সাইবার সচেতনতা মাস (ক্যাম) অক্টোবর-২০১৯ টুলকিট

সাইবার সচেতনতা মাস (ক্যাম)-২০১৯ এর ক্যাম্পেইনে আপনাকে স্বাগত। সাইবার নিরাপত্তা সচেতনতা তৈরিতে ***ক্যাম*** সরকার ও অন্যান্য প্রতিষ্ঠানগুলোর মধ্যকার একটি সম্মিলিত প্রচেষ্টা। যেখানে দেশের প্রতিটি নাগরিককে এটা নিশ্চিত করা হয় যে, অনলাইনে নিরাপদ ও সুরক্ষিত থাকতে যেসব জিনিস প্রয়োজন তার সবই আমাদের আছে। যুক্তরাষ্ট্রের ডিপার্টমেন্ট অব হোমল্যান্ড সিকিউরিটি ও ন্যাশনাল সাইবার সিকিউরিটি অ্যালায়েন্স (এনসিএসএ) এর যৌথভাবে পরিচালিত মাসব্যাপী ক্যাম্পেইনে *সাইবার ক্রাইম অ্যাওয়ারনেস ফাউন্ডেশন (সিসিএ ফাউন্ডেশন)* অংশীদার হিসেবে কাজ করছে।

এই বছরের থিম ***'Own IT. Secure IT. Protect IT.' (তথ্যপ্রযুক্তিকে নিয়ন্ত্রণ করো, নিরাপদ করো, সুরক্ষিত করো)***। অনলাইন নিরাপত্তায় প্রতিটি ব্যক্তিরই যে গুরুত্বপূর্ণ ভূমিকা রয়েছে তার ওপর জোর দেবে এই ক্যাম্পেইন। একইসঙ্গে বাসাবাড়ি ও কর্মস্থলে সাইবার নিরাপত্তা জোরদারে সক্রিয় পদক্ষেপ গ্রহণের ওপরও গুরুত্ব আরোপ করবে। এ লক্ষ্যে অক্টোবর জুড়ে আমরা নানা পরিকল্পনা হাতে নিয়েছি।

আপনি আপনার বন্ধু-বান্ধব, প্রতিবেশী, অফিসের সহকর্মী কিংবা ভ্রমণসঙ্গী, যে কারো সঙ্গে অনলাইনেট নিরাপদ থাকার বিষয়গুলো নিয়ে আলোচনা করতে পারেন। এতে বিষয়গুলো সম্পর্কে অন্যরা যেমনি জানবে তেমনি আপনারও ভালোভাবে রপ্ত হবে। নিচে এই বছরের থিমের বিস্তারিত তথ্যগুলো উল্লেখ করা হলো-

২০১৯ সালের থিম 'Own IT. Secure IT. Protect IT.'
(তথ্যপ্রযুক্তিকে নিয়ন্ত্রণ করো, নিরাপদ করো, সুরক্ষিত করো)

#BeCyberSmart

সাইবার সচেতনতা মাসের (ক্যাম) মূল বার্তা

আমরা এবারের থিমটাকে তিনটি অংশে ভাগ করেছি। মাসজুড়ে সিসিএ ফাউন্ডেশনের উদ্যোগে বিভিন্ন ইভেন্ট ও কার্যক্রম পরিচালনায় সহায়তায় নিম্নে উল্লেখিত মূল বার্তাগুলো উপস্থাপন করা হলো। সাইবার সচেতনতা মাসে ব্যক্তিগতভাবে আপনি যেসব ভূমিকা রাখতে পারেন এমন কিছু সম্ভাব্য বিষয় তুলে ধরা হলো-

'Own IT. (তথ্যপ্রযুক্তিকে নিয়ন্ত্রণ করো)

আপনার ডিজিটাল প্রোফাইল সম্পর্কে বিস্তর ধারণা রাখুন: বাসাবাড়ি, স্কুল-কলেজ, কর্মস্থলসহ আমাদের দৈনন্দিন জীবনযাপনের প্রতিটি ক্ষেত্রে ইন্টারনেটভিত্তিক ডিভাইসের উপস্থিতি রয়েছে। ইন্টারনেটের অবিরাম সংযোগ উদ্ভাবন ও আধুনিকায়নের সুযোগ করে দিচ্ছে। কিন্তু একই সঙ্গে এতে সম্ভাব্য সাইবার নিরাপত্তা হুমকির সুযোগও

