# সিকিউরিটির কিছু প্রচলিত অতিকথন

তাসনুভা মাহ্‌মুদ

বিশ্ব সংসারে প্রচুর অতিকথন বা ভুল ধারণা বা মিথ আছে, যা আমরা অনেকেই বিশ্বাস করলেও প্রকৃত অর্থে সত্য নয়। বিস্ময়কর হলেও সত্য, আধুনিক বিজ্ঞানের চরম উৎকর্ষের মাঝেও এসব ভুল ধারণা তথা মিথ আঁকড়ে ধরে থাকেন বা থাকতে ভালোবাসেন অনেকেই কোনো যৌক্তিক কারণ ছাড়াই। বিজ্ঞানের আধুনিক আবিষ্কার কমপিউটার ব্যবহারকারীরাও কমপিউটিং বিশ্বে কমপিউটার ব্যবহার সংশ্লিষ্ট অনেক ভুল ধারণা মনেপ্রাণে বিশ্বাস করে থাকেন। ইতোপূর্বে কমপিউটার জগৎ-এ কমপিউটিং বিশ্বে প্রচলিত কিছু ভুল ধারণা বা মিথ সম্পর্কে আলোচনা করা হয়েছিল।

এবার কমপিউটার জগৎ-এর নিয়মিত বিভাগ পাঠশালায় কমপিউটিং বিশ্বে প্রচলিত কিছু অতিকথন সম্পর্কে আলোকপাত করা হয়েছে। কেননা, আমরা মনে করি কমপিউটিং বিশ্বের ব্যবহারকারীরা হবেন সব ধরনের অতিকথন তথা কুসংস্কারমুক্ত। কিন্তু অতিকথনমুক্ত হতে হলে প্রথমেই জানতে হবে অতিকথন কোনগুলো, প্রযুক্তি বিশ্বে কেনো এসব প্রচলিত কথা অতিকথন হিসেবে গণ্য করা হয়।

বর্তমানে কমপিউটিং বিশ্বে সবচেয়ে আলোচিত বিষয়গুলোর মধ্যে অন্যতম একটি হলো সিস্টেমের সার্বিক সিকিউরিটি তথা নিরাপত্তা। এ সত্য উপলব্ধিতে এবার কমপিউটার জগৎ-এর নিয়মিতি বিভাগ পাঠশালায় উপস্থাপন করা হয়েছে সিকিউরিটি সংশ্লিষ্ট কিছু প্রচলিত ভুল ধারণা, যেগুলো সম্পর্কে সিকিউরিটি বিশেষজ্ঞ, কনসালট্যান্ট, ভেন্ডর এবং এন্টারপ্রাইজ সিকিউরিটি ম্যানেজারদের অভিমত হলো– এসব ধারণা মোটেও সত্য নয়, এগুলো মিথ।

## অধিকতর সিকিউরিটি বা নিরাপত্তামূলক ব্যবস্থা

সিকিউরিটি বিশেষজ্ঞ এবং অতিসম্প্রতি প্রকাশিত 'Liars and Outliers'-এর গ্রন্থের রচয়িতাসহ আরও কয়েকটি গ্রন্থের রচয়িতা Bruce Schneier ব্যাখ্যা করে দেখান, 'অধিকতর নিরাপত্তা ব্যবস্থা নেয়া অপরিহার্যভাবে সবসময় ভালো নয়।' প্রথম নিরাপত্তা ব্যবস্থা সবসময় ভারসাম্য বজায় রাখে এবং কখনও কখনও বাড়তি নিরাপত্তামূলক ব্যবস্থা নেয়া ভালোর চেয়ে খারাপই হয়ে থাকে। তিনি আরও উল্লেখ করেন, বাড়তি নিরাপত্তামূলক ব্যবস্থা নেয়া হয় ঝুঁকি কমানোর প্রবণতায়। তবে এক পর্যায়ে অতিরিক্ত সিকিউরিটি বা নিরাপত্তামূলক ব্যবস্থা নেয়া তেমন যুক্তিসঙ্গত কাজ হিসেবে গণ্য করা যায় না। কেননা কমপিউটিং বিশ্বে শতভাগ নিরাপত্তা অর্জন করা কোনোভাবে সম্ভব নয়। তাই কখনও কখনও বাড়তি নিরাপত্তামূলক ব্যবস্থা নেয়াটা নৈতিকভাবে সমর্থনযোগ্য হতে পারে এবং এ ক্ষেত্রে পরের ইচ্ছে পূরণে সম্মতি জ্ঞাপন করাটা হলো অনৈতিক সিদ্ধান্ত বলা যায়।

