হ্যান্ডবুক

ভোটের মাঠে সাংবাদিক

শারীরিক ও ডিজিটাল ঝুঁকি ব্যবস্থাপনায় করণীয়

digitally right

সূচিপত্র

সূচিপত্র

ভূমিকা

বাংলাদেশে জাতীয় সংসদ নির্বাচন অনুষ্ঠিত হওয়ার কথা রয়েছে ২০২৬ সালের জানুয়ারিতে। আসন্ন নির্বাচন দেশের জন্য একটি গুরুত্বপূর্ণ মাইলফলক। নির্বাচনের সময়ে প্রতিটি মুহূর্তের খবর জানার জন্য মানুষের আগ্রহ বেড়ে যায়। সেই চাহিদা পূরণে সবচেয়ে গুরুত্বপূর্ণ ভূমিকা পালন করে গণমাধ্যম। মাঠপর্যায়ে প্রতিনিয়ত ঘটতে থাকা ঘটনাগুলো জানতে জনগণ তাকিয়ে থাকে সাংবাদিকদের দিকে।

এমন একটি গুরুত্বপূর্ণ সময়ে সাংবাদিক হিসেবে আপনার দায়িত্ব অত্যন্ত চ্যালেঞ্জিং। বস্তুনিষ্ঠ তথ্য পরিবেশন এবং সত্য তুলে ধরার জন্য আপনাকে থাকতে হয় মাঠের সবচেয়ে সক্রিয় অংশে। রাজনৈতিক দলগুলোর প্রচার কার্যক্রম যেমন কভার করতে হয়, তেমনি নির্বাচনকেন্দ্রিক সংঘাত, উত্তেজনা বা সহিংসতাও তুলে ধরতে হয়। অনেক ক্ষেত্রে আইনশৃঙ্খলা রক্ষাকারী বাহিনী ও রাজনৈতিক কর্মীদের সংঘর্ষের মধ্যে রিপোর্ট করতে গিয়ে আপনার শারীরিক ঝুঁকির আশঙ্কা তৈরি হতে পারে। আবার সঠিক, নিরপেক্ষ প্রতিবেদন প্রকাশের কারণে আপনি হতে পারেন কোনো গোষ্ঠী বা ব্যক্তির লক্ষ্যবস্তু।

ঝুঁকি কেবল মাঠেই নয়, থাকতে পারে ডিজিটাল স্পেসেও। আপনি অনলাইন হয়রানি, ব্যক্তিগত তথ্য ফাঁস, ট্রল বা সংঘবদ্ধ আক্রমণের শিকার হতে পারেন। এমনকি ব্যক্তিগত অ্যাকাউন্ট হ্যাক করার চেষ্টাও হতে পারে, যা পেশাগত ও আর্থিক ক্ষতির কারণ হয়ে দাঁড়াতে পারে।

বিগত নির্বাচনগুলোতে সহিংস সংঘর্ষ, ভিন্নমতের দমন এবং সংবাদমাধ্যমকে ভয় দেখানোর মতো ঘটনা দেখা গেছে। নির্বাচনী পরিস্থিতি আরও বেশি প্রতিযোগিতামূলক এবং সংঘাতপূর্ণ হয়ে ওঠার কারণে, নির্বাচন কভার করা সাংবাদিকদের অনলাইন এবং অফলাইন উভয় ক্ষেত্রেই তীব্র নিরাপত্তা ঝুঁকির সম্মুখীন হওয়ার আশঙ্কা রয়েছে।

২০২৬ সালের জাতীয় নির্বাচনে সাংবাদিকদের জন্য শারীরিক ও নিরাপত্তা ঝুঁকি আগের তুলনায় বাড়বে বলে জানা যায় ডিজিটালি রাইটের এক সাম্প্রতিক গবেষণায়। নির্বাচনের সময়ে সাংবাদিকদের সম্মুখীন হওয়া হুমকি এবং কীভাবে সেগুলোর মোকাবিলা করা যায়, তা আরও ভালোভাবে বোঝার জন্য দেশের ১৯টি জেলার ২০১ জন সাংবাদিকের একটি জরিপ এবং ১০টি সাক্ষাৎকারে পাওয়া তথ্যের ভিত্তিতে সেই গবেষণা তৈরি করা হয়।

“হাই রিস্ক, লো প্রিপেয়ার্ডনেস: জার্নালিস্ট সেফটি ইন ২০২৬ ইলেকশন” শিরোনামের সেই গবেষণা থেকে জানা যায়,

- ৮৯% সাংবাদিক নির্বাচন কভার করার সময় আক্রমণ বা মারধরের আশঙ্কা করছেন।
- ৭৬% সাংবাদিক মৌখিক হয়রানির ভয় পাচ্ছেন, অন্যদিকে ৭১% সাংবাদিক ভয়ভীতি প্রদর্শন বা হুমকির আশঙ্কা করছেন।
- নারী সাংবাদিকদের মধ্যে ৫০% যৌন হয়রানি, এবং ৪০% যৌন আক্রমণের ভয় করছেন।

নির্বাচনী সংবাদ সংগ্রহের সময় শারীরিক হুমকির পাশাপাশি ডিজিটাল হয়রানি বেড়ে যাবারও আশঙ্কা করছেন সাংবাদিকেরা।

- ৭৫ শতাংশ সাংবাদিক আশঙ্কা করছেন তাদের নিজেদের বা সংশ্লিষ্ট সংবাদমাধ্যমের বিরুদ্ধে অপতথ্য ছড়ানো হতে পারে।
- ৬৫ শতাংশের কাছে হ্যাকিং একটি বড় ঝুঁকি।
- ৮০% নারী সাংবাদিক অনলাইনে নজরদারি নিয়ে উদ্বেগ প্রকাশ করেছেন।

উত্তরদাতাদের অর্ধেকের বেশি মনে করেন, তাদের বিশ্বাসযোগ্যতা নষ্ট করার উদ্দেশ্যে মানহানিকর প্রচারও চালানো হতে পারে।

এই হ্যান্ডবুকটি একটি নির্দেশিকা হিসেবে কাজ করবে, যা আপনাকে নির্বাচনকালীন সময়ে মাঠ পর্যায়ে এবং অনলাইনে সম্ভাব্য শারীরিক ও ডিজিটাল ঝুঁকিগুলো মোকাবিলা করতে সাহায্য করবে। আমাদের লক্ষ্য, আপনি যেন নিরাপত্তা নিশ্চিত করে আপনার পেশাগত দায়িত্ব সঠিকভাবে পালন করতে পারেন।

কেন এই হ্যান্ডবুক?

বাংলাদেশে নির্বাচনের সময় রাজনৈতিক উত্তেজনা প্রায়শই চরমে পৌঁছায়, যার ফলস্বরূপ সাংবাদিকেরা সরাসরি সংঘাত বা চাপের সম্মুখীন হতে পারেন। সহিংসতা, হুমকি, হয়রানি এবং ডিজিটাল আক্রমণের ঘটনা বৃদ্ধি পায়। এই হ্যান্ডবুকটি তৈরি করা হয়েছে সেইসব সুনির্দিষ্ট চ্যালেঞ্জের কথা মাথায় রেখে, যা একজন রিপোর্টার, ফটোসাংবাদিক বা সম্পাদককে মোকাবিলা করতে হয়। এর মাধ্যমে, আপনারা ঝুঁকিগুলো আগে থেকে চিনতে পারবেন এবং সেগুলো মোকাবিলায় প্রয়োজনীয় ব্যবহারিক কৌশল অবলম্বন করতে পারবেন।

হ্যান্ডবুকের লক্ষ্য

এই হ্যান্ডবুকের মূল লক্ষ্য হলো, সাংবাদিকদের জন্য একটি শক্তিশালী নিরাপত্তা প্রোটোকল প্রতিষ্ঠা করা। এটি শারীরিক নিরাপত্তা, ডিজিটাল সেফটি, ডেটা সুরক্ষা এবং মানসিক স্থিতিশীলতা বজায় রাখার ব্যবহারিক দিকগুলো নিয়ে আলোচনা করবে। আমরা আশা করি, এই নির্দেশিকা অনুসরণ করে সাংবাদিকেরা নির্ভয়ে, নিরাপদে এবং পূর্ণাঙ্গ পেশাদারিত্বের সঙ্গে তাদের দায়িত্ব পালন করতে সক্ষম হবেন, যাতে সংবাদ সংগ্রহ প্রক্রিয়ার কোনো পর্যায়েই নিরাপত্তার কারণে আপস করতে না হয়।

এছাড়াও, এই নির্দেশিকা অনুসরণ করে সাংবাদিকেরা যা জানতে পারবেন:

তথ্য যাচাই বা ফ্যাক্টচেকিং

কীভাবে নির্বাচনের সময় ছড়িয়ে পড়া ভুল তথ্য ও গুজব যাচাই করে সঠিক প্রতিবেদন তৈরি করতে হয় এবং অপতথ্য থেকে নিজেদের রক্ষা করতে হয়।

অনলাইন হয়রানি ও ঘৃণাসূচক বক্তব্য মোকাবিলা

সাংবাদিকদের নিয়ে অপতথ্য ছড়ানো হলে, বা তারা অনলাইন হয়রানি কিংবা ঘৃণাসূচক বক্তব্যের শিকার হলে কী করতে হবে এবং কোথায় সহায়তা চাইতে হবে তার নির্দেশনা।

শারীরিক ঝুঁকি ও নিরাপত্তায় করণীয়

নির্বাচনী সময়ে মাঠে দায়িত্ব পালনরত সাংবাদিকদের শারীরিক নিরাপত্তার ঝুঁকি উল্লেখযোগ্যভাবে বৃদ্ধি পায়। সমাবেশ, প্রচার–প্রচারণা, ভোটকেন্দ্র ও বিক্ষোভ-প্রতিবাদে ভিড়, উত্তেজনা ও সহিংসতা দ্রুত পরিস্থিতি সংকটজনক করে তুলতে পারে। আগের নির্বাচনের সময়গুলোতে রাজনৈতিক পরিবেশ উত্তপ্ত হলে সাংবাদিকেরা প্রায়ই উদ্দেশ্যপ্রণোদিত হামলা, ডিভাইস ভাঙচুর, লাইভ কাভারেজে বাধা এবং চলাচলে সীমাবদ্ধতার সম্মুখীন হন।

২০২৫ সালে সাংবাদিকদের ওপর সংঘটিত বিভিন্ন হামলা ও হেনস্তার ঘটনা নির্বাচনী সময়ে ঝুঁকির মাত্রা আরও স্পষ্টভাবে তুলে ধরে। যেমন, গত অক্টোবরে কুমিল্লার দেবীদ্বারে সংবাদ সংগ্রহ করতে যাওয়া আট সাংবাদিকের ওপর হামলার ঘটনা ঘটে। আবার নভেম্বরে আরেক জেলা পিরোজপুরে সংবাদ সংগ্রহের কাজে গেলে রাজনৈতিক দলের কর্মীরা সাংবাদিকের মোবাইল ও বিভিন্ন ডিভাইস ছিনিয়ে নেয় বলে জানা যায় প্রতিবেদনে।

তাই মাঠে নামার আগে নিরাপত্তা পরিকল্পনা তৈরি করা, ঝুঁকি মূল্যায়ন করা, অবস্থান ও চলাচলের নিরাপদ পথ চিহ্নিত করা, দ্রুত সরে যাওয়ার কৌশল জানা এবং সহকর্মীদের সঙ্গে নিরবচ্ছিন্ন যোগাযোগ বজায় রাখা অত্যন্ত জরুরি।

এই ধরনের পরিস্থিতিতে নিজের নিরাপত্তা নিশ্চিত করতে নিচের পদক্ষেপগুলো মেনে চলা অপরিহার্য:

১.১ রিপোর্টিংয়ের সময় প্রয়োজনীয় জিনিস সঙ্গে রাখুন

শারীরিক পরীক্ষার জন্য একটি সুসজ্জিত প্রাথমিক চিকিৎসা কিট সঙ্গে রাখুন। সেখানে ছোটখাটো আঘাত, কাটা বা ফোস্কার চিকিৎসার জন্য পর্যাপ্ত ব্যান্ডেজ, অ্যান্টিসেপটিক ওয়াইপস, জীবাণুনাশক মলম, এবং ব্যক্তিগত প্রয়োজনীয় ওষুধপত্র (যেমন- ব্যথা উপশমকারী, অ্যালার্জির মেডিসিন) রাখুন। কাঁদানে গ্যাসের সংস্পর্শে এলে চোখ ধোয়ার জন্য ছোট এক বোতল পানি সঙ্গে রাখুন। মুখ ও চোখ মোছার জন্য ভিজে ওয়াইপস টিস্যু এবং নিরাপত্তা গগলস বা চশমা রাখুন। এছাড়া জনবহুল এলাকায় কাভারেজের পর দ্রুত হাত পরিষ্কারের জন্য হ্যান্ড স্যানিটাইজার সঙ্গে রাখুন।

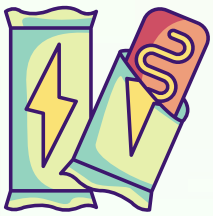
এক নজরে

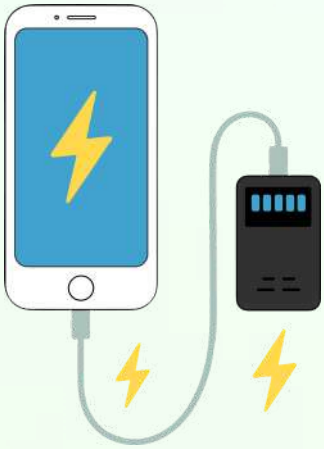
- ব্যান্ডেজ
- অ্যান্টিসেপটিক ওয়াইপস
- জীবাণুনাশক মলম
- ব্যক্তিগত প্রয়োজনীয় ওষুধপত্র
- খাবার পানি
- নিরাপত্তা গগলস বা চশমা
- হ্যান্ড স্যানিটাইজার

দীর্ঘ সময় মাঠে কাজ করার সময় শারীরিক সক্ষমতা বজায় রাখতে পর্যাপ্ত খাবার সঙ্গে রাখুন।

ডিহাইড্রেশন বা পানিশূন্যতা রোধের জন্য কমপক্ষে ২ থেকে ৩ লিটার বিশুদ্ধ পানীয় জল এবং ইলেক্ট্রোলাইট ভারসাম্য রক্ষার জন্য ওআরএস (ORS) বা স্যালাইন মিশ্রিত পানি রাখুন।

দ্রুত শক্তি সরবরাহকারী উচ্চ শক্তির স্ন্যাকস (যেমন: এনার্জি বার, ড্রাই ফ্রুটস বা খেজুর) সঙ্গে রাখুন, যা সহজে বহনযোগ্য এবং দীর্ঘ সময় শক্তি ধরে রাখতে সাহায্য করে।





