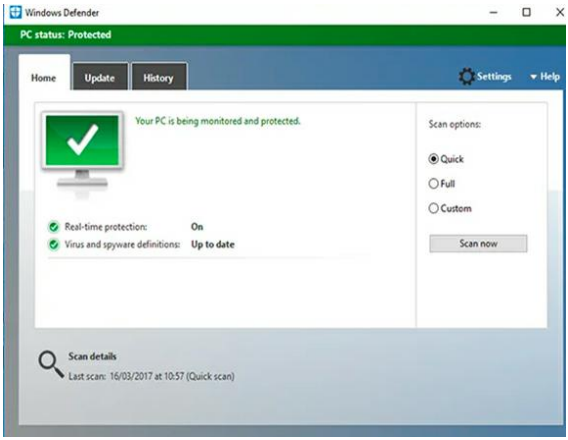
সাইবার স্বাস্থ্যবিধির হ্যান্ডবুক

সাইবার সিকিউরিটি সেন্টার অফ এক্সেলেন্স (সিএস-সিওই)
তথ্য প্রযুক্তি ও বৈদ্যুতিন বিভাগ
পশ্চিমবঙ্গ সরকার
https://cscoe.itewb.gov.in

সাধারণ কম্পিউটার ব্যবহার

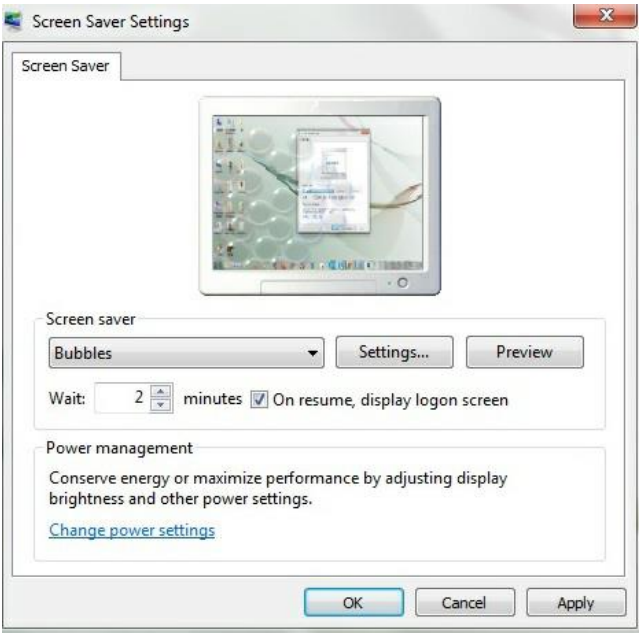
১। পাসওয়ার্ড কমপক্ষে ১০-টি ক্যারেক্টার-বিশিষ্ট হওয়া আবশ্যক যেটি অবশ্যই অক্ষর, সংখ্যা এবং বিশেষ ক্যারেক্টারের সমন্বয়ে তৈরি হবে।

২। অ্যান্টিভাইরাসের ব্যবহার আবশ্যিক। অ্যান্টিভাইরাস অবশ্যই নির্দিষ্ট যন্ত্রের জন্য উপযুক্ত মূল্যে কেনা এবং লাইসেন্সবিশিষ্ট সফটওয়ার এপ্লিকেশন হতে হবে। বিনামুল্যে উপলব্ধ অ্যান্টিভাইরাস সফটওয়ার ইন্সটল করা যাবে না।



৩। কম্পিউটার ছেড়ে ওঠার সময় [উইন্ডোজ + এল] অথবা [কনট্রোল + অল্ট + ডেল] কি চেপে কম্পিউটারটি লগঅফ করতে হবে।

৪। স্ক্রিনসেভার দুই মিনিটের টাইম-আউট পিরিয়ড সহ সক্রিয় রাখতে হবে।

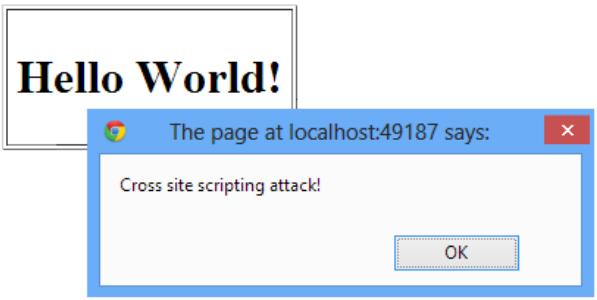


৫। বিশ্বাসযোগ্য এবং বৈধ উৎস হলেও অপ্রয়োজনীয় প্রোগ্রাম ডাউনলোড করবেন না।

৬। অফিসের কাজে সাধারণের ব্যবহৃত অথবা সাইবার ক্যাফের কম্পিউটার ব্যবহার করবেন না।

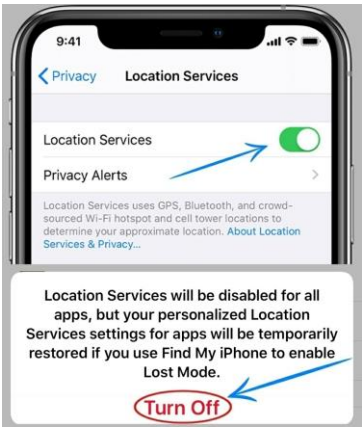
৭। গোপনীয় এবং সুরক্ষিত ডকুমেন্ট-এর জন্য পাসওয়ার্ড সুরক্ষাব্যবস্থা সক্রিয় রাখতে হবে।

৮। উপযুক্ত উৎস থেকে পেলেও বিশ্বাসযোগ্য নয় এমন লিংকে ক্লিক করা বাঞ্ছনীয় নয়। উদাহরণস্বরূপ: ক্রিকেট খেলার স্কোর দেখানো ওয়েবসাইট বা বিমানের টিকিট বুকিং পেজ।



৯। সর্বদা সবুজ অথবা ধূসর প্যাডলকবিশিষ্ট "https" ব্যবহার করুন। যদি তা হলুদ বা লাল রঙের হয়, তবে বুঝতে হবে যে ওই ওয়েবসাইটটি সুরক্ষিত নয়।

১০। ভ্রমণকালীন সময়ে এমন কোনো পরিসেবা ব্যবহার করবেন না যাতে আপনার লোকেশন প্রয়োজন পড়ে।