## ডিনায়েল অব সার্ভিস সমস্যা ব্যান্ডউইডথ সংশ্লিষ্ট

র‍্যাডওয়্যার কোম্পানির সিকিউরিটি সলিউশন্সের ভাইস প্রেসিডেন্ট কার্ল হারবার্জার (Carl Herberger) বলেন, 'শহুরে এলাকায় প্রচুর অতিকথন প্রচলিত আছে, যা দীর্ঘদিন ধরে আমরা শুনে আসছি, যার কোনো বাস্তব ভিত্তি নেই।' তার মতে, আইটি পেশাজীবীদের মধ্যে এমন অনেক লোক আছেন, যারা দৃঢ়ভাবে বিশ্বাস করেন যদি ব্যান্ডউইডথ বেশি হয়, তাহলে ডিস্ট্রিবিউটেড ডিনায়েল অব সার্ভিস (DDoS) অ্যাটাকের শিকার হওয়ার সম্ভাবনা বেড়ে যাবে। তিনি দাবি করেন, যেহেতু গত বছরে সংঘটিত অর্ধেকের বেশি ডিনায়েল অব সার্ভিস অ্যাটাকের সাক্ষ-প্রমাণে ব্যান্ডউইডথের কোনো বৈশিষ্ট্য পাওয়া যায়নি বরং সেগুলো ছিল অ্যাপ্লিকেশনকেন্দ্রিক। এ ক্ষেত্রে হামলাকারীরা অ্যাপ্লিকেশনে আঘাত হানে এবং সার্ভিসে বাধা সৃষ্টি করার লক্ষ্যে সুযোগ নেয়। এমন অবস্থায় ব্যান্ডডউইডথ বেশি থাকলে হামলাকারীদের জন্য ভালো হয়। আসলে ইদানীং মোট ডিনায়েল অব সার্ভিস অ্যাটাকের মাত্র এক-চতুর্থাংশকে দায়ী করা যায় অতিরিক্ত ব্যান্ডউইডথকে, যেখানে ব্যবহারকারী যুক্ত থাকেন।

## নিয়মিত ৯০ দিন পরপর পাসওয়ার্ড পরিবর্তন

আরেকটি জনপ্রিয় মিথ প্রচলিত আছে যে, পাসওয়ার্ডের মেয়াদ নিয়মিতভাবে অবসান হওয়া উচিত। এ প্রসঙ্গে কমপিউটার সিকিউরিটি বিশেজ্ঞ RSA-এর EMC সিকিউরিটি ডিভিশনের চিফ সায়েন্টিস্ট Aris Juels বলেন, এমন কথা হলো ডাক্তারদের উপদেশ 'প্রতিদিন গড়ে ৮ গ্লাস করে পানি পান করার মতো'। কেউ জানেন না বা বলতে পারেন না যে কোথা থেকে এমন কথা এসেছে বা এটি একটি ভালো উপদেশ। আরিস জুয়েলস আরও বলেন, প্রকৃত অর্থে সম্প্রতি এক গবেষণার সূত্র ধরে উপদেশ দেয়া হয়েছে যে নিয়মিতভাবে পাসওয়ার্ডের মেয়াদ অবসান ঘটানোর ফলে কোনো উপকার হয় না। সম্প্রতি RSA LABs-এর গবেষণার সূত্রে বলা হয়েছে যে, যদি কোনো প্রতিষ্ঠান নিয়মিতভাবে পাসওয়ার্ডের অবসান ঘটাতে চায়, তাহলে যেনো তা হয় র‍্যান্ডম সিডিউল অনুযায়ী, নির্দিষ্ট বা ফিক্সড দিনে যেনো না হয়।