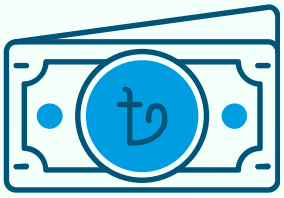
রিপোর্টিংয়ের সময়ে নিরবচ্ছিন্ন সংযোগ এবং রেকর্ডিং কার্যকারিতা বজায় রাখা গুরুত্বপূর্ণ। তাই মোবাইল ফোন ও রেকর্ডিং ডিভাইসের জন্য অতিরিক্ত ব্যাটারি এবং ন্যূনতম ১০,০০০ mAh ক্ষমতাসম্পন্ন পাওয়ার ব্যাংক সম্পূর্ণরূপে চার্জ করে রাখুন।

রাতের কাভারেজ বা বিদ্যুৎ বিভ্রাটের সময় ব্যবহারের জন্য অতিরিক্ত ব্যাটারিসহ একটি শক্তিশালী টর্চলাইট বা হেডল্যাম্প সঙ্গে রাখুন।

অপ্রত্যাশিত বৃষ্টি, ধুলা বা কাঁদানে গ্যাস থেকে ডিভাইস সুরক্ষিত রাখতে প্লাস্টিক কভার বা ডাস্ট কভার সঙ্গে রাখতে পারেন।

ভেঙে যেতে পারে এমন কোনো জিনিস সঙ্গে রাখবেন না।

চোর কিংবা ছিনতাইকারী আপনার ডিভাইসের প্রতি আকৃষ্ট হতে পারে কি না বিবেচনা করুন। মূল্যবান জিনিসপত্র এবং নগদ অর্থের পরিমাণ সীমিত রাখুন।



আপনার কাছে অবশ্যই সঠিক স্বীকৃতিপত্র বা প্রেস আইডেন্টিফিকেশন কার্ড থাকতে হবে। ফ্রিল্যান্স সাংবাদিকদের ক্ষেত্রে, নিয়োগকর্তা বা সংবাদ সংস্থার কাছ থেকে পাওয়া একটি অনুমতিপত্র সঙ্গে রাখা সহায়ক হতে পারে। তাই এ ধরণের পরিচয়পত্র সঙ্গে রাখুন। এছাড়া আবেদনের ভিত্তিতে নির্বাচন কমিশনের পক্ষ থেকেও সাংবাদিক পাস কার্ড দেওয়া হবে। নির্বাচনের সময়ে এই কার্ডটি অবশ্যই সঙ্গে রাখুন। কেবলমাত্র নিরাপদ পরিবেশেই পরিচয়পত্রটি দৃশ্যমান করুন। এটি গলায় ফিতা দিয়ে ঝুলিয়ে রাখা এড়িয়ে চলুন, যা আক্রমণের সময় একজন হামলাকারীকে সুবিধা দিতে পারে। এর পরিবর্তে, এটি বেল্টে ক্লিপ দিয়ে লাগিয়ে রাখুন।

১.২ সঠিক পোশাক পরিধান করুন

শক্ত সোলের, লেইসযুক্ত এবং গোড়ালির ভারবহন করে এমন মজবুত জুতা পরুন। স্যান্ডেল বা স্লিপ-অন জুতা সম্পূর্ণরূপে পরিহার করুন, যা দ্রুত চলাচল বা দৌড়ানোর সময় বাধা হয়ে যেতে পারে বা বিপজ্জনক হতে পারে।

সংবাদমাধ্যমের নাম লেখা নেই, এমন নিরপেক্ষ পোশাক পরিধান করুন। রাজনৈতিক স্লোগান, সংবাদমাধ্যমের ব্র্যান্ডিং সম্বলিত পোশাক, সামরিক প্যাটার্নের পোশাক, এবং দাহ্য পদার্থ (যেমন: নাইলন) দিয়ে তৈরি পোশাক পরিধান করা এড়িয়ে চলুন। ঢিলেঢালা পোশাক পরিহার করুন, কারণ তা টেনে ধরার সুযোগ তৈরি করতে পারে।

কখনো কখনো আপনার সংবাদ প্রতিষ্ঠানের পরিচিতি সম্বলিত (লোগো বা নামসহ) পোশাক (যেমন: জ্যাকেট বা টি-শার্ট) আপনার জন্য রক্ষাকবচ হতে পারে, আবার কখনো ঝুঁকির কারণও হতে পারে। এজন্য আগে পরিস্থিতি বা ঝুঁকি পর্যালোচনা করে সিদ্ধান্ত নিন, কখন সেটি আপনার পরতে হবে।

নারী সাংবাদিকদের জন্য ওড়না শারীরিক সুরক্ষার জন্য মারাত্মক ঝুঁকি তৈরি করতে পারে। ভিড়ের মধ্যে এটি সহজেই আক্রমণকারীরা টেনে ধরতে পারে, বা গলায় পেঁচিয়ে শ্বাসরোধের চেষ্টা করতে পারে। আবার ভিড়ের মধ্যে ওড়না কোনো বস্তুতে আটকে গিয়ে পড়ে যাওয়ার কারণ হতে পারে। তাই:

- এটি এমনভাবে পরুন যাতে কোনো আলগা প্রান্ত না থাকে এবং সহজে টেনে খোলা না যায়। অথবা এমন পোশাক পরিধান করুন যেটি ওড়নার বিকল্প হতে পারে।

- ওড়নার দুই প্রান্ত এবং মাঝের অংশগুলো একাধিক সেফটি পিন বা ছোট ক্লিপ ব্যবহার করে পোশাকের সঙ্গে শক্তভাবে আটকে দিন। এই সেফটি পিনগুলো প্রয়োজনে আপনি আত্মরক্ষার কাজেও ব্যবহার করতে পারেন।

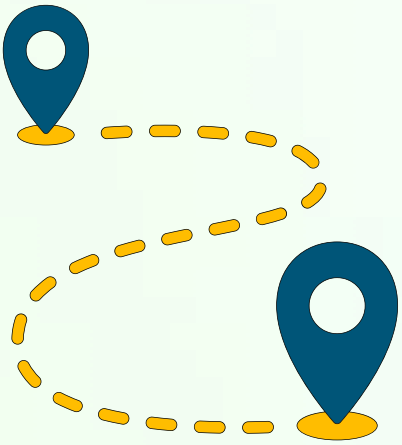
- যদি ওড়না বা হিজাব ব্যবহার করেন, তবে লম্বা চুল ওড়নার বাইরে আলগা রাখবেন না। চুল শক্তভাবে বেঁধে নিন এবং সম্ভব হলে ওড়নার ভেতরে রাখুন, যেন পিছন দিক থেকে কেউ চুল টেনে আক্রমণ করতে না পারে।

১.৩ তাৎক্ষণিক ঝুঁকি বিচার করুন ও বিকল্প পথের খোঁজ করুন

একটি জমায়েত বা সমাবেশ যেকোনো মুহূর্তে সহিংস বা শত্রুভাবাপন্ন হয়ে উঠতে পারে। এই ধরনের পরিস্থিতি মোকাবিলায় দ্রুত প্রতিক্রিয়া এবং পূর্বপরিকল্পনা অত্যন্ত জরুরি। তাই:

- যেখানে যাচ্ছেন সেই জায়গা নিয়ে আগেই গবেষণা করুন। মানচিত্রে (যেমন- গুগল ম্যাপ) সেখানে প্রবেশ করা বা দ্রুত বেরিয়ে যাওয়ার পথ দেখে নিন।
- যেখানে সুযোগ আছে, আগেরদিন গিয়ে রেকি করে আসুন। আশপাশে কী আছে এবং বিপদে পড়লে কোথায় আশ্রয় নেবেন— ঠিক করে রাখুন।

ঘটনাস্থলে পৌঁছানোর পর সংঘাতময় পরিস্থিতি তৈরি হতে পারে। তাই আপনার অবস্থান থেকে বেরিয়ে যাওয়ার সমস্ত পথ চিহ্নিত করুন। বিশেষ করে সরু গলি বা বন্ধ গেটগুলো চিহ্নিত করে রাখুন। পরিস্থিতি প্রতিকূল হলে যেন দ্রুত সেখান থেকে নিরাপদে বেরিয়ে যেতে পারেন।



- যদি দলবেঁধে কাজ করেন, তবে জরুরি পরিস্থিতিতে কোথায় মিলিত হবেন সেই স্থানটি আগে থেকেই নির্ধারণ করে রাখুন।

যানবাহন ও বিকল্প পরিবহন:

- আপনার যানবাহন এমন নিরাপদ জায়গায় (বড় রাস্তা বা ফাঁকা জায়গা) রাখুন, যেখান থেকে সংঘাতময় সময়ে সহজেই বেরিয়ে যাওয়া যায়।

- জরুরি পরিস্থিতিতে আপনার জন্য একটি বিকল্প পরিবহন ব্যবস্থা নিশ্চিত করুন।

- পরিস্থিতির সংবেদনশীলতা বিবেচনা করে ডিভাইস ও যানবাহন থেকে সংবাদমাধ্যমের লোগো সরিয়ে দিন, যাতে আপনার উপস্থিতি কম মনোযোগ আকর্ষণ করে।

আগাম প্রস্তুতি:

মনে রাখবেন, নিরাপত্তা সব সময় নির্দিষ্ট পরিস্থিতির ওপর নির্ভর করে। কোথাও গণমাধ্যমের গাড়ি দেখে মানুষ নিরাপদে যাবার পথ করে দেবে, আবার কোথাও একই গাড়ি দেখে হামলা করতে পারে। তাই,

- সার্বিক পরিস্থিতি, সেখানকার রাজনৈতিক পরিবেশ, আপনার গণমাধ্যম সম্পর্কে স্থানীয় প্রভাবশালীদের ধারণা, নির্দিষ্ট ব্যক্তি বা গোষ্ঠীর পূর্ব প্রতিক্রিয়া — এগুলো সম্পর্কে তথ্য সংগ্রহ করুন এবং পরিকল্পনা করুন।

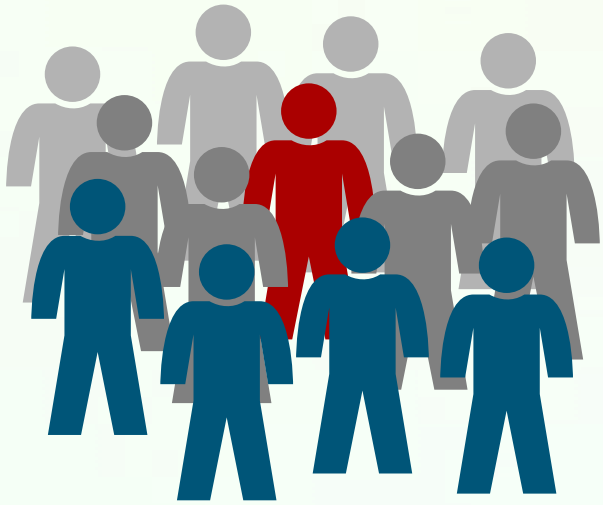
- আপনার পরিকল্পনা কাজে না-ও আসতে পারে। তাই বিকল্প পরিকল্পনাও রাখুন, বিশেষ করে ঝুঁকিপূর্ণ বলে পরিচিত এলাকার ক্ষেত্রে।

- নির্দিষ্ট সেই এলাকার স্থানীয় প্রশাসন, চেনা ব্যক্তি ও রাজনীতিবিদ, নিরাপত্তা বাহিনীর কর্মকর্তা বা পুলিশের কর্মকর্তাদের ফোন নম্বর নিজের সংগ্রহে রাখুন এবং নিজের একজন সহকর্মীকে দিয়ে রাখুন, যেন হামলার পরিস্থিতি তৈরি হলে তাদের সঙ্গে দ্রুত যোগাযোগ করা যায়।

জমায়েতের মেজাজ বোঝা:

জমায়েতের মেজাজ বোঝার চেষ্টা করুন। সেখানে উপস্থিত থাকা অন্যান্য সাংবাদিক বা স্থানীয়দের সঙ্গে কথা বলে পরিস্থিতির সামগ্রিক তথ্য নিন।

- যদি এমন বুঝতে পারেন যে সংঘাত হতে পারে কিংবা সাংবাদিকদের উপর আক্রমণ হতে পারে তাহলে দুরত্ব বজায় রাখুন।



- দেখুন, অন্য সাংবাদিকের সাথে কী আচরণ করা হচ্ছে। জমায়েতটি যে দলের বা ব্যক্তির, তাদের আপনার বা কোনো গণমাধ্যম সম্পর্কে বিরূপ অবস্থান আছে কি না।

- জমায়েতটি কি মারমুখী বা উচ্ছৃঙ্খল, আশপাশে প্রতিযোগী পক্ষের কোনো জমায়েত আছে, যা হঠাৎ উত্তেজনা তৈরি করতে পারে? সেটিও যাচাই করুন।

- ভিড়ের বাইরে অবস্থান করুন এবং মাঝখানে ঢুকে যাওয়া এড়িয়ে চলুন, যেখান থেকে বের হওয়া কঠিন হবে।

- সংঘাত বেঁধে গেলে বা সহিংসতা শুরু হলে নিরাপদ দূরত্ব থেকে এবং একটু উঁচু অবস্থান থেকে ছবি বা ভিডিও তুলুন। যেখানেই অবস্থান নিচ্ছেন সেখান থেকে দ্রুত সরে যাওয়ার পথ আছে কি না দেখে নিন। পথ মাত্র একটি হলে এবং সেটি ঘিরে ফেললে আপনি বিপদে পড়তে পারেন।

- এমন পরিস্থিতিতে আপনার রেকির অভিজ্ঞতা কাজে আসবে। আগে রেকি না করতে পারলে, ঘটনাস্থলে পৌঁছে একটু সময় নিয়ে এলাকাটি পর্যবেক্ষণ করুন এবং নিরাপদ জায়গা ও পথ খুঁজে নিন। না পেলে, আগে থেকেই সাবধান হোন।

পুলিশ ও নিরাপত্তা বাহিনীর আচরণ:

ভিড় ও জমায়েত নিয়ে কর্তৃপক্ষের মনোভাব কী এবং তারা কেমন আচরণ করতে পারে, সেদিকে সব সময় খেয়াল রাখুন। জনতা উত্তেজিত হলে পুলিশ বেশি আক্রমণাত্মক হয়ে উঠতে পারে।

- দাঙ্গা নিয়ন্ত্রণের সরঞ্জাম বা দাঙ্গা নিয়ন্ত্রণের পোশাক পরিহিত পুলিশের আগমন, লাঠির ব্যবহার, বা কাঁদানে গ্যাস ছোড়ার মতো দৃশ্যমান ইঙ্গিতগুলো বিপদ সংকেত বা রেড ফ্ল্যাগ। এমন লক্ষণ দেখামাত্রই নিরাপদ স্থানে সরে যান বা দ্রুত প্রস্থানের পরিকল্পনা শুরু করুন।

