



অনলাইনে বিচরণকালে
আপনি কি একা?

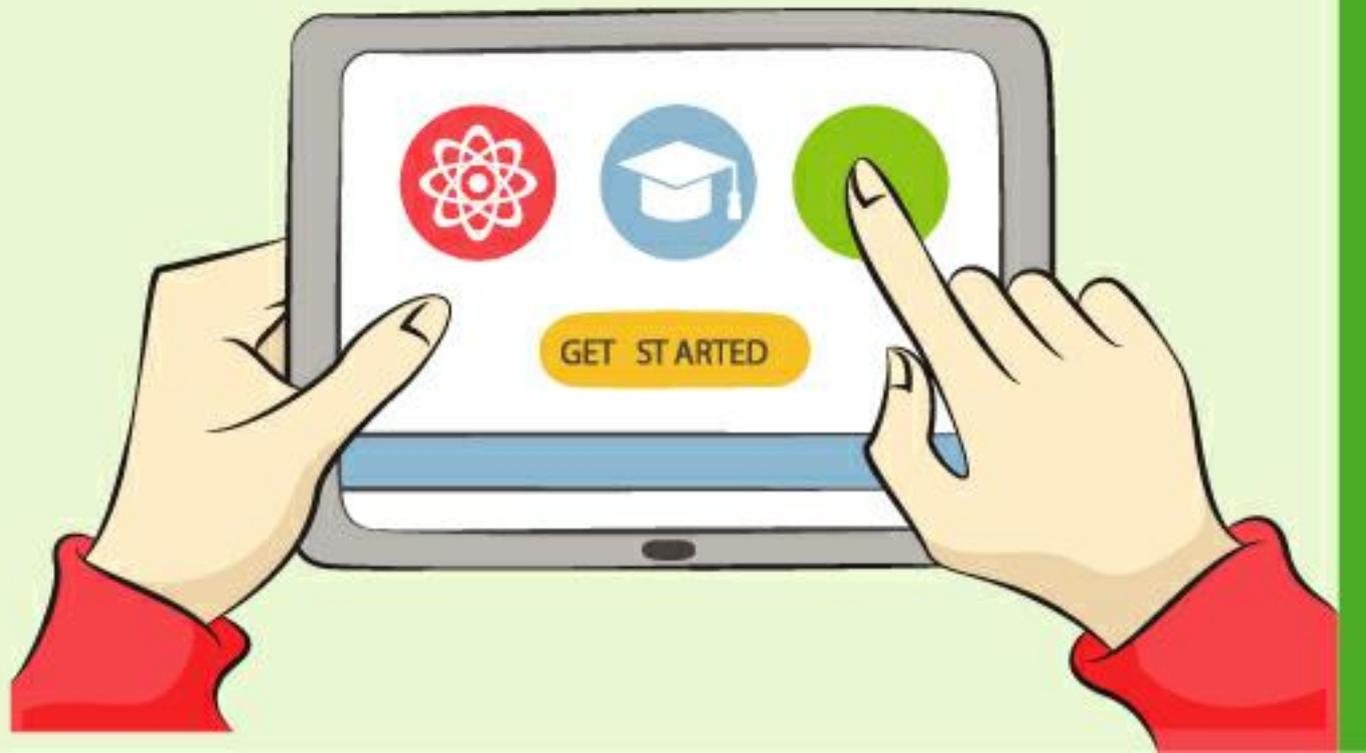
কেউ কি আপনাকে বা
আপনার অনলাইন কার্যকলাপ
পর্যবেক্ষণ করছে?

আপনি কি কারও লক্ষ্যবস্তু?



