ফিশিং স্ক্যাম এড়িয়ে যাবেন যেভাবে

তাসনীম মাহ্‌মুদ

ভাইরাস, ট্রোজান এবং ক্ষতিকর প্রোগ্রাম ব্যবহারকারীর অপারেটিং সিস্টেম এবং অ্যাপসমূহকে আক্রমণ করে। আর ফিশিং স্ক্যাম হলো নিজেকে বিশ্বাসযোগ্য সত্তা হিসেবে ছদ্মবেশে ব্যবহারকীর নাম, পাসওয়ার্ড এবং ক্রেডিট কার্ড সম্পর্কিত সংবেদনশীল তথ্য হাতিয়ে নেয়ার জালিয়াতি প্রচেষ্টা। প্রকৃত অর্থে ফিশিং আক্রমণের মূল লক্ষ্য ব্যবহারকারী। এ লেখায় ব্যবহারকারীরা কীভাবে তাদের ব্যক্তিগত তথ্য সুরক্ষিত করবেন এবং ফিশিং স্ক্যামকে এড়িয়ে চলবেন, তা তুলে ধরা হয়েছে।

আপনি হয়তো শুনে থাকবেন, ম্যালওয়্যার লেখা এখনকার দিনে এক ব্যবসায় এবং কিছু নগদ অর্থ উপার্জনের উপায়ে পরিণত হয়েছে। এ জন্য দরকার আপনার কোডিং দক্ষতা আরও বৃদ্ধি করা যাতে ট্রোজান তৈরি করতে পারেন, যা অতীতের অ্যান্টিভাইরাস প্রোগ্রামগুলো পায় এবং ব্যাংক অ্যাকাউন্ট লগইন চুরি করে অথবা অন্য কোনো লাভজনক কাজ সম্পাদন করে। এরপর আপনাকে আপনার অশুভ সফটওয়্যার ইঞ্জিনিয়ারিংয়ের বিস্ময়কর ডিস্ট্রিবিউশনের জন্য একটি উপায় খুঁজে বের করতে হবে। কিন্তু এ কাজটি করা সহজ নয়। আপনি যদি সত্যি সত্যি ডার্কসাইটে যেতে চান, তাহলে সঙ্গত কারণেই প্রশ্ন কেন কিছু ফিশিং ওয়েবসাইট বেছে নেবেন না এবং তাদের পাসওয়ার্ড দেয়ার জন্য ক্লুলেস নেট নাগরিক তথা নেটিজেনদের কেন পাবেন না?

ম্যালওয়্যার কোড লেখা বেশ কঠিন। অ্যান্টিভাইরাস-পরিপূর্ণ পরিবেশে টিকে থাকতে পারে এমন ম্যালিশাস প্রোগ্রাম কোড লেখা আরো কঠিন। তাই অপারেটিং সিস্টেম এবং এর সিকিউরিটি ক্ষমতা হ্যাক করার পরিবর্তে ফিশিং স্ক্যামে ব্যবহারকারীকে বোকা বানানোর চেষ্টা করা অনেক সহজ।

কভিড-১৯ ফ্যাক্টর

বিপুলসংখ্যক লোক ঘরে বসে আটকে রয়েছেন, বিনোদন খুঁজছেন ইন্টারনেটে। এর ফলে ফিশিং স্ক্যামারেরা পেয়েছে শিকারের স্বর্গরাজ্য। ফিশিং স্ক্যামারেরা বিগেনারদের কাছ থেকে সাধারণ প্রশংসাপত্র চুরি, জালিয়াতি করার জন্য পেয়েছে বৃহত্তর অডিয়েন্স। কিন্তু এই অভূতপূর্ব মহামারীর মাধ্যমে যে ভয়, অনিশ্চয়তা এবং সন্দেহের সৃষ্টি হয়েছিল তা একেবারে নতুন ধরনের স্ক্যামগুলোর জন্য নিখুঁত ক্যারেক্টার তৈরি করে।