- কখনো কখনো সংঘাতে পুলিশের পেছনে থাকাকে নিরাপদ বলে মনে করা হয়। কিন্তু এটাও পরিস্থিতির ওপর নির্ভরশীল। এতে অপর পক্ষ আপনাকে টার্গেট করতে পারে।

- আবার কখনও পুলিশই সংবাদ মাধ্যমের ওপর চড়াও হওয়ার নজির আছে। তাই সবসময় পরিস্থিতির ওপর আপনার প্রচ্ছন্ন ধারণা আপনাকে অবস্থান নিতে সাহায্য করবে।

- কোনো গবেষণা বা পরিস্থিতি পর্যালোচনা না করেই ঘটনাস্থলে সংবাদ সংগ্রহ শুরু করা — আপনাকে বিপদে ফেলতে পারে।

ফটো সাংবাদিকদের বিশেষ সতর্কতা:

ফটো সাংবাদিকদের সংঘাতের ঘটনাগুলো আরও কাছ থেকে কাভার করতে হয় বলে তারা বেশি ঝুঁকিতে থাকেন। তাই:

- শ্বাসরোধের ঝুঁকি এড়াতে, ক্যামেরার ফিতা গলায় ঝুলিয়ে রাখবেন না।

- কিছু সময় পরপরই ভিউফাইন্ডার থেকে চোখ সরিয়ে চারপাশে খেয়াল করুন।

- ঘটনার ছবি তোলার পর দ্রুত ভিড় ত্যাগ করুন।

অনেক ফটো সাংবাদিক বিপদে পড়েন কারণ ক্যামেরায় চোখ থাকায় তিনি তাৎক্ষণিক ঝুঁকি বুঝে উঠতে পারেন না। ছবি তুলতে তুলতে তারা বিপজ্জনক জায়গাতেও এগোতে থাকেন।

- আগেই ঘটনাস্থল পর্যালোচনা করে নিন এবং অত্যন্ত বিপজ্জনক স্থানে রিপোর্টারকে সঙ্গে রাখুন বা অন্য ফটো সাংবাদিকদের সঙ্গে থাকুন। আপনার চোখ ভিউফাইন্ডারে থাকাকালীন তারা যেনো আপনাকে প্রয়োজনীয় দিকনির্দেশনা দিতে পারেন।

১.৪ মৌখিক আক্রমণ প্রতিরোধে যা করবেন

রাজনৈতিক সমাবেশ বা বিক্ষোভের সময় সংবাদমাধ্যমের প্রতি বিদ্বেষপূর্ণ মনোভাব দেখা যেতে পারে, যার ফলে গালিগালাজ বা লাঞ্ছনার শিকার হওয়া স্বাভাবিক। এমন পরিস্থিতিতে যা করতে পারেন:

- মানসিকভাবে প্রস্তুত থাকুন। যদি জমায়েত বা বক্তব্য দেওয়া নেতাকর্মীরা সংবাদমাধ্যমের প্রতি বিদ্বেষী হন, তাহলে গালিগালাজ শোনার জন্য মানসিকভাবে প্রস্তুত থাকুন।

- গালিগালাজের কোনো প্রতিক্রিয়া দেখাবেন না বা উপস্থিত জনতার সঙ্গে তর্কে জড়াবেন না। মনে রাখবেন, অন্যরা পেশাদার না হলেও আপনি একজন পেশাদার। পরিস্থিতি শান্ত হতে দিন এবং প্রয়োজনে অপেক্ষা করুন। তারপর আপনার কাজ করে যান এবং প্রতিবেদন তৈরি করুন।

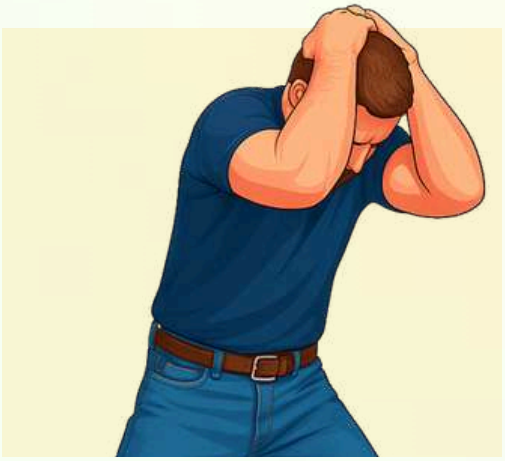
- কোনো বস্তু নিক্ষেপের ঝুঁকি বিবেচনা করুন। যদি ভিড় থেকে থুতু বা কোনো কিছু ছুড়ে মারার আশঙ্কা থাকে, কিন্তু রিপোর্টিং একান্ত জরুরি হয় তাহলে একটি হুডযুক্ত, জলরোধী টুপি বা জ্যাকেট পরার কথা বিবেচনা করুন।

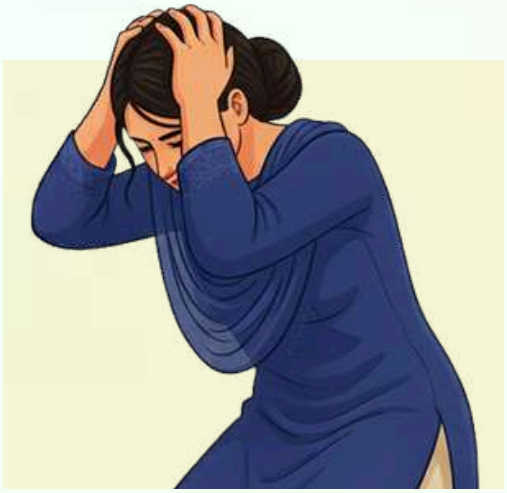
- আগ্রাসন প্রশমন করুন। আক্রমণকারীকে শনাক্ত করতে শারীরিক অঙ্গভঙ্গি বোঝার চেষ্টা করুন এবং আপনার নিজের শারীরিক অভিব্যক্তি ব্যবহার করে পরিস্থিতি শান্ত করার চেষ্টা করুন।

- আক্রমণকারীকে পর্যবেক্ষণে রাখুন, এবং শান্তভাবে কথা বলুন। বিপজ্জনক ব্যক্তি থেকে অন্তত এক হাত সমান দূরত্বে থাকুন। হাত দিয়ে ধরে রাখার চেষ্টা করা হলে, উত্তেজিত না হয়ে দৃঢ়ভাবে নিজেকে মুক্ত করে দ্রুত দূরে সরে যান।

১.৫ শারীরিক আক্রমণ থেকে বাঁচতে যা করবেন

- **মাথা রক্ষা করুন:** সংঘাত বেড়ে গেলে বা আঘাতের আশঙ্কা থাকলে, নিজের একটি হাত মুক্ত রেখে সেটি দিয়ে আপনার মাথার সুরক্ষা নিশ্চিত করুন। বিশেষ করে, মাথার পেছনের অংশ ও ঘাড় রক্ষা করার চেষ্টা করুন।





- **পিছিয়ে যাওয়া:** মাটিতে পড়ে যাওয়ার মতো পরিস্থিতি এড়াতে ছোট ছোট কিন্তু সুচিন্তিত পদক্ষেপের মাধ্যমে ধীরে ধীরে পেছনে সরে যান। কখনো আক্রমণকারীর দিকে পিঠ দিয়ে দৌড়াবেন না, এতে আপনি সহজে আঘাতের লক্ষ্যবস্তু হতে পারেন।

- **দলগত সুরক্ষা:** যদি দলবদ্ধভাবে কাজ করেন, তবে একসঙ্গে থাকুন এবং একে অপরের হাত ধরে রাখুন। এটি আপনাদের বিচ্ছিন্ন হওয়া থেকে রক্ষা করবে এবং একটি ঢাল তৈরি করবে।

- **নিরাপদ স্থান চিহ্নিত করা:** সম্ভব হলে, তাৎক্ষণিক আঘাত থেকে বাঁচতে নিকটস্থ কোনো শক্ত কাঠামো বা উঁচু স্থানের পেছনে আশ্রয় নিন।

- **ডিভাইসের সুরক্ষার চেয়ে নিজেকে গুরুত্ব দিন:** যদি আপনাকে চারপাশ থেকে ঘিরে ধরা হয় এবং আক্রমণকারী আপনার ডিভাইস (ক্যামেরা, ফোন, মাইক্রোফোন) চায়, তবে তা দিয়ে দিন। মনে রাখুন, ডিভাইসের থেকে আপনার জীবনের মূল্য অনেক বেশি। কোনো ডিভাইসের জন্য তর্ক বা প্রতিরোধ করবেন না।

- **আক্রমণের ঘটনা সংরক্ষণ করুন:** আক্রমণের ঘটনার ছবি-ভিডিও কখনো কখনো আদর্শ সাংবাদিকতার উদাহরণ হতে পারে। তবে মনে রাখবেন, আক্রমণকারী ব্যক্তির ছবি তোলা পরিস্থিতিকে আরও খারাপ করে তুলতে পারে। নিজের সুরক্ষা নিশ্চিত করার পর, যদি পরিস্থিতি শান্ত হয়, তারপর সাক্ষ্য ও প্রমাণ সংগ্রহের চেষ্টা করুন।

- **চিকিৎসা ও মানসিক সহায়তা নিন:** আঘাত গুরুতর হোক বা না হোক, অবিলম্বে চিকিৎসা সহায়তা নিন এবং ঘটনাটি আপনার উর্ধ্বতন কর্তৃপক্ষকে জানান। আপনার মানসিক স্বাস্থ্যের প্রতি খেয়াল রাখুন এবং প্রয়োজন হলে মানসিক সহায়তা নিন।

১.৬ গ্রেপ্তার, আটক বা অপহরণের ঝুঁকি থাকলে যা করবেন

যেসব সাংবাদিক এমন রিপোর্টিংয়ে কাজ করছেন যেখানে আইনশৃঙ্খলা বাহিনী বা রাজনৈতিক দলের নেতাকর্মীদের দ্বারা গ্রেপ্তার, আটক বা অপহরণের ঝুঁকি আছে, তাদের জন্য ব্যক্তিগত সুরক্ষা ও যোগাযোগ কৌশল নিশ্চিত করা আবশ্যক। আটক বা অপহরণের মতো ঘটনা মোকাবিলায় পূর্বপ্রস্তুতিই হলো সবচেয়ে কার্যকর সুরক্ষা। এমন সময়ে একজন রিপোর্টার যা করতে পারেন:

রিপোর্টের আগে যোগাযোগ ও আইনি সহায়তা নিশ্চিত করুন :

- কর্মস্থল, পরিবার এবং বিশ্বস্ত বন্ধুদের সঙ্গে একটি সুনির্দিষ্ট যোগাযোগ ব্যবস্থা তৈরি করুন। কখন, কোন মাধ্যমে আপনি যোগাযোগ করবেন তা স্পষ্ট জানিয়ে দিন। কতক্ষণ যোগাযোগ না করলে তা বিপজ্জনক হিসেবে গণ্য হবে তা নির্দিষ্ট করুন ও জানিয়ে দিন। নিখোঁজ হওয়ার আশঙ্কা থাকলে দ্রুত কর্তৃপক্ষের সঙ্গে যোগাযোগ করার জন্য আপনার সম্পাদক বা একজন সহকর্মীর নাম ও যোগাযোগের বিস্তারিত তথ্য পরিবারের কাছে দিয়ে রাখুন।

- আপনার পক্ষে কাজ করতে প্রস্তুত একজন আইনজীবীর নাম ও যোগাযোগের নম্বর আগে থেকেই ঠিক করে রাখুন। ফোন ডিরেক্টরিতে সংরক্ষণের পাশাপাশি, এটি একটি কাগজের টুকরা বা নিজের হাতে সাংকেতিক উপায়ে লিখে রাখুন, যাতে ডিভাইস বাজেয়াপ্ত হলেও তথ্যটি খুঁজে পাওয়া যায়।

- নিশ্চিত করুন যে আপনার কাছে সঠিক, বৈধ এবং হালনাগাদকৃত পরিচয়পত্র (যেমন: প্রেস ক্রেডেনশিয়াল, জাতীয় পরিচয়পত্র, ড্রাইভিং লাইসেন্স, পাসপোর্ট) আছে। কর্তৃপক্ষ চাইলে দ্রুত তা দেখাতে প্রস্তুত থাকুন।

- গ্রেপ্তার বা আটকের মুখে আপনার প্রতিক্রিয়া কেমন হবে তা নিয়ে মানসিকভাবে প্রস্তুত থাকুন। পরিস্থিতি অনুযায়ী পুলিশ মাত্রাতিরিক্ত বল প্রয়োগ করতে পারে। এই বিষয়ে সচেতন থাকুন এবং সংযত প্রতিক্রিয়া দেখানোর পরিকল্পনা করুন। আটকের ঘটনা ঘটলে শান্ত থাকা এবং পেশাদারিত্ব বজায় রাখা পরিস্থিতিকে নিয়ন্ত্রণ করতে সাহায্য করতে পারে। গ্রেপ্তারকারী অফিসারের প্রতি সশ্রদ্ধ ভাব বজায় রাখার চেষ্টা করুন। টুপি বা সানগ্লাস পরে থাকলে তা খুলে ফেলুন এবং প্রতিরোধ করা থেকে বিরত থাকুন।

- গ্রেপ্তারের ছবি বা ভিডিও ধারণের আগে সতর্ক থাকুন। এই কাজটি পুলিশকে উত্তেজিত করতে পারে এবং আপনার ডিভাইসগুলো ক্ষতিগ্রস্ত বা বাজেয়াপ্ত হতে পারে। সম্ভব হলে, আপনার ব্যাগ ও ইলেকট্রনিক ডিভাইসগুলোকে আপনার দৃষ্টিসীমার মধ্যে রাখুন এবং বাজেয়াপ্ত করার আগে তথ্য এনক্রিপ্ট বা ক্লাউডে আপলোড করার চেষ্টা করুন।

- অ্যাজমা, ডায়াবেটিস বা অন্যান্য জরুরি স্বাস্থ্য পরিস্থিতি সম্পর্কে দ্রুত পুলিশকে অবহিত করুন। আপনার স্বাস্থ্যগত অবস্থা নিয়ন্ত্রণের জন্য প্রয়োজনীয় ওষুধ বা সাম্প্রতিক মানসিক স্বাস্থ্য সমস্যার ইতিহাস থাকলে তা স্পষ্ট করে জানান।