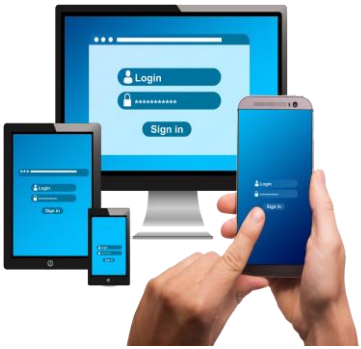
১১। সাধারণ মানুষের ব্যবহৃত কম্পিউটার বা পাসওয়ার্ড মুক্ত ওয়াইফাই কানেকশনের সাহায্যে অর্থনৈতিক লেনদেন করবেন না। এতে আপনার তথ্য অবিশ্বাসযোগ্য ও অপরিচিত সাধারণ জনগণ পড়ে নিতে পারে।

পাসওয়ার্ড ব্যবস্থাপনা

১২। অন্যের সামনে পাসওয়ার্ড দেবেন না। যদি মনে হয় আপনার পাসওয়ার্ডের গোপনীয়তা নষ্ট হয়েছে, তাহলে সঙ্গে সঙ্গে সেটি পরিবর্তন করুন।

১৩। সন্দেহজনক কার্যকলাপ (যথা— ধীরগতির সিস্টেম, ডেস্কটপ বা সফটওয়ার এপ্লিকেশনে অপরিচিত উৎস থেকে অপরিচিত কোনো ফাইলের ইন্সটলেশন) আইটি টিমের কাছে রিপোর্ট করুন।

১৪। পুরোনো পাসওয়ার্ড পুনরায় ব্যবহার করবেন না। সামাজিক ইঞ্জিনিয়ারিং অথবা কি-লগ প্যাটার্ন পর্যবেক্ষণ করে আগে ব্যবহৃত পাসওয়ার্ডকে ক্র্যাক করা সহজ।

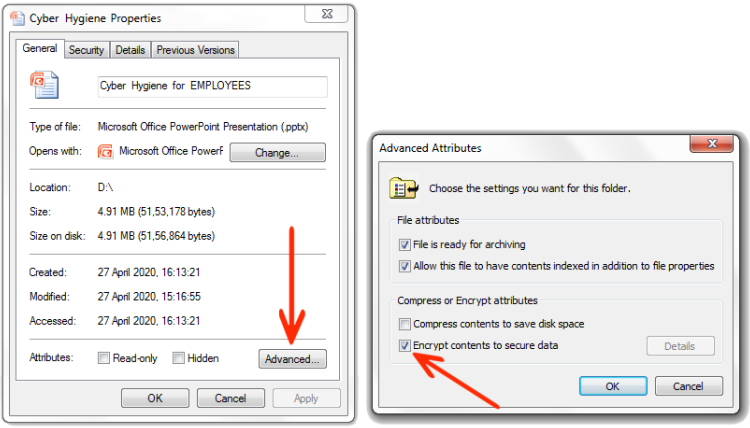


১৫। কম্পিউটার, নোটবুক অথবা নোটিসবোর্ডে পাঠযোগ্য উপায়ে পাসওয়ার্ড সংরক্ষণ করবেন না।

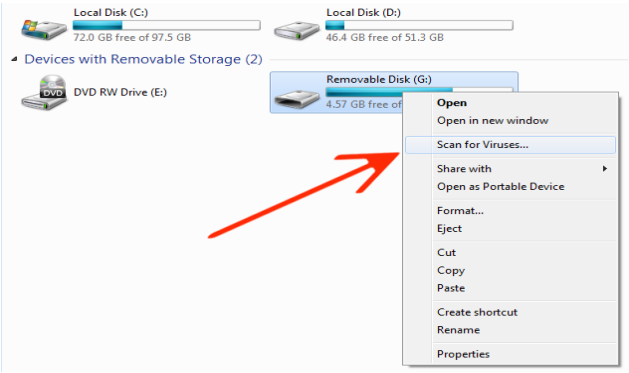
১৬। প্রচলিত প্রথায় পাসওয়ার্ড, যেমন- পরিবারের নাম, পোষ্যের নাম, বন্ধুর নাম, জন্মদিন ইত্যাদি, ব্যবহার করবেন না।

রিমুভেবল ইনফরমেশন স্টোরেজ মিডিয়া

১৭। কোনো স্টোরেজ মিডিয়াতে কপি করার আগে তথ্যকে এনক্রিপ্ট করুন।



১৮। যে মিডিয়া ফাইলগুলি মেশিন থেকে পৃথক করা সম্ভব সেগুলিকে অ্যান্টিভাইরাস ব্যবহার করে স্ক্যান করুন।



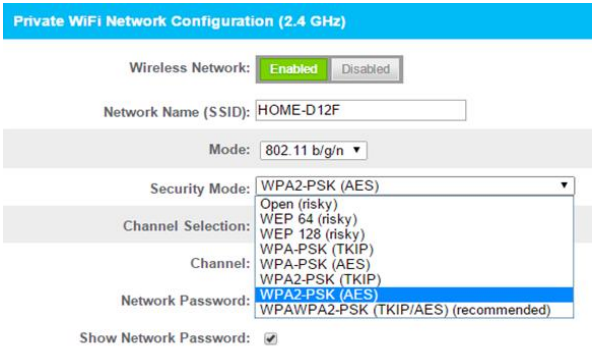
পাবলিক টার্মিনাল

১৯। আন্তর্জালের মাধ্যমে লেনদেনের সময় অন্যকে আপনার পিছন থেকে উঁকি দিতে দেবেন না।

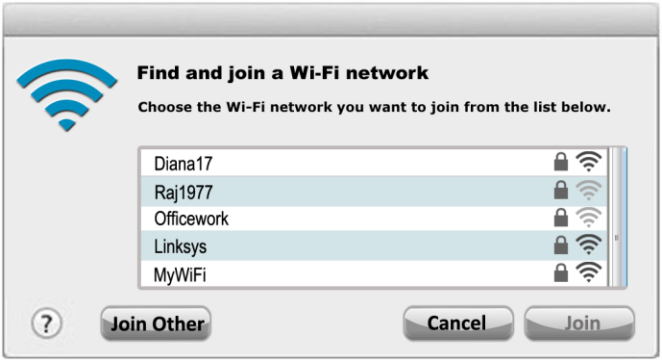
২০। ডেস্কের উপর ব্যক্তিগত তথ্য অথবা গোপনীয় তথ্য সমন্বিত ফাইল ফেলে রাখবেন না। স্থানত্যাগের পূর্বে ডেস্ক পরিষ্কার করুন, স্ক্রিন লক করুন এবং গোপন এবং সুরক্ষিত ডকুমেন্ট সরিয়ে ফেলুন।

