

শক্তিশালী পাসওয়ার্ড তৈরির নিয়ম

- কমপক্ষে ৮-১২ অক্ষরের পাসওয়ার্ড রাখা
- পাসওয়ার্ডে বড় (A-Z) ও ছোট (a-z) হাতের অক্ষর দেয়া
- সংখ্যা (0-9) ব্যবহার করা
- @, #, \$, % ইত্যাদি বিশেষ চিহ্ন যোগ ব্যবহার করা
- নিজের নাম, জন্মতারিখ, ফোন নম্বর ব্যবহার না করা
- “123456” বা “password” এরকম পাসওয়ার্ড না দেয়া
- সব অ্যাকাউন্টে একই পাসওয়ার্ড ব্যবহার না করা
- নিয়মিত (৩-৬ মাসে) পাসওয়ার্ড পরিবর্তন করা

সাইবার Bullying এবং করণীয়

খুব সহজভাবে বলা যায় ডিজিটাল মাধ্যমে কাউকে হয়রানি করার নামই সাইবার Bullying। কারো নামে অনলাইন মাধ্যমে মিথ্যা তথ্য ছড়ানো, আক্রমণাত্মক মেসেজ, কমেণ্ট বা পোস্ট করা, হুমকি দেয়া, কাউকে অপমানজনক, আপত্তিকর এবং অশ্লীল কথা বলা, ট্রল করা, কারো চেহারা নিয়ে উদ্দেশ্যপ্রণোদিতভাবে মজা করা, যৌন হয়রানি করা, আপত্তিকর মেসেজ বা ছবি পাঠানো ইত্যাদি উপায়ে সাইবার Bullying হতে পারে।

করণীয়

- অচেনা লোকের বাজে মন্তব্যকে এড়িয়ে চলুন ও রিপোর্ট করুন
- Bullying এর শিকার হলে স্ক্রিনশট রেখে দিন
- বাবা-মা, শিক্ষক বা বড় কাউকে বিষয়টি জানান
- যে Bullying করে তাকে ব্লক করুন
- সোশ্যাল মিডিয়া প্র্যাটফর্মে রিপোর্ট করুন
- নিজে Bullying করা থেকে বিরত থাকুন
- প্রয়োজনে পুলিশের সাহায্য নিন

সাইবার স্মার্ট হবার উপায়

- সবসময় শক্তিশালী পাসওয়ার্ড ব্যবহার করুন
- অচেনা কারো সাথে ব্যক্তিগত তথ্য শেয়ার করা যাবেনা
- নিয়মিত নিজের ডিভাইস ও অ্যাপস আপডেট রাখুন
- সাইবার Bullying হলে নীরব না থেকে জানিয়ে দিন
- গোপনীয়তা রক্ষায় সোশ্যাল মিডিয়ার সেটিংস ঠিক করুন
- বেশি ভালো অফার মানেই বেশি বিপদ, সতর্ক থাকুন
- প্রযুক্তির সুবিধা নিন, কিন্তু নিরাপদে থেকে
- নিজে সচেতন হোন, অন্যদের সচেতন করুন

সাইবার অপরাধের শিকার হলে করণীয়

- বাবা-মা, শিক্ষক বা অভিভাবককে জানাতে হবে
- মেসেজ, ছবি বা পোস্টের স্ক্রিনশট সংরক্ষণ করতে হবে
- ভুল করেও অপরাধীর সাথে ঝগড়ায় জড়ানো যাবে না
- প্রতারক বা অপরাধীকে ব্লক করে দিতে হবে
- পুলিশের সাইবার ইউনিটের সাথে যোগাযোগ করতে হবে
- অ্যাপসের প্রাইভেসি সেটিংস ঠিক করতে হবে
- বিস্তারিত তথ্যের জন্য ভিজিট করুন www.ncsa.gov.bd
- জাতীয় সাইবার নিরাপত্তা এজেন্সির হেল্পলাইন ৩৩৩ (৮) নম্বরে ফোন করতে হবে