- সুযোগ পেলে জড়িত পুলিশ কর্মকর্তাদের শনাক্ত করা যায় এমন তথ্য যেমন তাদের নাম, ব্যাজ নম্বর, বিভাগ এবং সহজেই শনাক্তযোগ্য বৈশিষ্ট্য (যেমন: ট্যাটু, গোঁফ/দাঁড়ি) লক্ষ্য করুন এবং সম্ভব হলে লিপিবদ্ধ করুন। আশেপাশে

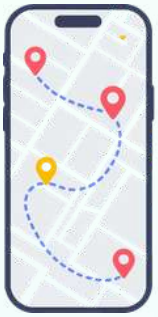
থাকা প্রত্যক্ষদর্শীদের প্রতি মনোযোগ দিন এবং প্রয়োজনে তাদের আপনার অফিস বা আইনজীবীর সঙ্গে যোগাযোগ করতে বলুন।

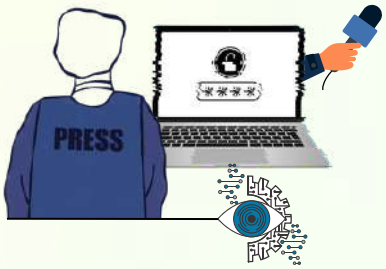
- যদি পুলিশ অফিসাররা ভয় দেখিয়ে বা প্রলোভন দিয়ে আপনাকে কোনো অপরাধ স্বীকার করতে বাধ্য করার চেষ্টা করে, তবে শান্তভাবে আপনার নিজের ভাষ্যে অটল থাকুন। আপনি যা করেননি তা স্বীকার না করে আইনি সহায়তা বা আপনার আইনজীবীর আগমন পর্যন্ত অপেক্ষা করুন। যদি কোনো পুলিশ অফিসার দ্বারা লাঞ্ছিত হন বা আঘাতের শিকার হোন, তবে আঘাতের স্থান, চিকিৎসা ও হাসপাতালে যাওয়ার প্রমাণ (যেমন, মেডিকেল রিপোর্ট) অবশ্যই সংরক্ষণ করুন। ঘটনার জন্য দায়ী ব্যক্তিদের নাম ও বাহ্যিক বিবরণ দ্রুত নথিবদ্ধ করুন।

অপহরণের ঝুঁকি থাকলে চলাচলে পরিবর্তন আনুন:

- যদি এমন মনে হয় যে আপনি অপহরণের ঝুঁকিতে আছেন (যেমন: হুমকি, সতর্কতা বা নজরদারির প্রমাণ), তবে এই তথ্যটি সহকর্মী, বন্ধু এবং পরিবারের কাছে অত্যন্ত গোপনীয়তার সঙ্গে জানান। কর্মস্থলে আসা-যাওয়া বা রাতের বেলা চলাচল বিশেষভাবে বিপজ্জনক হতে পারে। আপনার চলাচলের অভ্যাসে পরিবর্তন আনুন এবং কোনো প্রকার নির্দিষ্ট প্যাটার্ন বা রুট অনুসরণ করা এড়িয়ে চলুন।

- ঝুঁকির মাত্রা বেশি হলে, আপনি স্মার্টফোনে একটি ট্র্যাকিং অ্যাপ্লিকেশন যুক্ত করতে পারেন। জরুরি সহায়তার প্রয়োজন হলে আপনার সুনির্দিষ্ট অবস্থান শেয়ার করে এমন ট্র্যাকিং অ্যাক্সেস বিশ্বস্ত সহকর্মী বা পরিবারের সঙ্গে শেয়ার করুন।





ডিজিটাল ঝুঁকি ও নিরাপত্তায় করণীয়

নির্বাচন কভার করার সময় সাংবাদিকেরা শারীরিক ঝুঁকির পাশাপাশি বিভিন্ন ধরনের ডিজিটাল হুমকির মুখোমুখি হতে পারেন। মাঠে রিপোর্টিংয়ের সময় ডিভাইস জব্দ হওয়া, ডিজিটাল যোগাযোগে নজরদারি চালানো, ইন্টারনেট ব্যবহারে হঠাৎ সীমাবদ্ধতা সৃষ্টি, কিংবা অনলাইন অ্যাকাউন্ট হ্যাক করে আর্থিক প্রতারণা বা ব্যক্তিগত ক্ষতি করার মতো আক্রমণ বেড়ে যেতে পারে। সংবেদনশীল নথি, সূত্রের পরিচয় বা অপ্রকাশিত প্রতিবেদনসমূহ ফোন বা ল্যাপটপে থাকলে ডিভাইস জব্দের ফলে সেগুলো ফাঁস হওয়ার গুরুতর ঝুঁকি থাকে। তাই রাজনৈতিকভাবে উত্তপ্ত বা নজরদারিমূলক পরিবেশে কাজ করা সাংবাদিকদের জন্য ডিজিটাল সুরক্ষা আগেই নিশ্চিত করা অপরিহার্য। ডিজিটাল সুরক্ষা নিশ্চিতে সাংবাদিকেরা নিচের পদ্ধতি ও টুলগুলো ব্যবহার করতে পারেন:

২.১ অনলাইন অ্যাকাউন্টের সুরক্ষা নিশ্চিত করুন

নির্বাচনের সময়ে সাংবাদিকেরা নিজ প্রতিষ্ঠানে বা সহকর্মীদের সঙ্গে তথ্য আদান-প্রদানের জন্য ডিজিটাল মাধ্যমের ব্যবহার করে থাকে। ইমেইল, সামাজিক মাধ্যমের বিভিন্ন অ্যাপ যেমন– হোয়াটসঅ্যাপ, মেসেঞ্জার, সিগন্যাল, বা অন্য অনলাইন মাধ্যমে। এখন প্রশ্ন হলো, যদি এই অ্যাকাউন্টগুলো হ্যাক হয়ে যায়, বা নজরদারির কারণে তথ্য আগেভাগে ফাঁস হয় তাহলে সেটি সাংবাদিকদের ঝুঁকির কারণ হতে পারে। তাই অ্যাকাউন্টের সুরক্ষা এখন অপরিহার্য।

ভোটকেন্দ্রে গোপন ব্যালটের সুরক্ষা যেমন জরুরি, তেমনি অনলাইন অ্যাকাউন্টের সুরক্ষাও জরুরি। অনলাইন এসব অ্যাকাউন্টের সুরক্ষার জন্য কয়েকটি সহজ পদ্ধতি রয়েছে।

শক্তিশালী পাসওয়ার্ড

অনলাইন সুরক্ষার প্রথম ধাপ হচ্ছে একটি শক্তিশালী পাসওয়ার্ড। পাসওয়ার্ড যত শক্তিশালী হবে আপনার অ্যাকাউন্ট তত সুরক্ষিত থাকবে। একটি দুর্বল পাসওয়ার্ড (যেমন: 123456, password, iloveyou, মোবাইল নম্বর বা নিজের নাম) হ্যাকাররা কয়েক সেকেন্ডের মধ্যেই অনুমান করে ফেলতে পারে। তাই এ ধরনের পাসওয়ার্ড কখনই ব্যবহার করা উচিত নয়।

শক্তিশালী পাসওয়ার্ড তৈরি করবেন যেভাবে

- লম্বা এবং জটিল পাসওয়ার্ড চিন্তা করুন।

  পাসওয়ার্ডটি কমপক্ষে ১৪ অক্ষরের হওয়া উচিত।

  এতে বড় হাতের অক্ষর (A-Z), ছোট হাতের অক্ষর (a-z), সংখ্যা (0-9), এবং চিহ্ন (!, @, #, $, %)—এই চার ধরনের মিশ্রণ ব্যবহার করুন।

  উদাহরণ: AmiValo@manush2025!

- সহজে অনুমানযোগ্য তথ্য এড়িয়ে চলুন।

  আপনার নাম, জন্ম তারিখ, পোষা প্রাণীর নাম, বা প্রিয় সিনেমার নাম সহজেই অনুমানযোগ্য। তাই এ ধরনের তথ্য পাসওয়ার্ডে ব্যবহার করা থেকে বিরত থাকুন।

- পাসফ্রেজ ব্যবহার করুন।

  সম্পূর্ণ একটি বাক্যকে পাসওয়ার্ড হিসেবে ব্যবহার করা (যাকে পাসফ্রেজ বলে) একটি চমৎকার কৌশল। এটি মনে রাখাও সহজ, আবার হ্যাক করাও কঠিন। উদাহরণ: AmarSonarBanglaAmiTomayValobashi! থেকে হতে পারে Asb@tv!2025

পাসওয়ার্ড ম্যানেজার ব্যবহার

কাজের ক্ষেত্রে নানান ধরণের অনলাইন অ্যাকাউন্ট ব্যবহার করতে হয় আমাদের। প্রত্যেকটির জন্য আলাদা আলাদা শক্তিশালী পাসওয়ার্ড তৈরি করা এবং মনে রাখা প্রায় অসম্ভব। এখানেই কাজে আসে পাসওয়ার্ড ম্যানেজার। এটি একটি ডিজিটাল ভল্ট বা চাবির গোছা, যা আপনার সমস্ত পাসওয়ার্ডকে নিরাপদে সংরক্ষণ করে এবং এনক্রিপ্ট করে রাখে।

বিনামূল্যে এবং ওপেন-সোর্সে জনপ্রিয় এবং বিশ্বস্ত পাসওয়ার্ড ম্যানেজারগুলোর মধ্যে এই তিনটি উল্লেখযোগ্য:

পাসওয়ার্ড ম্যানেজার ব্যবহারের জন্য আপনাকে শুধু একটি মাস্টার পাসওয়ার্ড মনে রাখতে হবে, যা দিয়ে আপনি পাসওয়ার্ড ম্যানেজারের ভল্টটি খুলতে পারবেন। এই ভল্টে আপনার সব পাসওয়ার্ড সুরক্ষিতভাবে এক জায়গায় থাকে।

এছাড়া পাসওয়ার্ড ম্যানেজার আপনাকে আরও যে সুবিধা দেবে:

শক্তিশালী পাসওয়ার্ড তৈরি: এটি আপনার জন্য স্বয়ংক্রিয়ভাবে শক্তিশালী এবং ইউনিক পাসওয়ার্ড তৈরি করে দেবে।

নিরাপদ সংরক্ষণ: আপনার পাসওয়ার্ডগুলো এনক্রিপ্টেড অবস্থায় সংরক্ষিত রাখবে, ফলে কেউ সেগুলো পড়তে পারবে না।

স্বয়ংক্রিয় ব্যবহার: লগইন করার সময় এটি স্বয়ংক্রিয়ভাবে আপনার ইউজারনেম ও পাসওয়ার্ড পূরণ করে দেয়, যা সময় বাঁচায় এবং ফিশিং থেকে সুরক্ষা দেয়।

এ সম্পর্কে আরও বিস্তারিত জানতে পারবেন এই লেখাতে।

টু ফ্যাক্টর অথেন্টিকেশন (2FA)

টু-ফ্যাক্টর অথেন্টিকেশন বা 2FA হলো আপনার অ্যাকাউন্টের জন্য একটি বাড়তি নিরাপত্তা স্তর। এটি চালু থাকলে, পাসওয়ার্ড দেওয়ার পরেও আপনাকে দ্বিতীয় একটি প্রমাণ দাখিল করতে হয় লগইন করার জন্য। তাই যদি কোনোভাবে আপনার পাসওয়ার্ড অন্য কেউ জেনেও যায় টু-ফ্যাক্টর অথেন্টিকেশন বা 2FA চালু থাকলে দ্বিতীয় ধাপে নিজেকে প্রমাণ করার উপায় তার কাছে থাকবে না ফলে সে আর আপনার অ্যাকাউন্টে লগইন করতে পারবে না।

টু-ফ্যাক্টর অথেন্টিকেশন বিভিন্ন ধরনের হতে পারে:

ফোনে পাঠানো কোড

এটি সবচেয়ে প্রচলিত পদ্ধতি। লগইন করার সময় আপনার মোবাইল নম্বরে একটি ওয়ান-টাইম পাসওয়ার্ড (OTP) পাঠানো হয়।

অথেন্টিকেটর অ্যাপের কোড

গুগল অথেন্টিকেটর বা Authy-এর মতো অ্যাপ ব্যবহার করে একটি সময়-ভিত্তিক কোড জেনারেট করা যায়, যা প্রতি ৩০ সেকেন্ডে পরিবর্তিত হয়। এটি এসএমএসের চেয়ে বেশি নিরাপদ।

বায়োমেট্রিক্স

আপনার আঙুলের ছাপ বা ফেস আইডি।

ফিজিক্যাল সিকিউরিটি কি

এটি এমন এক ধরনের সুরক্ষা ব্যবস্থা যেখানে পরিচয় যাচাইয়ের জন্য একটি বাস্তব ডিভাইস ব্যবহার করা হয়। যেমন- YubiKey-এর মতো একটি ইউএসবি ডিভাইস, যা ডিভাইসে প্রবেশ করিয়ে বা স্পর্শের মাধ্যমে ব্যবহারকারীর পরিচয়ের প্রমাণ দেয়।

এ সম্পর্কে আরও জানতে পড়ুন এই লেখাটি।

২.২ ডিভাইস ও ডেটার সুরক্ষা নিশ্চিত করুন

নির্বাচনী কাভারেজের সময় সাংবাদিকেরা হ্যাকিং ও নজরদারির উচ্চ ঝুঁকিতে থাকেন। তাই তাদের ব্যবহৃত ডিভাইসের সুরক্ষার পাশাপাশি ডিভাইসে থাকা ডেটা বা তথ্যের সুরক্ষা নিশ্চিত করা জরুরি। এজন্য সাংবাদিকেরা কিছু টুলের সহায়তা নিতে পারেন।

অ্যান্টিভাইরাস ব্যবহার করুন

বিভিন্ন ধরণের ম্যালওয়্যার (Malware) যেমন, ভাইরাস (Virus),

কি-লগার (keylogger), স্পাইওয়্যার (Spyware) বা র‍্যানসমওয়্যার (Ransomware) থেকে ডিভাইস ও সংবেদনশীল ডেটা রক্ষা করার জন্য একটি নির্ভরযোগ্য অ্যান্টিভাইরাস সফটওয়্যার ব্যবহার করা অত্যন্ত জরুরি। অ্যান্টিভাইরাস সফটওয়্যার হলো আপনার ডিভাইস এবং ইন্টারনেট থেকে আসা ক্ষতিকারক ফাইলগুলোর মধ্যে একটি প্রতিরক্ষা প্রাচীর। এটি কয়েকটি ধাপে আপনার সুরক্ষা নিশ্চিত করে:

সনাক্তকরণ (Detection): ভাইরাস ডেফিনিশন/সিগনেচার স্ক্যানিং: অ্যান্টিভাইরাস সফটওয়্যারটি একটি ডেটাবেস ব্যবহার করে, যেখানে হাজার হাজার পরিচিত ম্যালওয়্যার কোডের "সিগনেচার" সংরক্ষণ করা থাকে। যখন আপনি কোনো ফাইল ডাউনলোড বা খুলতে যান, তখন সফটওয়্যারটি সেই ফাইলের কোডের সাথে ডেটাবেসের কোড মিলিয়ে দেখে। যদি কোড মিলে যায়, তবে এটি সনাক্ত হয়।

হিউরিস্টিক বিশ্লেষণ (Heuristic Analysis): এটি এমন একটি পদ্ধতি, যা কোডের নির্দিষ্ট বৈশিষ্ট্য বা সন্দেহজনক আচরণ বিশ্লেষণ করে। এই পদ্ধতিটি এমন নতুন বা অজানা ম্যালওয়্যার সনাক্ত করতে সাহায্য করে, যার সিগনেচার এখনও ডেটাবেসে যোগ হয়নি।

রিয়েল-টাইম মনিটরিং (Real-time Monitoring): অ্যান্টিভাইরাস সব সময় ডিভাইসে সক্রিয় থাকে। যখন কোনো ফাইল ডাউনলোড হয়, ইমেল অ্যাটাচমেন্ট খোলা হয়, বা কোনো অ্যাপ্লিকেশন ইনস্টল করার চেষ্টা করা হয়, তখন এটি তাৎক্ষণিক স্ক্যান করে। ফলে ক্ষতিকারক কোড সিস্টেমে প্রবেশ করার আগেই ব্লক হয়ে যায়।

প্রতিরোধ ও অপসারণ (Prevention & Removal): যদি কোনো ম্যালওয়্যার সনাক্ত হয়, তবে অ্যান্টিভাইরাস তাৎক্ষণিকভাবে ফাইলটিকে "কোয়ারেন্টাইন" (Quarantine) করে ফেলে বা ডিভাইস থেকে অপসারণ (Remove) করে। র‍্যানসমওয়্যার যা আপনার ফাইল এনক্রিপ্ট করার চেষ্টা করে, সেটিকেও এটি ব্লক করে ডেটা সুরক্ষিত রাখে।

পরিচিত কিছু অ্যান্টিভাইরাসের মধ্যে ক্যাসপারেস্কি, ইসেট, অ্যাভাস্ট, এভিরা অন্যতম।

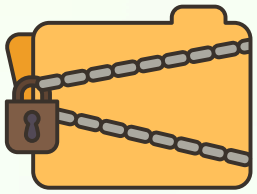
ডিভাইসের সুরক্ষা নিশ্চিতে এগুলোর মধ্যে একটি ব্যবহার করতে পারেন। পাশাপাশি অ্যান্টিভাইরাস সফটওয়্যার এবং এর ভাইরাস ডেফিনিশন ডেটাবেস সবসময় হালনাগাদ করে রাখুন।

আবার ক্ষতিকারক সফটওয়্যার (ম্যালওয়্যার), ভাইরাস, ট্রোজান, ফিশিং এবং অন্যান্য সাইবার হুমকি শনাক্ত করতে ভাইরাসটোটাল (VirusTotal) ব্যবহার করতে পারেন। এটি একটি অনলাইন প্ল্যাটফর্ম, যা বিভিন্ন অ্যান্টিভাইরাস ইঞ্জিন এবং নিরাপত্তা টুল ব্যবহার করে ফাইল, লিংক এবং ওয়েবসাইট স্ক্যান করে সাইবার হুমকি শনাক্তে সহায়তা করে।

VirusTotal

প্ল্যাটফর্মটি বিভিন্ন অ্যান্টিভাইরাস ইঞ্জিন, যেমন: ক্যাসপারস্কি (Kaspersky), অ্যাভাস্ট (Avast), ম্যাকাফিসহ (McAfee) অন্যান্য নিরাপত্তা টুলস ব্যবহার করে ফাইল বা ইউআরএল বিশ্লেষণ করে। সন্দেহজনক ফাইল বা লিঙ্কের জন্য একটি বিস্তারিত স্ক্যান রিপোর্ট তৈরি করে, যাতে ব্যবহারকারীরা বুঝতে পারেন যে এটি নিরাপদ না ক্ষতিকর।

ভাইরাসটোটাল সম্পর্কে বিস্তারিত জানতে পড়ুন এই লেখাটি।



এনক্রিপশন পদ্ধতি ব্যবহার করুন

রিপোর্টের প্রয়োজনে মোবাইলে বা অনলাইনে আপনি প্রতিনিয়ত যেসব মেইল, মেসেজ আদানপ্রদান করছেন, কথা বলছেন, সেগুলো অন্য কেউ দেখে বা শুনে ফেলুক– তা নিশ্চয়ই চাইবেন না। ব্যক্তিগত এসব ডেটা সুরক্ষিত রাখার অন্যতম উপায় এনক্রিপশন পদ্ধতির ব্যবহার। এর মাধ্যমে আপনার একটি বার্তা বা মেইল শুধু তিনিই দেখতে পারবেন, যাকে উদ্দেশ্য করে এটি পাঠানো হয়েছে। মাঝখানে কোনো সংস্থা বা হ্যাকার সেখানে আড়ি পাততে পারবে না।

সহজ ভাষায় এনক্রিপশন হচ্ছে এক ধরনের ডেটা সুরক্ষা পদ্ধতি যেখানে তথ্যগুলো বদলে দেওয়া হয় গাণিতিক কিছু অ্যালগরিদম ব্যবহার করে। যেটিকে বলা হয় সাইফার। এভাবে এনক্রিপশনের মাধ্যমে আপনি যখন একটি টেক্সট বা ছবি পাঠান, তখন সেগুলো এমন কিছু প্রতীক ও সংকেতে পরিণত নয়, যা থেকে বার্তাটির মূল অর্থ বোঝার উপায় থাকে না। এনক্রিপ্ট করা এই টেক্সট যখন নির্দিষ্ট প্রাপকের কাছে পৌঁছায়, তখনই কেবল সেটি আবার ফিরে আসে মূল অবস্থায়। যেখানে টেক্সটটি পড়া যাবে বা ছবিটি দেখা যাবে। ফলে এনক্রিপ্ট করা বার্তাটি যদি প্রাপক থেকে প্রেরকের মাঝখানে অন্য কারো হাতে পড়েও যায়, তাহলেও কেউ সেটির অর্থ উদ্ধার করতে পারবে না।

এনক্রিপশন নির্ভর ইমেইলের জন্য ব্যবহার করতে পারেন প্রোটনমেইল বা টুটানুটার মতো মেইল সার্ভিস। এগুলোতে শুরু থেকেই এনক্রিপশন ব্যবস্থা চালু থাকে। ইয়াহু বা জিমেইল থেকে পাঠানো মেইলগুলোও আপনি এনক্রিপ্ট করে নিতে পারেন। তবে এজন্য ব্যবহার করতে হবে মেইলভেলপের মতো সেবা।

আপনি যদি চান যে, আপনার পাঠানো ব্যক্তিগত বার্তা বা ফোনকল অন্য কেউ দেখে বা শুনে না ফেলে, তাহলে অবশ্যই এমন কোনো সেবা ব্যবহার করা উচিৎ, যেখানে এন্ড-টু-এন্ড এনক্রিপশন পদ্ধতি চালু আছে। এই ব্যবস্থাটি নিশ্চিত করে যে, প্রেরক ও প্রাপক ছাড়া অন্য কেউ বার্তাগুলো পড়তে পারবে না। এজন্য ব্যবহার করতে পারেন সিগন্যাল অ্যাপ। এটি একটি ফ্রি ও নিরাপদ মেসেজিং অ্যাপ, যা আপনার যোগাযোগের গোপনীয়তাকে সর্বোচ্চ গুরুত্ব দেয়। সিগন্যাল সম্পর্কে আরও জানতে এই লেখাটি পড়তে পারেন।

অন্যদিকে দ্রুত টিম সমন্বয়ের জন্য হোয়াটসঅ্যাপ সুবিধাজনক হলেও মেটাডেটা সংরক্ষন করায় অত্যন্ত সংবেদনশীল কাগজ বা প্রমাণ এই প্ল্যাটফর্মের মাধ্যমে শেয়ায় না করাই ভালো। আবার সাধারণ মোবাইল এসএমএস (SMS) এনক্রিপ্টেড নয়, তাই এটি ব্যবহার করুন কেবল জরুরি ক্ষেত্রে।

শুধু ইমেইল, কল বা মেসেজের ক্ষেত্রেই নয়, এনক্রিপশন জরুরি ডেটা সুরক্ষার জন্যও। আপনি যদি স্মার্টফোন বা ল্যাপটপে রিপোর্ট সংক্রান্ত গুরুত্বপূর্ণ তথ্য জমা রাখেন, এবং সেগুলো অন্য কারো হাতে পড়ে তাহলে আপনার বা আপনার প্রতিষ্ঠান ক্ষতিগ্রস্থ হওয়ার আশঙ্কায় থাকে। তেমনটি যেন কোনোভাবেই না হয়– তা নিশ্চিত করতে পারেন ফাইল এনক্রিপশনের মাধ্যমে।

ডিভাইসে ফাইল এনক্রিপশনের জন্য ব্যবহার করতে পারেন বিটলকার, ভেরাক্রিপ্ট, বা ফাইলভল্টের মতো সার্ভিস।

বিটলকার হলো মাইক্রোসফট উইন্ডোজ অপারেটিং সিস্টেমের একটি বিল্ট-ইন এবং শক্তিশালী ডিস্ক এনক্রিপশন ফিচার। এর মূল লক্ষ্য হলো আপনার হার্ড ড্রাইভ, রিমুভেবল ড্রাইভ এবং অন্যান্য স্টোরেজ ডিভাইসগুলোতে থাকা ডেটাকে সর্বোচ্চ নিরাপত্তা প্রদান করা। ডেটা এনক্রিপশন প্রযুক্তি ব্যবহারের মাধ্যমে, বিটলকার নিশ্চিত করে যে আপনার সমস্ত ব্যক্তিগত বা স্পর্শকাতর তথ্য সুরক্ষিত থাকবে। কোনো অননুমোদিত ব্যক্তি যদি আপনার ডিভাইসটি চুরি করে বা হার্ডওয়্যারটিতে বিনা অনুমতিতে প্রবেশের চেষ্টা করে, তবুও তারা এনক্রিপ্ট করা ডেটা ব্যবহার করতে পারবে না।

তবে যদি আপনার অ্যাপলের ম্যাক ডিভাইস থাকে সেক্ষেত্রে ডিভাইসের হার্ডওয়্যারের ওপর ভিত্তি করে ডেটা সুরক্ষার স্তর ভিন্ন হয়। আপনার ম্যাকে যদি অ্যাপল সিলিকন (Apple silicon) চিপ অথবা অ্যাপল টি২ সিকিউরিটি চিপ থাকে, তাহলে আপনার ডিভাইসের ডেটা স্বয়ংক্রিয়ভাবে এনক্রিপ্টেড থাকে। এক্ষেত্রে, ফাইলভল্ট (FileVault) চালু করলে আপনার ডেটা সুরক্ষায় একটি অতিরিক্ত স্তর যুক্ত হয়। এর ফলে কেউ আপনার লগইন পাসওয়ার্ড ছাড়া ডেটা ডিক্রিপ্ট করতে বা অ্যাক্সেস করতে পারবে না। অন্যদিকে, আপনার ম্যাকে যদি অ্যাপল সিলিকন বা টিং চিপ না থাকে, তবে আপনার ডেটা এনক্রিপ্ট করার জন্য ফাইলভল্ট অবশ্যই চালু করতে হবে। ফাইলভল্ট নিশ্চিত করে যে আপনার ডেটা সংরক্ষিত এবং অননুমোদিত প্রবেশ থেকে সুরক্ষিত।

এছাড়া প্রয়োজনে আপনি ভেরাক্রিপ্টও ব্যবহার করতে পারেন। ভেরাক্রিপ্ট একটি ফ্রি ও ওপেন-সোর্স সফটওয়্যার, যা আপনার গুরুত্বপূর্ণ ডেটা সুরক্ষিত রাখতে সহায়তা করে। এটি এনক্রিপ্টেড কন্টেইনার তৈরি করতে দেয়, যেখানে আপনি সংবেদনশীল ফাইলগুলো নিরাপদে সংরক্ষণ করতে পারেন। এছাড়াও, আপনি আপনার পুরো হার্ড ড্রাইভ বা নির্দিষ্ট পার্টিশন এনক্রিপ্ট করতে পারেন। এটি শক্তিশালী এইএস (AES) এনক্রিপশন অ্যালগরিদম ব্যবহার করে।

ভেরাক্রিপ্ট লুকানো ভলিউম তৈরি করতে পারে, যা অতিরিক্ত গোপনীয়তা নিশ্চিত করে। এটি উইন্ডোজ, ম্যাকওএস ও লিনাক্সে কাজ করে এবং ইউএসবি ড্রাইভ থেকেও চালানো যায়। এই টুল ব্যবহার করে আপনি কোনো এক রিপোর্টের যাবতীয় তথ্য, নথি ও অন্যান্য গুরুত্বপূর্ণ ডেটা সুরক্ষিত রাখতে পারেন। সহজ ব্যবহার এবং শক্তিশালী নিরাপত্তা ব্যবস্থার জন্য ভেরাক্রিপ্ট হয়ে উঠেছে জনপ্রিয় ও নির্ভরযোগ্য।

ভেরাক্রিপ্ট কীভাবে ইনস্টল করবেন তা জানতে পারবেন এই লেখাতে।

২.৩ নিরাপদে তথ্য সংগ্রহ, শেয়ার ও সংরক্ষণ করুন

নির্বাচনের মাঠে যেকোনো ছবি, ভিডিও বা অডিও যা আপনি জোগাড় করবেন, তা শুধু প্রমাণই নয়, কখনো কখনো আপনার নিরাপত্তা ঝুঁকির কারণও হয়ে দাঁড়ায়। টেলা (Tella) হচ্ছে এমন একটি মোবাইল অ্যাপ যার মাধ্যমে আপনি নিরাপদভাবে ছবি তোলা, এনক্রিপ্টেডভাবে সংরক্ষণ ও জরুরি সময়ে দ্রুত মুছে ফেলার সুবিধা পাবেন।

প্রথমে, অ্যাপ ইনস্টল করে একটি শক্ত পিন (PIN) বা পাসফ্রেজ সেট করে নিন। এরপর টেলার “হোয়াইটলিস্ট/ভল্ট” বা গোপন স্টোরেজ ব্যবহার করে এই ফাইলগুলো ডিভাইসের সাধারণ গ্যালারিতে দেখা না যায় তা নিশ্চিত করুন।