তৈরি হয়েছে, যা আপনার সর্বাপেক্ষা গুরুত্বপূর্ণ ব্যক্তিগত তথ্য বেহাত করে দিতে পারে। তাই আপনি দৈনন্দিন যেসব ডিভাইস ও অ্যাপ ব্যবহার করেন সেগুলো সম্পর্কে ভালো ধারণা রাখুন। এটা অনলাইনে আপনি ও আপনার তথ্যকে নিরাপদ ও সুরক্ষিত রাখতে সাহায্য করবে।

আলোচনার সম্ভাব্য টপিকসসমূহ

- প্রাইভেসি (ব্যক্তিগত তথ্য সুরক্ষা) সেটিংস
- সেইফ সোশ্যাল মিডিয়া পোস্টিং - সামাজিক যোগাযোগ মাধ্যমে পোস্ট দেয়ার সময় সতর্ক থাকা।
- ইন্টারনেট অব থিংকস/স্মার্ট টেকনোলজি

Secure IT (তথ্যপ্রযুক্তিকে নিরাপদ করো)

আপনার ডিজিটাল প্রোফাইলকে নিরাপদ করুন: সাইবার অপরাধীরা সরলবিশ্বাসী ভুক্তভোগীদের কাছ থেকে ব্যক্তিগত তথ্য হাতিয়ে নিতে খুবই পারদর্শী। প্রযুক্তি বিকাশের সঙ্গে সঙ্গে তাদের তথ্য হাতিয়ে নেওয়ার কলাকৌশলও আরও জটিল হচ্ছে। আপনার ব্যবহৃত ডিভাইস ও সফটওয়্যারের নিরাপত্তা বৈশিষ্ট্যগুলো সম্পর্কে জানার মাধ্যমে এসব সাইবার হুমকির বিরুদ্ধে সুরক্ষা গড়ে তুলুন। ব্যক্তিগত তথ্য ভালোভাবে সংরক্ষণে আপনার ডিভাইসে মাল্টি-ফ্যাক্টর অথেনটিকেশনের (বহুস্তরের নিরাপত্তা) মতো অধিকতর ব্যবস্থাগুলো প্রয়োগ করুন।

সম্ভাব্য বিষয়সমূহ

- শক্তিশালী পাসওয়ার্ড তৈরি করা
- মাল্টি-ফ্যাক্টর অথেনটিকেশন
- ইকমার্স
- জিরো ট্রাস্ট
- ফিশিং থেকে সুরক্ষা

Protect IT - তথ্যপ্রযুক্তি সুরক্ষিত করো

আপনার ডিজিটাল প্রোফাইল রক্ষণাবেক্ষণ করুন: অনলাইনে করা আপনার প্রত্যেকটি ক্লিক, শেয়ার, সেন্ড ও পোস্টকে সাইবার অপরাধীরা কাজে লাগাতে পারে। তাই সাইবার অপরাধের শিকার হওয়া থেকে নিজেকে রক্ষায় আপনাকে অবশ্যই আপনার ডিজিটাল প্রোফাইল বুঝতে হবে, নিরাপদ করতে হবে এবং তার সঠিক রক্ষণাবেক্ষণ সম্পর্কে জানতে হবে।

সাইবার সচেতনতা মাসে শেয়ার করার মতো অত্যন্ত গুরুত্বপূর্ণ কিছু টিপস তুলে ধরা হলো-

- **লগইনে দুই স্তরের নিরাপত্তা ব্যবস্থা নিশ্চিত করুন:** আপনার অ্যাকাউন্টে আপনি ছাড়া আর কেউ যেন ঢুকতে না পারে সেটা নিশ্চিত করতে মাল্টি-ফ্যাক্টর অথেনটিকেশন (এমএফএ) বা টু ফেক্টর