ওয়াইফাই নেটওয়ার্ক

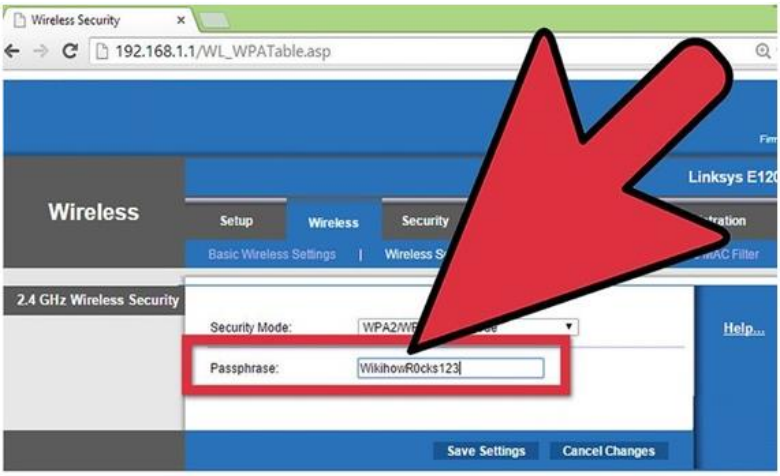
২১। তারবিহীন রাউটার বা অন্যান্য যন্ত্রের জন্য WPA2 অথবা উচ্চতর এনক্রিপশন ব্যবহার করুন।



২২। নিজের পরিচয় প্রকাশ করবেন না; ডিফল্ট নেটওয়ার্ক ডিভাইসের এবং সার্ভিস সেট আইডেন্টিফায়ারের নাম নিয়মিত পরিবর্তন করুন।



২৩। নেটওয়ার্ক ডিভাইস অর্থাৎ যন্ত্রের ডিফল্ট নামটি পরিবর্তন করুন।



২৪। ম্যাক আইডি ফিল্টারটি সক্রিয় করে অননুমোদিত অ্যাক্সেস এড়িয়ে চলুন।

সামাজিক যোগাযোগ মাধ্যম ব্যবহার

২৫। সমস্ত সরকারি চাকুরিজীবী, চুক্তির ভিত্তিতে নিযুক্ত কর্মী এবং প্রকল্পের সঙ্গে যুক্ত ব্যক্তিরা সামাজিক যোগাযোগ মাধ্যমে অথবা অ্যাপ্লিকেশনে দপ্তর সংক্রান্ত তথ্য প্রকাশ করবেন না।

সোশ্যাল ইঞ্জিনিয়ারিং আক্রমণ প্রতিরোধ

২৬। অবিশ্বাসযোগ্য অথবা অননুমোদিত মিটিং, ফোন বা ইমেলের মাধ্যমে সরকারি তথ্য প্রকাশ অথবা ভাগ করে নেবেন না। অনেকসময় আক্রমণকারী বিশ্বাসযোগ্যতা অর্জন করে গোপনীয় দাপ্তরিক তথ্য হাতিয়ে নিয়ে তথ্যের অপব্যবহার করতে পারে।

২৭। ফিশিং অ্যাটাক এড়িয়ে যান—অবিশ্বাসযোগ্য ইমেল খুলবেন না। এমন কোনো ইমেল অ্যাটাচমেন্ট খুলবেন না যা বর্তমান কোনো সরকারি কমিউনিকেশনের জন্য অপ্রাসঙ্গিক। যদি কোনো মেসেজ বা ইমেল-এ জরুরি পরিস্থিতির অবস্থা জানানো হয় অথবা যদি তা কোনো চাপ সৃষ্টি করে বিক্রয়ের কৌশল বলে মনে হয়, তাহলে

কোনো লিংকে ক্লিক করা অথবা অ্যাপ্লিকেশন খোলার সময় সতর্ক থাকুন।

২৮। ভিশিং অ্যাটাক এড়িয়ে চলুন। যদি কোনো উৎস সম্পূর্ণ যাচাই করা ও বিশ্বাসযোগ্য না হয়, তবে ফোন কলের মাধ্যমে গোপন ও সংরক্ষিত তথ্য প্রকাশে বিরত থাকুন। এমন কোনো তথ্য বা সংখ্যা জিজ্ঞাসা করুন যা যাচাই করে নেওয়া সম্ভব; যেমন, উচ্চপদস্থ ব্যক্তির নাম (যদি ফোন করা ব্যক্তি সরকারি দপ্তরের কর্মী সেজে ফোন করে থাকেন)। কোনো গুরুত্বপূর্ণ তথ্য দেওয়ার আগে ফোন করা ব্যক্তির পরিচয় সম্পর্কে সম্পূর্ণ নিশ্চিত হওয়ার চেষ্টা করুন।

২৯। মধুচক্র অথবা *কুইড প্রো কুও* দুর্নীতি সম্পর্কে সতর্ক থাকুন। এখানে আক্রমণকারী প্রকৃত ব্যক্তির ছদ্মবেশে তথ্য অপহরণের চেষ্টা করে।

৩০। অপরিচিত উৎস থেকে আগত ফোন, মেসেজ, ইমেল ইত্যাদির মাধ্যমে আসা বিদেশি লটারির পুরষ্কার, বেদেশ থেকে আসা তহবিল ট্রান্সফারের প্রস্তাব এড়িয়ে চলুন। এগুলি দুর্নীতির মাধ্যমে আপনার কাছ থেকে অর্থ অথবা তথ্য অপহরণের উপায়।

আরো কিছু ডোমেন-নির্দিষ্ট ব্যাবহারিক সচেতনতা

সাধারণ কম্পিউটার ব্যবহার:

১। স্ক্রিনে গোপনীয় এবং সুরক্ষিত তথ্য খোলা থাকা অবস্থায় কম্পিউটার ছেড়ে যাবেন না।