টেলা কীভাবে ইনস্টল ও ব্যবহার করবেন তা জানতে এই লিঙ্কগুলো (১, ২) অনুসরণ করুন।

তথ্য সংগ্রহের পর সেটির সঠিক সংরক্ষণও জরুরি। নিয়মিতভাবে এনক্রিপ্টেড ব্যাকআপ না থাকলে তা স্থায়ীভাবে হারিয়ে যেতে পারে। এ কারণেই সংগ্রহ করা তথ্যের সংরক্ষণের জন্য এনক্রিপ্টেড ক্লাউড ব্যাকআপ রাখতে পারেন। নেক্সটক্লাউড এমনই একটি টুল যা ব্যবহার করে ফাইলের ব্যাকআপ রাখতে পারেন। এর ব্যবহার অনেকটা গুগল ড্রাইভের মতো হলেও পার্থক্য হচ্ছে এখানে নিজে হোস্ট করলে পুরো কন্ট্রোল থাকে ব্যবহারকারীর উপর; সার্ভার-সাইড কনফিগার করে ক্লায়েন্ট-সাইড এনক্রিপশন সক্রিয় রাখলে তৃতীয় পক্ষ ফাইল পড়তে পারবে না। আবার প্রোটন ড্রাইভও একই রকমের টুল যার এনক্রিপশন সুবিধা থাকায় ব্যবহারকারী ছাড়া কেউ ফাইল পড়তে পারে না।

নির্বাচন সম্পর্কিত কোনো ফাইল আপনার কোনো সহকর্মী বা প্রতিষ্ঠানের সঙ্গে শেয়ারের ক্ষেত্রে ডিসরুট (Disroot) টুলটি ব্যবহার করুন। এটি অস্থায়ী ও গোপনীয় লিঙ্ক তৈরির জন্য উপযুক্ত। শুধু শেয়ার করার সময় ডাউনলোড সীমা ও মেয়াদ নির্ধারণ করুন এবং পাসওয়ার্ড একটি আলাদা চ্যানেলে পাঠান; তাহলে সহজেই আপনার কোনো সহকর্মী সেটি ডাউনলোড করতে পারবে।

২.৪ ইন্টারনেট কার্যক্রম গোপন রাখতে ভিপিএন ব্যবহার করুন

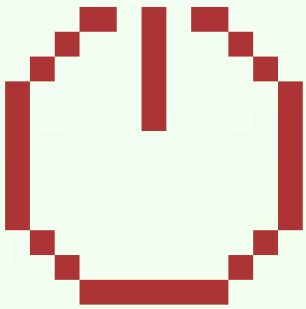
আপনার ইন্টারনেট কার্যক্রম গোপন রাখতে ভার্চুয়াল প্রাইভেট নেটওয়ার্ক বা ভিপিএন (VPN) ব্যবহার করতে পারেন। বিভিন্ন ধরনের গুরুত্বপূর্ণ ব্যক্তিগত তথ্য ও অবস্থানের গোপনীয়তা রক্ষার্থে, সেন্সরশিপ এড়িয়ে ব্লক করা হয়েছে এমন ওয়েবসাইট ব্রাউজ করতে কিংবা যেকোনো ধরনের স্পর্শকাতর কন্টেন্ট ব্রাউজ করতে ভিপিএন ব্যবহার করা হয়।

ভিপিএন ইন্টারনেটের একটি ভার্চুয়াল “টানেল” যার মাধ্যমে ডাটা কম্পিউটার থেকে আদান প্রদান করতে পারে। ভিপিএন আপনার কম্পিউটার এবং এর সার্ভারের মধ্যে একটি গোপন ও নিরাপদ সংযোগ স্থাপন করে। আপনি ভিপিএন সার্ভারে যুক্ত থাকা অবস্থায় যা কিছু করবেন সেগুলো একটি এনক্রিপটেড টানেলের মধ্যে দিয়ে আদান প্রদান করা হবে এবং আপনার নিজের ইন্টারনেটের আইপি অ্যাড্রেস পরিবর্তন হয়ে যে সার্ভারে যুক্ত আছেন সেটি দেখাবে। যা আপনাকে গোপনীয়তা এবং নিরাপত্তা প্রদান করে।

ধরুন আপনি কোনো একটি হোটেলে রয়েছেন অথবা কোনো একটি মেট্রো স্টেশনে, এইসব জায়গাগুলোতে পাওয়া ফ্রি ওয়াইফাই নেটওয়ার্কে আপনি যদি আপনার কম্পিউটার বা মোবাইল ফোন কানেক্ট করে ব্যবহার করেন সেখানে আপনার প্রাইভেসি লঙ্ঘন ও তথ্য চুরি হওয়ার আশঙ্কা থাকতে পারে কারণ আপনি জানেন না সেই নেটওয়ার্ক নিরাপদ কি না। সেক্ষেত্রে আপনি ভিপিএন অ্যাপ্লিকেশন ব্যবহার করে আপনার ইন্টারনেট সংযোগ নিরাপদ করতে পারেন।

তবে ভিপিএন ব্যবহার করতে হলে অবশ্যই একটি ভালো মানের খুঁজে বের করা উচিত। কারণ এগুলো আপনার সব ধরনের অনলাইন কার্যক্রম এমনকি ডিভাইসের সব কার্যক্রমেও নজর রাখতে পারে। বিনামূল্যে ব্যবহার করা যায় এমন ভিপিএনের মধ্যে প্রোটন ভিপিএন (Proton VPN), সাইফন (Psiphon), টানেলবিয়ার (TunnelBear) অন্যতম। এ সম্পর্কে আরও জানতে এই লেখাটি পড়তে পারেন।

২.৫ ইন্টারনেট শাটডাউনের মতো পরিস্থিতির প্রস্তুতি রাখুন



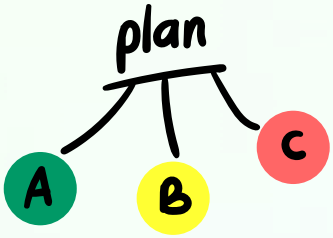
সংঘাতপূর্ণ এলাকা এবং রাজনৈতিক অস্থিরতাকে কেন্দ্র করে তথ্য ছড়ানো বন্ধ করতে বিশ্বজুড়ে ইন্টারনেট শাটডাউন বা আংশিক যোগাযোগ বিচ্ছিন্ন রাখা হয়। আন্দোলন দমাতে কিংবা নির্বাচনের সময়ে, ইন্টারনেট শাটডাউনের একাধিক নজির রয়েছে বাংলাদেশেও। এমন সময়ে অন্যদের তুলনায় একজন সাংবাদিকের জন্য পেশাদারি দায়িত্ব পালন অর্থাৎ তথ্য সংগ্রহ কঠিন হয়ে পড়ে। পাশাপাশি মাঠ থেকে রিপোর্টিংয়ে সংবাদ আদান-প্রদানও মারাত্মক ঝুঁকির মধ্যে পড়ে।

তবে শাটডাউন যে ধরনেরই হোক না কেন– সে সময় কাজ চালিয়ে যাওয়ার জন্য ভালো প্রস্তুতি থাকা জরুরি। নিচের তথ্যগুলো ইন্টারনেট শাটডাউনের সময় সাংবাদিকদের জন্য সহায়ক হতে পারে:

- শাটডাউনের আগে যোগাযোগ বিচ্ছিন্ন হওয়ার ঝুঁকি অনুমান করে নিউজরুম এবং সহকর্মীদের সঙ্গে সম্মিলিত পরিকল্পনা তৈরি করুন। নাগরিক অস্থিরতা বা নির্বাচনের সময় শাটডাউন ঘটতে পারে তা অনুমান করুন। কোন অঞ্চলে শাটডাউনের প্রবণতা বেশি, তা চিহ্নিত করে প্রস্তুতি নিন।

- ইন্টারনেট ছাড়া তথ্য সংগ্রহ ও প্রেরণের পদ্ধতি নিয়ে পরিকল্পনা করুন। ল্যান্ডলাইন বা সাধারণ ফোন কলের ব্যবহার বিবেচনা করা যেতে পারে, তবে মনে রাখবেন সংবেদনশীল কথোপকথনের জন্য ল্যান্ডলাইন নিরাপদ নয়। কোনো এলাকায় ইন্টারনেট শাটডাউন দেখা গেলে সেখানে থাকা সহকর্মীদের কীভাবে সমর্থন দেওয়া হবে—তা নিয়ে সুনির্দিষ্ট কৌশল তৈরি করুন।

- একাধিক বিকল্প টুল ইনস্টল করে রাখুন। একটি পরিষেবা ব্লক হয়ে গেলে বিকল্প হিসেবে ব্যবহারের জন্য একাধিক এন্ড-টু-এন্ড এনক্রিপশন যোগাযোগের অ্যাপ্লিকেশন ডাউনলোড ও সেট আপ করে রাখুন। অ্যাপগুলোর নিরাপত্তা দুর্বলতা সম্পর্কে সচেতন থাকুন।



- শাটডাউনের মাত্রাভেদে যোগাযোগ সচল রাখতে সঠিক টুলের ব্যবহার অপরিহার্য। আংশিক শাটডাউনের ক্ষেত্রে ব্লক করা সাইটগুলোতে অ্যাক্সেস পেতে একাধিক ভিপিএন পরিষেবা ডাউনলোড ও সেট আপ করুন। ইন্টারনেট পরিষেবা প্রদানকারীরা প্রায়শই ভিপিএন ব্লক করে, তাই বিকল্প হিসেবে কয়েকটি বিকল্প রাখা আবশ্যক। তবে সম্পূর্ণ শাটডাউনে ভিপিএন কার্যকর নয়।

- ইন্টারনেট ছাড়াই ডেটা আদান-প্রদান করার জন্য ব্লুটুথ, ওয়াইফাই (Wi-Fi) ডিরেক্ট এবং নিয়ার ফিল্ড কমিউনিকেশন (NFC) ব্যবহার করা শিখুন ও অনুশীলন করুন। এই কৌশলগুলো আপনার ফোনের সেটিংসেই পাওয়া যায়।

- ইন্টারনেট সংযোগ ছাড়াই মেসেজিংয়ের জন্য ব্রায়ার (Briar), বিটচ্যাট (Bitchat) বা ব্রিজফাইয়ের (Bridgefy) মতো পিয়ার-টু-পিয়ার (P2P) মেসেজিং টুলগুলো ডাউনলোড ও সেট আপ করে রাখুন। এধরনের অ্যাপগুলি ব্লুটুথ এবং ফোনের ওয়াইফাই রেডিও ব্যবহার করে এনক্রিপ্টেড মেসেজিং সুবিধা দেয়। এগুলো দিয়ে সাধারণত ১০০ মিটারের মধ্যে টেক্সট মেসেজ পাঠাতে পারে। আপনি যাকে মেসেজ করতে চাচ্ছেন, সে যদি এই সীমার বাইরে থাকে, তাহলে আপনার মেসেজটি আশেপাশের অন্যান্য ব্রিজফাই ব্যবহারকারীদের ডিভাইসের মাধ্যমে রিলে রেসের মতো করে এক ডিভাইস থেকে অন্য ডিভাইসে লাফিয়ে তার কাছে পৌঁছায়। এই পদ্ধতিতে তৈরি হয় একটি নির্ভরযোগ্য "মেশ নেটওয়ার্ক" যা ইন্টারনেট বা মোবাইল নেটওয়ার্ক ছাড়াই কাজ করে। এগুলোর মধ্যে ব্রিজফাই এবং বিট চ্যাট অ্যান্ড্রয়েড (Android) এবং আইওএস (IOS) উভয় ডিভাইসেই ব্যবহার করা যায়, ফলে আপনি দূরবর্তী অঞ্চলে বা নেটওয়ার্ক বিঘ্নিত অবস্থায়ও সংযুক্ত থাকতে পারেন।

ব্রিজফাই অ্যাপ কিভাবে ইনস্টল ও ব্যবহার করবেন তা জানতে পারবেন এই লেখাতে।

অপতথ্য ও অনলাইন হয়রানি প্রতিরোধে করণীয়

তথ্য সংগ্রহ এবং নিরপেক্ষভাবে সঠিক প্রতিবেদন প্রকাশ করা একজন সাংবাদিকের প্রধান দায়িত্ব হলেও, বর্তমানে অপতথ্য এবং রাজনৈতিক প্রোপাগান্ডার ব্যাপক বিস্তার এই কাজকে কঠিন করে তুলেছে। বিশেষত নির্বাচনকালীন সময়ে ছড়ানো ভুল তথ্য সাংবাদিকদের কাজের পরিবেশকে মারাত্মকভাবে প্রভাবিত করে এবং জনমনে চরম বিভ্রান্তি সৃষ্টি করে।

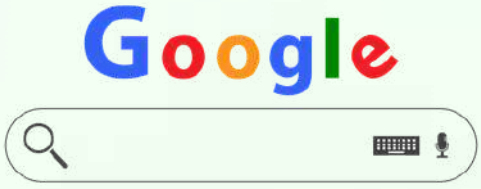
অনলাইন থেকে পাওয়া বা দেখা কোনো তথ্য, ছবি বা ভিডিও যাচাই না করে কখনই প্রতিবেদনে ব্যবহার করা উচিত নয়। কারণ ভুল বা বিভ্রান্তিকর তথ্য রিপোর্টে গেলে তার প্রভাব কেবল নির্দিষ্ট প্রতিবেদনের ওপরই নয়, বরং পুরো নির্বাচনী প্রক্রিয়া, জনমত ও আইনশৃঙ্খলা পরিস্থিতির ওপরও পড়তে পারে। তাই যেকোনো সংবাদ প্রতিবেদন প্রকাশের আগে, তথ্যের উৎস, প্রকাশের তারিখ ও সময়, এবং ঘটনার প্রেক্ষিত অন্যান্য নির্ভরযোগ্য উৎসের সঙ্গে মিল আছে কি না, তা পুঙ্খানুপুঙ্খভাবে যাচাই করা আবশ্যক। বর্তমানে শুধু ঘটনাস্থলে উপস্থিত থাকা নয়, বরং তথ্যের সত্যতা যাচাই বা ফ্যাক্টচেকিং করাও সাংবাদিকতার একটি অপরিহার্য অংশ।

নির্বাচনী সময়ে টার্গেটেড অনলাইন প্রচারণা এবং অনলাইন হয়রানি বেড়ে যাওয়ারও আশঙ্কা থাকে। সংবাদমাধ্যমের কর্মীরা প্রায়শই আক্রমণকারীদের মূল লক্ষ্যে পরিণত হন, অথবা সমন্বিত হয়রানি ও ভুল তথ্য প্রচারের শিকার হন। ফলস্বরূপ সাংবাদিকদের নিজেদের বা সংশ্লিষ্ট প্রতিষ্ঠানের নামেও মিথ্যা তথ্য ছড়াতে দেখা যায়। এই ধরনের আক্রমণ সাংবাদিককে সোশ্যাল মিডিয়া ব্যবহার থেকে বিরত থাকতে এবং একপ্রকার অফলাইনে থাকতে বাধ্য করে, যা তাদের কাজের স্বাধীনতায় প্রভাব ফেলতে পারে।

