর প্রভাব ফেলে? ২৮

প্রশ্ন ৫৯। সোশ্যাল মিডিয়া কি আপনার তথ্য ব্যবসায়িক কাজে ব্যবহার করে? ২৮

প্রশ্ন ৬০। সোশ্যাল মিডিয়ায় কিভাবে ভুয়া খবর শনাক্ত করা যায়? ২৮

প্রশ্ন ৬১। গুগল থেকে ছবি ডাউনলোড করে সোশ্যাল মিডিয়ায় ব্যবহার করা কি ঠিক? ২৮

প্রশ্ন ৬২। আমার অ্যাকাউন্টের নাম কি দেওয়া উচিত? ২৮

প্রশ্ন ৬৩। স্যোশাল মিডিয়াতে লগইন করার পূর্বে করনীয় বিষয়? ২৮

প্রশ্ন ৬৪। আমার স্যোশাল মিডিয়া একাউন্ট আমার ডিভাইস ছাড়া অপরিচিত কোন ডিভাইসে লগইন আছে কিনা কিভাবে বুঝব?..২৯

অধ্যায়-৮: মহিলা ও কিশোরীদের সাইবার নিরাপত্তা ৩০

প্রশ্ন ৬৫। আমার একটা ব্যক্তিগত ছবি সোশ্যাল মিডিয়ায় কেউ ছড়িয়ে দিয়েছে। এখন আমার করণীয় কি? আমি কিভাবে বন্ধ করতে পারি? ৩০

প্রশ্ন ৬৬। অন্য ব্যক্তি আমার ব্যক্তিগত ভিডিও ইউটিউবে আপলোড করেছে। এক্ষেত্রে আমার করণীয় কি? এই ভিডিও বন্ধ করার উপায় কি?... ৩০

প্রশ্ন ৬৭। আমার ছবি এবং ভিডিও আমার বয়ফ্রেন্ড/ছেলে বন্ধুকে দিয়েছিলাম। পরবর্তীতে সে বিদেশী একটি অ্যাডাল্ট সাইটে সেই ছবি এবং ভিডিও ছড়িয়ে দেয়। এক্ষেত্রে এই ছবি/ভিডিও গুলো কিভাবে বন্ধ করবো?. ৩০

প্রশ্ন ৬৮। আমার ফেসবুক আইডি থেকে ছবি নিয়ে এডিট করে সোশ্যাল মিডিয়ায় ছড়িয়ে দেয়া হয়েছে এবং কল করে আমাকে বিরক্ত করা হচ্ছে। এক্ষেত্রে করণীয় কি? ৩০

প্রশ্ন ৬৯। আমার ম্যাসেঞ্জারে অশ্লীল ছবি, পর্ণোগ্রাফি পাঠিয়ে হয়রানি করা হচ্ছে। আমি কিভাবে বন্ধ করতে পারি? ৩১

প্রশ্ন ৭০। আমার নাম, ছবি ব্যবহার করে ফেইক আইডি খুলে বিভিন্ন জনকে কল গার্ল হিসেবে আমার নম্বর প্রদান করা হচ্ছে। আমার করণীয় কি? ৩১

প্রশ্ন ৭১। ব্রেক আপ হয়ে যাওয়ার পর আমার বয়ফ্রেন্ড/ছেলে বন্ধু বিভিন্ন ব্যক্তিগত ছবি ও ভিডিও ছড়িয়ে দেয়ার হুমকি দিয়ে ব্ল্যাকমেইল করে টাকা দাবি করছে। আমার করণীয় কি?...৩১

প্রশ্ন ৭২। আমার নিজের একটি ডিজিটাল ছবি আমি অনলাইনে পরিচয় হওয়া কোন ব্যক্তির কাছে দেখাতে চাই। এটা কি সেই ব্যক্তির কাছে পাঠানো ঠিক হবে? ৩১

অধ্যায়-৯: অনলাইনে শিশুদের নিরাপত্তা.. ৩২

প্রশ্ন ৭৩। আমার বাচ্চা রাত জেগে ইন্টারনেট ব্যবহার করে। আমি কিভাবে মনিটর করতে পারি? ৩২

প্রশ্ন ৭৪। আমার বাচ্চারা পড়াশোনার জন্য ল্যাপটপ ব্যবহার করে কিন্তু সেখানে বিভিন্ন ধরণের অ্যাডাল্ট অ্যাড আসে। সেটা কিভাবে বন্ধ করা যায়?... ৩২

প্রশ্ন ৭৫। তরুন বা শিশুদের জন্য অনলাইনে কি কোন বুলিং বিরোধী টুলস আছে কি ?........................৩৩

প্রশ্ন ৭৬। আমার ছেলেমেয়েরা অতিরিক্ত ডিজিটাল ডিভাইস ব্যবহার করছে। এক্ষেত্রে করণীয় কি? ৩৩

প্রশ্ন ৭৭। আমার ছেলেমেয়েরা ডিজিটাল ডিভাইস ব্যবহার করে অযাচীত/ ক্ষতিকর সাইট ব্রাউস করছে। এক্ষেত্রে করণীয় কি?...৩৩

প্রশ্ন ৭৮। ডিজিটাল ডিভাইস থেকে শিশুকে দূরে রাখতে করণীয় ৩৪

অধ্যায়-১০: সরকারি দপ্তরে সাইবার নিরাপত্তা... ৩৫

সম্ভাষণ (Greetings)

<u>Opening Greetings:</u> আসসলামু আলাইকুম, ডিজিটাল নিরাপত্তা এজেন্সির Help Desk থেকে XXX বলছি, কিভাবে সহযোগিতা করতে পারি।

<u>Holding Greetings:</u> খুবই দুঃখিত স্যার। আপনাকে সঠিক তথ্যটি দেওয়ার জন্য আমার কিছুটা সময়ের প্রয়োজন, আমি কি আপনাকে কিছু সময়ের জন্য অপেক্ষায় রাখতে পারি?

<u>Unhold Greetings:</u> সময় দিয়ে সহযোগিতা করার জন্য অসংখ্য ধন্যবাদ।

<u>Further Greetings:</u> ধন্যবাদ স্যার । আর কোনো তথ্য দিয়ে সহযোগিতা করতে পারি কি?

<u>End Greeting:</u> ডিজিটাল নিরাপত্তা এজেন্সির Help Desk-এ কল করার জন্য আপনাকে অসংখ্য ধন্যবাদ। আর কোন বিষয়ে কি আমি আপনাকে সাহায্য করতে পারি?

কল সেন্টার অপারেটর কর্তৃক অনুসরনীয় উত্তম চর্চাসমূহ

করনীয়:

- প্রফুল্ল ও উৎসাহী ভঙ্গিতে সম্ভাষণ জানান।
- কলার/সেবাপ্রার্থী বিচলিত বা উত্তেজিত হয়ে উঠলে ঠান্ডা মেজাজে তাকে শান্ত করতে চেষ্টা করুন।
- শুরুতেই সেবাপ্রার্থীর নাম জেনে নিন এবং তার নাম ব্যবহার করে (জনাব/মিজ XXX) সম্বোধন করুন। এর ফলে তিনি আপনার সঙ্গে সমস্যা নিয়ে আলাপ করতে স্বাচ্ছন্দ্য বোধ করবেন।
- সেবাপ্রার্থীর সমস্যা মনযোগ দিয়ে শুনুন। তিনি কেন কল করেছেন এবং তার সমস্যা প্রকৃতপক্ষে কি তা চিহ্নিত করার অন্যতম উপায় হলো মনযোগ দিয়ে তার বক্তব্য শোনা।
- সমস্যা সম্পর্কে বিস্তারিত/সুনির্দিষ্ট ধারনা পাওয়ার জন্য অনুসন্ধানমূলক (probing) প্রশ্ন করুন।
- মার্জিত ভাষায় প্রশ্ন করুন।
- সেবাপ্রার্থীর গোপনীয়তা রক্ষা করুন।
- কলার উত্যক্ত করার চেষ্টা করলে অথবা অশালীন ভাষা ব্যবহার করলে তাকে প্রথমে সেবা সম্পর্কে বুঝিয়ে বলুন। এতে তিনি শান্ত না হলে এ বিষয়ে আইনী ব্যবস্থা নেওয়া হতে পারে তা তাকে জানিয়ে দিন।

বর্জনীয়:

- কলারের/প্রশ্নকারীর একান্ত ব্যক্তিগত কোনো বিষয়ে প্রশ্ন করা যাবে না।
- গোপনীয় কোনো তথ্য বা পাসওয়ার্ড জানতে চাওয়া যাবে না।
- ক্রেডিট কার্ড, ব্যাংক একাউন্ট বা মোবাইল ফাইনান্সিয়াল সার্ভিস সংক্রান্ত কোনো গোপনীয় তথ্য জানতে চাওয়া যাবে না।
- কলের মাঝে হুট করে লাইন কেটে দিবেন না। পুরো আলাপ সমাপ্ত হতে দিন।
- সেবাপ্রার্থীকে কোনো অসত্য তথ্য প্রদান করবেন না। আপনার প্রতিষ্ঠান যে সেবা প্রদান করেন না সে সম্পর্কে কোনো মিথ্যা আশ্বাস প্রদান করবেন না।
- সেবাপ্রার্থীকে দীর্ঘ সময়ের জন্য অপেক্ষায় রাখবেন না।
- যথাযথ অনুমোদন ব্যাতীত কোনো তথ্য অন্য কারো সাথে শেয়ার করা যাবে না।

অধ্যায়-১: ডিজিটাল ডিভাইসের নিরাপদ ব্যবহার

প্রশ্ন ১। কিভাবে শক্তিশালী পাসওয়ার্ড সেট করা যায়?

- কমপক্ষে ৮ থেকে ১২ অক্ষরের পাসওয়ার্ড দিন।
- ইংরেজী ছোট হাতের এবং বড় হাতের অক্ষর ও সংখ্যা মিশিয়ে পাসওয়ার্ড তৈরী করুন।
- পাসওয়ার্ডে স্পেশাল ক্যারেক্টার (যেমন, $★~#@[= ইত্যাদি) যোগ করুন।
- পাসওয়ার্ডে কখনই নিজের নাম, জন্ম তারিখ, গ্রামের নাম, বাবার নাম কিংবা ফোন নাম্বার দিবেন না।
- QWERTY বা ABCDEFG বা 123456 ইত্যাদি সহজ পাসওয়ার্ড ব্যবহার করবেন না।
- প্রতিটি একাউন্টের জন্য অনন্য পাসওয়ার্ড ব্যবহার করুন।
- পাসওয়ার্ড কখনই কাউকে বলবেন না।
- অন্যের ফোনে বা কম্পিউটারে লগইন করলে তা লগআউট করতে ভুলবেন না।
- নিয়মিত পাসওয়ার্ড পরিবর্তন করুন।

প্রশ্ন ২। আমার পাসওয়ার্ড কিভাবে নিরাপদে সংরক্ষণ করতে পারি?

- শক্তিশালী পাসওয়ার্ড ব্যবহার করুন।
- টু-ফ্যাক্টর অথেনটিকেশন ব্যবহার করুন। (প্রশ্ন ১৬ থেকে বিস্তারিত)
- পাসওয়ার্ড কোথাও লিখে রাখবেন না।
- পাসওয়ার্ড কারো নিকট প্রকাশ করবেন না।
- পাসওয়ার্ড ম্যানেজার এ্যাপ ব্যবহার করুন।
- অপ্রয়োজনীয় এ্যাপ ও ব্রাউজার এক্সটেনশন রিমুভ করুন।
- সম্ভব হলে নিজের প্রতিষ্ঠানের বা সরকারের তৈরি এনক্রিপশন এলগরিদম ব্যবহার করে পাসওয়ার্ড সংরক্ষণ করুন।

প্রশ্ন ৩। কিভাবে এলার্ট নোটিফিকেশন ব্যবহার করা যায়?

- আপনার ফোনের সেটিংস অ্যাপ খুলুন।
- নোটিফিকেশন ট্যাপ করুন এবং ম্যানেজ নোটিফিকেশন চাপুন।
- যেকোনো একটি অ্যাপ চাপুন।
- সতর্কতা (alert) নির্বাচন করুন।

প্রশ্ন ৪। নতুন ব্যবহারকারী তার ডিভাইস সুরক্ষিত রাখতে কি কি করবেন?

- শক্তিশালী পাসওয়ার্ড/প্যাটার্ন ব্যবহার করুন।
- Advanced Security Option/বায়োমেট্রিক ফিচার যেমন- ফেস রিকগনিশন, আইরিশ স্ক্যানার থাকলে সেগুলো ব্যবহার করতে পারেন।
- সুনির্দিষ্ট কোনো ফাইল/ অ্যাপ সিকিউরড করতে চাইলে তার জন্য আলাদা ফাইল এনক্রিপশন / ২ ফ্যাক্টর অথেনটিকেশন ব্যবহার করুন।

প্রশ্ন ৫। পার্সোনাল কম্পিউটার সুরক্ষার ক্ষেত্রে করণীয় কি?

- একাউন্টে লগ ইনের জন্য পাসওয়ার্ড ব্যবহার করুন।
- উইন্ডোজ ডিফেন্ডার অন রাখুন।
- এন্টি-ভাইরাস ব্যবহার করুন।
- উইন্ডোজ সবসময় হালনাগাদ রাখুন।
- সিকিউরড (Secured) নয় এমন ওয়েবসাইট ব্রাউজ করা থেকে বিরত থাকতে হবে। (প্রশ্ন ২০ থেকে বিস্তারিত)

  বি.দ্র.: আপনি যদি উইন্ডোজ ১১, ১০ বা ৮ ব্যবহার করে থাকেন, তবে আগে থেকেই উইন্ডোজ ডিফেন্ডার ইন্সটল হয়ে আছে। আর তা চেক করার জন্য আপনি টাস্কবারের Show Hidden Icons অপশনটিতে ক্লিক করে দেখে নিতে পারেন।

প্রশ্ন ৬। ডিজিটাল ডিভাইস/ কম্পিউটার সিস্টেমে পাসওয়ার্ড হ্যাক করে/ বেআইনি প্রবেশ রোধে কি করণীয়?

- ডিজিটাল ডিভাইসের সেটিংসে গিয়ে পাসওয়ার্ড/ প্যাটার্ন/ বায়োমেট্রিক লক করুন।
- গুরুত্বপূর্ণ ফাইলসমুহকে এনক্রিপ্ট (Encrypt) করে রাখুন।
- কোন অবস্থাতেই মোবাইল ফোনকে অযত্ন অবস্থায় ফেলে রাখবেন না।
- প্রয়োজন না থাকলে অথবা নতুন/অপরিচিত জায়গায় গেলে বা রাস্তায় চলাচলের সময় মোবাইলের ব্লু-টুথ, ওয়াই ফাই অফ করে রাখুন এবং খেয়াল রাখুন ব্লুটুথ যেন আটোমেটিক অন না হয়ে যায়।

  বি.দ্র.: এনক্রিপশন হলো তথ্যের এমন একটি রূপান্তকরন প্রক্রিয়া যার মাধ্যমে তথ্যগুলি অননুমোদিত (unauthorized) ব্যবহারকারীদের কাছে অপঠনযোগ্য করে তোলা হয়।

প্রশ্ন ৭। কিভাবে নিরাপদে ইউএসবি পেনড্রাইভ ব্যবহার করতে পারি?

