সাইবার নিরাপত্তা সচেতনতা মাস

অক্টোবর ২০২৪

সেনাসদর, জিএস শাখা, (আইটি পরিদপ্তর)

সাইবার হামলা এবং এর প্রতিরোধ

আসুন সচেতন হই

তথ্য প্রযুক্তির নিরাপত্তা নিশ্চিত করি
সাইবার সুরক্ষিত সেনাবাহিনী গড়ি

সাইবার নিরাপত্তা সচেতনতা

সাইবার নিরাপত্তা সচেতনতা মাস

প্রতিবছর অক্টোবর মাস আন্তর্জাতিকভাবে সাইবার নিরাপত্তা সচেতনতা মাস হিসেবে পালিত হয়ে থাকে। সাইবার নিরাপত্তা সচেতনতা মাস মূলত ডিজিটাল প্রযুক্তির ব্যবহারকারীরা কিভাবে নিজেদের ব্যবহার করা সফটওয়্যার, হার্ডওয়্যার এবং সর্বোপরি নিজেদের তথ্য নিরাপদ রাখতে পারেন সেই বিষয়ে আলোকপাত করে।

২০০৪ সালে মার্কিন যুক্তরাষ্ট্রের হোমল্যান্ড সিকিউরিটি বিভাগ এবং ন্যাশনাল সাইবার সিকিউরিটি অ্যালায়েন্স সাইবার নিরাপত্তার গুরুত্ব এবং কীভাবে ডিজিটাল প্রযুক্তির ব্যবহারকারীরা নিজেদের তথ্য নিরাপদ রাখতে পারে সেই বিষয়ে জনসচেতনতা বাড়ানোর লক্ষ্যে মাসব্যাপী একটি উদ্যোগ নেয়। এরই ধারাবাহিকতায় প্রতি বছর অক্টোবর মাসে বিশ্বের বিভিন্ন দেশে পালিত হচ্ছে সাইবার নিরাপত্তা সচেতনতা মাস।

বাংলাদেশে ২০১৬ সাল থেকে সাইবার নিরাপত্তা সচেতনতা মাস আনুষ্ঠানিকভাবে পালন শুরু হয়। আশা করা হচ্ছে খুব অল্প সময়ের মধ্যে এই কার্যক্রম আমাদের সকল বাংলাভাষীদের মধ্যে ব্যাপকভাবে বিস্তৃতি লাভ করবে এবং পৌঁছে যাবে দেশের সব প্রতিষ্ঠান, তরুণ সমাজসহ প্রতিটি মানুষের কাছে।

মূল প্রতিপাদ্য বিষয়

আমরা প্রতিনিয়ত ইন্টারনেটের মাধ্যমে সংযুক্ত হচ্ছি এবং আমাদের অনেক সংবেদনশীল তথ্য অনলাইনে আছে। ফলে ইন্টারনেট থেকে উপকৃত হওয়ার সাথে সাথে সাইবার হামলার ঝুঁকিও বাড়ছে। তাই এ বছর বাংলাদেশ সেনাবাহিনীর আইটি পরিদপ্তর কর্তৃক নির্ধারিত সাইবার নিরাপত্তা সচেতনতা মাস ২০২৪ এর মূল প্রতিপাদ্য বিষয় "তথ্য প্রযুক্তির নিরাপত্তা নিশ্চিত করি- সাইবার সুরক্ষিত সেনাবাহিনী গড়ি"।

তথ্য প্রযুক্তির নিরাপত্তা নিশ্চিত করি
সাইবার সুরক্ষিত সেনাবাহিনী গড়ি

সাইবার হামলা

সাইবার হামলা হল কম্পিউটার, কম্পিউটার সিস্টেম বা নেটওয়ার্কে অননুমোদিতভাবে প্রবেশ করে ক্ষতি করার প্রচেষ্টা। এর মূল উদ্দেশ্য হল কম্পিউটার বা সিস্টেমকে অকার্যকর করা, নিয়ন্ত্রণে আনা অথবা সিস্টেমে রাখা ডাটা পরিবর্তন, মুছে ফেলা বা চুরি করা। যে কোনো ব্যক্তি বা গ্রুপ বিভিন্ন কৌশল ব্যবহার করে সাইবার হামলা চালাতে পারে। সাইবার হামলার ফলে অনেক সরকারি ও বেসরকারি প্রতিষ্ঠানের গুরুত্বপূর্ণ তথ্য হ্যাকারদের হাতে চলে যায় এবং তারা এই তথ্যের বিনিময়ে মুক্তিপণ দাবি করে। এছাড়াও, হ্যাকাররা প্রতারণার মাধ্যমে ব্যক্তিগত স্পর্শকাতর তথ্য যেমন সোশ্যাল মিডিয়া একাউন্টের ইউজারনেম ও পাসওয়ার্ড, ক্রেডিট কার্ডের পিন ইত্যাদি চুরি করে।

সাইবার নিরাপত্তা

সাইবার নিরাপত্তা বলতে বোঝায় আমাদের ব্যক্তিগত তথ্য, কম্পিউটার এবং অন্যান্য ডিজিটাল ডিভাইসকে হ্যাকিং ও বিভিন্ন সাইবার আক্রমণ থেকে রক্ষা করা। সাইবার নিরাপত্তার নিশ্চিতের মাধ্যমে তথ্য চুরি, ম্যালওয়্যার এবং অন্যান্য সাইবার বিপদের বিরুদ্ধে সুরক্ষিত থাকা সম্ভব। অসাবধানতাবশতঃ একটি ক্লিকেই শক্তিশালী ম্যালওয়্যার আমাদের ডিভাইসে প্রবেশ করতে পারে। তাই সাইবার নিরাপত্তার হুমকিগুলো সম্পর্কে স্পষ্ট ধারণা থাকলে, এই জগতে নিরাপদ থাকা সহজ হবে।