অথেনটিকেশন (টুএফএ) চালু করে রাখুন। ইমেইল, ব্যাংকিং, সোশ্যাল মিডিয়া ও লগিং করার প্রয়োজন হয় এমন যে কোনো সার্ভিস ব্যবহারে এই সুবিধাটি ব্যবহার করুন। এছাড়া স্মার্টফোনের মতো ট্রাস্টেড মোবাইল ডিভাইস ও অথেনটিকেশন অ্যাপ ব্যবহারের মাধ্যমে শক্তিশালী নিরাপত্তা ব্যবস্থা নিশ্চিত করতে পারেন।

❖ **পাসওয়ার্ড প্রোটকল ঢেলে সাজানো:** ন্যাশনাল ইনস্টিটিউট ফর স্ট্যান্ডার্ড অ্যান্ড টেকনোলজির (এনআইএসটি) নির্দেশনা মতে, প্রত্যেকের দীর্ঘতম পাসওয়ার্ড ব্যবহার করা উচিত। ভিন্ন ভিন্ন সাইটের জন্য ভিন্ন ভিন্ন সৃজনশীল পাসওয়ার্ড ব্যবহার করুন। এটা সাইবার অপরাধীদের আপনার অ্যাকাউন্টে প্রবেশ করা থেকে প্রতিরোধ করবে। এমনকি একটি অ্যাকাউন্টে কোনোভাবে ঢুকতে পারলেও বাকিগুলোতে আপনাকে সুরক্ষিত রাখবে। প্রয়োজনে পাসওয়ার্ড ম্যানেজার ব্যবহার করে প্রতিটি অ্যাকাউন্টের জন্য ভিন্ন ভিন্ন ও জটিল পাসওয়ার্ড তৈরি করুন এবং তা স্মরণে রাখুন।

❖ **ইন্টারনেটে যুক্ত হলেই অবশ্যই সুরক্ষা নিশ্চিত করতে হবে:** কম্পিউটার, স্মার্টফোন, গেম ডিভাইস অথবা অন্যান্য নেটওয়ার্ক ডিভাইস যাই হোক না কেন তাতে ভাইরাস ও ম্যালওয়্যারের বিরুদ্ধে উৎকৃষ্ট প্রতিরক্ষা ব্যবস্থা গড়ে তুলতে হবে। এজন্য সর্বশেষ নিরাপত্তা সফটওয়্যার, ওয়েব ব্রাউজার ও অপারেটিং সিস্টেম আপডেট রাখতে হবে। সম্ভব হলে স্বয়ংক্রিয় আপডেটে সাইন আপ করে রাখুন এবং অ্যান্টি ভাইরাস সফটওয়্যার ব্যবহার করে আপনার ডিভাইস সুরক্ষিত করুন।

❖ **অপরিচিতদের সম্পর্কে অত্যন্ত সতর্ক থাকুন:** সাইবার অপরাধীরা ভুক্তভোগীদের বোকা বানাতে ফিশিং ট্যাক্টিক ব্যবহার করে থাকে। কারো পরিচয় সম্পর্কে নিশ্চিত না হলে তার পাঠানো ইমেইলে ক্লিক করবেন না। এমনকি বিস্তারিত সঠিক মনে হলেও বা ইমেইল 'ফিশিং' বলে মনে হলে তার উত্তর দেবেন না। ইমেইলে পাঠানো কোনো লিংক বা অ্যাটাচমেন্টে ক্লিক করা যাবে না। বিশেষ কোনো প্রেরকের ইমেইল আসা বন্ধ করতে 'জাঙ্ক' বা 'ব্লক' অপশন ব্যবহার করতে হবে।