- যতটা সম্ভব পেন ড্রাইভ ব্যবহার পরিহার করুন। এর পরিবর্তে ইমেইল/গুগল ড্রাইভ ব্যবহার করুন।
- পেন ড্রাইভে রাইট প্রটেকশন সুইচ থাকলে তা অন করুন, না থাকলে রাইট প্রটেকশন সফটওয়্যার ব্যবহার করুন। (সার্চ করলে সফটওয়্যার এর নাম জানা যাবে)

- ইউএসবি এন্টি-ভাইরাস ব্যবহার করুন।
- প্রাইভেসি রক্ষা করতে চাইলে বা ব্যক্তিগত/গোপনীয় তথ্যের নিরাপত্তার জন্য এনক্রিপশন সফটওয়্যার ব্যবহার করতে পারেন।
- পেন ড্রাইভ ওপেন করার পুর্বে ভাইরাস স্ক্যান করুন।

প্রশ্ন ৮। আমার ডকুমেন্ট/সফটওয়্যার/কম্পিউটার খুলতে পারছি না। অথবা আমি ভাইরাস/ ম্যালওয়্যার দ্বারা আক্রান্ত হয়েছি। এখন কি করতে পারি?

(ক) কম্পিউটার রিস্টোর করুন (Last known good backup থেকে)। স্টার্ট মেনু থেকে All Programs→ Accessories→ System Tools→ System Restore নির্বাচন করুন।

(খ) ভাইরাস স্ক্যান করুন। ভাইরাস দূর করতে না পারলে সবকিছু মুছে ফেলে ক্লিন ইন্সটল করুন। এ বিষয়ে আপনার দপ্তরের সিস্টেম এনালিস্ট/মেইন্টেনেন্স ইঞ্জিনিয়ার/প্রোগ্রামারের সহায়তা নিন।

(গ) উইন্ডোজ এবং অন্যান্য সফটওয়্যার হালনাগাদ করুন। স্টার্ট মেনুতে update লিখে সার্চ করুন।

(ঘ) মোবাইল ডিভাইস হলে ফ্যাক্টরি রিসেট করুন।

- বেশিরভাগ ফোনে সেটিংস অ্যাপের মাধ্যমে আপনার ফোন রিসেট করতে পারেন।
- যদি আপনার ফোনের সেটিংস অ্যাপ খুলতে না পারেন, তাহলে ফোনের পাওয়ার এবং ভলিউম বোতাম ব্যবহার করে ফ্যাক্টরি রিসেট করার চেষ্টা করতে পারেন।
- ফোন প্রস্তুতকারকের সাপোর্ট সাইটে আরও বিস্তারিত জানতে পারবেন।

প্রশ্ন ৯। ডিজিটাল ডিভাইস/ কম্পিউটার সিস্টেম হতে কোনো তথ্য উপাত্ত সংগ্রহ/ স্থানান্তর রোধে কি করণীয়?

- গুরুত্বপূর্ণ তথ্য উপাত্ত এনক্রিপ্ট করে রাখুন।
- ফাইল সহজে শেয়ার করা যায় এমন সফটওয়্যার ব্যবহার থেকে বিরত থাকুন (যেমন: ShareIt)।
- প্রয়োজন না থাকলে অথবা নতুন/অপরিচিত জায়গায় গেলে বা রাস্তায় চলাচলের সময় মোবাইলের ব্লু-টুথ, ওয়াই ফাই অফ করে রাখুন এবং খেয়াল রাখুন যেন ব্লুটুথ যেন আটোমেটিক অন না হয়ে যায়।
- **Near Field Communication (NFC)** জাতীয় কোন প্রযুক্তি কার্যকর থাকলে সতর্ক থাকুন
- মোবাইলকে অপরিচিত কোনো ব্যক্তির হাতে/ব্যাগের কাছাকাছি না রাখুন।

বি.দ্র.: “**Near Field Communication**” দ্বারা অনেক কম দূরত্বের দুটি ডিভাইসের মধ্যে কমিউনিকেট করা যায়।

প্রশ্ন ১০। আমার মোবাইলে আমার ব্যক্তিগত ছবি ছিলো। আমি কারো সাথে এটা শেয়ার করি নি। এটা কিভাবে সোশ্যাল মিডিয়াতে/ফেসবুকে ছড়িয়ে গেলো?

(ক) আপনি কি ডিভাইসটি মেরামত করতে দিয়েছিলেন?

আপনার ডিভাইসটি কোনো কারণে নষ্ট হলে, আপনি স্বাভাবিকভাবেই সেটি মেরামত করতে দিবেন। কিন্তু সেখান থেকেই আপনার অতি ব্যক্তিগত ছবি বা ভিডিও দিয়ে ব্ল্যাকমেইল করা হতে পারে। এ থেকে পরিত্রাণের জন্য নিচের ধাপগুলো অনুসরণ করতে পারেন:

- কোন ডিভাইস নষ্ট হলে বা নষ্ট হওয়ার উপক্রম হলে সেই ডিভাইস থেকে সামাজিক যোগাযোগ মাধ্যমে কানেক্টেড সমস্ত কিছু থেকে লগআউট করুন;
- সকল ডাটা সিকিউর ডিলিট করুন;
- যে ধরনের ছবি দিয়ে মানুষকে ব্ল্যাকমেইল করা যায়, এ ধরনের ছবি বা ভিডিও করার প্রয়োজন নেই। তারপরও অতি ব্যক্তিগত ছবি বা ভিডিও করলে তা নিরাপদে রাখার দায়িত্ব ব্যক্তিকেই নিতে হবে।

(খ) আপনি ডিভাইসটি অন্য কাউকে ব্যবহার করতে দিয়েছিলেন?

অন্য কাউকে মোবাইল ব্যবহার করতে দিলে আপনার চোখের আড়াল হতে দিবেন না। একান্তই যদি দিতে হয় তবে দেওয়ার আগে গেস্ট মোড চালু করুন। অ্যান্ড্রয়েডে গেস্ট মোড চালু করতে হলে যে ধাপগুলো অনুসরণ করুন:

- ➢ নোটিফিকেশন বারটি টানতে স্ক্রিনের উপর থেকে নীচে সোয়াইপ করুন।
- ➢ উপরে ডানদিকে আপনার প্রোফাইল ছবিতে দুবার আলতো চাপুন।
- ➢ এখন আপনি তিনটি আইকন দেখতে পাবেন - আপনার গুগল অ্যাকাউন্ট, অতিথি (গেস্ট) যোগ করুন এবং ব্যবহারকারী যুক্ত করুন।
- ➢ অতিথি (গেস্ট) যোগ করতে আলতো চাপুন।
- ➢ এখন আপনার স্মার্টফোন গেস্ট মোডে চলে যাবে।

(গ) আপনার ইমেইল/গুগল/ড্রাইভ/ফটোস একাউন্ট অন্য কোনো ডিভাইসে লগইন করেছিলেন কিনা?

অন্য ডিভাইসে লগইন করলে সেখান থেকে কেউ ছবি নিয়ে থাকতে পারে।

(ঘ) আপনার মোবাইলে কি পাসওয়ার্ড/প্যাটার্ন সেট করা আছে?

না থাকলে চালু করুন।

প্রশ্ন ১১। পাবলিক ওয়াই-ফাই ব্যবহারের বিষয়ে কি কি সতর্কতা অবলম্বন করা প্রয়োজন?

- ওয়াই-ফাই এর নাম লক্ষ্য করুন। সম্ভব হলে দায়িত্বপ্রাপ্ত কারো নিকট থেকে বা ওয়েবসাইট থেকে ভেরিফাই করে নিন।
- শেয়ারিং অপশন বন্ধ করুন।
- VPN ব্যবহার করুন (ব্যবহারের পদ্ধতি জানিয়ে দেওয়া যেতে পারে)।
- HTTPS ব্যবহার করুন (ব্যবহারের পদ্ধতি জানিয়ে দেওয়া যেতে পারে)।
- ফায়ারওয়াল চালু করুন (চালু করার পদ্ধতি জানিয়ে দেওয়া যেতে পারে)।
- এন্টি ভাইরাস ব্যবহার করুন (ফ্রি এন্টি ভাইরাসের নাম জানিয়ে দেওয়া যায়)।

প্রশ্ন ১২। পার্সোনাল ওয়াইফাই পার্শ্ববর্তী অন্য কেউ ব্যবহার করলে করণীয় কি?

- রাউটার এর ডিফল্ট ইউজার আইডি, পাসওয়ার্ড চেঞ্জ করুন।
- সহজে অনুমানযোগ্য নয় এমন ওয়াইফাই পাসওয়ার্ড সেট করুন।
- সম্ভব হলে SSID/ওয়াইফাই এর নাম গোপন রাখুন।

অধ্যায়-২: নিরাপদ ইন্টারনেট ব্যবহার

প্রশ্ন ১৩। ফিশিং ও স্পুফিং কি?

- **ফিশিং** একধরনের সাইবার আক্রমণ যেক্ষেত্রে একটি বিশ্বস্ত একাউন্ট থেকে পাঠানো ইমেইলের মত হুবুহ দেখতে নকল ইমেইলের মাধ্যমে আক্রমন করা হয়। এর উদ্দেশ্য হয় ক্রেডিট কার্ড এবং লগইন তথ্যের মতো সংবেদনশীল ডেটা চুরি করা বা ভুক্তভোগীর মেশিনে ম্যালওয়্যার ইনস্টল করা। ফিশিং মেইলে ভয়, কৌতূহল এবং লোভের মতো আবেগ ব্যবহার করা হয়, যার ফলে প্রাপকরা সংযুক্তি খুলতে বা লিঙ্কে ক্লিক করতে আগ্রহী হয়।
- **স্পুফিং**-এর মূল লক্ষ্য ব্যক্তিগত তথ্য চুরি করা, অর্থ চুরি করা, নেটওয়ার্ক নিয়ন্ত্রণ বাইপাস করা বা সংক্রামিত সংযুক্তি বা লিঙ্কের মাধ্যমে ম্যালওয়্যার ছড়িয়ে দেওয়া। ওয়েবসাইট, ইমেইল, ফোন কল, টেক্সট, আইপি ঠিকানা এবং সার্ভারের মাধ্যমে স্পুফিং ঘটতে পারে।
- ফিশিং এর উদ্দেশ্য হল ব্যবহারকারীকে নিজে থেকে ব্যক্তিগত তথ্য প্রদান করার জন্য উৎসাহী করা। স্পুফিংয়ের উদ্দেশ্য হলো অপরাধ সংঠনের জন্য তথ্য চুরি করা বা ছদ্মবেশ ধারণ করা। উভয় প্রক্রিয়াই ছদ্মবেশ ধারণ এবং তথ্যের মিথ্যা উপস্থাপনের মাধ্যমে প্রতারণামূলক কার্যক্রম সম্পাদন করে।

প্রশ্ন ১৪। আমাকে অযাচিতভাবে বিজ্ঞাপন মেইল/এসএমএস প্রেরণ করা হয়েছে। সেক্ষেত্রে করণীয় কি?

- মেইলটিকে স্প্যাম হিসেবে চিহ্নিত করুন।
- মেইলের সেটিংস অপশনে গিয়ে সংশ্লিষ্ট সেন্ডারকে ব্লক করুন।
- BTRC অযাচিত এসএমএস এর অপশন বন্ধ করার জন্য সুযোগ দিয়েছে। সেটা কার্যকর করা যেতে পারে। (১২১*১১০১# ডায়াল করে ডু নট ডিস্টার্ব সেবা চালু করা যাবে)

প্রশ্ন ১৫। সন্দেহজনক ইমেইল/মেসেজ কিভাবে চিহ্নিত করব?

- আপনাকে পাসওয়ার্ড বা অন্য কোনো ব্যক্তিগত তথ্যসহ ই-মেইলের জবাব দিতে বলে থাকলে।
- ইমেইলে আপনার অ্যাকাউন্টের বিশদ বিবরণ জানতে চাইলে।
- ইমেইল ঠিকানা লক্ষ্য করুন। দুর্বল ব্যাকরণ এবং ভুল বানান আছে কিনা।
- ডোমেইন নাম ঠিক আছে কিনা। অপরিচিত ডোমেইন হলে তার সত্যতা যাচাই করুন।
- প্রলোভন প্রদান করে থাকলে।

- ইমেইল/মেসেজে যোগাযোগের জন্য ইমেইল/ফোন নম্বর/ঠিকানা দেওয়া থাকলে তা পরিহার করুন, বরং নিজে যোগাযোগের ফোন নম্বর/ইমেল ঠিকানা খুঁজে বের করুন।

প্রশ্ন ১৬। জিমেইল/ফেসবুক একাউন্টে প্রমাণীকরণ ধাপ (authentication step) কিভাবে যোগ করব?

দ্বি-ধাপ যাচাইকরণ বা প্রমাণিকরণ (2 factor authentication নামেও পরিচিত), এর মাধ্যমে আপনার অ্যাকাউন্টে সুরক্ষার একটি অতিরিক্ত স্তর যুক্ত করতে পারেন। এর ফলে আপনার পাসওয়ার্ড চুরি হয়ে গেলেও আপনার একাউন্টে প্রবেশ প্রতিরোধ করা যাবে।

- বিকল্প এক: আপনার ফোন নম্বর যোগ করুন এবং এসএমএস এর মাধ্যমে কোড প্রেরণ চালু করুন। আপনি এসএমএস এর মাধ্যমে একটি নিশ্চিতকরণ কোড পাবেন।
- বিকল্প দুই: প্রমাণীকরণ (authentication) অ্যাপ চালু করুন। অ্যাপটি আপনাকে সেট-আপ করার ধাপগুলি জানিয়ে দিবে।

(ক) জিমেইলের ক্ষেত্রে

- আপনার গুগল অ্যাকাউন্ট খুলুন।
- নেভিগেশন প্যানেলে, security (নিরাপত্তা) নির্বাচন করুন।
- “Signing in to Google,” (গুগলে প্রবেশ করুন) এর অধীনে, 2-Step Verification (দ্বি-ধাপ যাচাইকরণ) নির্বাচন করুন এবং তারপরে শুরু করুন।
- পরবর্তী ধাপগুলি অনুসরণ করুন।

(খ) ফেসবুকের ক্ষেত্রে-

- উপরের ডান দিকে ক্লিক করুন। নিচে স্ক্রোল করুন এবং সেটিংস চাপুন।
- নিচে স্ক্রোল করুন এবং নিরাপত্তা এবং লগইন চাপুন।
- নিচে স্ক্রোল করুন এবং Use two-factor authentication (দুই-ফ্যাক্টর প্রমাণীকরণ ব্যবহার করুন) চাপুন। এই সময় আপনার পাসওয়ার্ড লিখতে বলা হতে পারে।
- প্রমাণীকরণ অ্যাপ ব্যবহার করুন অথবা এসএমএস ব্যবহার করুন চাপুন।

প্রশ্ন ১৭। জিমেইল/ফেসবুক একাউন্ট পুনরুদ্ধার কিভাবে করব?