## অভিজ্ঞতা ও বিচক্ষণতার ওপর আস্থা রাখা

ফোনিক্স সানস বাস্কেটবল টিমের ইনফরমেশন টেকনোলজির ভাইস প্রেসিডেন্ট বিল বোল্ট বলেন, 'একজন কর্মচারী বারবার কারও কাছ থেকে একটি ই-মেইল পাচ্ছে যেখানে উল্লেখ করা হচ্ছে আপনার সিস্টেম একটি নতুন ভাইরাসে আক্রান্ত' অথবা ইন্টারনেটে আসন্ন অন্যান্য বিপদ উদ্ভূত হয়েছে এবং এগুলো আইটি ডিপার্টমেন্টের সাথে সংযোগ স্থাপন করবে। তবে অনুসন্ধানে জানা যায়, শেয়ার্ড প্রবণতাগুলো নতুন হওয়ার কারণে কখনওই মনে হয় না সাধারণভাবে নিষ্পন্ন হয়। আসলে বেশিরভাগ সময় মূল আতঙ্কটা হলো সুপরিচিত ম্যালওয়্যারের হুমকি, যা এক যুগ আগে শনাক্ত হয়।

## পাসওয়ার্ডকে শক্তিশালী করতে র‍্যান্ডম ব্যবহার করা

বাস্তবতার নিরিখে পাসওয়ার্ড দেয়ার চেষ্টা করা। সিমেনটেক সিকিউরিটি ডিরেক্টর কেভিন হ্যালি বলেন, 'পরিপূর্ণভাবে র‍্যান্ডম পাসওয়ার্ড শক্তিশালী হতে পারে, তবে এ ক্ষেত্রে অসুবিধাও আছে যথেষ্ট।' এ ধরনের পাসওয়ার্ড মনে রাখা যথেষ্ট কঠিন হয়ে থাকে এবং খুব ধীরে ধীরে টাইপ করতে হয়, যা অনেকেই ট্র্যাক করতে পারে। এ ক্ষেত্রে বাস্তবতা হলো, পাসওয়ার্ড খুব সহজে তৈরি করা যায়, যা হবে যেমন শক্তিশালী তেমনই র‍্যান্ডমের মতো। লক্ষণীয়, কিছু সাধারণ কৌশল ব্যবহার করে এসব পাসওয়ার্ড তৈরি করলে মনে রাখা বেশ সহজ হয়। এসব পাসওয়ার্ড হবে ন্যূনতম ১৪ ক্যারেক্টার দীর্ঘ, যেখানে ব্যবহার হবে আপার এবং লোয়ার কেস লেটার, দুটি সংখ্যা, দুটি সিম্বল ইত্যাদি বৈশিষ্ট্যসংবলিত পাসওয়ার্ড যথেষ্ট শক্তিশালী এবং এমনভাবে ফরমুলেট করা হয় যাতে সহজে মনে রাখা যায়। সিমেনটেকের সিকিউরিটি ডিরেক্টর কেভিন হ্যালি আরও বলেন, কিছু কিছু খুব ঝুঁকিপূর্ণ পরিবেশে ৩০ দিন পর পাসওয়ার্ডের মেয়াদ উত্তীর্ণ করা ভালো উপদেশ হলেও সব ক্ষেত্রের জন্য তা প্রযোজ্য নয়। কেননা এ ধরনের সংক্ষিপ্ত সময়ের জন্য পাসওয়ার্ড ব্যবহারকারীদেরকে একটা ভবিষ্যৎ প্যাটার্নের জন্য প্ররোচিত করে অথবা তাদের পাসওয়ার্ডের কার্যকারিতা কমে গেছে। তার মতে, পাসওয়ার্ডের মেয়াদ ৯০ থেকে ১২০ দিনের জন্য হলে অধিকতর বাস্তবসম্মত ও ভালো হয়।

## কমপিউটার ভাইরাস মনিটরিং

সর্বসাধারণের কাছে কমপিউটার ভাইরাস একটি মিথ ছাড়া আর কিছুই নয়। 'জি ডাটা সফটওয়্যার নর্থ আমেরিক' কোম্পানির প্রেসিডেন্ট ডেভিড পেরি বলেন, 'সহজ কথায় বলা যায়, সর্বসাধারণের বেশিরভাগই বিশ্বাস করেন, ম্যালওয়্যার টার্মটি এসেছে টেলিভিশন এবং মুভির সায়েন্স ফিকশন থেকে।' সম্ভবত সবচেয়ে জনপ্রিয় ধারণা হলো, যেকোনো কমপিউটার ভাইরাস স্ক্রিনে দৃশ্যমান লক্ষণ রেখে ▸

যায়, প্রদর্শন করে ফাইল অদৃশ্য হয়ে লক্ষ্যের বাইরে চলে গেছে অথবা কমপিউটার নিজেই ঝুঁকির মধ্যে পড়েছে। ডেভিড পেরি আরও বলেন, 'সমস্যা দৃশ্যমান না হওয়ার অর্থই হলো সিস্টেম ম্যালওয়্যারমুক্ত।'