❖ **ব্যক্তিগত ও স্পর্শকাতর তথ্য দেওয়া থেকে বিরত থাকুন:** ব্যক্তিগত ঠিকানা থেকে শুরু করে কোথায় কফি খেতে পছন্দ করেন সেসব তথ্য সোশাল মিডিয়ায় দেওয়া থেকে বিরত থাকুন। অনেক মানুষ তা উপলব্ধি করে না। আপনাকে, আপনার প্রিয়জন কাউকে অথবা অনলাইন এবং ফিজিক্যাল ওয়ার্ল্ডের কোনো কিছুকে টার্গেট করতে এসব তথ্য অপরাধীদের প্রয়োজন হয়। সামাজিক নিরাপত্তা নাম্বার, অ্যাকাউন্ট নাম্বার ও পাসওয়ার্ড গোপন রাখুন। সেই সঙ্গে নিজের সম্পর্কে সুনির্দিষ্ট তথ্য গোপন রাখুন। পুরো নাম, ঠিকানা, জন্মতারিখ এমনকি অবসর যাপনের পরিকল্পনার মতো স্পর্শকাতর তথ্য প্রকাশ থেকে বিরত থাকুন। কোনো জায়গায় অবস্থানকালে লোকেশন সার্ভিস বন্ধ রাখুন। নতুবা এই মুহূর্তে আপনি কোথায় আছেন বা কোথায় নেই তা তারা জেনে যাবে।

❖ **আপনার অ্যাপে নজর রাখুন:** সবসময় ইন্টারনেটের সঙ্গে যুক্ত থাকে এমন যন্ত্রপাতি, ডিজিটাল খেলনাসামগ্রী ও ডিভাইস একটি মোবাইল অ্যাপের মাধ্যমে পরিচালিত হয়ে থাকে। আপনার মোবাইল

ডিভাইস সন্দেহজনক অ্যাপে পরিপূর্ণ থাকতে পারে। এসব অ্যাপ ব্যাকগ্রাউন্ডে চালু করা থাকতে পারে। অথবা আগে থেকেই কিছু বিষয়ে অনুমতি (ডিফল্ট পারমিশন) নেওয়া থাকে। অথচ আপনি তার খবরই রাখেন না। ফলে আপনার অজান্তে আপনার ব্যক্তিগত তথ্য সংগ্রহ করা হচ্ছে এবং তা হাতিয়ে নেওয়া হচ্ছে। এটা আপনার পরিচিতি ও প্রাইভেসিকে (ব্যক্তিগত তথ্যের সুরক্ষা) ঝুঁকিতে রেখেছে। তাই আপনি আপনার মোবাইলের অ্যাপ পারমিশন ভালো করে যাচাই করে দেখুন। আপনার যেসব অ্যাপ প্রয়োজন নেই এবং যেগুলো আপনি আর ব্যবহার করেন না সেগুলো মুছে ফেলুন। আর কেবল বিশ্বস্ত ভেন্ডরস ও উৎস থেকে অ্যাপ ডাউনলোড করবেন।

- **ইন্টারনেটে যুক্ত থাকার সময় সুরক্ষিত থাকুন:** বিমানবন্দর, হোটেল বা ক্যাফের মতো পাবলিক ওয়ারলেস হটস্পটে যুক্ত হওয়ার আগে ওই নেটওয়ার্কটি বৈধ কর্তৃপক্ষের কি না তা নিশ্চিত হোন। এজন্য নেটওয়ার্কের নাম ও সঠিক লগইন প্রক্রিয়া যথাযথ কর্মকর্তাদের কাছ থেকে নিশ্চিতভাবে জেনে নিন। আর যদি আপনি অনিরাপদ পাবলিক ইন্টারনেট ব্যবহার করেন সেক্ষেত্রে ভালো 'ইন্টারনেট স্বাস্থ্যবিধির' চর্চা করুন। যেখানে পাসওয়ার্ড ও ক্রেডিট কার্ডের প্রয়োজন হয় সেখানে ব্যাংকিংয়ের মতো স্পর্শকাতর কর্মকাণ্ড পরিচালনা থেকে বিরত থাকুন। ফ্রি ওয়াই-ফাই এর চেয়ে বিকল্প হিসেবে ব্যক্তিগত হটস্পট নিরাপদ। অনলাইন শপিং ও ব্যাংকিংয়ের সময় যেসব সাইট https:// দিয়ে শুরু হয়েছে কেবল সেগুলো ব্যবহার করুন।

আরো বিস্তারিত জানতে ভিজিট করুন: CCABD.ORG/RESOURCE