প্রেক্ষাপট বাংলাদেশ

গত কয়েক দশকে বাংলাদেশে তথ্যপ্রযুক্তির ব্যবহার বেড়েছে ব্যাপক পরিসরে। দেশের জনগোষ্ঠীর বিশাল একটি অংশ এখন মোবাইল ও ইন্টারনেট-ভিত্তিক সেবা গ্রহণ করছে। বাংলাদেশ টেলিকমিউনিকেশন রেগুলেটরি কমিশন (BTRC) এর প্রকাশ করা তথ্য মতে, দেশে সক্রিয় মোবাইল সিমের সংখ্যা এখন ১৮ কোটির বেশি এবং এর মধ্যে ১১ কোটির বেশি সংযোগে ব্যবহার হচ্ছে ইন্টারনেট। দেশে প্রতিদিন এমএফএস, ইন্টারনেট ভিত্তিক ওয়েব ব্যাংকিং পরিষেবা এবং ডেবিট, ক্রেডিট কার্ড ইত্যাদির মাধ্যমে গড়ে প্রায় আটশ থেকে এক হাজার কোটি টাকার লেনদেন হচ্ছে। কিন্তু সাইবার নিরাপত্তা বিষয়ক যথাযথ শিক্ষা না থাকার ফলে ডিজিটালি নিজের তথ্য ও ডিভাইসের সঙ্গে সঙ্গে ঝুঁকিতে পড়ছে আর্থিক সম্পদও।

তথ্য প্রযুক্তির নিরাপত্তা নিশ্চিত করি
সাইবার সুরক্ষিত সেনাবাহিনী গড়ি

সাইবার নিরাপত্তা হুমকিসমূহ

অ্যাডওয়্যার,
র‍্যানসমওয়্যার

ভাইরাস, স্পাইওয়্যার,
ট্রোজান হর্স

ব্যাকডোর, কী-লগার,
ফিশিং ই-মেইল

ডেটা লিক, ডেটা ব্রিচ
ডি-ডস আক্রমণ

অপরিচিত USB
ড্রাইভ ব্যবহার

ক্র্যাক সফটওয়্যার
বা এপ্লিকেশন ব্যবহার

অরক্ষিত মোবাইল,
ডেস্কটপ/ল্যাপটপ

ফ্রি ওয়াই-ফাই,
ঝুঁকিপূর্ণ অনলাইন লেন

তথ্য প্রযুক্তির নিরাপত্তা নিশ্চিত করি
সাইবার সুরক্ষিত সেনাবাহিনী গড়ি

সাইবার নিরাপত্তা সতর্কতা

শক্তিশালী পাসওয়ার্ড ব্যবহার করুন

আপনার পাসওয়ার্ড গোপন রাখুন

শুধুমাত্র বিশ্বাসযোগ্য নেটওয়ার্কে সংযুক্ত হোন

সন্দেহজনক লিঙ্কে ক্লিক করবেন না

আপনার ডিভাইস আপডেট রাখুন

নিরাপদ VPN সংযোগ ব্যবহার করুন

বিশ্বস্ত ওয়েবসাইট থেকে কেনাকাটা করুন

সতর্কতার সাথে ফাইল ডাউনলোড করুন

তথ্য প্রযুক্তির নিরাপত্তা নিশ্চিত করি
সাইবার সুরক্ষিত সেনাবাহিনী গড়ি

সাইবার নিরাপত্তা সম্পর্কিত গুরুত্বপূর্ণ পরিভাষা

ম্যালওয়্যার (Malware)

ম্যালওয়্যার (Malware) হল এক ধরণের ক্ষতিকর সফটওয়্যার। সাধারণ ম্যালওয়্যারের উদাহরণ হিসেবে ভাইরাস, ট্রোজান, স্পাইওয়্যার, এডওয়্যার ইত্যাদি উল্লেখযোগ্য।

ডাটা থেফট (Data Theft)

ডাটা থেফট হল কোনো প্রতিষ্ঠান বা ব্যক্তির ব্যবহৃত ডাটাবেস, ডিভাইস এবং সার্ভারে সংরক্ষিত তথ্য অসাধু উদ্দেশ্যে, সংশ্লিষ্ট প্রতিষ্ঠান বা ব্যক্তির অনুমতি ছাড়াই চুরি বা ব্যবহার করা।

ডাটা থেফট কখনও কখনও অনিচ্ছাকৃতভাবে ঘটতে পারে। উদাহরণস্বরূপ, একজন ব্যক্তি একটি অসুরক্ষিত ফ্ল্যাশ ড্রাইভে কর্মস্থলের তথ্য সংরক্ষণ করতে পারে, যা অননুমোদিত ব্যক্তির কাছে অসাবধানতাবশতঃ স্থানান্তরের মাধ্যমে তথ্য চুরির সম্ভাবনা সৃষ্টি করতে পারে।

র‍্যানসমওয়্যার (Ransomware)

র‍্যানসমওয়্যার হল একটি ক্ষতিকর সফটওয়্যার যা কম্পিউটারকে সংক্রমিত করে এবং ব্যবহারকারীর ব্যবহারে সীমাবদ্ধতা সৃষ্টি করে, যতক্ষণ না মুক্তিপণ প্রদান করা হয়। এটি সাধারণত কম্পিউটার স্ক্রিনে একটি সতর্কতা প্রদর্শন করে এবং ভুক্তভোগীদের কাছ থেকে অর্থ আদায়ের চেষ্টা করে।