গুগল জানিয়েছে, এপ্রিল মাসে তারা প্রতিদিন ভাইরাসসংশ্লিষ্ট ১৮ মিলিয়ন স্ক্যাম ব্লক করে। গুগল একটি ভালো কাজ করে। অনুমান করা হচ্ছে এটি ৯৯.৯ শতাংশ স্প্যাম এবং ফিশিং ই-মেইল ব্লক করে। যদিও প্রতিদিন ১৮০০০ অনাকাঙ্ক্ষিত মেসেজ অজানা সংখ্যক ভুক্তভোগীর কাছে পৌঁছে।

ভাইরাস স্ক্যামার শুধু আপনার পাসওয়ার্ড হাতিয়ে নেয়ার জন্য যাচ্ছে না, তারা আপনার টাকা চায়। তারা অনলাইনে ব্যক্তিগতভাবে কাজ করে। মহামারী সম্পর্কিত কোনো সংযোগ বহনকারীর ই-মেইল সম্পর্কে সতর্ক থাকুন বিশেষ করে যদি এটি আপনাকে কোনো লিঙ্কে ক্লিক করতে বা একটি ফাইল ডাউনলোড করতে অনুরোধ করে। যদি ফেইক ই-মেইল আপনাকে তাৎক্ষণিকভাবে উদ্বিগ্ন করে, তাহলে প্রোভাইড করা লিঙ্ক ব্যবহার করার পরিবর্তে সরাসরি সোর্সে অ্যাক্সেস করুন।

ধরুন, আপনি একটি ফ্রেইস যেমন "stimulus check" দেখতে পেলেন, তাহলে ধরে নিতে পারেন আপনি স্ক্যামের দিকে তাকিয়ে আছেন। ধরা যাক, আপনি ব্যক্তিগতভাবে কভিড-১৯ সম্পর্কিত কোনো জালিয়াতির অথবা স্ক্যামের মুখোমুখি হননি। এজন্য গুগলকে ধন্যবাদ।

সুনির্দিষ্ট ধরনের হুমকির হাত থেকে নিজেকে রক্ষা করার জন্য কভিড-১৯ স্ক্যাম স্পট করবেন এবং এড়িয়ে চলবেন তা জানার জন্য নিচে বর্ণিত ধাপগুলো অনুসরণ করুন :

ফিশিং স্ক্যাম যেভাবে কাজ করে

ক্রেডেনশিয়াল-স্টিলিং তথা প্রশংসাপত্র চুরি ফিশিং স্ক্যাম চালানোর মূল চাবিকাঠি এমন একটি সুরক্ষিত ওয়েবসাইটের প্রতিরূপ তৈরি করা, যা বেশিরভাগ অথবা কিছু লোককে বোকা বানানোর জন্য যথেষ্ট। ক্লাসিয়েস্ট ফেইকের সাথে প্রতিটি লিঙ্ক আসল সাইটে যায়– অপরাধীদের কাছে আপনার ব্যবহারকারীর নাম এবং পাসওয়ার্ড জমা দেয়া ছাড়া। প্রতারকেরা তাদের উদ্দেশ্য হাসিলের জন্য এমন একটি ইউআরএল তৈরি করার চেষ্টা করতে পারে, যা দেখতে অনেকটা বৈধ বলে মনে হতে পারে। যেমন paypal.com-এর পরিবর্তে সম্ভবত pyapal.com অথবা paypal.security.reset.com হতে পারে।

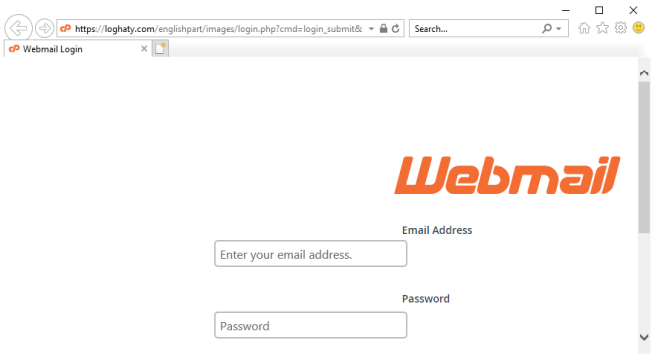
তবে প্রতিটি ফিশিং পেজ ভালো করা হয় না। কিছু ভুল রং ব্যবহার করে অথবা হাস্যকরভাবে অনুকরণ করা পেজ ম্যাচ করাতে ব্যর্থ হয়। অন্যদের কাছে সম্পূর্ণরূপে অপ্রত্যায়িত ইউআরএলএস (URLs) যেমন admin.dentistry.com/forms, অথবা X8el87.journal.com।