এনহ্যান্সিং ডিজিটাল গভর্নমেন্ট এন্ড ইকোনমি প্রকল্প

ইয়ুথ টাওয়ার (লেভেল-৩, ৪ ও ৫), ৮২২/২ রোকেয়া সরণী,
ঢাকা-১২১৬, বাংলাদেশ

সাইবার নিরাপত্তা সহজ পথ



সাইবার নিরাপত্তা

সাইবার নিরাপত্তা হচ্ছে ইন্টারনেট ও ডিজিটাল জগতে নিজের তথ্য, ডিভাইস যেমন মোবাইল, ল্যাপটপ ইত্যাদি সুরক্ষিত রাখার নিয়ম ও ব্যবস্থা। এর মধ্যে আছে শক্তিশালী পাসওয়ার্ড ব্যবহার, অপরিচিত লিংকে ক্লিক না করা, ব্যক্তিগত তথ্য শেয়ার না করা, সোশ্যাল মিডিয়া ঠিকভাবে ব্যবহার করা ইত্যাদি বিষয়। যেহেতু আজকাল শিশু থেকে বৃদ্ধ সকলেই স্মার্টফোন, ট্যাব ও ইন্টারনেট ব্যবহার করছে-তাই সবার জন্য সাইবার নিরাপত্তা জানা খুবই জরুরি। সাইবার নিরাপত্তা শেখা মানে হলো অনলাইনে নিজেকে নিরাপদ রাখা শেখা।

অনলাইনে নিরাপদ থাকার সহজ উপায়

আমাদের দৈনন্দিন জীবনের একটা বড় অংশ আমরা অনলাইনে থাকি বা থাকতে হয়। তাই বাস্তব জগতের মতো অনলাইন পরিসরেও এখন নিরাপদ থাকা গুরুত্বপূর্ণ। চলুন দেখে নেওয়া যাক অনলাইনে নিরাপদ ও সুরক্ষিত থাকার কয়েকটি সহজ উপায়।

- ব্যক্তিগত তথ্য এবং পাসওয়ার্ড গোপন রাখুন
- সামাজিক যোগাযোগমাধ্যমে তথ্য দেওয়ার ক্ষেত্রে সতর্ক থাকুন
- শক্তিশালী পাসওয়ার্ড ব্যবহার করুন
- টু-ফ্যাক্টর অথেনটিকেশন ব্যবহার করুন
- নির্ভরযোগ্য ওয়েবসাইট থেকে অনলাইন কেনা-কাটা করুন
- অনলাইন লেন-দেনের পর সেই সাইট থেকে লগ আউট করুন
- সন্দেহজনক ওয়েবসাইট, ই-মেইল ও লিংক থেকে সতর্ক থাকুন
- ফ্রী বা পাবলিক ওয়াই-ফাই ব্যবহারে সতর্ক থাকুন

ডিজিটাল ডিভাইস সুরক্ষিত রাখতে করণীয়

আপনার ব্যক্তিগত ডিভাইস বিশেষ করে ডেস্কটপ, ল্যাপটপ, মোবাইল ফোন ইত্যাদি যাতে সুরক্ষিত থাকে সেই জন্য আপনাকে কিছু বিষয়ে খেয়াল রাখতে হবে।

- ডিভাইসে পাসকোড, পিন বা প্যাটার্ন লকের ব্যবস্থা রাখুন
- অ্যাপ ডাউনলোড করার ক্ষেত্রে অ্যাপটির রিভিউ পড়ুন
- ডিভাইসের অপারেটিং সিস্টেম এবং অ্যাপ আপডেট রাখুন
- ব্যবহার না হলে ডিভাইসের ওয়াই ফাই এবং ক্লুটথ বন্ধ রাখুন
- খুব জরুরি না হলে ফ্রী ওয়াই ফাই-ব্যবহার থেকে বিরত থাকুন
- ডিভাইস সম্পূর্ণ চার্জ হয়ে গেলে সেটি চার্জার থেকে খুলে রাখুন
- ডেস্কটপ বা ল্যাপটপে আপডেটেড এন্টিভাইরাস ব্যবহার করুন