২। [উইন্ডোজ+এল] অথবা [কন্ট্রোল+অল্ট+ডেল] কি ব্যবহার করে কম্পিউটার লক করে তবেই কম্পিউটার ছেড়ে উঠুন।

৩। অপ্রয়োজনীয় প্রোগ্রাম ডাউনলোড করবেন না।

৪। অফিসের কাজে সাধারণের ব্যবহৃত অথবা সাইবার ক্যাফের কম্পিউটার ব্যবহার করবেন না।

৫। [শিফট+ডিলিট] কি ব্যবহার করে পাবলিক কম্পিউটার ব্যবহার করে ডাউনলোড করা সব ডকুমেন্ট ডিলিট করুন।

সাধারণ ইন্টারনেট ব্রাউজিং:

৬। সব সময় পূর্বে ইন্সটল করা ও আপডেটেড ওয়েব ব্রাউজার ব্যবহার করুন।

৭। ইন্টারনেট সংযোগ আছে এমন কম্পিউটারে কোনো তথ্য সঞ্চয় অথবা আদানপ্রদান করবেন না।

৮। ব্রাউজার চাইলেও ‘সেভ পাসওয়ার্ড’ অপশন সিলেক্ট করবেন না।

৯। ব্রাউজিং-এর সময় পপ আপ ব্লকার সবসময় সক্রিয় রাখুন।

১০। সাধারণ মানুষের ব্যবহৃত কম্পিউটার বা পাসওয়ার্ড মুক্ত ওয়াইফাই কানেকশনের সাহায্যে অর্থনৈতিক লেনদেন করবেন না।

পাসওয়ার্ড ব্যবস্থাপনা:

১১। ন্যূনতম দশ ক্যারেক্টার বিশিষ্ট শক্তিশালী পাসওয়ার্ড ব্যবহার করুন, যা অক্ষর, সংখ্যা এবং বিশেষ ক্যারেক্টারের সমন্বয়ে গঠিত।

১২। বিভিন্ন অ্যাকাউন্টের জন্য বিভিন্ন পাসওয়ার্ড ব্যবহার করুন। একটি একাউন্ট হ্যাক্ড হলেও অন্য অ্যাকাউন্টগুলি সুরক্ষিত থাকবে।

১৩। পাসওয়ার্ড হ্যাক্ড হয়েছে বলে সন্দেহ হলে তৎক্ষণাৎ পাসওয়ার্ড পরিবর্তন করুন।

১৪। রিমেম্বার পাসওয়ার্ড অপশনটি বেছে নেবেন না।

রিমুভেবল ইনফরমেশন স্টোরেজ মিডিয়া:

১৫। রিমুভেবল মিডিয়া ফাইলকে অনুমতি ব্যতীত অফিসের বাইরে নেবেন না।

১৬। ব্যবহারের পর রিমুভেবল মিডিয়ার কনটেন্টগুলি ডিলিট করুন।

পাবলিক টার্মিনাল:

১৭। পাবলিক কম্পিউটারে সমস্ত ব্রাউজারগুলি বন্ধ না করে এবং অ্যাকাউন্ট থেকে লগ আউট না করে পাবলিক কম্পিউটার বন্ধ করবেন না।

ওয়াইফাই নেটওয়ার্ক:

১৮। তারবিহীন যন্ত্রের ফার্মওয়্যার নিয়মিত আপডেট করুন।

১৯। অননুমোদিত অ্যাক্সেস প্রতিরোধ করার জন্য রাউটারের রিমোট ম্যানেজমেন্ট ফিচারটি নিষ্ক্রিয় রাখুন।

সোশ্যাল ইঞ্জিনিয়ারিং আক্রমণ প্রতিরোধ:

২০। অবিশ্বাসযোগ্য ইউআরএল-এ ক্লিক করবেন না। কোনো লিংকে ক্লিক করার আগে "http" আইকনের শংসাপত্রের ভ্যালিডিটি চেক করুন।

২১। যদি কোনো মেসেজ বা ইমেল–এ জরুরি পরিস্থিতির অবস্থা জানানো হয় অথবা যদি তা চাপ সৃষ্টি করে বিক্রয়ের কৌশল বলে মনে হয়, তাহলে কোনো লিংকে ক্লিক করা অথবা অ্যাপ্লিকেশন খোলার সময় সতর্ক থাকুন।

২২। অপরিচিত উৎস থেকে আগত ফোন, মেসেজ ইমেল ইত্যাদির মাধ্যমে আসা বিদেশি লটারির পুরষ্কার, বিদেশ থেকে আসা তহবিল ট্রান্সফারের প্রস্তাব এড়িয়ে চলুন।

২৩। কোনো কারণে কারো কাছে আপনার নিজস্ব পাসওয়ার্ড প্রকাশ করে থাকলে তা তৎক্ষণাৎ পরিবর্তন করুন।

সোশাল ইঞ্জিনিয়ারিং আক্রমণ প্রতিরোধ:

২৪। মোবাইল বা কম্পিউটারে অ্যান্টিভাইরাস ইন্সটল করা আছে কিনা নিশ্চিত করুন।

২৫। মোবাইল বা নেট ব্যাংকিং-এর ক্রেডেন্সিয়াল প্রকাশ করবেন না।

২৬। সুরক্ষিত পাসওয়ার্ড ব্যবহার করুন, যা কারও পক্ষে আন্দাজ করা কঠিন। পাসওয়ার্ডটি অক্ষর, সংখ্যা এবং বিশেষ ক্যারেক্টারের সমন্বয়ে গড়ে তুলুন।

২৭। নেট ব্যাংকিং একাউন্টে প্রবেশের জন্য ভার্চুয়াল কি-প্যাড ব্যবহার করুন।

২৮। মোবাইল ব্যাংকিং-এর জন্য আপনার ব্যাংকের যাচাইকৃত এপ্লিকেশন ব্যবহার করুন।

২৯। মোবাইল ব্যাংকিং-এর জন্য এমন কিছু সাধারণ পিন ব্যবহার করবেন না যা সহজে আন্দাজ করা যায়।