(ক) জিমেইলের ক্ষেত্রে

- পাসওয়ার্ড ভুলে গেলে ‘পাসওয়ার্ড মনে নেই’ (forgot password) বাটনে চাপুন। পরবর্তী নির্দেশনাসমূহ অনুসরণ করুন।
- ইমেইল এড্রেস ভুলে গেলে ‘ইমেল আইডি ভুলে গেছেন?’ (forgot email?) বাটনে চাপুন। পরবর্তী নির্দেশনাসমূহ অনুসরণ করুন।

- আরও বিস্তারিত জানতে support.google.com/accounts লিঙ্কে ভিজিট করুন।

(খ) ফেসবুকের ক্ষেত্রে

- আপনি যে অ্যাকাউন্টটি পুনরুদ্ধার করতে চান তার প্রোফাইলে যান।
- কভার ছবির নীচে, more বাটন এবং Find support বা রিপোর্ট প্রোফাইল নির্বাচন করুন।
- Something else সিলেক্ট করুন, তারপর submit চাপুন।
- Recover this account (এই অ্যাকাউন্টটি পুনরুদ্ধার করুন) চাপুন এবং ধাপগুলি অনুসরণ করুন।

আরও বিস্তারিত জানতে Facebook Help Centre (www.facebook.com/help/) লিঙ্কে ভিজিট করতে পারেন।

প্রশ্ন ১৮। আমি একটি সন্দেহজনক ইমেল বা বার্তা পেয়েছি/আমি অচেনা কারো কাছ থেকে একটি সংযুক্তি সহ একটি ইমেল পেয়েছি। আমার কি করা উচিত?

- নিশ্চিত হওয়ার পূর্বে ইমেইল খুলবেন না বা কোনো লিঙ্কে ক্লিক করবেন না।
- যে প্রতিষ্ঠান থেকে ইমেইল প্রেরণ করা হয়েছে বলে দাবি করা হচ্ছে তার ওয়েবসাইট পরীক্ষা করুন। লক্ষ্য করুন সেখানে বলেছে কিনা তারা কখনোই আপনার পাসওয়ার্ড চাইবে না।
- সন্দেহজনক মেইল হিসেবে নিশ্চিত হলে স্প্যাম হিসেবে চিহ্নিত করুন।

প্রশ্ন ১৯। নিরাপদে ইন্টারনেট ব্যবহারের জন্য আমি কি করতে পারি?

- অপরিচিত/সন্দেহজনক একাউন্ট থেকে প্রাপ্ত মেইল খুলবেন না।
- আপনার ডিভাইসগুলি নিয়মিত হালনাগাদ করুন।
- শক্তিশালী পাসওয়ার্ড ব্যবহার করুন। (প্রশ্ন-১)
- টু-ফ্যাক্টর অথেনটিকেশন ব্যবহার করুন। (প্রশ্ন-১৬)
- অস্বাভাবিক মনে হয় এমন লিঙ্কগুলিতে ক্লিক করবেন না।
- অনিরাপদ পাবলিক ওয়াই-ফাই ব্যবহার এড়িয়ে চলুন। (প্রশ্ন-১১)
- নিয়মিত আপনার ডেটা ব্যাক-আপ করুন।
- ব্যাংক এবং আর্থিক প্রতিষ্ঠানের তথ্যের বিষয়ে সতর্ক থাকুন।

প্রশ্ন ২০। নকল ওয়েবসাইট কিভাবে চিনতে পারব?

- এড্রেস বার লক্ষ্য করুন। তালা চিহ্ন আছে কিনা?
- ডোমেইন নাম চেক করুন।
- ডোমেইনের বয়স চেক করুন (ডমেইন এজ চেকার দিয়ে)।

- দুর্বল ব্যাকরণ এবং ভুল বানান লক্ষ্য করুন।
- যোগাযোগের তথ্য নির্ভরযোগ্য কিনা তা লক্ষ্য করুন।

প্রশ্ন ২১। পরিচিত কারো কাছ থেকে সন্দেহজনক বার্তা পেলে কি ধরণের সতর্কতা অবলম্বন করা উচিত?

- যদি ঘনিষ্ঠ কোন বন্ধু বা ফেসবুক বন্ধুর কাছ থেকে কোন ইমেইল, মেসেঞ্জারে বার্তা, বা পোস্ট পান, যা তার স্বাভাবিক আচরণের সঙ্গে মেলে না, সবচেয়ে ভালো হবে সেটায় ক্লিক না করা বা সাড়া না দেওয়া।
- যেমন কেউ হয়তো লিখতে পারে, সে কোথাও বেড়াতে গিয়ে বিপদে পড়েছে অথবা আপনার মেসেঞ্জারে এমন একটি লিংক পাঠিয়েছে, যা পাঠানোর কোন কারণ নেই। এক্ষেত্রে তাকে আলাদাভাবে ফোন করে বা বার্তা পাঠিয়ে জিজ্ঞেস করতে পারেন।
- এ ধরণের সন্দেহজনক কিছু দেখলে স্যোশাল মিডিয়া কর্তৃপক্ষকে রিপোর্ট করুন।

প্রশ্ন ২২। আমি আমার ইন্টারনেট সার্ভিস প্রদানকারীর কাছ থেকে আমার পাসওয়ার্ড চাওয়ার একটি বার্তা পাই। তারা বলে আমার একাউন্ট ঠিক করার জন্য তাদের দরকার। আমার কি পাসওয়ার্ড তাদের দেওয়া উচিত হবে?

- আপনার অ্যাকাউন্টের পাসওয়ার্ড কখনই কাউকে দেওয়া উচিত নয় (এমনকি আপনার ঘনিষ্ঠ বন্ধুদেরও)।
- ইন্টারনেট সেবা প্রদানকারী অথবা কোন বৈধ প্রতিষ্ঠান কখনই আপনার কাছে পাসওয়ার্ড চাইবে না।
- হ্যাকাররা আপনার পাসওয়ার্ড পাওয়ার জন্য ইন্টারনেট সেবা প্রদানকারী বা অন্য কোনো বৈধ সংস্থার মিথ্যা পরিচয় দিতে পারে।
- আপনার ইন্টারনেট সেবা প্রদানকারীকে বিষয়টি ফোনে/ইমেইলে অবহিত করুন।

প্রশ্ন ২৩। আমি ফেসবুক, ইউটিউব বা কোনো সোশ্যাল মিডিয়ায় একটি পোস্ট দেখেছি, যেখানে অংশগ্রহণকারীরা সন্ত্রাস, জিহাদ এবং এরকম কিছু নিয়ে আলোচনা করেছে। আমার কি করা উচিৎ?

- পোস্টের স্ক্রিনশট নিন।
- সংশ্লিষ্ট লিঙ্ক এবং রেফারেন্স উল্লেখ করে সমস্যাটির বিষয়ে আপনার BGD-EGOV CIRT/NCERT-কে রিপোর্ট করুন।
- নিকটস্থ থানায় অবহিত করুন।

অধ্যায়-৩: হ্যাকিং/পরিচয় চুরি/র‍্যানসামওয়্যার

প্রশ্ন ২৪। অনলাইনে হুমকি বা পরিচয় চুরির শিকার হলে কি করব?

(ক) আপনি কি যে প্ল্যাটফরমের মাধ্যমে হুমকি প্রদান করা হচ্ছে তার এডমিন এর সঙ্গে যোগাযোগ করে বিষয়টি অবহিত করেছেন?

- না হলে যোগাযোগ করুন।
- হ্যাঁ হলে এবং তিনি কোনো সমাধান না দিয়ে থাকলে নিকটস্থ থানার সঙ্গে যোগাযোগ করুন (যোগাযোগের তথ্য প্রদান করুন)।

(খ) আপনার একাউন্ট পাসওয়ার্ড বা পরিচয় চুরি হয়ে থাকলে একাউন্ট পুনরুদ্ধারের চেষ্টা করুন। (প্রশ্ন ১৭)

(গ) পুনরুদ্ধারের পর দ্রুত পাসওয়ার্ড পরিবর্তন করুন। শক্তিশালী পাসওয়ার্ড ব্যবহার করুন এবং একটি প্রমাণীকরণ ধাপ (authentication step) যোগ করুন।

(ঘ) একই ধরণের পাসওয়ার্ড ব্যবহার করা হয়েছে এমন সকল একাউন্টের পাসওয়ার্ড পরিবর্তন করুন।

প্রশ্ন ২৫। আমি পরিচয় চুরির শিকার হয়েছি এবং ইতিমধ্যে হ্যাকারদের যোগাযোগের উত্তর দিয়েছি/কথামতো কাজ করেছি। এখন কি করনীয়?

- সংশ্লিষ্ট সোশ্যাল মিডিয়া এডমিনিস্ট্রেটরের কাছে রিপোর্ট করুন।
- গুরুত্বপূর্ণ সকল একাউন্টের পাসওয়ার্ড পরিবর্তন করুন।
- ব্যাংক স্টেটমেন্ট পরীক্ষা করুন। অস্বাভাবিক কিছু পরিলক্ষিত হলে সংশ্লিষ্ট ব্যাংক এবং আর্থিক প্রতিষ্ঠানের সঙ্গে যোগাযোগ করুন।
- প্রয়োজনে আইন প্রয়োগকারী সংস্থা/নিকটস্থ থানায় যোগাযোগ করুন।

প্রশ্ন ২৬। আমার পরিচয় চুরি (identity theft) কিভাবে প্রতিরোধ করব?

- ফিশিং এবং স্পুফিং সম্পর্কে সতর্ক থাকুন। (প্রশ্ন ১৩ থেকে বিস্তারিত)
- শক্তিশালী পাসওয়ার্ড ব্যবহার করুন এবং একটি প্রমাণীকরণ ধাপ (authentication step) যোগ করুন। (প্রশ্ন ১ এবং ২ থেকে বিস্তারিত)
- এলার্ট নোটিফিকেশন ব্যবহার করুন। (প্রশ্ন ৩ থেকে বিস্তারিত)
- আপনার মোবাইল ডিভাইসে পাসওয়ার্ড দিন।
- প্রাপ্ত মেইল/ম্যাসেজের লিংকে ক্লিক করা থেকে বিরত থাকুন। (প্রশ্ন ১৮ থেকে বিস্তারিত)
- www.haveibeenpwned.com- এর মতো সাইটগুলি বলতে পারে আপনার তথ্য কখনও প্রকাশিত হয়েছে কিনা, এমনকি ভবিষ্যতে যদি এটি ঘটে থাকে তবে আপনাকে সতর্কও করে।

প্রশ্ন ২৭। আমার হ্যাক হওয়া একাউন্ট পুনরুদ্ধার করেছি। এখন আমার কি করা প্রয়োজন?

- ইমেইল একাউন্ট হ্যাক হয়ে থাকলে পুনরুদ্ধারের পর আপনার ইমেল ফিল্টার এবং ফরওয়ার্ড করার অপশন পরীক্ষা করুন। হ্যাকররা অনেকক্ষেত্রেই ইমেইল ফরওয়ার্ডিং অপশন সেট করে যার ফলে আপনার সকল ইমেইলের একটি কপি তাদের কাছে চলে যায়। Gmail বা অন্য ইমেইল সেবাদানকারীর সাপোর্ট পেজে এ বিষয়ে বিস্তারিত জানা যাবে। (support.google.com/)
- হ্যাক হওয়া অ্যাকাউন্টের মতো পাসওয়ার্ড আছে এমন সকল অ্যাকাউন্টের পাসওয়ার্ড পরিবর্তন করুন। তারপরে হ্যাক হওয়া অ্যাকাউন্টে পাসওয়ার্ড রিসেট পাঠায় এমন অন্য সকল অ্যাকাউন্টের পাসওয়ার্ড পরিবর্তন করুন।
- টু-ফ্যাক্টর অথেনটিকেশন চালু করুন। এর ফলে ভবিষ্যতে কেউ একাউন্ট হ্যাক করতে চাইলে আপনার মোবাইলে নোটিফিকেশন পেয়ে যাবেন।
- আপনার একাউন্ট হ্যাক হয়েছিল এ বিষয়ে আপনার অ্যাকাউন্টের পরিচিতি, বন্ধু বা ফলোয়ারদের অবহিত করুন।
- ফিশিং ইমেইলের বিষয়ে সতর্ক থাকুন।

প্রশ্ন ২৮। আমার একাউন্ট হ্যাক/লক করে আমার কাছে টাকা চাইছে। এমন র‍্যানসমওয়্যার নোট পেলে কি করবেন? কম্পিউটার আনলক করার জন্য মুক্তিপণ দেওয়া কি উচিৎ হবে?

- র‍্যানসামওয়্যার নোট বা কম্পিউটারে প্রদর্শিত সমস্যা বা মেসেজের ছবি তুলুন বা স্ক্রিনশট নিন। ইমেইল বা অন্য কোনো প্রমাণক থাকলে তা সংগ্রহ করুন।

প্রোবিং প্রশ্ন: শুধু কি আপনার কম্পিউটার/একাউন্ট হ্যাক হয়েছে নাকি দপ্তরের সকল কম্পিউটার বা সার্ভার/সফটয়্যার সিস্টেম/নেটওয়ার্ক হ্যাক হয়েছে?

- শুধু আপনার কম্পিউটার হ্যাক হয়ে থাকলে তার নেটওয়ার্ক বিচ্ছিন্ন করুন। কারণ নেটওয়ার্কের সাথে যুক্ত থাকা অন্যান্য কম্পিউটারকেও র‍্যানসামওয়্যারটি আক্রমণ করতে পারে। ফায়ারওয়াল ব্যবহার করে পৃথক করুন বা নেটওয়ার্ক ডিসকানেক্ট করুন।
- র‍্যানসামওয়্যার একটিভ থাকাকালে ব্যাকআপ থেকে ফাইল রিস্টোর করতে যাবেন না, কোন লাভ হবে না। র‍্যানসামওয়্যারটি সিস্টেমে থাকলে নতুন ফাইলগুলো ও তাৎক্ষনিকভাবে আক্রান্ত হবে।
- সাইবার নিরাপত্তা সংক্রান্ত হলে বা দপ্তরের সকল কম্পিউটার বা সার্ভার/সফটয়্যার সিস্টেম/নেটওয়ার্ক হ্যাক হয়ে থাকলে ডিজিটাল নিরাপত্তা এজেন্সির আওতাধীন NCERT/BGD-eGOV CIRT এর সঙ্গে যোগাযোগ (ইমেইল অথবা ফোন নাম্বার জানানো হবে) করুন।
- হুমকি প্রদান করলে বা অর্থ চাইলে বা সাইবার ক্রাইমের উপাদান থাকলে আইন প্রয়োগকারী সংস্থার সঙ্গে যোগাযোগ করুন (নিকটস্থ থানার তথ্য জানানো হবে)।

- তথ্যের ব্যাকআপ থাকলে বা খুব গুরুত্বপূর্ণ তথ্য না থাকলে সকল তথ্য মুছে ফেলে ডিভাইস রিসেট করুন।

প্রশ্ন ২৯। র‍্যানসামওয়্যার আক্রমণ করে আমার ডিভাইস এর ডাটাকে নষ্ট করে দেওয়া হয়েছে। এক্ষেত্রে করণীয় কি?