হ্যাকিং এবং হ্যাকিং প্রতিরোধে করণীয়

ধরা যাক, কেউ একজন আপনার অনুমতি ছাড়াই আপনার কম্পিউটার, মোবাইল ফোন, বা অন্য কোনো ডিভাইসে ঢুকে গেল, এবং সেখান থেকে তথ্য চুরি করলো এবং ডিভাইসটির নিয়ন্ত্রণ নিয়ে নিলো। খুব সহজ ভাষায় এটাই হ্যাকিং। আমরা যারা ইন্টারনেট ব্যবহার করি তাদের সবারই হ্যাকিং সম্পর্কে প্রাথমিক ধারণা থাকা দরকার।

হ্যাকিং প্রতিরোধে করণীয়?

- একটি শক্তিশালী পাসওয়ার্ডের ব্যবহার করুন
- লোভনীয় হলেও অপরিচিত কোন লিংকে ক্লিক করবেন না
- পাইরেটেড সফটওয়্যার ব্যবহার থেকে বিরত থাকুন
- ডিভাইসে এন্টি-ভাইরাস সফটওয়্যার ব্যবহার করুন
- শুধু বিশ্বস্ত ওয়েবসাইটে অনলাইন শপিং করুন
- সব ধরনের পপ-আপ অ্যাডস/বিজ্ঞাপন এড়িয়ে যান
- ফ্রী ওয়াই-ফাই ব্যবহার থেকে বিরত থাকুন
- অ্যাকাউন্টে টু-স্টেপ ভেরিফিকেশন চালু করুন

সামাজিক যোগাযোগ মাধ্যমে করণীয়

- একান্ত ব্যক্তিগত তথ্য শেয়ার না করা
- অচেনা কাউকে ফ্রেন্ড রিকুয়েস্ট না পাঠানো
- অপরিচিত কারো ফ্রেন্ড রিকুয়েস্ট গ্রহণ না করা
- কাউকে আক্রমণ বা Bully না করা
- সন্দেহজনক লিংক বা বিজ্ঞাপনে ক্লিক না করা
- অতিরিক্ত সময় সোশ্যাল মিডিয়া ব্যবহার না করা
- ছবি বা ভিডিও শেয়ারের আগে অন্তত দু'বার ভাবা
- শক্তিশালী পাসওয়ার্ড ও টু-স্টেপ ভেরিফিকেশন চালু করা

অনলাইনে নিরাপদ শপিং ও করণীয়

- বিশ্বস্ত ওয়েবসাইট থেকে কেনাকাটা করুন
- ওয়েবসাইটে “https://” আছে কি না দেখে নিন
- সন্দেহজনক ও অতিরিক্ত সস্তা অফার থেকে দূরে থাকুন
- প্রোডাক্টের রিভিউ ও রেটিং দেখে অর্ডার করুন
- সম্ভব হলে অফিশিয়াল মোবাইল অ্যাপ ব্যবহার করুন
- শপিং সাইটে কার্ডের ডিটেইলস সেভ করে রাখবেন না
- প্রাইভেসি পলিসি এবং রিটার্ন পলিসি পড়ে নিন
- ওয়ান টাইম পাসওয়ার্ড (OTP) গোপন রাখুন

ফ্রি ওয়াই-ফাই ব্যবহারের আগে জেনে রাখুন

- বেশিরভাগ ফ্রী ওয়াই-ফাই নিরাপদ নয়
- ফ্রী ওয়াই-ফাইতে অটো কানেক্ট বন্ধ রাখুন
- ব্যাংকিং বা অনলাইন পেমেন্ট ফ্রী ওয়াই-ফাইতে নয়
- প্রয়োজনে VPN ব্যবহার করুন
- ফ্রী ওয়াই-ফাইতে ফাইল শেয়ারিং নিরাপদ নয়
- ব্যবহারের পর অ্যাকাউন্ট থেকে লগ আউট করুন
- শুধুমাত্র নির্ভরযোগ্য স্থানের ওয়াই-ফাই ব্যবহার করুন
- গুরুত্বপূর্ণ কাজে ফোনের ডাটা দিয়ে ব্রাউজিং করুন