৩০। সন্দেহজনক ইমেল আইডি থেকে আসা ফিশিং ইমেল সম্পর্কে সচেতন থাকুন।

৩১। প্যাডলকে থাকা “http” চিহ্নটি সবুজ কিনা নিশ্চিত করুন, তা যেন হলুদ বা লাল বর্ণের না হয়।

৩২। পাবলিক ওয়াইফাই ব্যবহার করে নেট ব্যাংকিং করবেন না।

৩৩। ক্যাফে বা সাধারণের জন্য উন্মুক্ত কম্পিউটার ব্যবহার করে নেট ব্যাংকিং করবেন না।

৩৪। আর্থিক লেনদেনের ক্ষেত্রে কোনো প্রতারণার স্বীকার হলে ফোন এবং ইমেলের মাধ্যমে ব্যাংকে জানান।

ইমেলের সুরক্ষিত ব্যবহার:

৩৫। ইমেলের লগইন ক্রেডেন্সিয়ালগুলি কারও সাথে ভাগ করবেন না।

৩৬। সাধারণ বা একাধিক ব্যাক্তির ব্যবহৃত সিস্টেম ব্যবহার করার সময় সিস্টেম থেকে লগআউট করতে ভুলবেন না।

৩৭। পাসওয়ার্ড ব্যবহার করুন।

৩৮। যিনি মেল পাঠাচ্ছেন তাঁর নাম ও ইমেল অ্যাড্রেস যাচাই করুন।

৩৯। যদি ইমেল অ্যাড্রেসটি সন্দেহজনক বা অবিশ্বাসযোগ্য মনে করেন, তাহলে কোনো অ্যাটাচমেন্ট বা লিংকে ক্লিক করবেন না।

৪০। লটারি জেতার বা বেওয়ারিশ সম্পত্তির প্রলোভন দেখানো কোনো লিংকে ক্লিক করবেন না।

৪১। ইমেলের মাধ্যমে কারও সাথে ডেবিট বা ক্রেডিট কার্ড অথবা নেট ব্যাংকিং-এর ডিটেল্‌স ভাগ করে নেবেন না।

সামাজিক মাধ্যমের সুরক্ষিত ব্যবহার:

৪২। একটি সামাজিক যোগাযোগ মাধ্যমের জন্য একটি নির্দিষ্ট একাউন্ট ব্যবহার করুন।

৪৩। লগইন ক্রেডেন্সিয়াল কাউকে দেবেন না।

৪৪। সামাজিক যোগাযোগ মাধ্যমের বাইরেও পরিচয় রয়েছে কেবলমাত্র এমন ব্যক্তিকেই যোগ করুন এবং বার্তা আদানপ্রদান করুন।

৪৫। অনেক প্রোফাইল সামাজিক যোগাযোগ মাধ্যমে থাকে যেগুলি নকল এবং সামাজিক ইঞ্জিনিয়ারিং-এর মাধ্যমে তথ্য আহরণের জন্য তৈরি করা হয়।

৪৬। কোনো ব্যক্তিগত তথ্য বা গোপনীয় নিজস্ব তথ্য বার্তামাধ্যমের মাধ্যমে জ্ঞাপন করবেন না।

৪৭। বিপরীত লিঙ্গের আকর্ষক প্রোফাইল থেকে দূরে থাকুন। এদের কাছে ব্যক্তিগত তথ্য প্রকাশ করবেন না। যাচাই না করে এই সমস্ত প্রোফাইলকে অ্যাড অথবা তাদের সাথে বার্তালাপের চেষ্টা করবেন না।

সামাজিক যোগাযোগ মাধ্যম ব্যবহার করে ভুয়ো খবর ছড়িয়ে দেওয়া:

৪৮। সামাজিক যোগাযোগ মাধ্যম ব্যবহার করে সবসময় ভুয়ো খবর ও ছবি ছড়িয়ে দেওয়া হয়।

৪৯। অন্যান্য সমস্ত সূত্র যাচাই না করে সামাজিক যোগাযোগ মাধ্যমে পাওয়া কোনো ছবি, ভিডিও বা খবর সত্য বলে ধরে নেবেন না।

৫০। হোয়াটস অ্যাপ ও ফেসবুকে ভুয়ো খবর ছড়িয়ে অনেক অনভিপ্রেত জনরোষ ও লাঞ্ছনার ঘটনা ঘটেছে।

৫১। সত্যতা যাচাই না করে যদি কোনো বিতর্কিত ছবি, ভিডিও বা খবর ফরোয়ার্ড করলে আপনি অপরাধের জন্য দোষী সাব্যস্ত হতে পারেন।

ডেবিট ও ক্রেডিট কার্ডের সুরক্ষিত ব্যবহার:

৫২। ক্রেডিট বা ডেবিট কার্ড নাম্বার, সিভিভি বা পিন কাউকে বলবেন না।

৫৩। বৈদ্যুতিন মাধ্যমে পেমেন্ট করার সময় সবুজ প্যাডলক ও “http” চিহ্ন সক্রিয় রয়েছে কিনা দেখে নিন। যাচাই না করে কোনো পোর্টাল, অ্যাপ্লিকেশন বা ওয়েবসাইটে কার্ডের ডিটেলস দেবেন না।

৫৪। এটিএম বা পিওএস মেশিনে কার্ড ব্যবহারের সময় মেশিনটি বিকৃত করা হয়েছে কিনা দেখে নিন।

৫৫। আপনার ব্যাংকের ডেবিট ও ক্রেডিট কার্ড সংক্রান্ত নির্দেশাবলি পড়ে নিন।

৫৬। কোনো অবৈধ লেনদেনের সন্দেহ হলে ফোন ও ইমেলের মাধ্যমে ব্যাংকে জানান।

৫৭। কার্ডের পিন, সিভিভি ইত্যাদি নাম্বার যদি কেউ ব্যাংক কর্মী সেজে দাবি করে জানতে চায় তাহলেও বলবেন না।

৫৮। কার্ডের কোনো ছবি কোথাও পাঠাবেন না বা কোথাও জমিয়ে রাখবেন না।

৫৯। কোনো আর্থিক লেনদেনের জন্য কার্ডের পিন কোনো কাগজে লিখবেন না, বা কোথাও কারো কাছে প্রকাশ করবেন না।