- আক্রান্ত কম্পিউটারকে প্রথমেই নেটওয়ার্ক থেকে পৃথক করে ফেলুন (ফায়ারওয়াল থেকে পৃথক করুন বা নেটওয়ার্ক ডিসকানেক্ট করুন)। আপনার নেটওয়ার্ককে বিচ্ছিন্ন করে ফেলুন। কারণ নেটওয়ার্কের সাথে যুক্ত থাকা অন্যন্য কম্পিউটারকেও র‍্যানসামওয়্যারটি আক্রমণ করতে পারে।
- র‍্যানসামওয়্যার একটিভ থাকাকালে ব্যাকআপ থেকে ফাইল রিস্টোর করবেন না। র‍্যানসামওয়্যারটি সিস্টেমে থাকলে নতুন ফাইলগুলো ও তাৎক্ষনিকভাবে আক্রান্ত হবে।
- তথ্যের ব্যাকআপ থাকলে বা খুব গুরুত্বপূর্ণ তথ্য না থাকলে সকল তথ্য মুছে ফেলে ডিভাইস রিসেট করুন।
- র‍্যানসামওয়্যার নোট বা কম্পিউটারে প্রদর্শিত সমস্যা বা মেসেজের ছবি তুলুন বা স্ক্রিনশট নিন। ইমেইল বা অন্য কোনো প্রমাণক থাকলে তা সংগ্রহ করুন।
- হুমকি প্রদান করলে বা অর্থ চাইলে বা সাইবার ক্রাইমের উপাদান থাকলে আইন প্রয়োগকারী সংস্থার সঙ্গে যোগাযোগ করুন (নিকটস্থ থানার তথ্য জানানো হবে)।

বি.দ্র.: র‍্যানসামওয়্যার সব ম্যালওয়্যার এর মধ্যে ক্ষতিকর বলা যেতে পারে কারণ এটি যে সিস্টেমে আঘাত করে সেখানকার সকল ডকুমেন্ট, ফাইল লক করে ফেলে ও ফাইলগুলোর শেষে একটি ইউনিক extension জুড়ে যায়। একটি Note দেওয়া থাকে যেখানে বলা হয় যে ফাইলগুলো আনলক করতে বা ফেরত পেতে key লাগবে এবং সেটি তাদের থেকে কিনতে একটি নির্দিষ্ট পরিমাণ অর্থ দেওয়া লাগবে। অর্থ পাঠানোর ঠিকানা ও দেওয়া থাকে। এই কি ছাড়া ফাইল আনলক করা সম্ভব হয়না, কি না থাকলে তখন একমাত্র উপায় থাকে সব ফরম্যাট দিয়ে নতুন করে উইন্ডোজ ইন্সটল করা।

প্রশ্ন ৩০। এসএমএস এর মাধ্যমে আমার কাছে একটি লিংক আসে। লিংকে ক্লিক করার পরই আমার জিমেইল আইডি হ্যাক হয়ে যায়। আমার করণীয় কি?

- জিমেইল/গুগল একাউন্ট পুনরুদ্ধারের জন্য প্রথমে gmail.com এ যান।
- ইমেইল এড্রেস ভুলে গেলে ‘ইমেল আইডি ভুলে গেছেন?’ (Forgot email?) লিঙ্কে ক্লিক করুন। পরবর্তী নির্দেশনাসমূহ অনুসরণ করুন।
- পাসওয়ার্ড ভুলে গেলে ‘পাসওয়ার্ড মনে নেই’ (forgot password) লিঙ্কে ক্লিক করুন। সর্বশেষ পাসওয়ার্ডটি লিখুন। পরবর্তী নির্দেশনাসমূহ অনুসরণ করুন।
- সর্বশেষ পাসওয়ার্ডটি মনে না থাকলে Try another way (অন্যভাবে চেষ্টা করুন) লিঙ্কে ক্লিক করুন।
- আরও বিস্তারিত জানতে support.google.com/accounts লিঙ্কে ভিজিট করুন।

অধ্যায়-৪: ফোন হারিয়ে গেলে করণীয়

প্রশ্ন ৩১। এন্ড্রয়েড ফোন হারিয়ে গেলে কি করণীয়?

(ক) ফোন উদ্ধার: ফোনটি উদ্ধার করতে হলে সেক্ষেত্রে আপনাকে নিকটস্থ থানায় যোগাযোগ করুন ফোন কেনার সময় যেই মানি রিসিপ্ট পেয়েছিলেন সেটি এবং ফোনের বক্সে থাকা ফোনের যাবতীয় তথ্য, প্রমাণ সহ, ফোনটি কিভাবে হারিয়েছে, কোথায় হারিয়েছেন সে সম্পর্কে বিস্তারিত লিখে নিয়ে থানায় যোগাযোগ করলে আইন শৃঙ্খলা রক্ষাকারী বাহিনী আপনাকে এ ব্যাপারে সহায়তা করবেন ।

(খ) লোকেশন জানা এবং তথ্য মুছে ফেলা/ডিভাইস সুরক্ষিত করার জন্য:

প্রোবিং প্রশ্ন- আপনার হারিয়ে যাওয়া এন্ড্রয়েড ফোনটিতে কি কোন গুগল একাউন্ট সাইন ইন করা ছিল?

যদি সাইন ইন করা না থেকে থাকে, যেহেতু আপনার ইমেইল টি হারানো ফোনে লগ ইন করা নেই, তাই আমি আন্তরিক ভাবে দুঃখিত, ইন্টারনেট এর মাধ্যমে যেভাবে আপনি ফোনের লোকেশনটি জানতে পারতেন ফোনটিকে নিরাপদ করতে পারতেন বা ফোনের ডাটা মুছে ফেলতে পারতেন সেটি সম্ভব নয়।

যদি সাইন ইন করা থেকে থাকে, সেক্ষেত্রে আপনার কাছে কি সেই গুগল একাউন্ট টির এক্সেস আছে?

- android.com/find লিঙ্কে যান।
- ফোনে ব্যবহৃত ইমেইল আকাউন্ট দিয়ে লগইন করুন। ফাইন্ড মাই ডিভাইস নামে একটা অপশন দেখাবে, যা ‘একসেপ্ট’ করুন।
- বাম পাশে আপনার ফোনের মোবাইলের ব্র্যান্ড ও মডেল নম্বর দেখতে পাবেন। আপনার ডিভাইসের লোকেশন (ইন্টারনেট সংযোগ থাকতে হবে) অপশনটি চালু থাকলে গুগল ম্যাপে অবস্থান দেখাবে। মনে রাখবেন, এখানে কিন্তু সম্ভাব্য কাছাকাছি লোকেশনই দেখানো হবে।
- বামে আরও ৩টি অপশন দেখতে পাবেন- (১) প্লে সাউন্ড, (২) সিকিউর ডিভাইস, (৩) ইরেজ ডিভাইস

  (১) মোবাইলকেও যদি আপনার এলাকাতেই দেখানো হয়, সে ক্ষেত্রে বাঁ দিকে থাকা (PLAY SOUND) অপশনটি ব্যবহার করুন। এর ফলে কম্পিউটার থেকেই আপনার মোবাইলে রিংটোন বাজানো যাবে। মোবাইল সাইলেন্ট মোডে থাকলেও কোনো সমস্যা নেই, পাঁচ মিনিট ধরে নিজেকে জানান দেবে মোবাইল।

  (২) সিকিউর ডিভাইস অপশন ব্যবহার করলে আপনার ডিভাইসটি লক হয়ে যাবে এবং আপনার একাউন্ট থেকে লগআউট হয়ে যাবে। এর ফলে আপনার মোবাইল ও ক্লাউডের (যেমন- জিমেইল, গুগল ড্রাইভ) তথ্য নিরাপদ থাকবে। তবে এরপর আর আপনি ফোনের অবস্থান জানতে পারবেন না।

  (৩) ইরেজ ডিভাইস ব্যবহার করলে ফোনের সব তথ্য মুছে যাবে। তবে এরপর আর আপনি ফোনের অবস্থান জানতে পারবেন না।

প্রশ্ন ৩২। আইফোন হারিয়ে গেলে কি করণীয়?

(ক) ফোন উদ্ধার: ফোনটি উদ্ধার করতে হলে নিকটস্থ থানায় যোগাযোগ করুন। ফোন কেনার সময় যে মানি রিসিপ্ট পেয়েছিলেন সেটি এবং ফোনের বক্সে থাকা ফোনের যাবতীয় তথ্যপ্রমাণসহ ফোনটি কিভাবে হারিয়েছে, কোথায় হারিয়েছেন সে সম্পর্কে বিস্তারিত লিখে থানায় যোগাযোগ করুন।

(খ) লোকেশন জানার জন্য

আপনার হারিয়ে যাওয়া আই ফোনটিতে কি আপনার Apple ID / Apple একাউন্ট দিয়ে icloud এ সাইন ইন / লগইন করা ছিল?

যদি থেকে থাকে, সেক্ষেত্রে আপনার কাছে কি আপনার সেই Apple ID / Apple একাউন্টটির এক্সেস আছে?

যদি Apple ID / Apple একাউন্ট টির এক্সেস থেকে থাকে:

- আপনার হারিয়ে যাওয়া iphone টির iOS Version, কি Version 13 or 13+ / পরবর্তী ভার্সন?
- যদি তা হয়ে থাকে সেক্ষেত্রে ফোনটিতে কি find my iPhone এবং offline findings option গুলি কি enable করা ছিল?
- আপনার হারিয়ে যাওয়া iphone টির iOS Version যদি 13 or 13+ না হয়, সেক্ষেত্রে যে process টি বলছি সেটি শতভাগ কাজ করবে কিনা নিশ্চিতভাবে বলা যাচ্ছে না।

যদি Apple ID / Apple একাউন্ট টির এক্সেস না থাকে:

- যেহেতু আপনার হারানো আই ফোনে - Apple ID / Apple একাউন্ট দিয়ে i cloud – লগ ইন করা নেই, তাই আমি আন্তরিক ভাবে দুঃখিত, ইন্টারনেট এর মাধ্যমে যেভাবে আপনি ফোনের লোকেশনটি জানতে পারতেন ফোনটিকে নিরাপদ করতে পারতেন বা ফোনের ডাটা মুছে ফেলতে পারতেন সেটি সম্ভব নয় ।

(গ) আপনার আইফোনটি ম্যাপে খুঁজে বের করার জন্য

- ➢ প্রথমে যে কোন ব্রাউজার থেকে icloud.com/find এই লিঙ্কে প্রবেশ করুন এবং আপনার Apple ID / Apple একাউন্টে সাইন ইন করুন।
- ➢ সেখানে Device নামে একটি option দেখতে পাবেন।
- ➢ Device এ click করলে আপনার Apple id দিয়ে যতগুলি ডিভাইস connected থাকবে সেগুলি দেখাবে, সেখান থেকে আপনার Device টি select করলে Map এ location দেখতে পারবেন।
- ➢ আপনার আই ফোনটি কোন নেটওয়ার্কের সাথে কানেক্টেড থাকলে তার বর্তমান লোকেশন খুঁজে বের করতে পারবেন। আপনার আই ফোনের এই অবস্থান শতভাগ সঠিক না হলেও কাছাকাছিই হবে।
- ➢ যদি কোন নেটওয়ার্কের সাথে কানেক্টেড না থাকে বা সুইচ অফ থাকে তাহলে Offline Findings অপশন এর মাধ্যমে ফোনটি খুঁজে বের করতে পারবেন।

(ঘ) আপনার আইফোনে রিং বাজানোর জন্য

- প্রথমে যে কোন ব্রাউজার থেকে icloud.com/find এই লিঙ্কে প্রবেশ করুন এবং আপনার Apple ID / Apple একাউন্টে সাইন ইন করুন।
- সেখানে Device নামে একটি option দেখতে পাবেন।
- Device এ click করলে আপনার Apple id দিয়ে যতগুলি ডিভাইস connected থাকবে সেগুলি দেখাবে। icloud.com/find address টিতে কিছু অপশন দেখতে পারবেন সেখান থেকে
- Play Sound অপশনটি বেছে নিন। এক্ষেত্রে আপনার ফোনটি অফলাইনে থাকলে কোন রিং হবে না। তবে কোন নেটওয়ার্কের সাথে কানেক্টেড থাকলে রিং হবে।
- আপনার ফোনটি যদি silent / vibration অবস্থায় ও থাকে আপনি Play sound অপশনটিতে যেয়ে click করলে ৫ মিনিট যাবত sound বাজতে থাকবে ।

(ঙ) আপনার আইফোনটি Secure করার জন্য

- প্রথমে যে কোন ব্রাউজার থেকে icloud.com/find এই লিঙ্কে প্রবেশ করুন এবং আপনার Apple ID / Apple একাউন্টে সাইন ইন করুন।
- সেখানে Device নামে একটি option দেখতে পাবেন।
- Device এ click করলে আপনার Apple id দিয়ে যতগুলি ডিভাইস connected থাকবে সেগুলি দেখাবে।
- icloud.com/find address টিতে কিছু অপশন দেখতে পারবেন সেখান থেকে Mark as lost অপশনটি বেছে নিন। আপনার পিন, পাসওয়ার্ড বা প্যাটার্ন ব্যবহার করে ফোনটি লক করে দিতে পারেন। আগে থেকে আপনার ফোনে কোন লক না থাকলেও এসময় আপনি লক সেট করতে পারবেন। এবং লক স্ক্রিনে আপনি মেসেজ বা ফোন নাম্বারও চাইলে এড করতে পারেন।

(চ) আইফোনের Data Erase করার জন্য

- ✓ প্রথমে যে কোন ব্রাউজার থেকে icloud.com/find এই লিঙ্কে প্রবেশ করুন এবং আপনার Apple ID / Apple একাউন্টে সাইন ইন করুন।
- ✓ সেখানে Device নামে একটি option দেখতে পাবেন।
- ✓ Device এ click করলে আপনার Apple id দিয়ে যতগুলি ডিভাইস connected থাকবে সেগুলি দেখাবে। icloud.com/find address টিতে কিছু অপশন দেখতে পারবেন সেখান থেকে
- ✓ Erase Device অপশনটি বেছে নিন। আপনার ফোনের সমস্ত ডাটা স্থায়ীভাবে ডিলিট করতে পারেন। মনে রাখবেন ডাটা মুছে দেয়ার পর আপনার ফোনের secure device / lock device and location অপশন আর কাজ করবে না।
- ✓ (মনে রাখবেন, Play sound / Mark as lost / Erase device এই সার্ভিস গুলো তখনই কাজ করবে, যখন আপনার হারানো ফোনটিতে কোন ইন্টারনেট কানেকশন থাকবে)

(ছ) অন্য কারো iPhone থেকে হারানো ফোনের লোকেশন দেখার জন্য

অন্য কারো iPhone থেকে find my iPhone App এ গেলে নিচের দিকে Help a Friend নামে একটি অপশন দেখতে পাবেন, সেখানে যেয়ে আপনার Apple id এবং Password দিয়ে login করবেন। সেখান থেকে আপনার Device টি select করলে ম্যাপে location দেখতে পারবেন

(জ) Forgot apple id's Password Recovery

- যেকোন ব্রাউজার থেকে apple id.apple.com এ যাবেন।
- এরপর forgot apple id or password অপশনটিতে ক্লিক করবেন।
- তারপর একটি নতুন পেজ আসবে সেখানে আপনাকে আপনার apple id টি ইনপুট করুন।
- এরপর continue অপশনে ক্লিক করবেন।
- এরপর নতুন একটি পেজ আসবে সেখানে I want to reset my password অপশন টি select করবেন। এরপর continue তে ক্লিক করবেন।
- তারপর password recovery এর জন্য একটি মাধ্যম সিলেক্ট করতে বলা হবে। সেখানে get an email অপশনটি select করে continue করবেন।
- এরপর ইমেইলে পাসওয়ার্ড রিকভারির লিংক দেওয়া হবে সেখানে ক্লিক করে নতুন করে পাসওয়ার্ড সেট করতে পারবেন।
- তারপর নতুন পাসওয়ার্ড টি রিটাইপ করবেন। ফাইনালি Reset Password অপশনটি সিলেক্ট করলে নতুন পাসওয়ার্ড টি Save হয়ে যাবে।
- এক্ষেত্রে কিছু বিষয় লক্ষ্য রাখবেন প্রিয় কারো নাম, নিজের ফোন নাম্বার অথবা জন্মতারিখ পার্সওয়ার্ড সেট করা থেকে বিরত থাকবেন এবং মিনিমাম ১২ ডিজিটের Capital letter, Small letter, number এবং Special Character-এর সমন্বয়ে একটি শক্তিশালী পার্সওয়ার্ড সেট করবেন।

প্রশ্ন ৩৩। Android মোবাইল সুরক্ষিত রাখতে করণীয় কী?