তথ্য প্রযুক্তির নিরাপত্তা নিশ্চিত করি
সাইবার সুরক্ষিত সেনাবাহিনী গড়ি

ফিশিং (Phishing)

ফিশিং বলতে প্রতারণার মাধ্যমে কারো ব্যক্তিগত তথ্য, যেমন ব্যবহারকারীর নাম ও পাসওয়ার্ড, ক্রেডিট কার্ডের তথ্য ইত্যাদি সংগ্রহ করার প্রক্রিয়া বোঝানো হয়। প্রতারকেরা ই-মেইল এবং ক্ষুদেবার্তার মাধ্যমে একটি সুপ্রতিষ্ঠিত ওয়েবসাইটের মতো ভুয়া পৃষ্ঠা তৈরি করে তথ্য চুরি করে থাকে।

স্পুফিং (Spoofing)

স্পুফিং হল এমন একটি পদ্ধতি যেখানে একজন সাইবার আক্রমণকারী একটি অনুমোদিত ডিভাইস থেকে ব্যবহারকারীর চাহিদাকৃত নকল একটি ওয়েবসাইট প্রদর্শন করে। এর মাধ্যমে ব্যবহারকারীর বিশ্বাস অর্জন করে তার তথ্য চুরি, ম্যালওয়্যার ছড়িয়ে দেওয়া বা এমনকি ব্যবহারকারীর ডিভাইসের নিয়ন্ত্রণ গ্রহণ করা সম্ভব হয়।

সাইবার ক্রাইম (Cyber Crime)

ইন্টারনেট ব্যবহার করে অপরাধমূলক উদ্দেশ্যে কোনো ব্যক্তি বা ব্যক্তিবর্গের বিরুদ্ধে ইচ্ছাকৃতভাবে সম্মানহানি, শারীরিক ও মানসিক ক্ষতির কারণ সৃষ্টি করার মাধ্যমে সাইবার অপরাধ ঘটানো হয়। এই অপরাধের পদ্ধতিগুলো নিম্নরূপ:

- সাইবার জালিয়াতি
- সাইবার সন্ত্রাস
- সাইবার চাঁদাবাজি
- সাইবার বুলিং
- সফটওয়্যার পাইরেসি
- ই-মানি লন্ডারিং

সাইবার হামলা প্রতিরোধে করণীয়

ডাটা এনক্রিপ্ট করুন এবং ব্যাকআপ তৈরি করুন

এনক্রিপশন হল একটি নিরাপত্তা প্রক্রিয়া যা আপনার ডেটাকে অকার্যকর করে তোলে যাতে অনুমোদিত ব্যক্তিরা তা পড়তে না পারে। এছাড়াও গুরুত্বপূর্ণ তথ্যের নিয়মিত ব্যাকআপ নেওয়া অত্যন্ত জরুরি। ব্যাকআপ নিশ্চিত করে যে, যদি কখনও সাইবার নিরাপত্তা লঙ্ঘন ঘটে বা আপনার ডেটা হারিয়ে যায়, তাহলে আপনার কাছে সর্বশেষ সুরক্ষিত কপি থাকবে।

সিস্টেম এবং সফটওয়্যার আপডেট রাখুন

সফটওয়্যার কোম্পানিগুলি নিয়মিতভাবে তাদের সিস্টেমগুলিতে নিরাপত্তা উন্নয়নের জন্য আপডেট প্রকাশ করে, যা সাইবার সুরক্ষার ত্রুটি এবং দুর্বলতাগুলি সংশোধন করে। এই ত্রুটিগুলি সাইবার অপরাধীরা ক্ষতিকর কর্মকাণ্ডের জন্য ব্যবহার করে থাকে। তাই আপডেট ইনস্টল করা আপনার ডিভাইস ও ডেটার সুরক্ষা নিশ্চিত করতে পারে।

পাবলিক ওয়াই-ফাই ব্যবহারে সাবধান হোন

পাবলিক ওয়াই-ফাই নেটওয়ার্ক এর নিরাপত্তা ব্যবস্থা সাধারণত অত্যন্ত দুর্বল হয়। সাইবার অপরাধীরা সেইসব দুর্বল পাবলিক ওয়াই-ফাই নেটওয়ার্ককে টার্গেট করে, যেখানে অনেক মানুষের আনাগোনা হয়। যেমন শপিং মল, বিমানবন্দর, রেলওয়ে স্টেশন, মেট্রো স্টেশন ইত্যাদি।

শক্তিশালী পাসওয়ার্ড ব্যবহার করুন

পাসওয়ার্ড ক্র্যাকিং প্রযুক্তি ব্যবহার করে সাধারণ পাসওয়ার্ড উন্মোচন করা যেতে পারে। তাই সবসময় শক্তিশালী পাসওয়ার্ড ব্যবহার করা উচিত এবং পাসওয়ার্ড শেয়ার করা এড়ানো উচিত। পাসওয়ার্ডের ক্ষেত্রে নীচে প্রদত্ত কিছু নিরাপত্তা ঝুঁকি প্রশমন কৌশল প্রয়োগ করা উচিতঃ

- লম্বা পাসওয়ার্ড তৈরি করুন।
- বিভিন্ন ধরনের বিশেষ অক্ষর ব্যবহার করুন, যেমনঃ @#$%&।
- পাসওয়ার্ড হিসেবে ব্যক্তিগত তথ্যের ব্যবহার এড়িয়ে চলুন।
- আভিধানিক শব্দ যেমনঃ password বা army123 ব্যবহার করবেন না।
- নিয়মিত পাসওয়ার্ড পরিবর্তন করুন।
- পাসওয়ার্ড ম্যানেজার ব্যবহার করুন।