৬০। কার্ড হারিয়ে গেলে বা চুরি হয়ে গেলে তৎক্ষণাৎ ব্যাংকে জানিয়ে কার্ড ব্লক করুন এবং যত তাড়াতাড়ি সম্ভব পুলিশে অভিযোগ জানান।

ল্যাপটপ বা মোবাইলের সুরক্ষিত ব্যবহার:

৬১। সবসময় আসল সফটওয়্যার এবং অপারেটিং সিস্টেম ব্যবহার করুন।

৬২। ল্যাপটপ বা মোবাইলে সর্বদা পাসওয়ার্ড ব্যবহার করুন।

৬৩। লাইসেন্সযুক্ত অ্যান্টিভাইরাস সফটওয়্যার ব্যবহার করুন।

৬৪। নিয়মিত ব্যবহার করেন না এমন এপ্লিকেশন বা সফটওয়্যার রাখবেন না।

৬৫। কাউকে বিশেষত অবিশ্বাসী লোকের হাতে মোবাইল বা ল্যাপটপ দেবেন না।

৬৬। নিয়মিত ল্যাপটপ বা মোবাইলে ভাইরাস স্ক্যান করুন।

৬৭। যে এপ্লিকেশন বা সফটওয়ার ব্যবহার করছেন সেগুলির নিয়মিত আপডেট সুনিশ্চিত করুন।

৬৮। সুরক্ষিত ও গ্রহণযোগ্য উপায়ে ইন্টারনেট পরিসেবা ব্যবহার করুন।

৬৯। স্বীকৃত ব্রাউজ়ার যেমন- গুগল ক্রোম, মোজ়িলা ফায়ারফক্স, ইন্টারনেট এক্সপ্লোরার ইত্যাদি ব্যবহার করে ব্রাউজিং করুন।

৭০। অননুমোদিত বা বেআইনি ওয়েবসাইট ব্যবহার করবেন না।

৭১। উৎস এবং তার কন্টেন্ট যাচাই না করে কোনো সন্দেহজনক লিংকে ক্লিক করবেন না।

৭২। সবুজ প্যাডলকে “https” লেখা কিনা যাচাই করুন যাতে আপনি কোনো নকল ওয়েবসাইটে পৌঁছে না যান।

৭২। টরেন্ট ব্যবহার করবেন না, কোনো বেআইনি কনটেন্ট ডাউনলোড করবেন না, এটি শাস্তিযোগ্য অপরাধ।

৭৩। সাধারণের ব্যবহৃত কম্পিউটার ব্যবহার করলে আপনার ব্রাউজিং কন্টেন্ট ক্লোজ ও ডিলিট করতে ভুলবেন না।

সাইবার অপরাধ সংক্রান্ত সচেতনতা

সাইবার পরিচয় অপহরণ এবং সাইবার-নকল:

এই সংক্রান্ত অপরাধ ও শাস্তিগুলির মধ্যে রয়েছে

৭৪। অন্যের নামে একটি নকল একাউন্ট খোলা এবং অপরের নাম ও লগইন ক্রেডেন্সিয়ালের অপব্যবহার।

৭৫। ইনফরমেশন টেকনোলজি আইন, ২০০০–এর ৬৬সি ও ৬৬ডি ধারা অনুযায়ী এটি অপরাধ।

৭৬। এই অপরাধ প্রমাণিত হলে তিন বছর জেল এবং সর্বাধিক এক লক্ষ টাকা পর্যন্ত জরিমানা হতে পারে।

কীভাবে রক্ষা পাওয়া যায়

৭৮। পাসওয়ার্ড ব্যবহার করুন।

৭৯। ফিশিং ইমেল চিহ্নিত করে এড়িয়ে চলুন।

৮০। নিরাপদ নেট ব্যাংকিং ও মোবাইল ব্যাংকিং ব্যবহার করুন।

৮১। ক্রেডিট ও ডেবিট কার্ডের পিন যাতে গোপন থাকে তা সুনিশ্চিত করতে হবে।

৮২। সুরক্ষিত উপায়ে সামাজিক যোগাযোগ মাধ্যম ব্যবহার করুন।

অশ্লীল কনটেন্ট পাঠানো ও প্রকাশ

অপরাধ ও শাস্তি:

৮৩। ইনফরমেশন টেকনোলজি আইন, ২০০০-এর ৬৭ ও ৬৭এ ধারা অনুযায়ী এটি অপরাধ।

৮৪। ৬৭ ধারা অনুযায়ী অশ্লীল কনটেন্ট পাঠালে তিন বছর জেল ও পাঁচ লাখ টাকা পর্যন্ত জরিমানা হতে পারে।

৮৫। ৬৭এ ধারা অনুযায়ী অশ্লীল কনটেন্ট ছাপা হলে পাঁচ বছর জেল ও দশ লাখ টাকা পর্যন্ত জরিমানা হতে পারে।

কীভাবে এড়ানো যায়:

৮৬। কাউকে অশ্লীল বা অবমাননাকর এমন কিছু পাঠাবেন না যা কোনো ব্যক্তি বা গোষ্ঠীর উপর বিরূপ প্রভাব ফেলে।

৮৭। মেসেঞ্জার বা হোয়াটস আপে কোনো নির্বিচার যৌনতা প্রকাশক জিনিস পাঠাবেন না।

৮৮। সেই মেসেজগুলি তৎক্ষণাৎ ডিলিট করবেন যাতে অনিচ্ছাকৃত ফরোয়ার্ড না হয়।

৮৯। নিরাপদ ব্রাউজ়ি অভ্যাস করুন।

ব্যক্তির সম্মতি ছাড়াই গোপনাঙ্গের ছবি তোলা, প্রকাশ ও আদানপ্রদানের মাধ্যমে ব্যক্তিগত পরিসরে হস্তক্ষেপ:

৯০। ইনফরমেশন টেকনোলজি আইন, ২০০০-এর ৬৬ই ধারা অনুযায়ী এটি অপরাধ।

৯১। তিন বছর জেল ও দুই লাখ টাকা পর্যন্ত জরিমানা হতে পারে।

৯২। শিশু পর্নোগ্রাফি— যৌন হয়রানি, ভিডিও ক্লিপ তোলা, প্রকাশ ও আদানপ্রদান অথবা এগুলির কোনো একটি আঠারোর কম বয়সী কারো উপর করলে ইনফরমেশন টেকনোলজি আইন, ২০০০-এর ৬৭বি ধারায় তা অপরাধ বলে গণ্য হয়।