- আপনার ফোন কোনও Wi-Fi-এর সঙ্গে যেন অটোমেটিক্যালি কানেক্টেড না হয়ে যায় খেয়াল করুন।
- হারিয়ে যাওয়া ফোন খুঁজে বের করার জন্য ফাইন্ড মাই ডিভাইস ব্যবহার করুন।
- শুধু অফিসিয়াল স্টোর (অ্যান্ড্রয়েড ফোনে গুগল প্লে স্টোর/ আইফোনে অ্যাপ স্টোর) থেকে অ্যাপ ইনস্টল করবেন।
- অপ্রয়োজনীয় অ্যাপ ডিলিট করুন।
- টু ফ্যাক্টর অথেনটিকেশন চালু করুন।
- অপরিচিত অ্যাপ ইনস্টল বন্ধ করুন।
- অ্যান্টিভাইরাস ব্যবহার করুন।

- প্রয়োজন ছাড়া ওয়াই ফাই ও ব্লুটুথ বন্ধ রাখুন।
- পাবলিক Wi-Fi এড়িয়ে চলুন।

প্রশ্ন ৩৪। ল্যাপটপ এ গুরত্বপূর্ণ অ্যাপ্লিকেশন অটো কারেক্ট/ পাসওয়ার্ড সেভ হয়ে থাকে। কিভাবে অটো কারেক্ট বন্ধ করা যায়?

(ক) Chrome ব্রাউজার এর ক্ষেত্রে:

- ক্রোম ব্রাউজারের ডান দিকে উপরে থ্রি ডট বা মেনু বাটনে ক্লিক করুন।
- তারপর যে সাব মেনু ওপেন হবে সেখান থেকে setting এ ক্লিক করুন।
- এখন আপনার সামনে একটি সেটিংস এর পেজ ওপেন হবে। সেখান থেকে Password বা Manage Password নামের একটি অপশন পাবেন। সেখানে ক্লিক করুন।
- সেখানে Password বা Manage Password এর উপর ক্লিক করলেই Save Password নামের একটি অপশন পাবেন যার নিচে আপনার সমস্ত সেভ করা পাসওয়ার্ড এবং ইউজার নেমের লিস্ট দেখতে পাবেন।
- এখন আপনি যেই সাইটগুলোর সেভ পাসওয়ার্ড ডিলেট করতে চাচ্ছেন সেই পাসওয়ার্ডের ডান পাশের থ্রি ডট বাটনে ক্লিক করলেই Remove নামের একটি অপশন পাবেন। সেখানে Remove বাটনে ক্লিক করলেই আপনার সেই পাসওয়ার্ডটি ডিলেট হয়ে যাবে। এভাবে আপনি যতগুলো ইচ্ছা সেভ পাসওয়ার্ড ডিলেট করতে পারবেন।

(খ) Firefox ব্রাউজার এর ক্ষেত্রে

- ফায়ারফক্স ব্রাউজারের ডান দিকে উপরে থ্রি ডট বা মেনু বাটনে ক্লিক করুন।
- তারপর যে সাব মেনু ওপেন হবে, সেখান থেকে Option বাটনে এ ক্লিক করুন।
- এখন আপনার সামনে একটি নামের পেজ ওপেন হবে। সেখানে বাম পাশ থেকে Privacy & Security বাটনে ক্লিক করুন।
- সেখান থেকে Saved Logins বাটনে ক্লিক করুন।
- এখন আপনার সেভ করা সমস্ত সাইটের পাসওয়ার্ড এবং ইউজার নেম চলে আসবে। আপনি ইচ্ছে মত এখান থেকে যেকোন সেভ পাসওয়ার্ড ডিলেট করতে পারবেন অথবা রিমুভ অল বাটনে ক্লিক করে এক সাথে সবগুলো ডিলেট করতে পারবেন।

অধ্যায়-৫: ব্যাংক/ফিনান্সিয়াল সার্ভিস সংক্রান্ত

প্রশ্ন ৩৫। আমি সন্দেহ করছি যে আমার ব্যাংক/বিকাশ/নগদ একাউন্টের তথ্য চুরি হয়েছে। এখন কি করব?

- ব্যাংক/মোবাইল ফিনান্সিয়াল সার্ভিসের হেল্পলাইনে কল করুন এবং তাদের সংশ্লিষ্ট ডিপার্টমেন্টে যোগাযোগ করুন।
- ব্যাংক আপনাকে ব্যক্তিগত তথ্যসহ ই-মেইলের জবাব দিতে বলবে না, অথবা ইমেইলে আপনার অ্যাকাউন্টের বিশদ বিবরণ জানতে চাইবে না। তাদের সাথে যোগাযোগের জন্য ইমেইলে কোনো ঠিকানা দেওয়া থাকলে তা পরিহার করুন, বরং নিজে যোগাযোগের ফোন নম্বর/ইমেল ঠিকানা খুঁজে বের করুন।
- সংশ্লিষ্ট প্রতিষ্ঠানের অফিসিয়াল ইমেইলে যোগাযোগ করুন।

(গ্রাহকের সুবিধার্থে বিকাশ হেল্পলাইন ১৬২৪৭, নগদ হেল্পলাইন ১৬১৬৭ নম্বর জানিয়ে দিতে হবে।)

প্রশ্ন ৩৬। মোবাইল ব্যাংকিং ও এটিএম কার্ড প্রতারণা এড়াতে করণীয় কী?

- এ ধরনের প্রতারণার ক্ষেত্রে প্রতারক ব্যক্তি নিজেকে বিকাশ, ইউক্যাশ, রকেট, নগদ বা অন্য যেকোন মোবাইল ব্যাংকিং প্রতিষ্ঠানের অথবা আপনার ব্যবহৃত এটিএম কার্ড (ডেবিট/ক্রেডিট) সংশ্লিষ্ট ব্যাংকের হেড অফিস, কোম্পানী অফিস বা আইটি শাখার কর্মকর্তা/কর্মচারী হিসেবে পরিচয় দিতে পারে। প্রতারক ব্যক্তিটি আপনার সাথে অত্যন্ত শুদ্ধ ভাষায় এবং মার্জিতভাবে কথা বলার চেষ্টা করবে। সিস্টেম মেইনটেনেন্স, তথ্য হালনাগাদ, কাস্টমার ভেরিফিকেশন বা অন্য কোন বিশেষ/জরুরী কারণ দেখিয়ে প্রতারক আপনার বিকাশ, ইউক্যাশ, রকেট, নগদ ইত্যাদির একাউন্টের বা এটিএম কার্ডের (ডেবিট/ক্রেডিট) গোপন পিন নম্বরটি জানতে চাইবে। পিন নম্বরটি তাকে না জানালে আপনার একাউন্টটি বন্ধ/স্থগিত করে দেয়া হবে মর্মে ভয় দেখাবে।
- কোন প্রতিষ্ঠান বা প্রতিষ্ঠানের কোন ব্যক্তি (কর্মকর্তা/কর্মচারী) কখনোই আপনার কোন একাউন্টের গোপন পিন নম্বর বা পাসওয়ার্ড জানতে চাইবেন না, এমনকি কেউ সেটি জানতে চাইতে পারেন না।
- এ ধরণের কলে বিচলিত না হয়ে কলটি কেটে দিন এবং পরবর্তীতে ঐ নম্বর থেকে আবার কল আসলে কল রিসিভ করা থেকে বিরত থাকুন।

প্রশ্ন ৩৭। বিকাশে অ্যাকাউন্ট রিকভার করার জন্য কোড চেয়েছিলো। কোড দেয়ার পরে আমার অ্যাকাউন্টে টাকা নাই। কি করতে পারি?

- যে নম্বর থেকে ফোন দেয়া হয়েছে সে নম্বর এবং কোন ট্রানজেকশন নম্বর থাকলে এগুলোসহ প্রথমে বিকাশ কলসেন্টার/হেল্পলাইনে যোগাযোগ করে বিষয়টি জানান ও পরামর্শ গ্রহণ করুন;
- যদি কাজ না হয়, তবে নিকটস্থ থানায় জিডি করুন এবং জিডি কপি ও ম্যাসেজসহ বিকাশ অফিসে যোগাযোগ করুন।

অধ্যায়-৬: মানহানী এবং সাইবার বুলিং

প্রশ্ন ৩৮। আমি মানহানীর শিকার হলে কি করব?

- আপনি কি যে ওয়েবসাইটে মানহানীকর তথ্য প্রকাশ করা হচ্ছে তার এডমিনিস্ট্রেটর এর সঙ্গে যোগাযোগ করে মানহানিকর তথ্য অপসারনের অনুরোধ করেছেন?

না হলে জানাতে হবে ওয়েবসাইটের নিচে contact us লিঙ্ক থেকে যোগাযোগের ইমেইল বা ফোন নম্বর পাওয়া যাবে। contact us এ তথ্য না থাকলে ওয়েব সার্চ করে খোঁজা যেতে পারে।

- যোগাযোগ করা হয়ে থাকলে এবং তাতে সাড়া পাওয়া না গেলে ডিজিটাল নিরাপত্তা আইন, ২০১৮ এর আওতায় মানহানীর অভিযোগে নিকটস্থ থানায়/আদালতে আইনের আশ্রয় গ্রহণ করুন।

প্রশ্ন ৩৯। কিভাবে একটি সাইবার হুমকি বা সাইবার অপরাধ রিপোর্ট করবেন?

- হুমকি সংক্রান্ত মেসেজের ছবি তুলুন বা স্ক্রিনশট নিন। ইমেইল বা অন্য প্রমাণক থাকলে তা সংগ্রহ করুন।
- দেশের সাইবার নিরাপত্তা সংক্রান্ত হলে বা দপ্তরের সকল কম্পিউটার বা সার্ভার/সফটয়্যার সিস্টেম/নেটওয়ার্ক হ্যাক হয়ে থাকলে ডিজিটাল নিরাপত্তা এজেন্সির আওতাধীন NCERT/BGD- eGOV CIRT এর সঙ্গে যোগাযোগ করুন। (ইমেইল অথবা ফোন নাম্বার জানানো হবে)
- সাইবার হুমকি হলে বা কোনো সাইবার অপরাধের উপাদান থাকলে নিকটস্থ থানার সঙ্গে যোগাযোগ করুন।

প্রশ্ন ৪০। বিভিন্ন আইডি এবং গ্রুপের মাধ্যমে আমার নামে অপ-প্রচার চালানো হচ্ছে। এগুলো বন্ধ করতে আমার করণীয় কি?

- যেসব আইডি থেকে অপপ্রচার চালানো হচ্ছে সেসব আইডির পোস্টের স্ক্রিনশট সংগ্রহ করুন।
- নিজের পরিচয়পত্রের (জাতীয় পরিচয়পত্র/পাসপোর্ট) কালার স্ক্যানড কপিসহ আইডিগুলোকে রিপোর্ট করুন।
- যেসব গ্রুপের মাধ্যমে অপ-প্রচার চালানো হচ্ছে সেসব গ্রুপের অ্যাডমিনদের কাছে স্ক্রিনশটসহ অভিযোগ করা যেতে পারে।
- উক্ত পদ্ধতিতেও অপপ্রচার বন্ধ না হলে সকল প্রমাণাদিসহ নিকটস্থ থানায় যোগাযোগ করুন।

প্রশ্ন ৪১। যদি কেউ আমাকে অনলাইনে উত্যক্ত করে তাহলে আমার কার সাথে কথা বলা উচিত?

- আপনি যদি মনে করেন যে আপনাকে উত্যক্ত করা হচ্ছে, তাহলে প্রথম পদক্ষেপ হল আপনার বিশ্বাসী কারো সাহায্য নেওয়া যেমন আপনার বাবা -মা, পরিবারের একজন ঘনিষ্ঠ সদস্য বা অন্য কোনো বিশ্বস্ত

প্রাপ্তবয়স্ক। আপনার স্কুলে আপনি একজন পরামর্শদাতা বা আপনার প্রিয় শিক্ষকের সাথে কথা বলতে পারেন।

- যদি কোনও সামাজিক প্ল্যাটফর্মে উত্যক্তের ঘটনা ঘটে থাকে, তাহলে উত্যক্তকারীকে ব্লক করতে পারেন এবং প্ল্যাটফর্মের এডমিনের কাছে তাদের বিরুদ্ধে অভিযোগ করতে পারেন।
- কী ঘটছে তা দেখাতে প্রমাণ সংগ্রহ করা - মেসেজ এবং সামাজিক যোগাযোগের পোস্টের স্ক্রিন শট সংগ্রহ করা সহায়ক হতে পারে।
- বুলিং বন্ধ করার জন্য, এটি চিহ্নিত করা প্রয়োজন এবং এটি রিপোর্ট করা গুরুত্বপূর্ণ। এটা বুলিকে বোঝাতে সাহায্য করতে পারে যে তাদের আচরণ অগ্রহণযোগ্য।
- আপনি যদি তাৎক্ষণিক বিপদে পড়েন, তাহলে নিকটস্থ থানায় যোগাযগ করুন।

প্রশ্ন ৪২। আমি সাইবার বুলিংয়ের সম্মুখীন হচ্ছি, কিন্তু আমি আমার বাবা-মায়ের সাথে এটি সম্পর্কে কথা বলতে ভয় পাই। আমি কিভাবে তাদের কাছে যেতে পারি?

