সাইবার নিরাপত্তা সচেতনতা মাস

★★ অক্টোবর ২০২১ ★★

সাইবার হুমকি এবং আমাদের করনীয়

সাইবার নিরাপত্তা সম্পর্কে সচেতন থাকুন
তথ্য প্রযুক্তির সঠিক ব্যবহার করি

সেনাসদর, জিএস শাখা (আইটি পরিদপ্তর)

সাইবার নিরাপত্তা
কেন গুরুত্বপূর্ণ?

সামরিক কর্মক্ষেত্রে এবং দৈনন্দিন জীবনে ইন্টারনেট ও আধুনিক প্রযুক্তির উপরে আমরা অনেক বেশী নির্ভরশীল। ইন্টারনেটের মাধ্যমে সকল ধরনের তথ্য চুরি এবং সাইবার হামলার পরিমানও দিনদিন বেড়েই চলেছে। ফলশ্রুতিতে সংবেদনশীল সরকারি ও ব্যক্তিগত তথ্য পাচার, অর্থনৈতিক লেনদেনে হস্তক্ষেপ, এমনকি সামাজিকভাবেও নানাবিধ সমস্যার সম্মুখীন হতে হয়। এজন্য যে কোন ধরনের সাইবার আক্রমন থেকে নিরাপদ থাকার জন্য সাইবার নিরাপত্তা সম্পর্কিত জ্ঞান থাকা অপরিহার্য ।

সাইবার নিরাপত্তা হুমকিসমূহ

- র‍্যানসামওয়্যার
- ফিশিং ই - মেইল
- সামাজিক যোগাযোগ মাধ্যম
- ফ্রি ওয়াই-ফাই
- ফ্রি সফটওয়্যার ও এপ্লিকেশন ব্যবহার
- অনিরাপদ স্থানে পাসওয়ার্ড সংরক্ষন করা
- অসুরক্ষিত মোবাইল ডিভাইস, ডেস্কটপ/ ল্যাপটপ
- ইন্টারনেট ভিত্তিক অন-লাইন লেনদেন
- বিভ্রান্তিকর, লোভনীয় ও প্রতারনামূলক ফাঁদ

সাইবার নিরাপত্তা সম্পর্কিত গুরুত্বপূর্ণ পরিভাষা

র‍্যানসামওয়্যার (Ransomware)

ক্ষতিকর সফটওয়্যার যা একটি কম্পিউটারকে সংক্রমিত করে এবং ব্যবহারকারীর ব্যবহার সীমাবদ্ধ করে রাখে, যতক্ষণ না মুক্তিপণ প্রদান করা হয়। এর মাধ্যমে প্রায়ই অন - স্ক্রিন সতর্কতা প্রদর্শন করে ভুক্তভোগীদের কাছ থেকে অর্থ আদায়ের চেষ্টা করা হয়ে থাকে।

ফিশিং (Phishing)

ইন্টারনেট ফিশিং বলতে প্রতারণার মাধ্যমে কারো ব্যক্তিগত তথ্য, যেমন ব্যবহারকারীর নাম ও পাসওয়ার্ড, ক্রেডিট কার্ডের তথ্য ইত্যাদি সংগ্রহ করাকে বোঝানো হয়ে থাকে। প্রতারকেরা এই পদ্ধতিতে কোনো সুপ্রতিষ্ঠিত ওয়েবসাইট সেজে মানুষের কাছ থেকে তথ্য চুরি করে থাকে। ই-মেইল এবং ক্ষুদেবার্তার মাধ্যমে ফিশিং হয়ে থাকে।

ম্যালওয়্যার (Malware)

ম্যালওয়্যার হল "ক্ষতিকর সফটওয়্যার" এর সংকোচন। সাধারন ম্যালওয়্যারের উদাহরণগুলির মধ্যে রয়েছে ভাইরাস, ট্রোজান ভাইরাস, স্পাইওয়্যার, এডওয়্যার ইত্যাদি।