৯৩। ৬৭বি ধারায় প্রথম অপরাধের ক্ষেত্রে পাঁচ বছর জেল ও দশ লাখ টাকা পর্যন্ত জরিমানা এবং পুনরাবৃত্তি হলে সাত বছর জেল ও দশ লাখ টাকা জরিমানা হতে পারে।

কীভাবে এড়ানো যায়:

৯৪। নিজের গোপনাঙ্গের ছবি নিজে তুলবেন না বা কাউকে তুলতে দেবেন না।

৯৫। অন্য কারো শরীরের গোপনাঙ্গের ছবি তুলবেন না।

৯৬। পাবলিক স্পেস যথা মলের ট্রায়ালরুমে সম্ভাব্য ক্যামেরার উপস্থিতি সম্পর্কে সচেতন থাকুন।

৯৭। কেউ যতই বিশ্বাসী হোক তাকে নিজের গোপনাঙ্গের ছবি বা ভিডিও তুলতে দেবেন না।

সাইবার সন্ত্রাস, একতা, প্রতিরক্ষা ও ভারতের সার্বভৌমত্বের পক্ষে ক্ষতিকারক

৯৮। ইনফরমেশন টেকনোলজি আইন, ২০০০–এর ৬৬এফ ধারা অনুযায়ী সাইবার সন্ত্রাসপ্রাধ; এতে যাবজ্জীবন কারাবাস হতে পারে।

৯৯। নাম থেকে বোঝা যায়, সাইবার সন্ত্রাস কম্পিউটার সংক্রান্ত রিসোর্সের অপব্যবহার সূচিত করে যা

- কোনো ব্যক্তির মৃত্যু বা আঘাতের জন্য দায়ী হতে পারে।
- সাধারণ মানুষের প্রয়োজনীয় জরুরি পরিসেবা ব্যাহত হতে পারে।
- বৈদেশিক সম্পর্কে নেতিবাচক প্রভাব পড়তে পারে।
- জাতীয় নিরাপত্তা, একতা ও সার্বভৌমত্ব ব্যহত হতে পারে।

নাগরিক-সচেতনতা প্রকল্প:

১০০। যে কোনো সাইবার কার্যকলাপ যা দেশ ও সমাজের একতার পক্ষে ভীতিপ্রদ, তার দিকে সতর্ক দৃষ্টি রাখতে হবে।

অ্যাপ্রুভার ও মিড লেভেল অফিসারদের কর্তব্য ও অকর্তব্যের নির্দেশ

১। সব ক্লাসিফায়েড কাজ একটি একক কম্পিউটার ব্যবহার করে করতে হবে।

২। গুরুত্বপূর্ণ তথ্য ও ফাইলের ব্যাক আপ রাখতে হবে।

৩। রিমোট অ্যাক্সেস বা রিমোট ফাইল শেয়ারিং অপশন সক্রিয় রাখা যাবে না।

৪। নিরাপদ লাইফ পার্জিং-এর জন্য নিরাপদ ডিলিশন সফটওয়ার ব্যবহার করতে হবে।

৫। জনসাধারণের জন্য উন্মুক্ত কম্পিউটারে প্রাইভেট ব্রাউজিং অন রাখতে হবে।

৬। গুগল ড্রাইভ, ড্রপ বক্স অথবা আই ক্লাউডের মতো বেসরকারি ক্লাউড সার্ভিসে তথ্য সংরক্ষণ করা চলবে না।

৭। সংস্থা থেকে দেওয়া রিমুভেবল স্টোরেজ মিডিয়াতেই কেবলমাত্র তথ্য সংরক্ষণ করতে হবে।

৮। পাবলিক কম্পিউটার প্রয়োজনে রিবুট করতে হবে।

৯। ব্যবহারের পর ক্যাশ ফাইল পরিষ্কার করতে হবে।

১০। তারবিহীন যন্ত্রের ফার্মওয়্যার নিয়মিত আপডেট করতে হবে।

১১। অননুমোদিত অ্যাক্সেস পরিহার করতে রাউটার থেকে রিমোট ম্যানেজমেণ্ট ফিচার নিষ্ক্রিয় রাখতে হবে।

সিস্টেম ও নেটওয়ার্ক অ্যাডমিনিস্ট্রেটরদের কর্তব্য ও অকর্তব্য

১। একাউন্ট ম্যানেজমেন্ট-এর মাধ্যমে অ্যাডমিনিস্ট্রেটর লগইন নিয়ন্ত্রণে রাখতে হবে।

২। সব সিস্টেমে সফটওয়্যার প্যাচ নিয়মিত আপডেট করুন।

৩। অ্যাডমিনিস্ট্রেটর-এর কাজের জন্য বিল্ট-ইন উইন্ডোজ় অ্যাডমিনিস্ট্রেটর একাউন্ট ব্যবহার করবেন না।

৪। সার্ভিস একাউন্ট হিসেবে জেনেরিক বা নর্মাল একাউন্ট ব্যবহার করবেন না।

৫। সিস্টেম রিবুট করবেন না যদি

- না জানেন কে লগ ইন করেছে
- সিস্টেম মনিটর সাসপেন্ড না করলে।

৬। সমস্ত গুরুত্বপূর্ণ সিস্টেমে নিয়মিত ব্যাক আপ রাখতে হবে।

৭। লগ ফাইল নিয়মিত দেখে এরর ও ওয়ার্নিং সম্পর্কে অবগত থাকতে হবে।

৮। ইউপিএস বা সার্জ প্রোটেক্টর–এর দ্বারা বিদ্যুৎ সরবরাহ নিয়ন্ত্রণ করতে হবে।

৯। ধুলোভরা পরিবেশে কম্পিউটার সিস্টেম ইন্সটল করবেন না।

১০। শক্তিশালী নিরাপত্তা প্রোটোকল ও পলিসি তৈরি করতে হবে।

১১। কম্পিউটারে 'শো হিডেন ফাইলস অ্যান্ড ফোল্ডার্স' অপশন সক্রিয় করতে হবে।

১২। নির্দিষ্ট ডকুমেনটেশশন সহ একটি ওয়ার্ক-ফ্লো প্রসেস চালু করতে হবে।

১৩। লিখিত অনুমতি ছাড়া কোনো সিস্টেম পরিবর্তন করবেন না।

১৪। যে কাজ শেষ করা যাবে না তার দায়িত্ব নেবেন না। শুক্রবার বিকেলের কাজ সম্পর্কে সতর্ক থাকুন।