- আপনি যদি সাইবার বুলিংয়ের সম্মুখীন হন, একজন বিশ্বস্ত প্রাপ্তবয়স্ক ব্যক্তির/ শিক্ষকের সাথে কথা বলতে পারেন, যার সাথে আপনি নিরাপদ কথা বলছেন, এটা একটি গুরুত্বপূর্ণ পদক্ষেপ।
- কথা বলার সময় লক্ষ্য করুন যে তাদের পূর্ণ মনোযোগ রয়েছে। আপনার জন্য সমস্যাটি কতটা গুরুতর তা ব্যাখ্যা করুন। মনে রাখবেন, তারা আপনার মতো প্রযুক্তির সাথে পরিচিত নাও হতে পারে, তাই কী ঘটছে তা বুঝতে আপনাকে তাদের সাহায্য করতে হতে পারে।

প্রশ্ন ৪৩। কিভাবে আমি আমার বন্ধুদের সাইবার বুলিংয়ের একটি ঘটনা রিপোর্ট করতে সাহায্য করতে পারি, বিশেষ করে যদি তারা এটি করতে না চায়?

- যে কেউ সাইবার বুলিংয়ের শিকার হতে পারে। যদি আপনি এটি আপনার পরিচিত কারো সাথে ঘটতে দেখেন, তাহলে সহায়তা দেওয়ার চেষ্টা করুন।
- মনে রাখবেন, আপনার বন্ধু খারাপ বোধ করতে পারে। তাদের প্রতি সদয় হোন। তারা কি বলতে পারে এবং কাকে বলবে সে বিষয়ে চিন্তা করতে সাহায্য করুন। তারা রিপোর্ট করার সিদ্ধান্ত নিলে তাদের সাথে যাওয়ার প্রস্তাব দিন। সবচেয়ে গুরুত্বপূর্ণভাবে, তাদের মনে করিয়ে দিন যে আপনি তাদের জন্য আছেন এবং আপনি সাহায্য করতে চান।

প্রশ্ন ৪৪। ইন্টারনেটে অ্যাক্সেস বন্ধ না করে আমরা কীভাবে সাইবার বুলিং বন্ধ করব?

- অনলাইনে থাকার অনেক সুবিধা আছে। আপনি যদি সাইবার বুলিংয়ের সম্মুখীন হন, তাহলে আপনি কিছু অ্যাপ মুছে ফেলতে পারেন বা কিছুক্ষণের জন্য অফলাইনে থাকতে পারেন। কিন্তু ইন্টারনেট বন্ধ করা দীর্ঘমেয়াদী সমাধান নয়।
- আপনার অ্যাকাউন্টের গোপনীয়তা সেটিংস সেট করে আপনি সিদ্ধান্ত নিতে পারেন কে আপনার প্রোফাইল দেখতে পারে, আপনাকে সরাসরি বার্তা পাঠাতে পারে বা আপনার পোস্টে মন্তব্য করতে পারে।

- অনলাইনে কোনোকিছু শেয়ার করার বিষয়ে সতর্ক থাকুন। অপরিচিত মানুষকে বন্ধু বানাবেন না।

প্রশ্ন ৪৫। সোশ্যাল মিডিয়ায় উত্যক্তের শিকার হচ্ছি। এই পরিস্থিতিতে কি করতে পারি?

- উত্যক্তকারীকে আনফ্রেন্ড করুন। আপনার টাইমলাইনে ফেসবুক চ্যাট বা পোস্টের মাধ্যমে শুধুমাত্র আপনার ফেসবুক বন্ধুরা আপনার সাথে যোগাযোগ করতে পারে। যদি আপনি তাকে আনফ্রেন্ড করেন তাহলে সে আপনার সাথে যোগাযোগ করতে পারবে না।
- উত্যক্তকারীকে ব্লক করুন। এটি সেই ব্যক্তিকে আপনাকে বন্ধু হিসাবে যোগ করা এবং আপনার টাইমলাইনে শেয়ার করা জিনিসগুলি দেখতে বাধা দেবে।
- আপনার সকল প্রাইভেসি সেটিংস ফ্রেন্ড অথবা "অনলি মি" সেট করুন।

যদি কেউ আপনাকে ফেসবুক/মেসেঞ্জার/সোশ্যাল মিডিয়াতে একটি বার্তা পাঠায় যা আপনার জন্য অস্বস্তিকর, তবে আপনি যা করতে পারেন:

- তাদের ম্যাসেজ ব্লক করুন তাহলে তারা মেসেঞ্জারে আপনার সাথে যোগাযোগ করতে পারবে না (যেমন আপনাকে বার্তা পাঠাবে বা আপনাকে কল করবে) অথবা ফেসবুক চ্যাটের মাধ্যমে আপনাকে বার্তা পাঠাতে পারবে না।
- উত্যক্তকারীকে রিপোর্ট করতে পারেন।
- কথোপকথন উপেক্ষা করুন।
- কথোপকথন মুছে ফেলুন। মনে রাখবেন এটি অন্য ব্যক্তির চ্যাট তালিকা থেকে কথোপকথন মুছে ফেলবে না। আপনি যদি কথোপকথনটি রিপোর্ট করতে চান তবে এটি মুছে ফেলার আগে একটি স্ক্রিনশট নিন।
- উত্যক্তকারীকে ব্লক করুন।
- সাইবার হুমকি হলে বা কোনো সাইবার অপরাধের উপাদান থাকলে নিকটস্থ থানার সঙ্গে যোগাযোগ করুন।

অধ্যায়-৭: সোশ্যাল মিডিয়ার নিরাপদ ব্যবহার

প্রশ্ন ৪৬। ফেসবুকে আমার নাম ও ছবি ব্যবহার করে ফেইক আইডি তৈরি করা হয়েছে। এটা কিভাবে বন্ধ করবো?

ফেক অ্যাকাউন্টের প্রোফাইলে যান। প্রোফাইলে গিয়ে (...) এ ক্লিক করে ফাইন্ড সাপোর্ট/রিপোর্ট প্রোফাইলের মাধ্যমে রিপোর্ট করুন;

(ক) আপনার জাতীয় পরিচয়পত্র আছে কিনা? জাতীয় পরিচয়পত্র থাকলে পরিচয়পত্রের কালার স্ক্যানড ইমেজ সংগ্রহ করুন;

(খ) যে অ্যাকাউন্ট বা পেইজ রিপোর্ট করবেন সে প্রোফাইল বা পেইজে যান।

- যদি আপনি নাম এবং পেইজ দিয়ে খুঁজে না পান, তাহলে আপনার কোন বন্ধুকে বলুন আপনার নামে যে ফেইক আইডি টি খোলা হয়েছে তার লিংকটি আপনাকে দিতে।

(গ) কভার ফটোর নিচে ক্লিক করুন।

- যদি আপনি একটি পেইজকে রিপোর্ট করতে চান, তাহলে Find support or report Page সিলেক্ট করুন। যদি আপনি একটি প্রোফাইলকে রিপোর্ট করতে চান, তাহলে Find support or report profile সিলেক্ট করুন।
- Follow the on-screen instructions for impersonation to file a report. স্ক্রিনে আসা নির্দেশনাগুলো অনুসরণ করুন।
- আপনি একটি ফর্ম পূরণের মাধ্যমেও ফেসবুক অ্যাকাউন্ট রিপোর্ট করতে পারেন।

(ঘ) রিপোর্টের পরের স্টেপের ধাপগুলো অনুসরণ করুন-

(ঙ) প্রোফাইল রিপোর্ট করার পর ৪৮-৭২ ঘন্টা পর্যন্ত অপেক্ষা করে বন্ধ না হলে নিকটস্থ থানায় যোগাযোগ করুন।

প্রশ্ন ৪৭। আমার ফেসবুক আইডি হ্যাকড হয়েছে। আমি ঢুকতে পারছি না। এখন কিভাবে আইডি উদ্ধার করবো?

(ক) যেকোন ব্রাউজার থেকে Facebook.com/hacked এই address গিয়ে My Account is Compromised অপশনটি সিলেক্ট করবেন;

- সেখানে আপনাকে আপনার হ্যাকড হওয়া ফেসবুক একাউন্টটির address (phone number/email address) এবং আগের পার্সওয়ার্ড টি দিতে হবে;
- এক্ষেত্রে Account টিতে 2FA অন করা থাকলে (phone number/email address) এ কোড যাবে;
- কোডটি সাবমিট করার পর, পার্সওয়ার্ড রিসেটের জন্য নতুন একটি পেজ আসবে , সেখান থেকে আপনি নতুন পার্সওয়ার্ড সেট করতে পারবেন।

(খ) ২ ফ্যাক্টর অথেনটিকেশন অন না থাকলে অথবা আপনার প্রোফাইলে ইমেইল ও মোবাইল নম্বর পরিবর্তন করে ফেলে থাকলে-

- আপনি যে অ্যাকাউন্টটি পুনরুদ্ধার করতে চান তার প্রোফাইলে যান;
- কভার ছবির নীচে, more বাটন এবং Find support বা রিপোর্ট প্রোফাইল নির্বাচন করুন;
- Something else সিলেক্ট, তারপর submit চাপুন;
- Recover this account (এই অ্যাকাউন্টটি পুনরুদ্ধার করুন) চাপুন এবং ধাপগুলি অনুসরণ করুন;
- আরও বিস্তারিত জানতে Facebook Help Centre (www.facebook.com/help/) লিঙ্কে ভিজিট করতে পারেন।

(গ) একাউন্ট উদ্ধার করতে না পারলে ডিজিটাল নিরাপত্তা এজেন্সির মাধ্যমে বিটিআরসি-এর সঙ্গে যোগাযোগ করুন।

প্রশ্ন ৪৮। হোয়াটস অ্যাপে অপরিচিত নম্বর থেকে কল করে অশালীন ভাষায় মন্তব্য ও কুরুচিপূর্ণ কথাবার্তা বলা হচ্ছে এবং কল কেটে দেয়ার সাথে সাথে বিভিন্ন অশ্লীল ছবি এবং ভিডিও পাঠাচ্ছে। আমার করণীয় কি?

হোয়াটস অ্যাপে অপরিচিত নম্বর থেকে কল করে অশালীন ভাষায় মন্তব্য ও কুরুচিপূর্ণ কথাবার্তা বলা হলে যে ব্যক্তির নম্বর থেকে মন্তব্য করা হচ্ছে সেই ব্যক্তির নম্বর রিপোর্ট এবং ব্লক করে দিতে হবে।

হোয়াটস অ্যাপে রিপোর্ট বা ব্লক করার নিয়ম:

(ক) যে ব্যক্তির নম্বর থেকে মন্তব্য করা হচ্ছে সেই ব্যক্তির চ্যাটবক্স ওপেন করে উপরে তিনটি ডট (.) চিহ্ন থেকে More অপশনে যেতে হবে;

- যদি আপনি প্রথমবারের মতো এই নম্বরের ব্যক্তির সাথে যোগাযোগ করে থাকেন, তাহলে আপনি চ্যাট ওপেন করে ব্লকে ট্যাপ করে ব্লক করে দিতে পারেন।
- অপরিচিত ফোন নম্বরের চ্যাট ওপেন করুন এবং ফোন নম্বর ট্যাপ করুন, Block Contact > Block or Report Contact > Report and Block, which will report and block the number.

বি.দ্র.: ব্লককৃত ব্যক্তি আপনাকে কল করতে পারবেন না বা আপনাকে ম্যাসেজ করতে পারবেন না। আপনার শেষবার অনলাইন হওয়ার সময়, স্ট্যাটাস আপডেট এবং প্রোফাইল ছবিতে যেকোন ধরণের পরিবর্তন ব্লককৃত কন্ট্যাক্টস দেখতে পারবেন না।

রিপোর্ট করার পদ্ধতি

- যাকে রিপোর্ট করতে চান, তার সাথে চ্যাট ওপেন করুন।
- কন্ট্যাক্ট নাম এর উপরে ট্যাপ করুন। তারপর রিপোর্ট কন্ট্যাক্ট এ ট্যাপ করুন।
- রিপোর্টে ট্যাপ করুন এবং ব্লক করুন।

এছাড়াও নিম্নের ধাপগুলো অনুসরণ করে পাঠানো অশ্লীল ভিডিও বা ছবি রিপোর্ট করা যাবে-

- ফটো বা ভিডিও ওপেন করবেন;
- নিচে কর্নারে More --- এ ট্যাপ করবেন;
- রিপোর্ট কন্ট্যাক্ট এ ট্যাপ করবেন।

Source: https://faq.whatsapp.com/

প্রশ্ন ৪৯। কিভাবে আমি আমার ব্যক্তিগত তথ্যকে সোশ্যাল মিডিয়ায় পরিচয় চুরি বা অপমান করার জন্য ব্যবহার করা থেকে বিরত রাখব?

অনলাইনে কিছু পোস্ট বা শেয়ার করার আগে ভালভাবে চিন্তা করুন। এটি চিরকাল অনলাইনে থাকতে পারে এবং পরে আপনার ক্ষতি করতে ব্যবহার করা যেতে পারে। আপনার ঠিকানা, টেলিফোন নম্বর বা আপনার স্কুলের নামের মতো ব্যক্তিগত বিবরণ দেবেন না। যদি শেয়ার করার প্রয়োজন হয়, তাহলে গোপনীয়তা "অনলি মি" সেট করুন।

আপনার সোশ্যাল মিডিয়া অ্যাপের গোপনীয়তা সেটিংস সম্পর্কে জানুন:

- আপনার অ্যাকাউন্টের গোপনীয়তা সেটিংস সেট করে আপনি সিদ্ধান্ত নিতে পারেন কে আপনার প্রোফাইল দেখতে পারে, আপনাকে সরাসরি বার্তা পাঠাতে পারে বা আপনার পোস্টে মন্তব্য করতে পারে।
- আপনি ক্ষতিকর মন্তব্য, বার্তা এবং ফটোগুলি রিপোর্ট করতে পারেন এবং সেগুলি সরানোর অনুরোধ করতে পারেন।
- 'আনফ্রেন্ডিং' ছাড়াও, আপনি আপনার প্রোফাইল দেখতে বা আপনার সাথে যোগাযোগ করতে বাধা দিতে মানুষকে সম্পূর্ণরূপে ব্লক করতে পারেন।
- আপনার প্রোফাইলে পোস্ট মুছে ফেলতে পারেন বা সেগুলো নির্দিষ্ট মানুষের কাছ থেকে লুকিয়ে রাখতে পারেন।

প্রশ্ন ৫০। হ্যাকার একটি সোশ্যাল সাইটের প্রোফাইল হ্যাক করেছে, এখন টাকা দাবি করছে। যদি ভিকটিম টাকা না দেয় তাহলে হ্যাকার তার প্রোফাইল থেকে অশ্লীল জিনিস ছড়াবে। এই পরিস্থিতিতে আমি কি করব?

- প্রথমত, সোশ্যাল মিডিয়া অ্যাকাউন্ট পুনরুদ্ধারের চেষ্টা করুন ।
- যদি পুনরুদ্ধার করা সম্ভব না হয় সেক্ষেত্রে প্রমাণসহ নিকটস্থ থানার সাথে যোগাযোগ করুন।

প্রশ্ন ৫১। কেউ কেউ সবসময় আমার ছবিতে মন্তব্য করছে এবং ব্যক্তিগত/পাবলিক গ্রুপে হয়রানিমূলক মন্তব্য পোস্ট করছে। আমি কি করতে পারি?