স্প্যামিং (Spamming)

অবাঞ্ছিত বার্তা (যেমন ই-মেইল, ক্ষুদেবার্তা/ ইন্টারনেট পোস্টিং), বিভ্রান্তিকর, লোভনীয় ও প্রতারনামূলক ফাঁদ যার মাধ্যমে ব্যবহারকারীকে অযাচিত কর্মকান্ডে বাধ্য করে।

সাইবার নিরাপত্তা সম্পর্কিত গুরুত্বপূর্ণ পরিভাষা

স্পুফিং (Spoofing)

স্পুফিং হল এমন একটি পদ্ধতি যেখানে একজন আক্রমনকারী একটি অনুনমোদিত ডিভাইস থেকে ব্যবহারকারীর চাহিদাকৃত নকল ওয়েবসাইট প্রদান করে ব্যবহারকারীর তথ্য চুরি, ম্যালওয়্যার ছড়িয়ে দেয়া এমনকি ব্যবহারকারীর ডিভাইসের নিয়ন্ত্রন নেয়ার মত কাজ করতে সক্ষম।

সাইবার নিরাপত্তার হুমকি নিরসনের উপায়সমূহঃ

শক্ত পাসওয়ার্ড ব্যবহার করুনঃ

- গোপনীয়তা নিশ্চিত করার জন্য শক্ত পাসওয়ার্ডই একমাত্র উপায়।
- অতি সাধারন, প্রচলিত পাসওয়ার্ড ব্যবহার পরিহার করুন।
- নিয়মিত পাসওয়ার্ড পরিবর্তন করুন।
- পাসওয়ার্ড শেয়ার করা থেকে বিরত থাকুন।
- পাসওয়ার্ড ব্যবহারের ক্ষেত্রে ২ ফ্যাক্টর অথেনটিকেশন চালু করুন।

মোবাইলের নিরাপত্তা বিধান করুনঃ

- শুধুমাত্র বিশ্বস্ত ইন্টারনেট ব্যবহার করুন।
- অটো লক, আঙ্গুলের ছাপ ও পিন ব্যবহার করুন।
- শুধুমাত্র বিশ্বস্ত অ্যাপ ব্যবহার করুন।
- অপরিচিত ও সন্দেহজনক নম্বর থেকে কল গ্রহণ ও প্রদান থেকে বিরত করুন।
- মোবাইলের সিকিউরিটি প্যাচ নিয়মিত আপডেট করুন।
- মোবাইলের সেটিংস থেকে বিভিন্ন এপ্লিকেশনের (ফোন বুক, ক্যামেরা, মাইক) প্রবেশাধীকার নিয়ন্ত্রন করুন।

ডেস্কটপ/ল্যাপটপ ব্যবহারে সতর্ক হউনঃ

- আপনার ডেস্কটপ এবং ল্যাপটপ ব্যবহারে আইটি নির্দেশনা মেনে চলুন।
- লাইসেন্সড সফটওয়্যার ব্যবহার বাধ্যতামূলক করুন।
- অ্যান্টিভাইরাস নিয়মিত আপডেট রাখুন।
- অপারেটিং সিস্টেমের প্যাচ নিয়মিত আপডেট করুন
- ক্র্যাক সফটওয়্যার ইনস্টল করা এড়িয়ে চলুন।
- একই কম্পিউটারে BANet ও ইন্টারনেট ব্যবহার থেকে বিরত থাকুন।
- অফিসিয়াল ডিভাইসে ব্যক্তিগত অপসারনযোগ্য ডিভাইস ব্যবহার থেকে বিরত থাকুন।
- সকল প্রকার পেনড্রাইভ ও এক্সটার্নাল হার্ডড্রাইভ স্ক্যানপূর্বক ব্যবহার করুন।