## আমরা হ্যাকারের লক্ষ্যবস্তু না

ক্রল (Kroll) কোম্পানির সাইবার সিকিউরিটি অ্যান্ড ইনফরমেশন অ্যাসুরেন্স প্র্যাকটিসের সিনিয়র ম্যানেজিং ডিরেক্টর অ্যালেন ব্রিল বলেন, কমপিউটার ব্যবহারকারীদের কাছ থেকে সচরাচর শুনে থাকি, 'আমরা হ্যাকারের লক্ষ্যবস্তু না।' এ ধরনের ব্যবহারকারীরা মনে করেন তাদেরকে হ্যাক করে লাভ নেই। কেননা তাদের ধারণা, তাদের কমপিউটারে মূল্যবান কোনো তথ্য নেই, যা হ্যাকাররা প্রত্যাশা করে। এ ধরনের ব্যবহারকারীদের মধ্যে অনেকেই বলে থাকেন, এরা সময়োপযোগী বা গুরুত্বপূর্ণ কেউ নন, কেননা তাদের ব্যবসায় প্রতিষ্ঠান ছোট হওয়ায় এরা সবসময় সবার নজরদারির অর্থাৎ রাডারের সীমার বাইরে থাকবেন। আবার অনেকেই সোশ্যাল সিকিউরিটি নম্বর, ক্রেডিট কার্ড ডাটা বা অন্যান্য মূল্যবান তথ্য নিরাপত্তার জন্য সংগ্রহ করার চেষ্টা করেন না। এ ধরনের মনোবৃত্তি ও ধারণা সম্পূর্ণ ভুল। কেননা হ্যাকার হ্যাক করার উদ্দেশ্যে বিশেষ ধরনের টুল ব্যবহার করে, যা সিস্টেমের নিরাপত্তা ব্যবস্থার ত্রুটি থাকলেই হ্যাক সফল হয়।

## ইদানীং সফটওয়্যার তেমন ভালো নয়

সিজিটাল কোম্পানির চিফ টেকনোলজি অফিসার গ্রে ম্যাকগ্র (Gary McGraw) বলেন, 'অনেক ব্যবহারকারী আছেন যারা জোরালো দাবি তোলেন তাদের ব্যবহার হওয়া সফটওয়্যারটি তেমন ভালো নয়, কেননা এতে হোল থাকে।' তার মতে, এক বা দুই যুগ আগের চেয়ে আজকের নিরাপদ কোডিং প্র্যাকটিস অনেক ভালো বোঝা যায় এবং এর জন্য পর্যাপ্ত পরিমাণে প্রয়োজনীয় টুলও আছে। তিনি আরও বলেন, উইন্ডোজ ৯৫ যুগের তুলনায় এখন অনেক বেশি সাধারণ সফটওয়্যার কোড লেখা হয়, কয়েক বর্গমাইলের কোড, যা আগের যেকোনো সময়ের চেয়ে অনেক বেশি। এই বিশাল ভলিউমের কোডের কারণে আজকের সফটওয়্যারগুলো ভলনিয়ারিবিলিটিপূর্ণ। ম্যাকগ্র আরও বলেন, 'পারফেকশন ইজ ইমপসিবল।'