ব্যক্তিগত তথ্য গোপন রাখুন

ইন্টারনেট ব্যবহার করার সময় হঠাৎ অপরিচিত মানুষের সাথে যোগাযোগ হতে পারে। যদি সরল বিশ্বাসে আমরা এই অপরিচিতদের কাছে আমাদের ব্যক্তিগত তথ্য যেমনঃ ঠিকানা, ফোন নম্বর, বা ছবি শেয়ার করি, তবে তারা সেই তথ্যের অপব্যবহার করতে পারে এবং আমাদের ক্ষতি করতে পারে। তাই অপরিচিতদের কাছে কখনোই ব্যক্তিগত তথ্য দেওয়া উচিত নয়। সুরক্ষিত থাকার জন্য সন্দেহজনক যোগাযোগ থেকে বিরত থাকা এবং যথাযথ নিরাপত্তা ব্যবস্থা গ্রহণ করা অত্যন্ত গুরুত্বপূর্ণ।

BANet ব্যাবহার করুন

আপনার ইউনিট, সংস্থা এবং ব্যাক্তিগত নিরাপত্তার কথা চিন্তাপূর্বক অফিশিয়াল কাজে সাধারণ ইন্টারনেট ব্যবহার এড়িয়ে চলুন এবং অফিশিয়াল প্রয়োজনে BANet ব্যবহার নিশ্চিত করুন। পাশাপাশি, তথ্যের নিরাপত্তা নিশ্চিত করতে নিয়মিত আপডেট এবং সুরক্ষা ব্যবস্থা তদারকি করুন।

তথ্য প্রযুক্তির নিরাপত্তা নিশ্চিত করি
সাইবার সুরক্ষিত সেনাবাহিনী গড়ি

ডেস্কটপ এবং ল্যাপটপ ব্যবহারে সতর্কতা

- কম্পিউটারে সবসময় লাইসেন্সড সফটওয়্যার ব্যবহার করুন।
- ডিভাইসের এন্টিভাইরাস নিয়মিত আপডেট রাখুন।
- ডেস্কটপ এবং ল্যাপটপে শক্তিশালী পাসওয়ার্ড দিন, যেমনঃ m#P52s@ap$V।
- ডিভাইসের লোকেশন ফিচার সব সময় অফ রাখুন।
- পাবলিক ওয়াই-ফাই ব্যবহার থেকে বিরত থাকুন।
- কম্পিউটারের অপারেটিং সিস্টেম নিয়মিত আপডেট করুন।
- গুরুত্বপূর্ণ ফাইল নিরাপদ এক্সটার্নাল ড্রাইভে সংরক্ষণ করুন।
- একই কম্পিউটারে BANet ও সাধারণ ইন্টারনেট ব্যবহার থেকে বিরত থাকুন।
- অফিসিয়াল ডিভাইসে ব্যক্তিগত পেনড্রাইভ/হার্ডড্রাইভ ব্যবহার থেকে বিরত থাকুন।
- সকল প্রকার পেনড্রাইভ ও এক্সটার্নাল হার্ডড্রাইভ স্ক্যানপূর্বক ব্যবহার করুন।
- সন্দেহজনক অ্যাটাচমেন্ট ডাউনলোড এবং ওপেন করা থেকে বিরত থাকুন।
- ফায়ারওয়াল চালু রাখুন এবং সুরক্ষিত নেটওয়ার্কে সংযুক্ত থাকুন।
- সফটওয়্যার ডাউনলোড করার সময় নির্ভরযোগ্য উৎস ব্যবহার করুন।
- ডিভাইসে অচেনা বা অজানা প্রোগ্রাম ইনস্টল করার আগে ভালোভাবে যাচাই করুন।
- ব্রাউজারের ক্যাশ এবং কুকি নিয়মিত ক্লিয়ার করুন।
- নিয়মিত ডাটা ব্যাকআপ নিন, যেন কোনো সমস্যা হলে আপনার তথ্য নিরাপদ থাকে।
- ডিভাইসের নিরাপত্তা নিশ্চিত করতে কম্পিউটার বন্ধ করার পূর্বে লগ আউট করুন।
- কম্পিউটারের হার্ডওয়্যার ও সফটওয়্যার নিরাপত্তা সম্পর্কিত আপডেটগুলি মেনে চলুন।

তথ্য প্রযুক্তির নিরাপত্তা নিশ্চিত করি
সাইবার সুরক্ষিত সেনাবাহিনী গড়ি

সোশ্যাল মিডিয়া ব্যবহারে সচেতন হোন

আমরা অধিকাংশ সময়ই ইন্টারনেট ব্যবহার করার ক্ষেত্রে সোশ্যাল মিডিয়াতে উল্লেখযোগ্য সময় ব্যয় করি। বিশেষ করে জনপ্রিয় প্ল্যাটফর্মগুলো যেমন ফেসবুক, মেসেঞ্জার, ইনস্টাগ্রাম এবং স্ন্যাপচ্যাটে ব্যবহারকারীর সংখ্যা ক্রমাগত বৃদ্ধি পাচ্ছে। এই বৃদ্ধির সাথে সাথে সাইবার দুষ্কৃতকারীর সংখ্যা ও তাদের কার্যক্রম বেড়ে চলেছে। তারা বিভিন্ন ধরনের ফাঁদ এবং স্ক্যাম তৈরি করে আপনার সোশ্যাল মিডিয়া একাউন্ট হ্যাক করার চেষ্টা করছে, যা আমাদের অনেকের অজানা।