অনলাইন আক্রমণ থেকে নিজেদের সুরক্ষিত রাখা কঠিন হলেও, কিছু সুনির্দিষ্ট পদক্ষেপ গ্রহণের মাধ্যমে সাংবাদিকেরা নিজেদের অ্যাকাউন্ট, সংবেদনশীল তথ্য এবং ব্যক্তিগত নিরাপত্তা আরও ভালোভাবে নিশ্চিত করতে পারেন। এই পদক্ষেপগুলো ঝুঁকি হ্রাস করতে এবং পেশাদার কার্যক্রম অব্যাহত রাখতে সহায়তা করবে।

৩.১ তথ্য যাচাই বা ফ্যাক্টচেকিংয়ের কৌশল

তথ্য যাচাইয়ের জন্য বিভিন্ন ধরনের পদ্ধতি ও কৌশল ব্যবহার করা যেতে পারে। অনলাইনে প্রকাশিত কোনো প্রতিবেদন, গবেষণা বা জরিপ দ্রুত ও নির্ভুলভাবে খুঁজে পেতে গুগলের অ্যাডভান্স সার্চ অত্যন্ত কার্যকর একটি টুল; সুনির্দিষ্ট কিওয়ার্ড, তারিখ, ডোমেইন বা ফাইলটাইপ নির্ধারণ করে অনুসন্ধানকে আরও নিখুঁত করা যায়।



ছবি যাচাইয়ের ক্ষেত্রে রিভার্স ইমেজ সার্চ ব্যবহার করলে ছবির মূল উৎস, আগের ব্যবহার, কিংবা এটি সম্পাদিত বা ভুয়া কি না, এসব বিষয় সহজেই তুলনা করে দেখা সম্ভব হয়।

একইভাবে ভিডিওর সত্যতা যাচাই করতে ইনভিডের (InVID) মতো বিশ্লেষণী টুল খুবই সহায়ক; এতে ভিডিওর ফ্রেম ভেঙে এর উৎস ও সত্যতা যাচাই করা যায়।

গুগলের অ্যাডভান্স সার্চ যেভাবে ব্যবহার করবেন:

সাংবাদিকতা ও তথ্য অনুসন্ধানের ক্ষেত্রে শুধু সাধারণ কিওয়ার্ড ব্যবহার যথেষ্ট নয়। গুগল সার্চে বুলিয়ান সার্চ টেকনিক (AND, OR, NOT) প্রয়োগ করলে আপনার অনুসন্ধানের ফলাফল আরও সূক্ষ্ম ও প্রাসঙ্গিক হয়ে ওঠে। এই উন্নত কৌশল ব্যবহার করে আপনি তথ্যের বিশাল সমুদ্র থেকে নিজের প্রয়োজনীয় তথ্য সহজে ফিল্টার করে বের করতে পারবেন। তিনটি প্রধান বুলিয়ান অপারেটর ব্যবহার করে আপনার অনুসন্ধানকে আরও নিখুঁত করে তুলুন:

AND অপারেটর: যদি একাধিক শব্দ আছে এমন কোনো বিষয় খোঁজ করতে চান, তাহলে সেই শব্দগুলো উদ্ধৃতি চিহ্নের মধ্যে রেখে AND দিয়ে সার্চ করুন। এটি নিশ্চিত করে যে আপনার অনুসন্ধানের ফলাফলগুলোতে উল্লেখ করা শব্দগুলো উপস্থিত থাকবে।

যেমন

OR অপারেটর: ফলাফলে যেকোনো একটি শব্দ থাকলেই হবে এমন চাইলে OR অপারেটর দিয়ে সার্চ করুন। এটি আপনার অনুসন্ধানের পরিধি বাড়ায়, যাতে আপনি একাধিক সমার্থক শব্দ বা সম্পর্কিত ধারণা দিয়ে অনুসন্ধান করতে পারেন। যেমন:

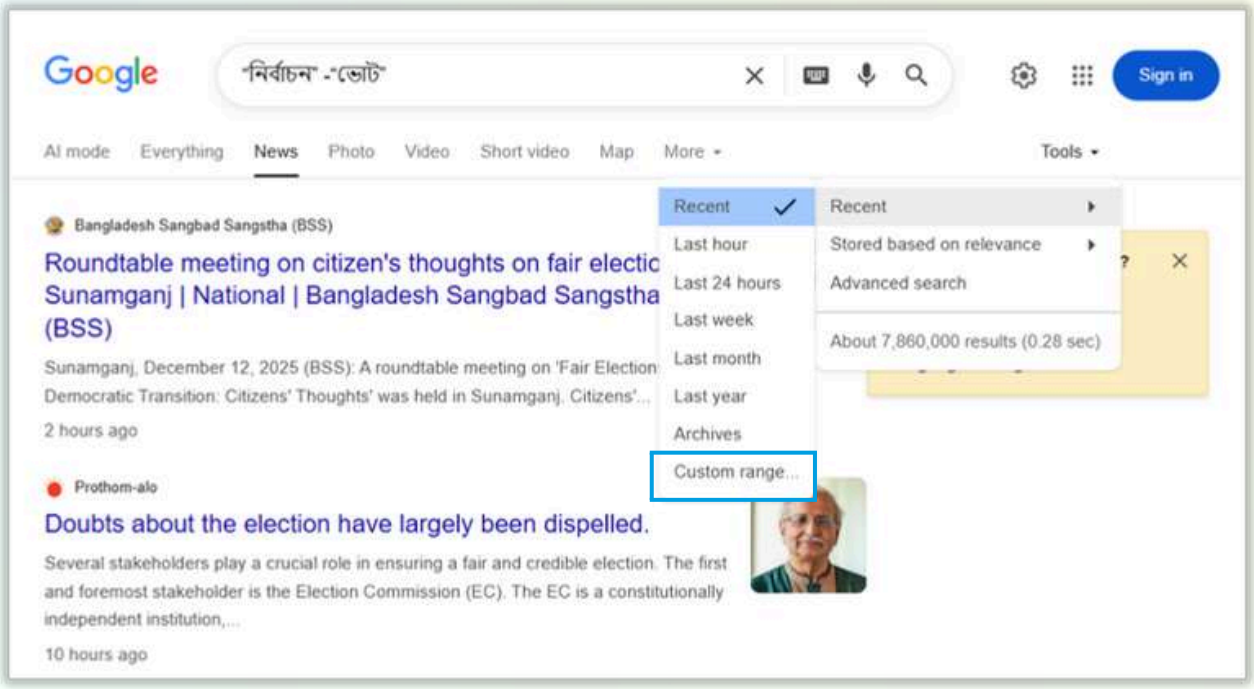
যেমন 

NOT অপারেটর: অপ্রাসঙ্গিক ফলাফল বাদ দিতে সাহায্য করে NOT অপারেটর। যখন একটি শব্দকে সার্চ করলে সেটি ফলাফলে ভুলভাবে সমার্থক শব্দগুলোও নিয়ে আসে তা বাদ দিতে এই অপারেটর ব্যবহার করা হয়। নির্দিষ্ট শব্দ বাদ দিতে এর আগে শুধু হাইফেন (-) যোগ করতে হয়।

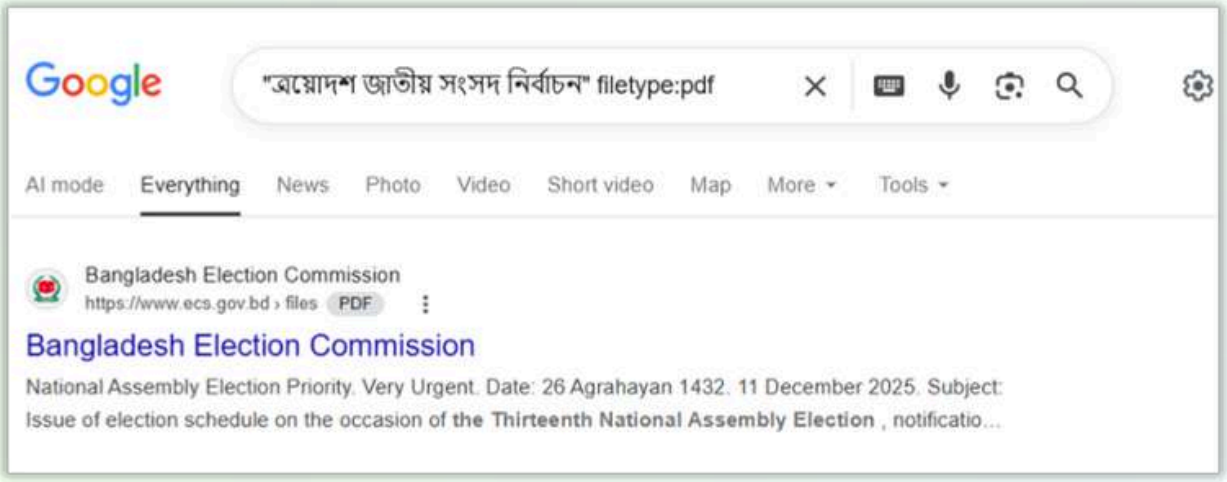
যেমন 

তথ্যকে আরও কার্যকরভাবে ব্যবহার করতে আপনি অনুসন্ধানের সুযোগকে নির্দিষ্ট সময় বা ফরম্যাটের ভিত্তিতে সীমাবদ্ধ করতে পারেন:

- নির্দিষ্ট সময় ধরে সার্চ করা: অনেক সময় আমরা শুধু সাম্প্রতিক তথ্য বা একটি নির্দিষ্ট সময়সীমার মধ্যে প্রকাশিত তথ্য খুঁজতে চাই। এটি গবেষণামূলক কাজ বা ডেটা সংগ্রহের জন্য অত্যন্ত কার্যকর। গুগল সার্চ ফলাফলের পৃষ্ঠায় থাকা “Tools” (টুলস) অপশনটি ব্যবহার করে সহজেই “Any time” (যেকোনো সময়) ড্রপডাউন মেনু থেকে সময়সীমা নির্বাচন করে নিতে পারেন।



- নির্দিষ্ট ফাইল ফরম্যাট (File Format): গবেষণামূলক প্রবন্ধ, প্রেজেন্টেশন স্লাইড বা অফিশিয়াল রিপোর্ট খুঁজতে চাইলে “filetype:” অপারেটরটি ব্যবহার করুন। এই কৌশলটি সরকারি নথি বা একাডেমিক ডেটা সংগ্রহের জন্যও বেশ কার্যকর।



রিভার্স ইমেজ সার্চ যেভাবে ব্যবহার করবেন:

অনলাইনে ছড়ানো ভুয়া খবরের বেশ বড় অংশ আসে পুরোনো ছবি নতুন প্রেক্ষাপটে ব্যবহার করার মাধ্যমে। আগের কয়েকটি জাতীয় নির্বাচনের সময়েও এমনটি দেখা গেছে। তাই নির্বাচনকেন্দ্রিক কোনো ছবি অনলাইনে ছড়াতে দেখলে তা রিভার্স ইমেজ সার্চের মাধ্যমে যাচাই করে নিন।

সন্দেহজনক ছবি যাচাইয়ের জন্য শুরুতে অনলাইনে দেখা ছবিটি আপনার ডিভাইসে (কম্পিউটার/মোবাইল) সংরক্ষণ করুন। ডেস্কটপে images.google.com ব্যবহার করুন অথবা মোবাইলে Google Lens বা Yandex Images ওপেন করুন। এরপর ক্যামেরা আইকনে ক্লিক করে ছবিটি আপলোড করুন অথবা ছবির URL পেস্ট করুন। যদি সেটি অনলাইনে আগেই আপলোড হয়ে থাকে তাহলে তার তথ্য আপনি সেখান থেকে যাচাই করে নিতে পারেন। ছবির প্রথম অনলাইন প্রকাশের তারিখ ও সময় যাচাই করুন।

ছবি যাচাইয়ের জন্য TinEye, Yandex, বা Baidu এর মতো বিকল্প টুলগুলো ব্যবহার করাও কার্যকর, যা গুগলের ফলাফলের বাইরেও ভিন্ন ডেটাবেস থেকে ছবি খুঁজে দিতে পারে।

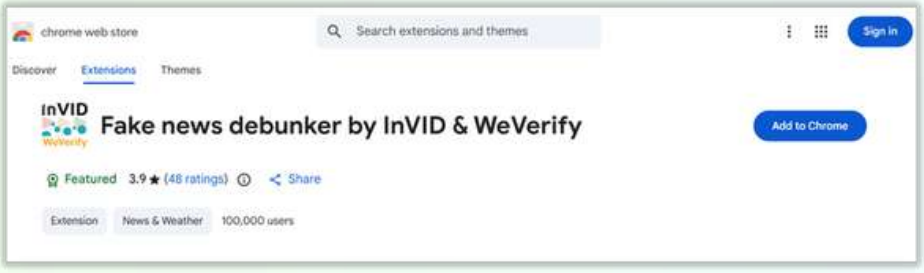
ভিডিও যাচাইয়ে ইনভিড যেভাবে ব্যবহার করবেন:

ভিডিও হচ্ছে ভুয়া কনটেন্ট ছড়ানোর সবচেয়ে সহজ মাধ্যম। ভিন্ন প্রেক্ষাপটের কিংবা পুরোনো ভিডিও, সম্পাদিত ভিডিও অথবা এআইয়ের মাধ্যমে তৈরী ভিডিও এখন নির্বাচনের সময় ভুল তথ্য ছড়ানোর একটি অন্যতম মাধ্যম হয়ে উঠেছে। এমনকি নির্বাচনে অংশ নেওয়া প্রার্থীদের নিয়েও ভুল তথ্য ছড়াতে দেখা যায় ভিডিওর ব্যবহার।

তাই সন্দেহজনক কোনো ভিডিও দেখলে তার লিঙ্ক কপি করে ইনভিড (InVID) টুলে গিয়ে কিফ্রেম ধরে সার্চ করে ভিডিওর সত্যতা সম্পর্ক নিশ্চিত হয়ে নিন।