যখন কোনো ফিশিং সাইটে আপনার ইউজারনেম এবং পাসওয়ার্ড এন্টার করবেন, তখন সাইট মালিকেরা আপনার অ্যাকাউন্টে সম্পূর্ণ অ্যাক্সেস পাবে। আপনি স্ক্যামে শিকার হয়েছেন তা উপলব্ধি করাতে

আপনাকে সত্যিকার সাইটগুলোতে ক্রেডেনশিয়াল প্রেরণ করতে হবে যাতে দেখে মনে হবে আপনি স্বাভাবিকভাবে লগইন করেছেন। একমাত্র ক্লু তখনই আসতে পারে যখন দেখবেন আপনার ব্যাংক অ্যাকাউন্ট খালি হয়ে গেছে অথবা আপনার ই-মেইলে লগইন করতে পারছেন না এবং আপনার বন্ধুরা বলছেন যে তারা আপনার কাছ থেকে স্প্যাম পাচ্ছেন। সুতরাং এ ধরনের হামলার বিরুদ্ধে নিজেকে প্রস্তুত রাখতে হবে।

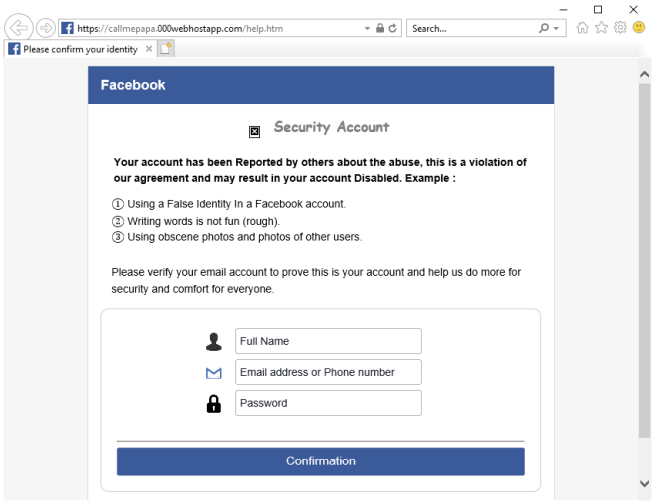
সুস্পষ্টভাবে বাদ দিন

কিছু ভুয়া ওয়েবসাইট অন্যের মনোযোগ আকৃষ্ট করার জন্য খুব খারাপভাবে বাস্তবায়ন করা হয়েছে। যদি আপনি কোনো সাইটের সাথে লিঙ্ক এবং তা যদি আবর্জনার মতো দেখায় তাহলে Ctrl + F5 চাপুন সম্পূর্ণ পেজ রিলোড করার জন্য যদি খারাপ অবয়বটি অপ্রত্যাশিত হয়। এরপরও যদি ঠিক না দেখায় তাহলে দূরে থাকুন।



চিত্র-১ : ওয়েবমেইলের ইন্টারফেস

উপরের পেজটি খেয়াল করুন। এর ফরম্যাটটি অদ্ভুত এবং ব্রাউজার উইন্ডোর উইডথ পরিবর্তন করার সাথে সাথে এটি আরও অদ্ভুততর হবে। ই-মেইল এবং পাসওয়ার্ডের জন্য লেবেল করা ফিল্ডগুলো সংশ্লিষ্ট ডাটা এন্ট্রি ফিল্ডগুলো থেকে পৃথকভাবে মুভ করানো হয়। এর ফলে সব কনটেন্ট কেন্দ্রীভূত করা কত কঠিন হবে?