- সমস্যাটি সমাধানের জন্য আপনি তাকে ব্লক করে দিন, এরপর রিপোর্ট করুন।
- ওয়েবসাইটের এডমিনিস্ট্রেটরের সঙ্গে যোগাযোগ করে হয়রানিমূলক তথ্য অপসারনের অনুরোধ করেছেন?

- না হলে জানাতে হবে। ওয়েবসাইটের নিচে contact us লিঙ্ক থেকে যোগাযোগের ইমেইল বা ফোন নম্বর পাওয়া যাবে। contact us এ তথ্য না থাকলে ওয়েব সার্চ করে খোঁজা যেতে পারে।
- যোগাযোগ করা হয়ে থাকলে এবং তাতে সাড়া পাওয়া না গেলে ডিজিটাল নিরাপত্তা আইন, ২০১৮ এর আওতায় মানহানীর অভিযোগে নিকটস্থ থানায়/আদালতে আইনের আশ্রয় গ্রহণ করুন।

প্রশ্ন ৫২। আমার এক বন্ধু ইচ্ছাকৃতভাবে আমার কিছু তথ্য সামাজিক যোগাযোগ মাধ্যমে প্রকাশ করেছে। এই বিষয়ে আমার কাকে রিপোর্ট করা উচিত এবং রিপোর্ট করার উপায় কী?

- প্রতিটি সোশ্যাল মিডিয়া প্ল্যাটফর্মেই এই বিষয়ে রিপোর্ট করার অপশন রয়েছে। এই অপশন ব্যবহার করে যথাযথ প্রমাণসহ এই ধরনের সমস্যাগুলি রিপোর্ট করতে পারেন।
- এছাড়া আপনি আপনার নিকটস্থ থানায় অভিযোগ করতে পারেন।

প্রশ্ন ৫৩। আমি অনলাইনে আছি এবং সোশ্যাল মিডিয়া/ চ্যাটরুমে অপরিচিত এক ব্যাক্তির সাথে চ্যাট করি । তাকে কি আমার ঠিকানা বা ফোন নম্বর দেওয়া ঠিক হবে যাতে আমরা একত্রিত হতে পারি?

- অনলাইনে আপনার সাথে পরিচয় হওয়া কাউকে আপনার নাম বা ঠিকানা দেওয়া উচিত নয়।
- আপনি যদি সত্যিই এই ব্যক্তির সাথে একটি "অফলাইন" কথোপকথন করতে চান, তাহলে প্রথমে ভালমতো যাচাই করুন। জনসমাগম আছে এমন স্থানে দেখা করুন। আপনার আত্মীয়/বন্ধু/নির্ভরযোগ্য কাউকে সঙ্গে রাখুন।

প্রশ্ন ৫৪। আপনি যদি সোশ্যাল মিডিয়ায় কিছু পোস্ট করেন, তাহলে কে তা দেখতে পাবে?

আপনি যদি সোশ্যাল মিডিয়ায় কিছু পোস্ট করেন এবং যদি প্রয়োজনীয় গোপনীয়তা সেটিংস নিশ্চিত না করেন তবে যে কেউ দেখতে সক্ষম হতে পারে।

প্রশ্ন ৫৫। আমি অনলাইনে কাদের কাছ থেকে ফ্রেন্ড রিকোয়েস্ট গ্রহণ করব?

- কেবলমাত্র সেই ব্যক্তিদের কাছ থেকে যারা আপনার পরিচিত।
- অপরিচিত বা যাদের সম্পর্কে আপনি নিশ্চিত নন তাদের বন্ধুত্বের অনুরোধ কখনই গ্রহণ করবেন না।
- এক্ষেত্রে হ্যাকাররা হয়তো মিথ্যা পরিচয়ে আপনার বন্ধু হয়ে আপনার টাইমলাইনে স্প্যাম ছড়াতে পারে, আপনাকে বিব্রতকর পোস্টে ট্যাগ করতে পারে বা ফিশিং লিঙ্ক পাঠাতে পারে।

প্রশ্ন ৫৬। আমি একজন ব্যক্তির কাছ থেকে একটি নতুন বন্ধু অনুরোধ পেয়েছি যার প্রোফাইল ছবি নেই, কিন্তু আমি আমার ক্লাসে এই নামে একজন সহপাঠী আছে। আমার কি ফ্রেন্ড রিকুয়েস্ট গ্রহন করা উচিত?

আপনার সহপাঠীকে ব্যক্তিগতভাবে জিজ্ঞাসা করুন যে সে প্রকৃতপক্ষে অনুরোধটি পাঠিয়েছে কিনা। সঠিক তথ্যটি জানার পরে উপযুক্ত সিদ্ধান্ত গ্রহণ করবেন।

প্রশ্ন ৫৭। আমি সোশ্যাল মিডিয়ায় কি ধরনের কন্টেন্ট পোস্ট করব?

আপনার পোস্টে সেই ধরণের বিষয়বস্তু থাকা উচিত যা আপনার বাস্তব জীবনের বন্ধুদের সাথে শেয়ার করা যায়। আপনার ব্যক্তিগত জীবন, কোন গোপনীয়তা বা কোন আইন বা সরকারী কার্যকলাপের বিরুদ্ধে যায় এমন কোন বিষয়বস্তু পোস্ট করা উচিত নয়।

প্রশ্ন ৫৮। সোশ্যাল মিডিয়া কীভাবে মানসিক স্বাস্থ্যের উপর প্রভাব ফেলে?

সোশ্যাল মিডিয়ায় ব্যবহার এর উপর মানসিক স্বাস্থ্যের প্রভাব সম্পর্কে অসংখ্য গবেষণা হয়েছে। এর বিভিন্ন নেতিবাচক প্রভাব রয়েছে, যেমন উদ্বেগ, বিষণ্নতা। এছাড়া সাইবার বুলিংয়ের ঝুঁকিতো আছেই। তবে কিছু ইতিবাচক দিকও আছে। অনলাইন ব্যবহারকারীদের নিজের মানসিক স্বাস্থ্যেকে বোঝা এবং যত্ন নেওয়া গুরুত্বপূর্ণ।

প্রশ্ন ৫৯। সোশ্যাল মিডিয়া কি আপনার তথ্য ব্যবসায়িক কাজে ব্যবহার করে?

তথ্য খুবই গুরুত্বপূর্ণ এবং আজকের বিশ্বে এর একটি বড় বাজার মূল্য রয়েছে। সোশ্যাল মিডিয়া আপনার ব্যক্তিগত তথ্য তাদের ব্যবসায়িক উদ্দেশ্যে ব্যবহার করতে পারে বা নাও করতে পারে। এটি আসলে সেই সোশ্যাল মিডিয়া ডেটা নীতির উপর নির্ভর করে। তবে ফ্রি সোশ্যাল মিডিয়া বা ওয়েবসাইট মূলত আপনার ডেটা ব্যবহার অর্থ উপার্জন করে থাকে।

প্রশ্ন ৬০। সোশ্যাল মিডিয়ায় কিভাবে ভুয়া খবর শনাক্ত করা যায়?

ভুয়া খবর মিথ্যা বা বিভ্রান্তিকর তথ্য বোঝায়। আপনি উৎস, লেখক, অন্যান্য উৎস চেক করে সহজেই একটি ভুয়া/মিথ্যা খবর সনাক্ত করতে পারেন। একটি সতর্ক/সমালোচনামূলক মানসিকতা বজায় রাখুন। ঘটনা, মন্তব্যগুলি, এটি একটি রসিকতা কিনা, ছবিগুলি সত্য কিনা চেক করার জন্য একটি Fact Checking (সত্য-যাচাই) সাইট ব্যবহার করুন।

প্রশ্ন ৬১। গুগল থেকে ছবি ডাউনলোড করে সোশ্যাল মিডিয়ায় ব্যবহার করা কি ঠিক?

ইন্টারনেট থেকে সরাসরি ফটো ডাউনলোড, কপি এবং পেস্ট করা ঠিক নয় । কপিরাইট আইন ইন্টারনেটে ছবিগুলিকে সংরিক্ষত করে। আপনি যদি তাদের অনুমতি ছাড়া কারো ছবি ব্যবহার করেন, তাহলে আপনি এটির জন্য দায়ী হবেন এবং মামলার ও সম্মুখীন হতে পারেন ।

প্রশ্ন ৬২। আমার অ্যাকাউন্টের নাম কি দেওয়া উচিত?

- পরিচয়পত্র অনুযায়ী আপনার নাম ব্যবহার করা উচিত। জাতীয় পরিচয়পত্র বা পাসপোর্ট বা ড্রাইভিং লাইসেন্স বা প্রাতিষ্ঠানিক আইডি কার্ড অনুযায়ী আপনার নাম ব্যবহার করা উচিত ।
- আপনি যদি বৈধ পরিচয় ব্যবহার করেন তবে এটি সহজেই সোশ্যাল মিডিয়া অ্যাকাউন্ট পুনরুদ্ধার করতে সাহায্য করবে ।

প্রশ্ন ৬৩। স্যোশাল মিডিয়াতে লগইন করার পূর্বে করনীয় বিষয়?

- কখনোই স্যোশাল মিডিয়ার লগইন তথ্য অন্য কোথাও প্রবেশ করানো যাবে না।
- অনেক সময় স্ক্যামাররা ভুয়া স্যোশাল মিডিয়ার ওয়েবসাইট তৈরি করে স্যোশাল মিডিয়াতে লগইন ইমেইল বা পাসওয়ার্ড চাইতে পারে। এরকম ক্ষেত্রে আগে সেই ওয়েবসাইটের url দেখে নিন।
- যেখানে অনেক ব্যক্তি একই কম্পিউটার ব্যবহার করেন, সেখানে অবশ্যই ব্যবহার শেষে লগআউট করুন।
- যদি লগআউট করতে ভুলে যান, তাহলে ফোন বা অন্য কোন কম্পিউটারে ফেসবুকে লগইন করে সিকিউরিটি এন্ড লগইন সেটিংয়ে গিয়ে দেখতে পাবেন, সর্বশেষ কোথায় আপনি লগইন করেছিলেন। সেখানে ডিভাইস সনাক্ত করে লগআউট করে দিতে পারেন।
- জিমেইলের ক্ষেত্রেও সেটিংস থেকে দেখতে পারেন আপনি আর কোথাও লগইন করে আছেন কিনা।

প্রশ্ন ৬৪। আমার স্যোশাল মিডিয়া একাউন্ট আমার ডিভাইস ছাড়া অপরিচিত কোন ডিভাইসে লগইন আছে কিনা কিভাবে বুঝব?

- অপরিচিত ডিভাইসে লগইনের বিষয়ে সতর্ক বার্তা গ্রহণের ব্যাপারে স্যোশাল মিডিয়া কর্তৃপক্ষ হতে প্রাপ্ত নির্দেশনা রয়েছে সেটি অনুসরণ করা যেতে পারে। যেমন ফেসবুক ও মেসেঞ্জার ব্যবহারের ক্ষেত্রে সেটিং থেকে একাউন্ট এবং মেসেঞ্জারের লগইনের বিষয়ে সতর্ক বার্তা (alert notification) চালু করে দিন। এরপর সেভ বাটনে ক্লিক করলে আপনার পাসওয়ার্ড চাইবে। এরপর থেকে কোথাও আপনার একাউন্ট লগইন হবে, তখন আপনাকে একটি বার্তা বা মেসেজ দিয়ে জানাবে ফেসবুক।

অধ্যায়-৮: মহিলা ও কিশোরীদের সাইবার নিরাপত্তা

প্রশ্ন ৬৫। আমার একটা ব্যক্তিগত ছবি সোশ্যাল মিডিয়ায় কেউ ছড়িয়ে দিয়েছে। এখন আমার করণীয় কি? আমি কিভাবে বন্ধ করতে পারি?

- নিজের আইডিতে এই ছবিসহ কেউ ট্যাগ করলে সেখানে আনট্যাগ করুন।
- সোশ্যাল মিডিয়ার এডমিনিস্ট্র্যাটর এর কাছে অভিযোগ/রিপোর্ট করুন।
- যেসব আইডিতে শেয়ার হয়েছে, সেসব আইডির স্ক্রিনশট নিতে হবে ছবিসহ।
- আপনার নিকটস্থ থানায় ঐ স্ক্রিনশটসহ অভিযোগ করুন।

প্রশ্ন ৬৬। অন্য ব্যক্তি আমার ব্যক্তিগত ভিডিও ইউটিউবে আপলোড করেছে। এক্ষেত্রে আমার করণীয় কি? এই ভিডিও বন্ধ করার উপায় কি?

(ক) এক্ষেত্রে যে ধাপগুলো অনুসরণ করবেন তা হলো:

- ইউটিউবে সাইন ইন করুন;
- ভিডিও প্লেয়ারের নিচে যেটা রিপোর্ট করতে চান, সেখানে ••• More ক্লিক করুন;
- ড্রপডাউন মেনু থেকে রিপোর্ট নির্বাচন করুন;
- ভিডিও রিপোর্ট করার কারণ নির্বাচন করুন;
- কোন অতিরিক্ত বর্ণনা থাকলে সেটা টাইমফ্রেমসহ বিস্তারিত উল্লেখ করুন।
- (খ) ৪৮-৭২ ঘন্টা অপেক্ষা করুন। বন্ধ না হলে লিংকসহ নিকটস্থ থানায় অভিযোগ করুন।

প্রশ্ন ৬৭। আমার ছবি এবং ভিডিও আমার বয়ফ্রেন্ড/ছেলে বন্ধুকে দিয়েছিলাম। পরবর্তীতে সে বিদেশী একটি অ্যাডাল্ট সাইটে সেই ছবি এবং ভিডিও ছড়িয়ে দেয়। এক্ষেত্রে এই ছবি/ভিডিও গুলো কিভাবে বন্ধ করবো?

- সংশ্লিষ্ট অ্যাডাল্ট সাইটের অ্যাডমিন/ওয়েবমাস্টার/স্টাফের সাথে যোগাযোগ করে পরিস্থিতি ব্যাখ্যাসহ ভিডিওটি বন্ধ করার জন্য রিপোর্ট করুন।
- ৪৮-৭২ ঘন্টা অপেক্ষা করুন। বন্ধ না হলে প্রয়োজনে লিংকসহ নিকটস্থ থানায় অভিযোগ করুন।

প্রশ্ন ৬৮। আমার ফেসবুক আইডি থেকে ছবি নিয়ে এডিট করে সোশ্যাল মিডিয়ায় ছড়িয়ে দেয়া হয়েছে এবং কল করে আমাকে বিরক্ত করা হচ্ছে। এক্ষেত্রে করণীয় কি?

- যেসব আইডি থেকে ছবি শেয়ার করা হচ্ছে সেসব আইডির স্ক্রিনশটসহ নিকটস্থ থানায় যোগাযোগ করুন।
- এডিটকৃত ছবি রিপোর্ট করুন।
- নিজের সোশ্যাল মিডিয়া প্রোফাইল লক করুন।

- উত্যক্তকারীকে ব্লক করুন।

প্রশ্ন ৬৯। আমার ম্যাসেঞ্জারে অশ্লীল ছবি, পর্ণোগ্রাফি পাঠিয়ে হয়রানি করা হচ্ছে। আমি কিভাবে বন্ধ করতে পারি?