সোশ্যাল মিডিয়া একাউন্ট থেকে তথ্য চুরি করে অর্থ হাতিয়ে নেওয়ার মতো ঘটনা প্রতিনিয়ত ঘটছে। হ্যাকাররা আপনার ব্যক্তিগত তথ্যের অপব্যবহার করে এবং পরিচয় চুরি করে ফেসবুক থেকে আপনার বন্ধুদেরকে ফেইক ম্যাসেজ পাঠিয়ে তাদের কাছ থেকে আর্থিক সাহায্য চাওয়া ছাড়াও আপনার নাম ব্যবহার করে মিথ্যা তথ্য প্রচার করার মাধ্যমে হয়রানিজনিত পরিস্থিতির সৃষ্টি করতে পারে। তাই সোশ্যাল মিডিয়া ব্যবহারের সময় সতর্ক থাকা অত্যন্ত গুরুত্বপূর্ণ।

আপনার অধীনস্থদের সঠিক দিকনির্দেশনা দিন

আপনার অধীনস্থ সকলকে সাইবার জগত সম্পর্কে সুস্পষ্ট ধারণা প্রদান করা অত্যন্ত গুরুত্বপূর্ণ। আধুনিক প্রযুক্তির সাথে সম্পৃক্ত থাকা যেমন প্রয়োজনীয়, তেমনি এই প্রযুক্তির অপব্যবহারের ফলে সৃষ্ট ঝুঁকি প্রতিরোধে সবাইকে প্রয়োজনীয় শিক্ষা ও সচেতনতা বৃদ্ধি করাও জরুরি। এছাড়াও নিয়মিত সাইবার নিরাপত্তা সম্পর্কে অধীনস্থদের প্রশিক্ষণ দেয়া যেতে পারে।

অপরিচিত লিংক ক্লিক হতে বিরত থাকুন

আপনি যখন আপনার ফোন বা কম্পিউটারের ব্রাউজারে কোনো ওয়েবসাইটের লিংক দেখছেন, তখন সেটা বৈধ এবং নিরাপদ কিনা যাচাই করুন। লিংকে ক্লিক করার আগে, চেষ্টা করুন সেটা যাচাই করার বা বিশেষজ্ঞের পরামর্শ নিন।

ফেসবুকের নিরাপত্তা

কিভাবে আপনার ফেসবুক প্রোফাইল লক করবেন?

আপনার Facebook প্রোফাইলে যান → প্রোফাইল থেকে More বা ... অপশনে ক্লিক করুন → Lock Profile অপশনে ক্লিক করুন → Lock Your Profile বাটনে ক্লিক করুন

ফেসবুকের পোস্ট কারা দেখতে পারবে, তা কিভাবে নির্ধারণ করবেন?

আপনার Facebook ওপেন করুন → What's on your mind? অপশনে ক্লিক করুন → আপনার স্ট্যাটাস বা ছবি পোস্ট করুন → Friends/Public অপশন সিলেক্ট করুন

ফেসবুকের ট্যাগ গোপনীয়তা কিভাবে নিশ্চিত করবেন?

আপনার Facebook ওপেন করুন → Menu বা ≡ অপশনে ক্লিক করুন → Settings & Privacy থেকে Settings এ যান → Profile & Tagging অপশনে ক্লিক করুন

Profile & Tagging অপশনে ক্লিক করুন → Tagging সেকশনে যান → Friends বা Only Me সিলেক্ট করুন

তথ্য প্রযুক্তির নিরাপত্তা নিশ্চিত করি
সাইবার সুরক্ষিত সেনাবাহিনী গড়ি

কিভাবে ফেসবুকের Location Off করবেন?

ফোনের Settings থেকে Apps এ যান › Facebook অ্যাপ সিলেক্ট করুন › Permission অপশনে ট্যাপ করুন › Location অপশন ট্যাপ করে Off করুন

কিভাবে Two-Factor Authentication চালু করবেন?

Menu বা ≡ অপশনে ক্লিক করুন › Settings & Privacy থেকে Settings এ যান › Accounts Centre থেকে Password & Security অপশনে ক্লিক করুন › Two Factor Authentication অপশনে যান

আপনার অ্যাকাউন্ট সিলেক্ট করুন ‹ SMS or WhatsApp সিলেক্ট করে Next বাটনে ক্লিক করুন ‹ Add Phone Number সিলেক্ট করে আপনার মোবাইল নম্বর দিন ‹ আপনার ফোন/WhatsApp এ পাঠানো কোডটি বসিয়ে Done বাটনে ক্লিক করুন

কিভাবে Restricted Friend তালিকায় কাউকে যুক্ত করবেন?

ফেসবুক Friend এর Profile এ যান › আইকনে ক্লিক করুন › Edit Friend List এ ক্লিক করুন › Restricted সিলেক্ট করুন

তথ্য প্রযুক্তির নিরাপত্তা নিশ্চিত করি
সাইবার সুরক্ষিত সেনাবাহিনী গড়ি

ই-মেইল এর নিরাপত্তা

Email এ Two-Step Verification কিভাবে On করবেন?

আপনার Email এ লগইন করুন > আপনার প্রোফাইলে ক্লিক করুন > ক্লিক Manage your Google Account > Security মেনু সিলেক্ট করুন

How you sign in to Google থেকে ক্লিক 2-Step Verification > Get Started বাটনে ক্লিক করুন > মোবাইল নম্বরটি দিন > Text Message/Phone Call এ ক্লিক করুন > Code টি দিন > Next এ ক্লিক করে Turn On বাটনে ক্লিক করুন

Email এ Recovery ফোন নাম্বার/ইমেইল কিভাবে Add করবেন?