নিরাপদ ইন্টারনেট ব্যবহার নিশ্চিত করুনঃ

- নিরাপদ ওয়েব-ব্রাউজার ব্যবহার করুন।
- ওয়েবসাইট পরিদর্শনের ক্ষেত্রে অন্যের দেয়া লিঙ্ক ব্যবহার পরিহার করুন। ব্রাউজারে নিজে url টাইপ করে ওয়েবসাইটে গমন করুন।
- সর্বদা অনুমোদিত উৎস থেকে সফ্টওয়্যার ডাউনলোড করুন।
- অরক্ষিত ওয়াইফাই জোনের সাথে সংযোগ স্থাপন করবেন না।
- অবাঞ্চিত সাইটের মাধ্যমে প্রতারনা থেকে রক্ষা পেতে ব্রাউজার অ্যাডঅন ব্যবহার করুন।
- যে কোন ওয়েবসাইটের বিভ্রান্তিকর, লোভনীয় ও প্রতারনামূলক প্রলোভনে প্ররোচিত হবেন না।

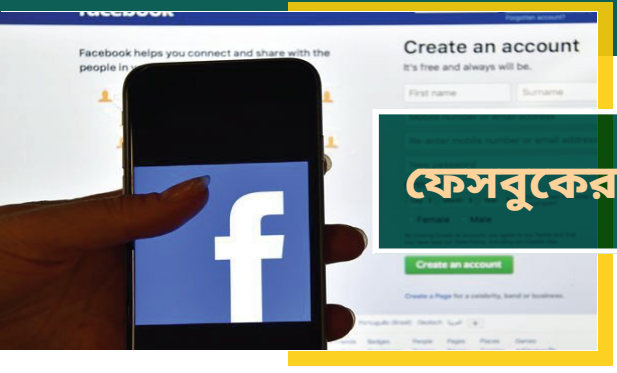
সোশ্যাল মিডিয়া সেটিংস সুরক্ষিত করুনঃ

- সামাজিক যোগাযোগ মাধ্যমগুলোর প্রদত্ত নিরাপত্তা এবং গোপনীয়তা অপশন ব্যবহার করুন।
- 2 ফ্যাক্টর অথেনটিকেশন ব্যবহার করুন
- সোশ্যাল মিডিয়াতে লগইন করার সময় মূল URL টাইপ করুন।
- "আমাকে লগ ইন রাখুন" বক্সটি চেক করা থেকে বিরত থাকুন।
- সামাজিক যোগাযোগ মাধ্যমে অপ্রয়োজনীয় তথ্য আদান-প্রদান থেকে বিরত থাকুন।
- সামরিক পোষাক পরিহিত অবস্থায় কোন ছবি পোস্ট করা থেকে বিরত থাকুন।
- সরকারি ইলেক্ট্রনিক ডিভাইসে সামাজিক যোগাযোগ মাধ্যম ব্যবহার পরিহার করুন।
- অপরিচিত বন্ধুর অনুরোধ থেকে নিজেকে সংযত রাখুন।

ফিশিং সম্পর্কে সচেতন থাকুন :

- অপরিচিত ই-মেইল, ক্ষুদেবার্তা, সামাজিক যোগাযোগ মাধ্যমে প্রেরিত লিংক বা ফাইলে ক্লিক করা হতে বিরত থাকুন
- যে কোন সংস্থার সাথে যোগাযোগের ক্ষেত্রে বিশ্বস্ত মাধ্যম (ফোন নম্বর, এপ বা ওয়েবসাইট) ব্যবহার করুন
- সর্বদা ওয়েবপেইজ এর সঠিক এড্রেস, ই-মেইল এর সঠিক প্রেরক নিশ্চিত হয়ে পরবর্তি পদক্ষেপ গ্রহন করুন।
- সন্দেহজনক লিঙ্ক বা Attachment এ ভুল বশত ক্লিক করার ফলে অন্য কোন সাইটে চলে গেলে তাতে লগ-ইন আইডি, পাসওয়ার্ড, অন্যান্য গুরুত্বপূর্ণ তথ্য দেয়া থেকে বিরত থাকুন।