## এসএসএল সেশনের মাধ্যমে ট্রান্সফার হওয়া সংবেদনশীল তথ্য নিরাপদ

আমেরিকার এনসিপি ইঞ্জিনিয়ারিংয়ের চিফ টেকনোলজি অফিসার রেইনার অ্যান্ডারসন বলেন, 'এসএসএল সেশনের মাধ্যমে কাস্টোমার বা পার্টনারদের কাছে সংবেদনশীল তথ্য সেন্ড করতে কোম্পানিগুলো সচরাচর ব্যবহার করে এসএসএল। কেননা এরা মনে করে এর মাধ্যমে তথ্য ট্রান্সফার করা নিরাপদ।' তিনি আরও বলেন, গত বছর সিটি গ্রুপ সিস্টেম ব্রিচের শিকার হয়, যা এ ক্ষেত্রে লিপিবদ্ধ করা যেতে পারে সমস্যা নিরীক্ষা করার জন্য। এটি কোনো স্বতন্ত্র ব্যাপার নয়। সম্প্রতি সুইস গবেষকেরা একটি মেমো প্রকাশ করেন, যেখানে বর্ণনা করা হয় ভলনিয়ারিবিলিটিকে কাজে লাগানোর মাধ্যমে তথ্য সংগ্রহ করে এসএসএল চ্যানেল দিয়ে ডাটা ট্রান্সমিট করা হয় ব্লক সাফ্যায়ার বাস্তবায়নের লক্ষ্যে, যেমন : AES। অ্যান্ডারসন আরও বলেন, এসএসএল সেশন সিকিউরিটি বিষয়ে যথেষ্ট সন্দেহ আছে এবং দুটি ভিন্ন ডকুমেন্টকে এনক্রিপ্ট করার জন্য কখনও একই কী স্ট্রিম ব্যবহার না করা, সম্ভবত আদর্শ উপায় হলো এই পিটফল এড়িয়ে যাওয়া। আরেকটি জনপ্রিয় সিকিউরিটি মিথ যা যেকোনো প্রবণতার সাথে কাজ করতে হয় যা ব্যবহার করে বিশ্বস্ত সার্টিফিকেট।

## এন্ডপয়েন্ট সিকিউরিটি সফটওয়্যার

এ প্রসঙ্গে এন্টারপ্রাইজ স্ট্র্যাটেজি গ্রুপের (ইএসজি) অ্যানালিস্ট জন অল্টসিক বলেন, 'আপাত দৃষ্টিতে মনে হয় বেশিরভাগ এন্টারপ্রাইজ সিকিউরিটি প্রফেশনাল এই স্টেটমেন্টের সাথে এক মত যে, এন্ডপয়েন্ট সিকিউরিটি পণ্য মূলত প্রায় সব একই ধরনের এবং কমোডিটি পণ্য।' তবে জন অল্টসিক এ ক্ষেত্রে দ্বিমত পোষণ করেন। এ প্রসঙ্গে তিনি বলেন, 'আমি বিশ্বাস করি এটি পুরোপুরি একটি মিথ।' এন্ডপয়েন্ট সিকিউরিটি পণ্য প্রটেকশন লেভেল এবং ফিচার/ফাংশনালিটির আলোকে অনেক ভিন্নতা রয়েছে। তিনি আরও মনে করেন, বেশিরভাগ অর্গানাইজেশন এন্ডপয়েন্ট সিকিউরিটি পণ্যের সক্ষমতার ব্যাপারে অবগত নয়, যেগুলো তাদের কাছে আছে। সুতরাং সর্বোচ্চ প্রতিরক্ষার জন্য এসব পণ্যকে যথাযথভাবে ব্যবহার না করই ভালো।

## নেটওয়ার্ক ফায়ারওয়ালে শতভাগ নিরাপদ

ইউনিভার্সিটি অব আরকানসাস ফর মেডিক্যাল সায়েন্সের ইনফরমেশন টেকনোলজি সিকিউরিটি অ্যানালিস্ট কেভিন বাটলার ফায়ারওয়াল অ্যাডমিনিস্ট্রেটর হিসেবে এক যুগের বেশি সময় কাজ করেন। তিনি বলেন, ফায়ারওয়াল সম্পর্কে প্রচুর মিথ আছে। বাস্তবতা মেনে নিয়ে তিনি গত কয়েক বছরে এসব মিথের কিছু কিছু বিশ্বাস করতে শুরু করেন। বাটলার বলেন, তিনি যেটি মেনে নিতে পারছেন না তা হলো 'ফায়ারওয়াল হলো হার্ডওয়্যারের অংশ' এবং 'যথাযথভাবে কনফিগার করা একটি ফায়ারওয়াল আপনাকে সব ধরনের হুমকি থেকে রক্ষা করবে।' আসলে তা নয়, ম্যালিশাস কনটেন্ট একটি এসএসএল কানেকশনে অ্যানক্যাপস্যুলেট হয়ে আপনার ওয়ার্কস্টেশনকে সংক্রমিত করবে। বাটলার আরও বলেন, তার জানা কয়েকটি অতিকথনের মধ্যে একটি হলো 'ফায়ারওয়াল ব্যবহার করলে কোনো অ্যান্টিভাইরাস সফটওয়্যারের প্রয়োজন হয় না এবং আরেকটি হলো, ব্র্যান্ড 'X' ফায়ারওয়াল জিরো-ডে হুমকি প্রতিরোধ করতে পারে। তার মতে, ফায়ারওয়াল প্রটেকশনের বিপরীতে নতুন সুযোগ কাজে লাগানো যায়, যা শনাক্ত হয় হুমকির তীব্রতা উপশমকারী হিসেবে। ফায়ারওয়ালকে কখনই প্রতিরোধের পরিমাপক হিসেবে গণ্য করা যায় না কজ