আপনার Email এ লগইন করুন > আপনার প্রোফাইলে ক্লিক করুন > ক্লিক Manage your Google Account > Security মেনু সিলেক্ট করুন

How you sign in to Google থেকে ক্লিক Recovery Phone/Email > Phone Number বা Email দিন > Next বাটনে ক্লিক করুন > ক্লিক Get Code > Code টি দিন

তথ্য প্রযুক্তির নিরাপত্তা নিশ্চিত করি
সাইবার সুরক্ষিত সেনাবাহিনী গড়ি

মোবাইলের নিরাপত্তা

মোবাইল ফোন নিরাপত্তার জন্য কিভাবে Screen Lock করবেন?

আপনার ফোনের Settings মেন্যুতে যান › Lock Screen অপশনে ট্যাপ করুন › Screen Lock Type অপশনে ট্যাপ করুন › ট্যাপ Pattern/ Pin/Password

একটি Strong Password দিন

কিভাবে মোবাইল ফোনের Location Off রাখবেন?

আপনার ফোনের Settings মেন্যুতে যান › Location অপশনে ট্যাপ করুন › ট্যাপ Turn Off Location

মোবাইল ফোনের Biometric Security কিভাবে সেট করবেন?

আপনার ফোনের Settings মেন্যুতে যান → Biometrics & Security অপশনে ট্যাপ করুন → Fingerprint/Face & Password অপশনে ট্যাপ করুন → Face/Fingerprint অপশনে ট্যাপ করুন

↓

ট্যাপ Add a Face/ Fingerprint → মোবাইল স্ক্রিনের নির্দেশনা অনুসরন করুন → Face/Fingerprint সেভ করুন

কিভাবে iPhone অথবা iPad আপডেট করবেন?

আপনার ডিভাইসটি Wi-Fi এর সাথে কানেক্ট করুন → Settings মেন্যুতে যান → General অপশনে ট্যাপ করুন → Software Update এ ট্যাপ করুন

↓

ট্যাপ Download and Install → I Agree বাটনে ক্লিক করুন → Update শেষ না হওয়া পর্যন্ত অপেক্ষা করুন

ডেস্কটপ/ল্যাপটপ এর নিরাপত্তা

ডিভাইসের Location কিভাবে Off করবেন?

ডিভাইসের Settings মেন্যুতে যান → Privacy অপশনে ক্লিক করুন → Location এ ক্লিক করুন → ডিভাইসের Location Off করুন

ডিভাইসের Password কিভাবে সেট করবেন?

ডিভাইসের Settings মেন্যুতে যান → Accounts অপশনে ক্লিক করুন → Sign in এ ক্লিক করুন → Password অপশন সিলেক্ট করুন → Add বাটনে ক্লিক করুন → Password সেট করে Next বাটনে ক্লিক করুন

তথ্য প্রযুক্তির নিরাপত্তা নিশ্চিত করি
সাইবার সুরক্ষিত সেনাবাহিনী গড়ি

কিভাবে Windows এ Firewall On করবেন?

Control Panel মেন্যুতে যান → Windows Defender Firewall সিলেক্ট করুন → ক্লিক Turn Windows Defender Firewall On or Off → সিলেক্ট Public/Private Network Settings → ক্লিক Turn on Windows Defender Firewall → OK বাটনে ক্লিক করুন

কিভাবে Windows এ অপারেটিং সিস্টেম Update করবেন?

ডিভাইসের Start মেন্যুতে যান → Settings এ ক্লিক করুন → ক্লিক Update & Security → Windows Update অপশনে যান → ক্লিক Check for Update → Install বাটনে ক্লিক করুন

সোশ্যাল মিডিয়ার নিরাপত্তা

- পাসওয়ার্ড নিয়মিত পরিবর্তন বা আপডেট করুন।
- সোশ্যাল মিডিয়ার গোপনীয়তা বা প্রাইভেসি সেটিংস সচল রাখুন।
- বন্ধুত্বের অনুরোধ গ্রহণ করার সময় সাবধান থাকুন।
- অচেনা ব্যক্তিদের সাথে যুক্ত হওয়ার আগে যাচাই করুন।
- আপনার একাউন্ট থেকে ঘন ঘন লগ-আউট করার অভ্যাস গড়ুন।
- কম্পিউটারে লগ-ইন তথ্য সংরক্ষণ করবেন না।
- আপনার ব্যক্তিগত তথ্য শুধুমাত্র বিশ্বাসযোগ্য বন্ধুদের সাথে শেয়ার করুন।
- ব্যক্তিগত বার্তায় বা কমেন্টে সংবেদনশীল তথ্য শেয়ার করা থেকে বিরত থাকুন।
- সন্দেহজনক লিঙ্ক বা অ্যাটাচমেন্টে ক্লিক করা থেকে বিরত থাকুন।
- আপনার একাউন্টে Two-Factor Authentication (2FA) চালু করুন।
- নিয়মিতভাবে আপনার একাউন্টের নিরাপত্তা সেটিংস পর্যালোচনা এবং আপডেট করুন।
- সোশ্যাল মিডিয়া প্ল্যাটফর্মের নিরাপত্তা আপডেট এবং নতুন ফিচার সম্পর্কে সচেতন থাকুন।

ইন্টারনেট ব্যাংকিং এর নিরাপত্তা

- আপনার অ্যাকাউন্টে শক্তিশালী পাসওয়ার্ড ব্যবহার করুন, যেমন: m#P52s@ap$V এবং একাধিক সেবার জন্য একই পাসওয়ার্ড ব্যবহার করবেন না।
- Two-Factor Authentication (2FA) চালু করুন।