১৫। নিয়মিত নিরাপত্তা অডিট ও টেস্ট করান।

১৬। নেটওয়ার্ক ও যন্ত্র নিয়মিত আপডেট করুন।

১৭। নিরাপত্তাহীন সফটওয়ারের ক্ষেত্রে অটোরান বা অটো প্লে ফিচার নিষ্ক্রিয় রাখুন।

১৮। নিম্নলিখিত পলিসি ও পদ্ধতিগুলি তৈরি ও অনুসরণ করুন।

- একটি মোবাইলের নিরাপত্তা পলিসি
- একটি কম্পিউটার ব্যবহার পলিসি
- একটি সামাজিক যোগাযোগ মাধ্যম পলিসি।
- একটি পাসওয়ার্ড পলিসি
- একটি ইমেল পলিসি
- একটি সর্বনিম্ন সুবিধার নিরাপত্তা পলিসি
- একটি বিজনেস কন্টিনিউইটি পরিকল্পনা
- একটি তথ্য ব্যাকআপ ও ডিজ়াস্টার রিকভারি পরিকল্পনা

১৯। ব্যবহারকারীদের আন্দাজ করা কঠিন এমন পাসওয়ার্ড ব্যবহার করার কথা মনে করিয়ে দিন।

২০। নন-অ্যাডমিন উদ্দেশ্যের জন্য অ্যাডমিন একাউন্ট ব্যবহার করবেন না।

২১। পাসওয়ার্ডের ভরসায় নেটওয়ার্ককে ফেলে রাখবেন না।

২২। প্রত্যেক চাকুরিজীবী যাতে নিয়মিত সিকিওরিটি আপডেট পায় তা সুনিশ্চিত করতে হবে।

২৩। অ্যান্টিভাইরাস আপডেটেড রাখুন।

২৪। ইমেল প্রোগ্রামগুলিকে কোনো এটাচমেন্ট অটো ওপেন করতে অনুমতি দেবেন না।

সিস্টেম ও নেটওয়ার্ক অ্যাডমিনিস্ট্রেটরদের কর্তব্য ও অকর্তব্য

একটি নতুন ধরনের জালিয়াতি চলছে যার মাধ্যমে রিমোট কানেকশন পদ্ধতি ব্যবহার করে কোনো ব্যক্তির সমস্ত তহবিল অপহরণ করা যেতে পারে। এটির মাধ্যমে ব্যবহারকারীরা ইন্টারনেট-এর মাধ্যমে একটি কম্পিউটার নেটওয়ার্ক দূর থেকে ব্যবহার করতে পারে। এই দুর্নীতির মধ্যে পড়ে ডিভাইস কন্ট্রোলিং অ্যাপ্লিকেশন যেমন— এনিডেস্ক, টিমভিউয়ার ইত্যাদি কোনো ব্যক্তির ফোনে ইন্সটল করে তার রিমোট অ্যাক্সেস কাজে লাগিয়ে ওটিপি ও অন্যান্য পাসওয়ার্ড হাতিয়ে নেওয়া।

মোডাস অপারেন্ডি:

- প্রতারক ব্যক্তি ব্যাংক ম্যানেজার পরিচয়ে অথবা কোম্পানি এক্সিকিউটিভ-এর ছদ্মবেশে কোনো ব্যক্তিকে ফোন করে কেওয়াইসি, ব্যাংক অ্যাকাউন্টের সঙ্গে ফোন নাম্বার লিংক করার কথা বলে রিমোট কানেকশন ইন্সটল করতে প্রলোভিত করে।

- ওই অ্যাপ্লিকেশন ইন্সটল করলেই প্রতারকেরা কানেকশন এনাব্‌ল করার জন্য অ্যাপ্লিকেশন আইডি ও পাসওয়ার্ড চেয়ে নেয়।
- ওই কানেকশন সফলভাবে করতে পারলেই প্রতারকরা ওই নির্দিষ্ট ব্যক্তির ডিভাইসটি নিয়ন্ত্রণ করতে পারে।
- অ্যাক্সেস পেলেই প্রতারকরা ওই ব্যক্তির কাজকর্ম নিয়ন্ত্রণ করে অ্যাপ্লিকেশন নাম্বার, পিন, ওটিপি ও অন্যান্য গোপনীয় ও সংরক্ষিত তথ্য রেকর্ড করে বেআইনি লেনদেন করতে পারে।

সতর্কতা:

- রিমোট কন্ট্রোল অ্যাপ্লিকেশন ইন্সটল করাতে চেয়ে কোনো ফোন এলে নিস্পৃহ থাকুন।
- কোনো ব্যাংক লেনদেনের আগে নিশ্চিত হয়ে নেবেন এরকম কোনো অ্যাপ্লিকেশন ব্যাকগ্রাউন্ডে চলছে কিনা।
- অপরিচিত ব্যক্তির সঙ্গে অ্যাকাউন্ট নাম্বার ইত্যাদি কোনো তথ্য আদানপ্রদান করবেন না।
- এনিডেস্ক বা টিম ভিউয়ার নিজেরা ম্যালওয়্যার নয়। প্রতারকেরা এগুলির অপব্যবহার করে তথ্য সংগ্রহ করে।
- এরকম ঘটনা ঘটলে নির্ভয়ে www.cybercrime.gov.in এবং www.reportphishing.in-এ রিপোর্ট করুন।

সাইবার সুরক্ষিত বাংলা – সাইবার সুরক্ষিত ভারত

https://cscoe.itewb.gov.in

১ম সংস্করণ ২০২০

সাইবার সিকিউরিটি সেন্টার অফ এক্সেলেন্স
ওয়েবেল ভবন, গ্রাউন্ড ফ্লোর
ইপি এবং জিপি ব্লক
সেক্টর ৫, বিধাননগর
সল্ট লেক, কলকাতা ৭০০০৯১
ফোন নম্বর: ০৩৩ - ২৩৫৭৫২১৮
ইমেল: **cscoe@wb.gov.in**