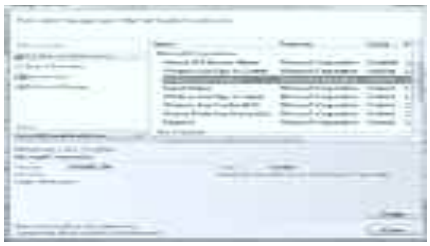
*ফিডব্যাক : mahmood_sw@yahoo.com*

# কমপিউটার রক্ষণাবেক্ষণের

*(৭৮ পৃষ্ঠার পর)*

Registry বাটনে ক্লিক করুন। এরপর স্ক্যান করুন। স্ক্যান শেষ হওয়ার পর Fix selected isues-এ ক্লিক করুন। সিক্লিনার টুল বর্তমান রেজিস্ট্রিকে ব্যাকআপ করার সুযোগ দেবে। এর ফলে প্রয়োজনে কোনো অ্যাকশনকে আবার আগের ভালো অবস্থায় ফিরিয়ে আনা যায়।

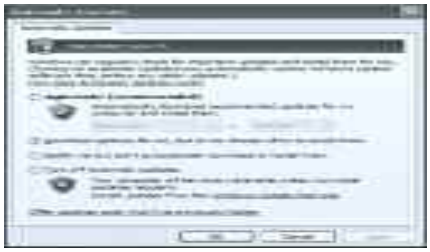
## ধাপ-১১ : ম্যানেজার অ্যাড-অনস



*চিত্র-১১ : ম্যানেজার অ্যাড-অনস*

কোন ওয়েব ব্রাউজার ব্যবহার করছেন, তা বিবেচ্য বিষয় নয় বিভিন্ন ধরনের অ্যাড-অনস ইনস্টল করার ক্ষেত্রে। কেননা, এখানে প্রয়োজনীয় ফিচার থাকতে পারে। তবে আপনার ব্রাউজার পারফরম্যান্স যদি বিজ্জনকভাবে নেমে যায়, তাহলে ধরে নিতে পারেন এ ক্ষেত্রে প্রধান আসামী হলো একটি অ্যাড-অনস। ইন্টারনেট এক্সপ্লোরার ব্যবহারকারীরা অ্যাড-অনস ভিউ এবং ডিজ্যাবল করতে পারেন। এজন্য ব্রাউজার উইন্ডো ওপেন করতে হবে টুল মেনু থেকে Manage Add-ons-এ ক্লিক করে। ফায়ারফক্সেও অনুরূপ ফিচার রয়েছে, যা অ্যাক্সেস করা যায় Tools মেনু থেকে Add-ons-এ ক্লিক করে।

## ধাপ-১২ : মাইক্রোসফট আপডেট



*চিত্র-১২ : অটোমেটিক আপডেট অপশন*

মাইক্রোসফট উইন্ডোজের জন্য আপডেট অবমুক্ত করে, যা সাধারণত সিকিউরিটির সাথে সম্পর্কযুক্ত। তবে কিছু কিছু বিষয় পারফরম্যান্সের সাথে সম্পর্কযুক্ত। সুতরাং এজন্য উইন্ডোজের অটোমেটিক আপডেট ফিচার অন থাকতে হয়। এজন্য এক্সপির স্টার্টে ক্লিক করে All Programs→Accessories→System Tools-এ ক্লিক করুন। এরপর Security Center-এ ক্লিক করতে হবে। পরবর্তী সময়ে আবির্ভূত উইন্ডোতে 'Automatic (recommended)' রেডিও বাটন যেনো সিলেক্ট করা থাকে তা নিশ্চিত করে এবং Ok-তে ক্লিক করুন। ভিস্তা এবং উইন্ডোজ ৭-এর ক্ষেত্রে স্টার্টে ক্লিক করে সার্চ বক্সে উইন্ডোজ আপডেট টাইপ করে এন্টার চাপুন। এরপর Change Settings লিঙ্কে ক্লিক করে ইম্পরটেন্ট আপডেট সেকশনে ক্লিক করে বেছে নিন 'Install Updates Automatically' অপশন কজ

*ফিডব্যাক : mahmood_sw@yahoo.com*