ম্যাসেঞ্জারে অশ্লীল ছবি, পর্ণোগ্রাফি পাঠিয়ে হয়রানি করা হলে নিচের ধাপগুলো অবলম্বন করুন-

(ক) যিনি ম্যাসেঞ্জারে অশ্লীল ছবি, পর্ণোগ্রাফি পাঠিয়ে হয়রানি করছেন তিনি যদি আপনার ফ্রেন্ডলিস্টে থেকে থাকেন, তাহলে তাকে আনফ্রেন্ড করুন।

(খ) উত্যক্তকারীকে ব্লক করুন।

(গ) উত্যক্তকারীর আইডি রিপোর্ট করুন।

- উত্যক্তকারীর অ্যাকাউন্টের প্রোফাইলে যান। প্রোফাইলে গিয়ে (...) এ ক্লিক করে ফাইন্ড সাপোর্ট/রিপোর্ট প্রোফাইলের মাধ্যমে রিপোর্ট করুন;
- রিপোর্টের পরের স্টেপের ধাপগুলো অনুসরণ করুন।

প্রশ্ন ৭০। আমার নাম, ছবি ব্যবহার করে ফেইক আইডি খুলে বিভিন্ন জনকে কল গার্ল হিসেবে আমার নম্বর প্রদান করা হচ্ছে। আমার করণীয় কি?

- প্রথমে ফেইক আইডিটির স্ক্রিনশট সংগ্রহ করে রাখুন এবং লিংকটি কপি করে রাখুন। নিজের পরিচয়পত্রের কালার স্ক্যানড কপিসহ ফেইক আইডি টিকে রিপোর্ট করুন।
- রিপোর্ট করার পরে বন্ধ না হলে আপনার নামে যে ফেইক আইডিটি খোলা হয়েছে সেটির লিংক ও স্ক্রিনশটসহ নিকটস্থ থানায় যোগাযোগ করুন।

প্রশ্ন ৭১। ব্রেক আপ হয়ে যাওয়ার পর আমার বয়ফ্রেন্ড/ছেলে বন্ধু বিভিন্ন ব্যক্তিগত ছবি ও ভিডিও ছড়িয়ে দেয়ার হুমকি দিয়ে ব্ল্যাকমেইল করে টাকা দাবি করছে। আমার করণীয় কি?

- আপনার কোন অ্যাকাউন্টে আপনার বয়ফ্রেন্ডের অ্যাকসেস আছে কিনা। যদি থেকে থাকে তাহলে সব ডিভাইস থেকে লগ আউট করুন এবং পাসওয়ার্ড চেঞ্জ করুন।
- যে মাধ্যমগুলোতে হুমকি দিচ্ছে (মোবাইলে কল/এসএমএস, ম্যাসেঞ্জার, হোয়াটস অ্যাপ) এগুলোর রেকর্ড সংরক্ষণ করে রেকর্ডসহ নিকটস্থ থানায় যোগাযোগ করুন।

প্রশ্ন ৭২। আমার নিজের একটি ডিজিটাল ছবি আমি অনলাইনে পরিচয় হওয়া কোন ব্যক্তির কাছে দেখাতে চাই। এটা কি সেই ব্যক্তির কাছে পাঠানো ঠিক হবে?

- শুধুমাত্র অনলাইনে পরিচয় হওয়া কাউকে আপনার নিজের ছবি পাঠানো উচিত নয় ।

অধ্যায়-৯: অনলাইনে শিশুদের নিরাপত্তা

প্রশ্ন ৭৩। আমার বাচ্চা রাত জেগে ইন্টারনেট ব্যবহার করে। আমি কিভাবে মনিটর করতে পারি?

উইন্ডোজ এ সার্চবারে গিয়ে "family options" ক্লিক করে আপনার বাচ্চার জন্য একটি অ্যাকাউন্ট খুলে প্যারেন্টাল কন্ট্রোল চালু (enable) করুন।

প্যারেন্টাল কন্ট্রোলে যে যে সুবিধাগুলো পাবেন:

- আপনার বাচ্চাকে অনলাইনে সুরক্ষিত রাখতে পারবেন;
- গুড স্ক্রিন টাইম হ্যাবিট সেট করতে পারবেন;
- আপনার বাচ্চার ডিজিটাল লাইফের ট্র্যাক রাখতে পারবেন।

প্যারেন্টাল কন্ট্রোল চালু করার পদ্ধতি:

(ক) কম্পিউটার এর ক্ষেত্রে উইন্ডোজ এ বিদ্যমান ফ্যামিলি প্যারেন্টাল কন্ট্রোল সিস্টেমটি কনফিগার করুন।

- ✓ প্যারেন্টাল কন্ট্রোল সিস্টেমটি কনফিগার করার উপায়-
- ✓ Windows 10 এর জন্য Start > Settings > Accounts > Family & Other Users > Add a Family Member > Add a Child > enter email > Close.
- ✓ Windows 8 এর জন্য Windows key + C > Change PC Settings > Accounts > Other Accounts > Add an Account.
- ✓ Windows 7 এর জন্য Start > enter Parental Controls in search > select child account > Enforce Current Settings > configure settings > Close.

(খ) মাইক্রোসফট ফ্যামিলি ওয়েবসাইট থেকে আপনি যতগুলো অ্যাকাউন্ট সংযুক্ত করেছেন সবগুলো দেখতে পারবেন। সব প্যারেন্টাল কন্ট্রোল সেটিংস বাই ডিফল্ট বন্ধ করা থাকে। আপনাকে এই অপশনটি চালু করুন আলাদাভাবে এই ফিচারটি পাওয়ার জন্য।

প্রশ্ন ৭৪। আমার বাচ্চারা পড়াশোনার জন্য ল্যাপটপ ব্যবহার করে কিন্তু সেখানে বিভিন্ন ধরণের অ্যাডাল্ট অ্যাড আসে। সেটা কিভাবে বন্ধ করা যায়?

(ক) ল্যাপটপে অ্যাডাল্ট অ্যাড বা বিজ্ঞাপন বন্ধ করার জন্য নিচের ধাপগুলো অনুসরণ করুন

- প্রথমে ব্রাউজারে যেতে হবে;
- "myactivity.google.com" নামের সাইটে ঢুকতে হবে;
- ফলাফল আসার পর "Welcome to My Activity" তে ঢুকবেন;
- এটিতে ঢোকার পর বামদিকে "Activity controls" এ যাবেন এবং ক্লিক করবেন;
- স্ক্রল করে নিচে এসে "Ad personalization" এর "Go to Ad Settings" এ ক্লিক করবেন এবং Ad personalization অফ করে দিবেন।

(খ) অ্যান্ড্রয়েড স্মার্টফোন থেকে অ্যাড বন্ধ করার জন্য সাধারণ কিছু নিয়ম রয়েছে:

- প্রথমে স্মার্টফোনের সেটিংসে যেতে হবে;
- সেখানে গিয়ে আমাদের বের করুন 'গুগল'কে;
- 'গুগলে' ঢোকার পরে শুরুতেই থাকা 'অ্যাডস' অপশনে ক্লিক করুন। ক্লিক করলে 'অ্যাডস পারসোনালাইজড' নামে একটি অপশন আসবে, সেটি অন করুন;
- এবার 'ইউর অ্যাডভারটাইজিং আইডি' নামের অপশনটি রিসেট করে দিতে হবে;
- রিসেট করার পর 'অ্যাডভারটাইজিং আইডি' পরিবর্তন হয়ে যাবে। আশা করা যায়, বিরক্তিকর বিজ্ঞাপন দেখা থেকে মুক্তি মিলবে।

প্রশ্ন ৭৫। তরুন বা শিশুদের জন্য অনলাইনে কি কোন বুলিং বিরোধী টুলস আছে কি?

- প্রতিটি সামাজিক প্ল্যাটফর্ম এ প্রাইভেসি অপশন রয়েছে যার মাধ্যমে আপনি কন্ট্রোল করতে পারবেন যে কে আপনার পোস্টে কমেন্ট করতে পারবে কে আপনার পোস্ট গুলো দেখতে পারবে। সেক্ষেত্রে প্রাইভেসি সেটিং 'অনলি মি' অথবা 'অনলি ফ্রেন্ড' রাখলে এই সমস্যা থেকে প্রতিকার পাওয়া সম্ভব হতে পারে।
- আপনি যদি আপনার নিরাপত্তা বা অনলাইনে আপনার সাথে ঘটেছে এমন কিছু নিয়ে উদ্বিগ্ন হন, তাহলে আপনার বিশ্বাসযোগ্য একজন প্রাপ্তবয়স্ক ব্যক্তির সাথে জরুরীভাবে কথা বলুন। এছাড়াও আইনি সহয়তার জন্য প্রমাণ সহ নিকটস্থ থানার সাথে যোগাযোগ করুন।

প্রশ্ন ৭৬। আমার ছেলেমেয়েরা অতিরিক্ত ডিজিটাল ডিভাইস ব্যবহার করছে। এক্ষেত্রে করণীয় কি?

কম্পিউটার এর ক্ষেত্রে উইন্ডোজ এ বিদ্যমান ফ্যামিলি প্যারেন্টাল কন্ট্রোল সিস্টেমটি কনফিগার করুন।

- প্যারেন্টাল কন্ট্রোল সিস্টেমটি কনফিগার করার উপায়-
- Windows 10 এর জন্য Start > Settings > Accounts > Family & Other Users > Add a Family Member > Add a Child > enter email > Close.
- Windows 8 এর জন্য Windows key + C > Change PC Settings > Accounts > Other Accounts > Add an Account.
- Windows 7 এর জন্য Start > enter Parental Controls in search > select child account > Enforce Current Settings > configure settings > Close.

প্রশ্ন ৭৭। আমার ছেলেমেয়েরা ডিজিটাল ডিভাইস ব্যবহার করে অযাচীত/ ক্ষতিকর সাইট ব্রাউস করছে। এক্ষেত্রে করণীয় কি?

(ক) প্যারেন্টাল কন্ট্রোল ই-মেইল অ্যাকাউন্ট ব্যবহার করুন।

- শিশুদের ই-মেইল অ্যাকাউন্টটি খোলার সময় তার জন্ম তারিখটি সংযুক্ত করার পর সেটি যদি ১৩ বছরের নিচে হয় তাহলে, গুগল আপনা-আপনিই বলবে যে, ওই অ্যাকাউন্টটি প্যারেন্টাল কন্ট্রোলের অধীনে হবে।
- সেক্ষেত্রে জানতে চাওয়া হবে যে, ওই অ্যাকাউন্টটি অন্য কার অ্যাকাউন্টটির মাধ্যমে নিয়ন্ত্রিত হবে অর্থাৎ সেখানে যেকোন একজন অভিভাবকের ই-মেইল অ্যাকাউন্ট চাইবে। এখানে বাবা কিংবা মায়ের একটা ই-মেইল অ্যাকাউন্ট দেয়ার সুযোগ থাকে।
- এরপর থেকে এই জি-মেইল অ্যাকাউন্ট পুরো ডিভাইসের অ্যাকাউন্ট লগ-ইন করা হবে তখন সে এটি দিয়ে কী কী খুঁজলো, কী কী অ্যাপ ইন্সটল করলো, ইউটিউব-ফেসবুকে কী দেখলো-সব কিছু তখন অভিভাবকের ই-মেইল অ্যাড্রেস থেকে দেখা যাবে।
- এমনকি ওই ডিভাইসটি নিয়ে শিশু কোথায় গেলো সেই স্থানটিও শনাক্ত করা সম্ভব হবে।

(খ) ফেসবুক, মেসেঞ্জার এবং ইউটিউব-এর চাইল্ড/কিডস ভার্সন আছে। সেক্ষেত্রে বাচ্চাদের একটি অ্যাকাউন্ট তৈরি করে দেয়া যায় যেটি তারা ব্যবহার করলেও অভিভাবকদের সুপারভাইজ করার সুযোগ থাকে।

প্রশ্ন ৭৮। ডিজিটাল ডিভাইস থেকে শিশুকে দূরে রাখতে করণীয়

- দেড় বছর বয়স পর্যন্ত শিশুর সামনে কোনো ডিভাইস আনবেন না। টিভি, স্মার্টফোন, ট্যাব, ইউটিউব চালিয়ে সন্তানকে খেতে অভ্যস্ত করবেন না। স্মার্টটিভিকেও শিশুর নাগালের বাইরে রাখুন।
- দেড় থেকে দু'বছর বয়সে শুধু শিক্ষামূলক প্রোগ্রাম। এসময় আপনি অবশ্যই সঙ্গে থাকবেন।
- স্কুলে ফোন নিষিদ্ধের পক্ষে সামাজিক সচেতনতা গড়ে তুলুন, যাতে আপনার সন্তান স্কুল পরিবেশেও নিরাপদ থাকতে পারে।
- আসক্ত হওয়ার মতো কোনো অবসর যেন তার না থাকে। সন্তানকে ঘরের কাজে সম্পৃক্ত করুন। খেলাধূলা, বইপড়া ও সৃজনশীল কাজে উৎসাহ দিন।
- ইলেকট্রনিক সব ডিভাইস সে কী কাজে ব্যবহার করছে, তার দিকে নজর রাখুন। কম্পিউটার, ল্যাপটপ, স্মার্টফোন বা প্যাড- যেটাই হোক, অপারেটিং সিস্টেমে এমন কোনো ফিচার অ্যাড করা যায় কি না, যা আপনার সন্তানের নিরাপদ ব্যবহারকে নিশ্চিত করবে, তা জানার চেষ্টা করুন।
- শিশুবান্ধব ব্রাউজিংয়ের ফিচারগুলো চালু করুন। অর্থাৎ ইন্টারনেট ঘাঁটতে গিয়ে আপনার শিশু যাতে ক্ষতিকর বা বয়স অনুপযোগী কোনো সাইটে ঢুকে যেতে না পারে, সে ব্যবস্থা করুন। আইএসপি-র সহযোগিতাও নিতে পারেন।

অধ্যায়-১০: সরকারি দপ্তরে সাইবার নিরাপত্তা

সরকারি দপ্তরের কোনো কর্মকর্তা/কর্মচারী ফোন করলে শুরুতেই প্রশ্ন করুন:

সমস্যাটি আপনার ব্যক্তিগত একাউন্টের সমস্যা বিষয়ক নাকি দাপ্তরিক একাউন্টের সমস্যা বিষয়ক?

- ব্যক্তিগত সমস্যা বিষয়ক হলে কল সেন্টার অপারেটর প্রশ্নের উত্তর দিবেন

সরকারি একাউন্ট বিষয়ক হলে আপনি কি আপনার দপ্তরের সিস্টেম এনালিস্ট/মেইন্টেনেন্স ইঞ্জিনিয়ার/প্রোগ্রামারকে সমস্যার বিষয়টি অবহিত করেছেন?

- অবহিত করে থাকলে তিনি কি পদক্ষেপ নিয়েছেন?
- অবহিত না করে থাকলে অনতিবিলম্বে অবহিত করুন।
- অবহিত করে থাকলে এবং তিনি সমাধান না দিতে পারলে কল সেন্টার অপারেটর প্রশ্নের উত্তর দিবেন।