ডিজিটাল হাইজিন কী

১. একজন ব্যক্তির ডিজিটাল পরিচয়, তথ্যাদি এবং ব্যবহৃত যেকোনো ডিজিটাল ডিভাইস নিরাপদ ও স্বাস্থ্যকর রাখার উপায়
২. ডিজিটাল জগতে ঝুঁকিপূর্ণ তথ্য থেকে নিজেকে নিরাপদ রাখার উপায় এবং নিরাপদ যোগাযোগের কৌশল জানা
৩. অনলাইনে সুরক্ষা কৌশল ও গোপনীয়তা রক্ষা এবং অনলাইন হুমকি সম্পর্কে জানার সক্ষমতা
৪. ডিজিটাল মাধ্যমে নিরাপত্তা নিশ্চিত যথাযথ টুলস ব্যবহার করতে পারা
৫. ই-মেইল, মেসেজিং অ্যাপ এবং সোশ্যাল মিডিয়া ব্যবহারে নিরাপদ থাকার উপায় জানা
৬. শক্তিশালী পাসওয়ার্ড এবং মাল্টি-ফ্যাক্টর অথেনটিকেশন তৈরি সম্পর্কে ধারণা থাকা
৭. যথাযথ অ্যান্টিভাইরাস এবং যথাযথ সূত্র থেকে ইন্টারনেট ব্যবহারের প্রয়োজনীয়তা জানা
৮. ডিভাইস এবং অ্যাপ আপ-টু-ডেট রাখাসহ ডিজিটাল জগতে ঝুঁকিমুক্ত থাকার উপায় জানা





ডিজিটাল নিরাপত্তায় বিবেচ্য বিষয়

আপনি কী নিরাপদ রাখতে চান



- মানুষের সঙ্গে যোগাযোগের তথ্য
- একান্ত ব্যক্তিগত তথ্য ও ছবি
- আর্থিক লেনদেন-সংক্রান্ত তথ্য
- আপনার কাজের নথিপত্র

সাইবার অপরাধীরা কী চায়



- আপনার তথ্য হাতিয়ে নেওয়া
- আপনার তথ্য নষ্ট করা
- আপনার পরিচয়-সংক্রান্ত তথ্য (ক্রেডেনশিয়াল) চুরি করা
- আপনার কার্যকলাপ পর্যবেক্ষণ করা
- আপনার বিভিন্ন সেবা বন্ধ করে দেওয়া

আপনার কিছুই গোপন নয়



- কখন কার সঙ্গে কী কথা বলছেন
- কাকে কী মেইল পাঠাচ্ছেন
- সামাজিক যোগাযোগমাধ্যমে কী করছেন
- কোথায় যাচ্ছেন, কার সঙ্গে আছেন
- কী দেখছেন, কী খুঁজছেন
- বাড়ি, অফিস, শিশুর স্কুল, সব গন্তব্য



ডিজিটাল নিরাপত্তায় করণীয়

১. পাসওয়ার্ড দিয়ে ফোন বা কম্পিউটার সব সময় লক করে রাখুন।
২. সুযোগ থাকলে ফোনে পাসওয়ার্ড ও ফিঙ্গার প্রিন্ট লক-দুটোই ব্যবহার করুন।
৩. তথ্য সুরক্ষায় অন্তত ১৪ ডিজিটের শক্তিশালী পাসওয়ার্ড ব্যবহার করুন এবং নির্দিষ্ট সময় পরপর তা পরিবর্তন করুন।
৪. পাসওয়ার্ড কখনো কোথাও লিখে রাখবেন না।