কিভাবে সাইবার হুমকি এড়ানো যায়



ফেসবুকের নিরাপত্তা:

- ফেসবুকের পোস্ট, কে বা কারা দেখতে পারবে, তা কিভাবে নির্ধারণ করবেন

ওপেন Facebook → Upload **ছবি অথবা** Status → **ক্লিক** Friends/ Public **অপশন**

- কিভাবে ফেসবুকে প্রোফাইল লক করবেন

ওপেন Facebook → প্রোফাইল থেকে More / ... অপশনে **ক্লিক** করুন → **ক্লিক** Lock Profile **অপশন** → **ক্লিক** Okay

ফেসবুকের ট্যাগ গোপনীয়তা কিভাবে নিশ্চিত করবেন

ওপেন Facebook → ক্লিক Menu / ≡ → ক্লিক Settings & Privacy --> Settings → Profile & Tagging অপশন থেকে Tagging এ যান → ক্লিক Edit অপশন → Select Friends/ Only Me

আপনার Restricted Friend তালিকায় কাউকে কিভাবে যুক্ত করবেন

ওপেন Facebook → Friend এর Profile এ যান → ক্লিক → ক্লিক Edit Friend List → সিলেক্ট Restricted

ফেসবুকের নিরাপত্তা

ফেসবুকের নিরাপত্তা

কিভাবে Two-Factor Authentication চালু করবেন

ওপেন Facebook → ক্লিক Settings & Privacy --> Settings → ক্লিক Password & security → নিচে Two Factor Authentication অপশন থেকে Use Two-Factor Authentication এ যান → ক্লিক Edit অপশন → ক্লিক Authentication app / Text message / Security key → Add মোবাইল নম্বর → Enter Code --> Done

কিভাবে ফেসবুকে Location Off করবেন

ক্লিক মোবাইল Settings → ক্লিক Facebook → ক্লিক Permission → Tap Location OFF

কিভাবে সাইবার হুমকি এড়ানো যায়

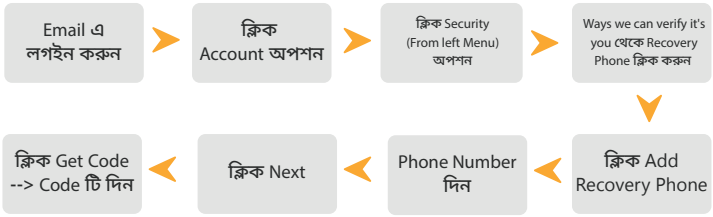
ই-মেইল এর নিরাপত্তা

Email এ 2-Factor Verification কিভাবে On করবেন

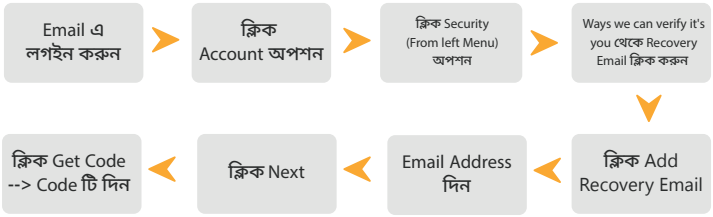
Email এ লগইন করুন → ক্লিক Account অপশন → ক্লিক Manage your Google Account → ক্লিক Security (From left Menu) অপশন → Signing into Google থেকে ক্লিক 2-Step Verification → ক্লিক OFF --> Get Started → মোবাইল নম্বরটি দিন --> ক্লিক Text Message / Phone Call → Code টি দিন --> ক্লিক Next -->ক্লিক Turn On

ই-মেইল এর নিরাপত্তা

Email নিরাপত্তার জন্য Recovery ফোন নম্বর কিভাবে Add করবেন



Email নিরাপত্তার জন্য Recovery ই-মেইল কিভাবে Add করবেন



কিভাবে সাইবার হুমকি এড়ানো যায়

মোবাইলের নিরাপত্তা

মোবাইল ফোন নিরাপত্তার জন্য কিভাবে Auto Lock করবেন

ক্লিক Settings → ক্লিক Lock Screen অপশন → ক্লিক Screen Lock Type অপশন → ক্লিক Pattern/ Pin/Password → একটি Strong Password দিন