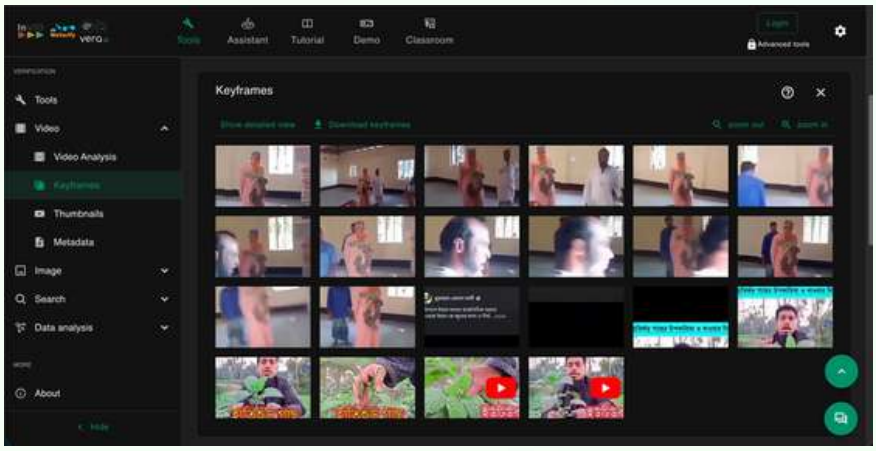
ধাপ ১: টুল ইনস্টলেশন এবং প্রস্তুতি

এক্সটেনশন ডাউনলোড: গুগল ক্রোম (Google Chrome), মজিলা ফায়ারফক্স (Mozilla Firefox) বা অন্য ব্রাউজার থেকে “InVid/WeVerify” এক্সটেনশনটি ডাউনলোড ও ইনস্টল করুন। যে ভিডিওটি যাচাই করতে চান, সেটির URL (লিঙ্ক) কপি করে নিন। এটি ইউটিউব, ফেসবুক বা অন্য কোনো প্ল্যাটফর্মের ভিডিও হতে পারে।



ধাপ ২: ভিডিও ফ্র্যাগমেন্টেশন (Keyframe Analysis)

ভিডিওর মূল প্রেক্ষাপট যাচাইয়ের জন্য এটি একটি গুরুত্বপূর্ণ ধাপ। ইনভিড ভিডিওকে ছবি আকারে বিভক্ত করে। ব্রাউজারে ইনভিড এক্সটেনশনটি চালু করুন এবং “Analysis” বা “Video Analysis” ট্যাবে যান। কপি করা ভিডিওর URL নির্দিষ্ট বক্সে পেস্ট করুন। এরপর “Keyframes” অপশনে ক্লিক করুন। ইনভিড স্বয়ংক্রিয়ভাবে ভিডিওটিকে বেশ কিছু স্থির চিত্র বা মূল ফ্রেমে (Keyframes) বিভক্ত করে দেবে, যা ভিডিওটির বিভিন্ন গুরুত্বপূর্ণ মুহূর্ত তুলে ধরে। ভিডিওটি আসল কি না বা পুরোনো কোনো ঘটনার দৃশ্য ব্যবহার করা হচ্ছে কি না, তা নিশ্চিত করতে মূল ফ্রেমগুলো দিয়ে রিভার্স ইমেজ সার্চ করুন।



রিভার্স ইমেজ সার্চের জন্য প্রদর্শিত মূল ফ্রেমগুলোর মধ্যে সবচেয়ে পরিষ্কার, অস্পষ্টতাহীন, বা সন্দেহজনক ফ্রেমগুলো নির্বাচন করুন। কারণ ফ্রেমগুলোতে কোনো ল্যান্ডমার্ক বা নির্দিষ্ট ব্যক্তি থাকলে যাচাই সহজ হয়। নির্বাচিত ফ্রেমটিতে ক্লিক করুন এবং টুলটির মাধ্যমে Google, Yandex, বা TinEye -এর মতো সার্চ ইঞ্জিন ব্যবহার করে রিভার্স ইমেজ সার্চ অপশনটি চালু করুন। সার্চ ফলাফলে আসা একই স্থির চিত্রের অন্য দৃশ্যগুলো বিশ্লেষণ করুন।

৩.২ অনলাইন হয়রানি প্রতিরোধে করণীয়

নির্বাচনকালীন সাংবাদিকেরা প্রায়শই টার্গেটেড অনলাইন হয়রানির শিকার হন। এই আক্রমণ থেকে নিজেদের, অ্যাকাউন্ট এবং ব্যক্তিগত তথ্য সুরক্ষিত রাখতে নিচের পদক্ষেপগুলো অনুসরণ করা আবশ্যক:

ঝুঁকি কমাতে অ্যাকাউন্ট সুরক্ষিত করুন

আক্রমণ শুরু হওয়ার আগেই ব্যক্তিগত তথ্য সুরক্ষিত করার জন্য নিম্নোক্ত কাজগুলো করুন:

- যখন আপনি কোনো নির্দিষ্ট এলাকা বা ভোটকেন্দ্রে দায়িত্ব পালন করতে যান, তখন সেখানকার অবস্থান শেয়ার করা বা ঘটনার সময়কার ছবি/লাইভ আপলোড করা অপরাধীদের জন্য সুযোগ তৈরি করতে পারে। লোকেশন শেয়ার করলে আপনার বা সহকর্মীদের অবস্থান সহজেই ট্র্যাক করা যায়, যা হয়রানি, তোঁড়জোড়, বা এমনকি শারীরিক ঝুঁকি বাড়িয়ে দেয়।

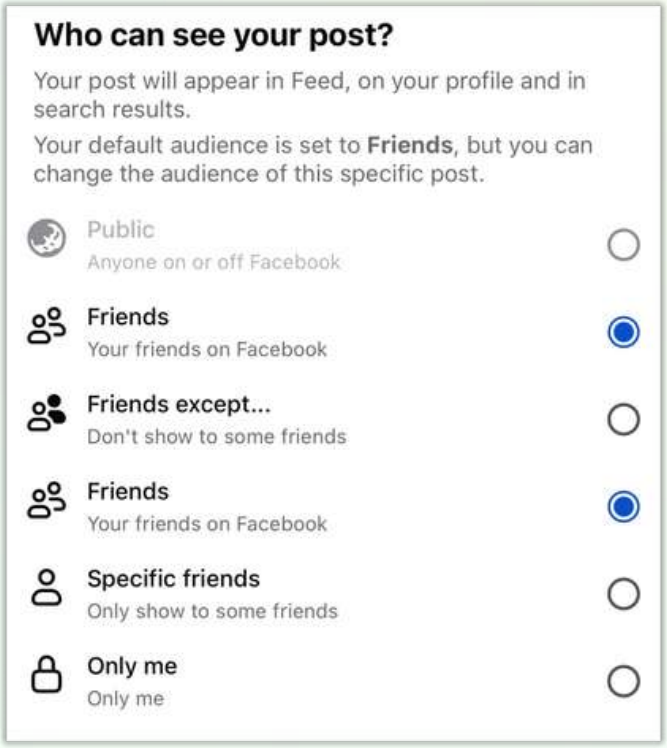
তাই মাঠে থাকা অবস্থায় ব্যক্তিগত সামাজিক মাধ্যমের অ্যাকাউন্টে ছবি, লাইভ ভিডিও বা অবস্থান শেয়ার করা থেকে বিরত থাকুন। যদি প্রমাণ বা খবর দ্রুত আদান-প্রেরণ করতে হয়, তাহলে সেটি এনক্রিপ্টেড চ্যানেলে সীমাবদ্ধ রাখুন বা শুধুমাত্র পরিচিতজনদের সঙ্গে শেয়ার করুন।

- পেশাগত ও ব্যক্তিগত অ্যাকাউন্ট আলাদা করুন। কাজের জন্য এবং ব্যক্তিগত ব্যবহারের জন্য আলাদা সামাজিক যোগাযোগ মাধ্যমের অ্যাকাউন্ট ব্যবহার করা সবচেয়ে নিরাপদ। যদি পেশাগত কাজে ফেসবুক ব্যবহার করেন, তবে নিশ্চিত করুন যেন ব্যক্তিগত ছবি এবং অন্যান্য তথ্য সীমাবদ্ধ করা থাকে।

- প্রতিটি অ্যাকাউন্টের জন্য আপনার গোপনীয়তা সেটিংস (Privacy Settings) নিয়মিত পর্যালোচনা করুন। নিশ্চিত করুন যে আপনার ছবি ও তথ্য কে কে দেখতে পারবে। আপনার জন্ম তারিখ এবং ব্যক্তিগত যোগাযোগের বিবরণের মতো স্পর্শকাতর তথ্য সরিয়ে ফেলুন বা গোপন রাখুন।

- আপনার অ্যাকাউন্ট পর্যবেক্ষণ করুন এবং এমন কোনো ছবি থাকলে তা মুছে ফেলুন যা আপনাকে অপমানিত করার উপায় হিসেবে ব্যবহার করা যেতে পারে। এটি অনলাইন হয়রানিকারীদের একটি সাধারণ কৌশল।

- আপনার ফেসবুক প্রোফাইলটি “লক” করে রাখুন। এতে অচেনা বা অপরিচিত কেউ আপনার প্রোফাইল পিকচার বা ছবিগুলো দেখতে পারবে না। আপনার পোস্টের অডিয়েন্স সবসময় “Friends” করে রাখুন যাতে যে কেউ আপনার পোস্ট দেখতে না পারে। পাশাপাশি অপরিচিতদের ফ্রেন্ড রিকোয়েস্ট বা ফলো রিকোয়েস্ট গ্রহণ করা থেকে বিরত থাকুন।



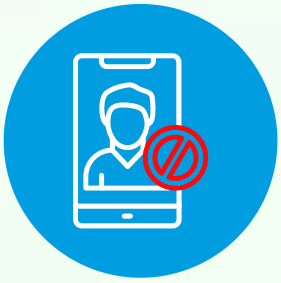
অনলাইন হয়রানির শিকার হলে যা করবেন

যদি অনলাইন হয়রানি বা সাইবার বুলিংয়ের শিকার হন, তবে শান্ত থাকুন এবং নিচের পদক্ষেপগুলো অনুসরণ করুন:

- প্রতিক্রিয়া জানাবেন না। যারা বুলিং করে, তাদের মূল উদ্দেশ্যই হলো আপনার প্রতিক্রিয়া বা মনোযোগ আকর্ষণ করা। তাদের বার্তা, কমেন্ট বা পোস্টের জবাব দেওয়া থেকে সম্পূর্ণরূপে বিরত থাকুন। প্রতিক্রিয়া দিলে তা কেবল আক্রমণকেই বাড়িয়ে দেবে।

- হয়রানিমূলক বার্তা, কমেন্ট বা পোস্টগুলোর স্ক্রিনশট বা রেকর্ড রাখুন। আইনি পদক্ষেপ বা প্ল্যাটফর্মে রিপোর্টের জন্য এই নথিগুলো গুরুত্বপূর্ণ প্রমাণ হিসেবে কাজ করবে।

- হয়রানিমূলক অ্যাকাউন্টগুলোকে দ্রুত ব্লক করুন এবং প্ল্যাটফর্মের (ফেসবুক, এক্স ইত্যাদি) নীতিমালা অনুযায়ী রিপোর্ট করুন। সোশ্যাল মিডিয়ার অপশনগুলো ব্যবহার করে দ্রুত পদক্ষেপ নিন।



- যদি হয়রানি গুরুতর হয় বা আপনার ব্যক্তিগত নিরাপত্তা হুমকির সম্মুখীন হয়, তবে একা লড়াই না করে সহায়তা নিন। অনলাইন হয়রানি সম্পর্কে আপনার সংবাদ প্রতিষ্ঠানের সঙ্গে কথা বলুন। হয়রানি গুরুতর হলে কী পদক্ষেপ গৃহীত হবে তা নিয়ে পরিকল্পনা তৈরি করুন এবং সহায়তা চান।

- পরিবার, বন্ধু, বা ঊর্ধ্বতন সহকর্মীর সঙ্গে ঘটনা শেয়ার করুন। বিশ্বস্ত কারো সঙ্গে আলোচনা করলে মানসিক চাপ কমতে পারে। যদি হয়রানির ঘটনা মারাত্মক হয়, তবে বাংলাদেশে সাইবার ক্রাইম ইনভেস্টিগেশন ডিভিশনে (সিসিআইডি) অভিযোগ করুন।

- সাইবার বুলিংয়ে আক্রান্ত ব্যক্তিরা প্রায়ই বিষণ্নতা, উদ্বেগ বা মানসিক চাপে ভোগেন। প্রয়োজনে কাউন্সেলিং বা মানসিক স্বাস্থ্য হেল্পলাইনে কল করে পেশাদার সহায়তা নিন।

তথ্যসূত্র

https://digitallyright.org/journalist-safety-preparedness-ahead-of-2026-elections/

https://cpj.org/2023/10/bangladesh-national-election-2024-journalist-safety-guide/

https://digitalsafetyschool.com/

যোগাযোগ ও রিসোর্স

ডিজিটাল জগতে কোনো অনলাইন হয়রানি বা আক্রমণের শিকার হলে যোগাযোগ করতে পারেন ডিজিটাল সেফটি স্কুলের হোয়াটসঅ্যাপ হেল্পলাইন নম্বরে অথবা সিগন্যাল অ্যাপে।

+৮৮০ ১৭১১-৩৯৫১৯৬

digitalsafetyschool.01

অথবা নিচের কিউআর কোড দুটি স্ক্যান করুন

অথবা হোয়াটসঅ্যাপে যুক্ত হতে এই লিংকে ক্লিক করুন

https://wa.me/qr/CFMG77IVFS3XF1

ডিজিটাল নিরাপত্তার খুঁটিনাটি ও অন্যান্য গুরুত্বপূর্ণ টিপস পেতে ভিজিট করুন:

digitalsafetyschool.com

ভুল, বিভ্রান্তিকর কিংবা অপতথ্যের ফাঁদ এড়াতে সহায়তা নিন:

dismislab.com

সামাজিক মাধ্যমে ডিসমিসল্যাবের সঙ্গে যুক্ত থাকুন

ফেসবুক ইনস্টাগ্রাম এক্স লিংকডইন

DIGITAL SAFETY SCHOOL

dismislab

জরুরি কিছু হটলাইন

জাতীয় জরুরি সেবা	৯৯৯
সরকারি যেকোনো তথ্য ও সেবা সম্পর্কে জানতে	৩৩৩
নারী ও শিশু নির্যাতন প্রতিরোধে	১০৯
চাইল্ড হেল্পলাইন	১০৯৮
সরকারি আইনগত সহায়তায় জাতীয় হেল্প লাইন	১৬৪৩০
স্বাস্থ্য বাতায়ন	১৬২৬৩

প্রকাশনায়

ডিজিটালি রাইট লিমিটেড

ঢাকা, বাংলাদেশ

www.digitallyright.org

সামাজিক মাধ্যমে ডিজিটালি
রাইটের সঙ্গে যুক্ত থাকুন

ফেসবুক

এক্স

লিংকডইন

digitally right