৫. পাবলিক ওয়াই-ফাই ব্যবহারের সময় ভিপিএন ব্যবহার করুন।
৬. আপনার ডিভাইসে এনক্রিপশন চালু রাখুন, যেন আপনার ডেটা চুরি হলেও তার অর্থ কেউ না বোঝে।
৭. প্রাত্যহিক জীবন সম্পর্কে বাইরের কেউ ধারণা পায়, এমন তথ্য সামাজিক যোগাযোগমাধ্যমে দেওয়া থেকে বিরত থাকুন।
৮. ডিজিটাল মাধ্যমে একান্ত ব্যক্তিগত ছবি শেয়ার করা বা আপলোড করার বিষয়ে সতর্ক থাকুন।
৯. যেখানে যাচ্ছেন, সেখানেই চেক-ইন দেওয়া থেকে বিরত থাকুন।
১০. অস্থায়ী বা একবার সাইন-ইন করার জন্য ডিসপোজেবল ইমেইল (<https://temp-mail.org/>) ব্যবহার করুন।
১১. কোনো লিংক শেয়ার করার সময় ডিফ্যাং বা নিষ্ক্রিয় করে শেয়ার করুন।
১২. ইমেইলের জন্য জটিল পাসওয়ার্ডের সঙ্গে টু-ফ্যাক্টর অথেনটিকেশন ব্যবহার করুন।
১৩. ব্যবহৃত ব্রাউজার আপডেট রাখুন এবং ‘ডু নট ট্র্যাক’ অপশন বা ‘ইনকগনিটো মোড’ ব্যবহার করুন।
১৪. সেলফোনে যথাসম্ভব কম তথ্য সংরক্ষণ করুন, যেন ফোন হাতছাড়া হলেও হয়রানির শিকার না হন।
১৫. রিমোট ওয়াইপ সেট করুন, যেন ডিভাইস হারিয়ে গেলে অন্য ডিভাইস থেকে আপনি হারানো ডিভাইসের সব তথ্য মুছে দিতে পারেন।
১৬. সাইবার নিরাপত্তায় নতুনত্ব সম্পর্কে প্রতিনিয়ত জানার চেষ্টা করুন।

অ্যাপ সতর্কতা



১. প্লে-স্টোর এবং অ্যাপস্টোর থেকেই শুধু অ্যাপ ডাউনলোড করুন।
২. ইমেইল, মেসেজ বা ওয়েবসাইটে পাওয়া লিংক থেকে অ্যাপ নামাবেন না।
৩. অ্যাপ বানিয়েছে কারা দেখে নিন। তারা আগে কী ধরনের অ্যাপ বানিয়েছে, তা চেক করুন।
৪. রেটিং এবং ডাউনলোড সংখ্যা লক্ষ করুন। রিভিউ পড়ে বোঝার চেষ্টা করুন অ্যাপে কী সমস্যা আছে।
৫. সার্চ করার সময় একই নামে একাধিক অ্যাপ দেখতে পেলে বানান, আইকন ও বিবরণ দেখে বোঝার চেষ্টা করুন।
৬. নির্দিষ্ট অ্যাপটি কী তথ্য চায় দেখে নিন। ডাউনলোডের পর সেটিংসে গিয়ে ঠিক করুন তাকে কী তথ্য দেবেন।
৭. অ্যাপটি আপনার মোবাইল থেকে কী ধরনের তথ্য সংগ্রহ করবে এবং কোন কোন তথ্য অন্যের সঙ্গে শেয়ার করবে, তা চেক করে নিন।
৮. অ্যাপটি নিয়মিত আপডেট রাখুন।

ডিজিটাল অভ্যাস

অপারেটিং সিস্টেম এবং অন্যান্য
সফটওয়্যার নিয়মিত আপডেট করুন



স্বীকৃত অ্যান্টিভাইরাস ব্যবহার করুন,
নিয়মিত আপডেট করুন এবং
লাইভ স্ক্যান চালু রাখুন

নেটওয়ার্ক ফায়ারওয়াল ব্যবহার করুন



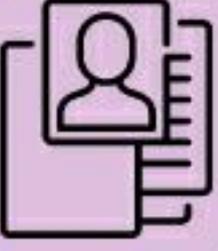
প্রাইভেসি সুরক্ষায় ব্যবহৃত রাউটারে
এনক্রিপশন চালু রাখুন

শক্তিশালী পাসওয়ার্ড (বড় হাতের এবং
ছোট হাতের অক্ষর, সংখ্যা এবং প্রতীক
সন্নিবেশিত) ব্যবহার করুন