মোবাইলের নিরাপত্তা

মোবাইল ডিভাইসের Biometrics Security কিভাবে করবেন

ক্লিক Settings → ক্লিক Biometrics & Security অপশন → ক্লিক Face recognition/ Fingerprints অপশন → Face/Fingerprint ডাটা Add করুন → Add Face/Fingerprints → মোবাইল স্ক্রিনের নির্দেশনা অনুসরন করুন → Face/Fingerprints সেভ করুন

মোবাইল ডিভাইসের Location Off কিভাবে রাখবেন

ক্লিক Settings → ক্লিক Location অপশন → ক্লিক Turn Off Location

সাইবার সচেতনতা মাস থেকে প্রত্যাশা

- সাইবার নিরাপত্তা সম্পর্কে নিজে ও অপরকে সচেতন রাখবো।
- ৩ মাস অন্তর পাসওয়ার্ড পরিবর্তন করবো।
- শক্তিশালী পাসওয়ার্ড ব্যবহার করবো।
- ভিন্ন ভিন্ন এ্যাপলিকেশনে পৃথক পাসওয়ার্ড ব্যবহার করবো।
- সামাজিক যোগাযোগ মাধ্যমের অ্যাকাউন্টের গোপনীয়তা সেটিংস এ নিরাপত্তা নিশ্চিত করবো।
- ইন্টারনেটে অপ্রয়োজনীয় তথ্য আদান-প্রদান থেকে বিরত থাকবো।
- BANet এর মাধ্যমে সেনাবাহিনীর ওয়েব-মেইল, ডিজিডাক ব্যবহার করবো।
- কোন অজানা/ সন্দেহজনক লিংকে ক্লিক করবো না।
- পাবলিক ই-মেইল সিস্টেমে কোন সংবেদনশীল বিষয়বস্তু শেয়ার করা যাবে না।
- যেকোনো ওয়েবসাইট ব্যবহার শেষে সর্বদা লগ আউট করবো।
- ইন্টারনেট ভিত্তিক আর্থিক লেনদেনের ক্ষেত্রে ফ্রি ওয়াই-ফাই ব্যবহার করবো না।

সাইবার সচেতনতা মাস থেকে প্রত্যাশা

- লাইসেন্সকৃত এন্টি ভাইরাস ও অপারেটিং সিস্টেম ব্যবহার করবো।
- স্ক্যান না করে কোন পেন-ড্রাইভ ব্যবহার করবো না।
- সামাজিক যোগাযোগ মাধ্যম হিসেবে ভাইবার, হোয়াটস অ্যাপ এর পরিবর্তে 'বার্তা' এর বহুল ব্যবহার নিশ্চিত করবো।
- অপরিচিত ও সন্দেহজনক এ্যাপলিকেশন ব্যবহারে বিরত থাকবো।
- ইন্টারনেট ও সামাজিক যোগাযোগ মাধ্যম ব্যবহার সংক্রান্ত সেনাসদরের MI/ IT/ PS পরিদপ্তরের আইটি নির্দেশনা মেনে চলবো।
- সরকারি মোবাইল, ল্যাপটপ অথবা কম্পিউটার এ সামাজিক যোগাযোগ মাধ্যম ব্যবহার করা থেকে বিরত থাকবো।
- পরিবার এবং সন্তানদের নিরাপদ ইন্টারনেট ও ওয়েবসাইট ব্যবহার নিশ্চিত করবো এবং মোবাইলে কথোপকথন ও তথ্য আদান-প্রদানে সচেতন থাকবো।

সাইবার নিরাপত্তা সম্পর্কে সচেতন থাকি তথ্য প্রযুক্তির সঠিক ব্যবহার করি

সেনাসদর, জিএস শাখা (আইটি পরিদপ্তর)