- পরিচিত এবং নিরাপদ ডিভাইস থেকে ইন্টারনেট ব্যাংকিং লেনদেন করুন।
- পাবলিক ওয়াইফাই নেটওয়ার্ক ব্যবহার করার থেকে বিরত থাকুন।
- ব্যাংকিং সেবার জন্য ব্যাংকের অফিসিয়াল সাইট ব্যবহার করুন।
- আপনার ব্যাংক অ্যাকাউন্টের স্টেটমেন্ট নিয়মিত চেক করুন যাতে কোনো অননুমোদিত লেনদেন সহজেই ধরা পড়ে।
- সন্দেহজনক ইমেল বা ম্যাসেজে দেওয়া লিঙ্কে ক্লিক করা থেকে বিরত থাকুন।

- নিরাপত্তার স্বার্থে ব্যক্তিগত তথ্য চাওয়া ইমেল বা ফোনকল এড়িয়ে চলুন।
- আপনার কম্পিউটার বা মোবাইলের নিরাপত্তা সফটওয়্যার নিয়মিত আপডেট করুন।
- ব্যাংকের যে কোন সেবার জন্য শুধুমাত্র ইমেইল বা ম্যাসেজের মাধ্যমে যোগাযোগ না করে ফোন কলে অথবা সরাসরি যোগাযোগ করুন।
- অনলাইন লেনদেন করার সময় সর্বদা সুরক্ষিত ও এনক্রিপ্টেড ওয়েবসাইটে লগইন করুন।

- ব্যাংকিং অ্যাপ ডাউনলোডের জন্য অফিসিয়াল প্লে স্টোর/এপ স্টোর ব্যবহার করুন।
- আপনার ব্যাংক অ্যাকাউন্টের নিরাপত্তা সম্পর্কিত কোনও সন্দেহজনক কার্যকলাপ দেখলে ব্যাংক কর্তৃপক্ষকে তৎক্ষণাৎ জানান।

তথ্য প্রযুক্তির নিরাপত্তা নিশ্চিত করি
সাইবার সুরক্ষিত সেনাবাহিনী গড়ি

কিভাবে আপনার সন্তানকে অনলাইনে নিরাপদ রাখবেন

বর্তমান যুগে, ইন্টারনেট আমাদের জীবনের একটি অপরিহার্য অংশ হয়ে উঠেছে। শিশুদের মধ্যেও এই প্রযুক্তির ব্যবহার বাড়ছে এবং তাই তাদের অনলাইন নিরাপত্তা নিয়ে অভিভাবকদের উদ্বিগ্ন হওয়া একেবারেই স্বাভাবিক। আপনার সন্তানকে অনলাইনে নিরাপদ রাখতে কিছু সহজ পদক্ষেপ গ্রহণ করা যেতে পারে, যা তাদের সুরক্ষিত রাখবে এবং সাইবার ঝুঁকি থেকে রক্ষা করবে।

- আপনার সন্তানকে ইন্টারনেট ব্যবহারের সঠিক নিয়ম শেখান। তাদের বুঝিয়ে বলুন যে কোন ধরনের তথ্য শেয়ার করা উচিত এবং কোনটা নয়। এছাড়াও, অনলাইনে তাদের পরিচয় গোপন রাখতে শেখান এবং অচেনা ব্যক্তিদের সাথে ব্যক্তিগত তথ্য শেয়ার করতে নিষেধ করুন।
- ইন্টারনেট ব্যবহারের সময় নিয়ন্ত্রণ করা গুরুত্বপূর্ণ। একটি সময়সূচি নির্ধারণ করুন যা আপনার সন্তানের অনলাইন সময় সীমিত করবে। অতিরিক্ত সময় স্ক্রীনের সামনে কাটানোর ফলে তাদের পড়াশোনা ও শারীরিক সুস্থতা ক্ষতিগ্রস্ত হতে পারে।
- আপনার সন্তানকে সুরক্ষিত ওয়েবসাইট এবং অ্যাপ্লিকেশন ব্যবহারে উৎসাহিত করুন। গেমিং, সোশ্যাল মিডিয়া এবং অন্যান্য অনলাইন প্ল্যাটফর্মের জন্য সঠিক সাইট নির্বাচন করুন।
- আপনার সন্তানের সঙ্গে আলাপ করুন এবং তাদের ইন্টারনেট অভিজ্ঞতা সম্পর্কে জানুন। কোন সমস্যা দেখলে বা কোনো সন্দেহজনক কার্যকলাপ হলে তা সঙ্গে সঙ্গে আলোচনা করতে বলুন।
- Parental Control বা অভিভাবক নিয়ন্ত্রণ সফটওয়্যার ব্যবহার করুন। এসব সফটওয়্যার আপনাকে আপনার সন্তানের অনলাইন কার্যকলাপ পর্যবেক্ষণ করতে এবং অপ্রয়োজনীয় বা ক্ষতিকর বিষয়বস্তু ব্লক করতে সহায়তা করবে।

সবশেষে আপনার সন্তানের ইন্টারনেট ব্যবহারের সময় তাদের পাশে থাকুন এবং একটি খোলামেলা যোগাযোগের সম্পর্ক গড়ে তুলুন। তাদের নিরাপত্তা নিয়ে উদ্বেগ থাকলে তা সঙ্গে সঙ্গে আলোচনা করুন এবং তাদের সহায়তা করুন