শুধু বিশ্বস্ত সূত্র থেকে সফটওয়্যার ডাউনলোড
করুন এবং নিয়মিত আপডেট করুন

জরুরি ফাইলের ক্ষেত্রে এক্সটার্নাল হার্ড ড্রাইভ
বা ক্লাউড স্টোরেজে ব্যাকআপ রাখুন



অনলাইনে, বিশেষত সামাজিক
যোগাযোগমাধ্যমে ব্যক্তিগত তথ্য শেয়ার
করা থেকে বিরত থাকুন

ই-মেইল এবং সামাজিক যোগাযোগমাধ্যমের
প্রাইভেসি সেটিং পর্যালোচনা করুন



বিভিন্ন অ্যাপ (যেমন কুইজ, অনলাইন গেমস
অথবা সার্ভে) যেখানে ব্যক্তিগত তথ্য সংগ্রহ
করে, সেখানে সতর্ক হোন

অনলাইনে ব্রাউজিংয়ের ক্ষেত্রে ভিপিএন
ব্যবহার করতে পারেন



অনলাইনে লেনদেনের ক্ষেত্রে কাজ শেষে
সাইন আউট নিশ্চিত করুন

অপরিচিত লিংকে প্রবেশের আগে
সতর্কতা অবলম্বন করুন



Clear History
Clear Cookies
Clear Cache

নির্ধারিত সময় পর পর ব্রাউজার থেকে ক্যাশ,
কুকিজ এবং ব্রাউজিং হিস্ট্রি মুছে ফেলুন

অব্যবহৃত অ্যাপ মুছে ফেলুন



ফরোয়ার্ডেড ম্যাসেজের ক্ষেত্রে
সতর্ক হোন

অনলাইনে ফাঁদের ব্যাপারে
সতর্ক থাকুন



RESPECT
PRIVACY

অন্যের গোপনীয়তাকে
সম্মান করুন

ব্যবহৃত গুগল অ্যাকাউন্টটি সচল থাকতে হবে, লোকেশন চালু থাকতে হবে, ফাইন্ড মাই ডিভাইস অপশনটি অন থাকতে হবে এবং মোবাইলটি ইন্টারনেটের সঙ্গে সংযুক্ত থাকতে হবে। বিস্তারিত জানুন এখানে: <https://android.com/find>

৩. আপনার ব্যবহৃত পাসওয়ার্ড কতটা শক্তিশালী, তা চেক করতে <https://passwordmonster.com/>
৪. আপনার ই-মেইল আইডি ব্যবহার করেছেন এমন কোনো সাইটে ডাটা চুরির ঘটনা ঘটলে তা জানতে <https://haveibeenpwned.com/>
৫. অস্থায়ী কাজে ব্যবহারের জন্য ডিসপোজেবল ই-মেইল তৈরি করতে <https://temp-mail.org/>
৬. অ্যানড্রয়েড মোবাইলে ব্যবহারের জন্য অ্যাপ ডাউনলোডের বিশ্বস্ত সূত্র <https://play.google.com/store/apps/>
৭. প্রতিটি অ্যাপ প্ল্যাটফর্মেরই রয়েছে কিছু শর্ত এবং নীতিমালা, তবে কিছু প্রকাশ্যে থাকলেও কিছু থাকে গোপনীয়। আপনার ব্যবহৃত অ্যাপের শর্তাবলি জানতে <https://tosdr.org/>
৮. আপনার জন্য সঠিক অ্যান্টিভাইরাস কোনটি জানতে হলে* <https://safetydetectives.com/>
৯. আপনার কম্পিউটারের এন্টিভাইরাস ঠিকভাবে কাজ করছে কি না তা পরীক্ষা করতে <https://eicar.org>

* আপনার কম্পিউটারে লাইসেন্সপ্রাপ্ত উইন্ডোজ অপারেটিং সিস্টেম থাকলে মাইক্রোসফট ডিফেন্ডার অ্যান্টিভাইরাস ব্যবহার করুন এবং নিয়মিত আপডেট করুন।