সাইবার সচেতনতা মাস থেকে প্রত্যাশা

প্রযুক্তির অগ্রগতির সাথে সাথে সাইবার অপরাধের পরিমাণও বাড়ছে। এই পরিস্থিতিতে সাইবার সচেতনতা মাস একটি গুরুত্বপূর্ণ উদ্যোগ, যা সকলের মধ্যে ডিজিটাল নিরাপত্তা সম্পর্কে সচেতনতা বৃদ্ধি করার উদ্দেশ্যে পালন করা হয়। সাইবার সচেতনতা মাস থেকে আমাদের প্রত্যাশা ও চাওয়াগুলো নীচে তুলে ধরা হলোঃ

- বাংলাদেশ সেনাবাহিনীর সকল সদস্যদের মধ্যে সাইবার নিরাপত্তা সম্পর্কে মৌলিক ধারণা বাড়বে। আমাদের তরুণ প্রজন্ম বিশেষ করে শিক্ষার্থীরা অনলাইন স্ক্যাম, ফিশিং এবং অন্যান্য সাইবার অপরাধ সম্পর্কে সচেতন হবে।
- সরকারি ও বেসরকারি প্রতিষ্ঠানগুলো তাদের সাইবার নিরাপত্তা নীতিমালা পর্যালোচনা করবে এবং কর্মীদের প্রশিক্ষণ দিবে।
- ইন্টারনেট ব্যবহারকারীরা তাদের অনলাইন আচরণ এবং ডেটা সুরক্ষার প্রতি গুরুত্ব দিবে।
- সাইবার নিরাপত্তা বিষয়ে বিভিন্ন কর্মশালা, সেমিনার এবং প্রশিক্ষণের আয়োজন করা হবে।
- সাইবার নিরাপত্তার বিষয়ে পারিবারিক এবং সামাজিক আলোচনা বৃদ্ধি পাবে।
- সাইবার সচেতনতা মাস সুরক্ষিত ডিজিটাল পরিবেশ গড়তে সাহায্য করবে এবং সাইবার অপরাধ প্রতিরোধে সহায়ক হবে।

সবশেষে সাইবার সচেতনতা মাস আমাদেরকে একটি নিরাপদ ডিজিটাল পরিবেশ গড়ে তোলার লক্ষ্যে আগ্রহী করে তুলবে। মানুষের মধ্যে সাইবার নিরাপত্তা সম্পর্কে সঠিক জ্ঞান অর্জন করার মাধ্যমে সাইবার অপরাধ প্রতিরোধে সাহায্য করবে।

তথ্য প্রযুক্তির নিরাপত্তা নিশ্চিত করি
সাইবার সুরক্ষিত সেনাবাহিনী গড়ি

সাইবার নিরাপত্তা সম্পর্কে জানা কেবল আমাদের ব্যক্তিগত সুরক্ষার জন্যই নয়, বরং আমাদের ডিজিটাল ডিভাইসসমূহের সঠিক ব্যবহার ও নিরাপত্তার জন্যও অত্যন্ত গুরুত্বপূর্ণ। সঠিক জ্ঞান অর্জন করে আমরা নিজের এবং অন্যদের সাইবার নিরাপত্তা নিশ্চিত করতে পারি এবং সাইবার অপরাধীদের হাত থেকে রক্ষা পেতে পারি। তাই সাইবার নিরাপত্তা সম্পর্কে জানা আমাদের সময়ের একটি অপরিহার্য প্রয়োজন।

সাইবার নিরাপত্তা সচেতনতা শিক্ষা

আপনি যদি সাইবার নিরাপত্তা সম্পর্কে আগ্রহী হন এবং এ সম্পর্কে আরও বিস্তারিত জানতে চান, তাহলে নিম্নলিখিত লিঙ্কগুলো ভিজিট করতে পারেন। এটি আপনার সাইবার নিরাপত্তা দক্ষতা ও সচেতনতা বৃদ্ধি করতে সহায়ক হবে।

- Army BA Net Portal: portal.army.mil.bd
- Cybersecurity NonProfit (CSNP): www.csnp.org
- CISA Cyber Essentials Starter Kit: www.cisa.gov
- Stay Safe Online (NCSA): www.staysafeonline.org
- Cyber Aware (UK Government): www.cyberaware.gov.uk
- Cybercrime Support Network: www.fightcybercrime.org

সাইবার নিরাপত্তা সচেতনতা মাস আমাদের সকলের জন্য একটি গুরুত্বপূর্ণ মাস যেখানে আমরা ডিজিটাল নিরাপত্তা নিয়ে সচেতন হওয়ার আহ্বান জানাই। এই মাসটি আমাদের মনে করিয়ে দেয় যে, সাইবার সুরক্ষা শুধু প্রযুক্তির বিষয় নয়, বরং আমাদের দৈনন্দিন জীবনের একটি গুরুত্বপূর্ণ অংশ। তাই আসুন আমরা সবাই এই মাসটিকে সচেতনতা বৃদ্ধি ও নিরাপদ ডিজিটাল ডিভাইসের ব্যবহারের অভ্যাস গড়ে তোলার মাধ্যমে উদযাপন করি এবং আমাদের অনলাইন জীবন ঝুঁকিমুক্ত ও নিরাপদ রাখি।

তথ্য প্রযুক্তির নিরাপত্তা নিশ্চিত করি
সাইবার সুরক্ষিত সেনাবাহিনী গড়ি

সাইবার নিরাপত্তা সচেতনতা মাস

অক্টোবর ২০২৪

তথ্য প্রযুক্তির নিরাপত্তা নিশ্চিত করি সাইবার সুরক্ষিত সেনাবাহিনী গড়ি

সেনাসদর, জিএস শাখা, (আইটি পরিদপ্তর)