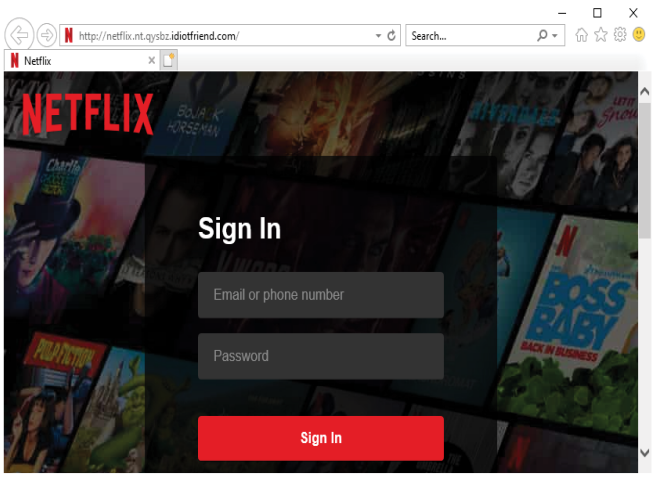


চিত্র-২ : ফিশিং পেজ তৈরি করা

যখন কোনো ফিশিং পেজ তৈরি করবেন, তখন তা আপাতদৃষ্টিতে সত্য বলে প্রতীয়মান হওয়াটা অপরিহার্য। একটি ফ্রি ওয়েব হোস্টিং সার্ভিস ব্যবহার করা এক ধরনের উপায়, যা আপনার পেজে এর ব্যানার অথবা আপনার ইউআরএলে এর ডোমেইন ছেড়ে দেয়। যখনই ফিশিং প্রোটেকশন টেস্ট করবেন, তখনই কোনো না কোনো সন্দেহজনক কিছুর মুখোমুখি হচ্ছেন, যেমন ফেসবুক 000webhostapp.com ব্যবহার করছে কে বিশ্বাস করবে?

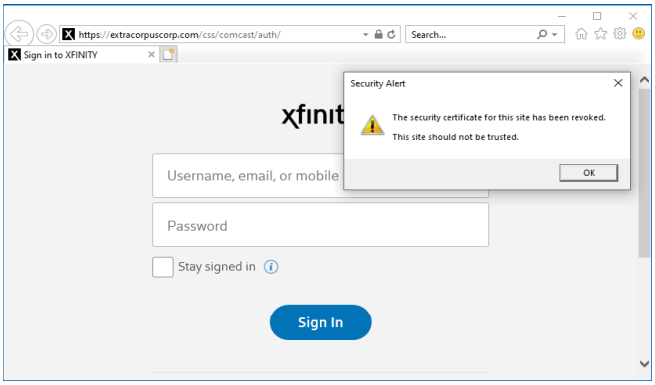
অ্যাড্রেস চেক করুন

আধুনিক ওয়েব ব্রাউজারগুলো অ্যাড্রেস বারে ফোকাস করা থেকে সরে আসছে। এটি এখন কমপক্ষে search-plus-address bar-এ পরিণত হয়েছে। তবে যখন কোনো পেজকে বৈধ বলে নিশ্চিত করেছেন, তখন এই অ্যাড্রেস বার খুবই গুরুত্বপূর্ণ এক রিসোর্স হিসেবে বিবেচনা করা হয়। সেরা ফিশ-স্নিফারগুলো নিমিষের মধ্যে চিহ্নিত করতে পারে অফ-কিলার ইউআরএল। ইউআরএলের প্রকৃত ডোমেইন অংশ অস্পষ্ট করার দিকে নজর দিন। এ অংশটি তাৎক্ষণিকভাবে .com, .net, .org-এর আগে বসে। ডোমেইনের আগে যা আসে তা হলো সাবডোমেইন। যদি fakery.paypal.com ব্যবহার করা হয়, তাহলে এটি হবে paypal.com-এর একটি সাবডোমেইন। তবে এর পরিবর্তে যদি paypal.fakery.com দেখা যায়, তাহলে তা হবে একটি ফ্যাকারি।



চিত্র-৩ : নেটফ্লিক্সে লগইন করা

ড্রপবক্স অ্যাকাউন্টে অথবা অন্যান্য অনলাইন স্টোরেজ অ্যাকাউন্টে ফিশিং হামলা চালিয়ে ব্যাংক লগইন ক্যাপচার করে চোরেরা যা পায় তাতে গ্যারান্টিযুক্ত ভ্যালু থাকে না। অন্যভাবে বলা যায়, লোকেরা এই অ্যাকাউন্টগুলোতে একই লেবেলের সতর্কতা প্রয়োগ করে না। পরবর্তী প্রযুক্তির অগ্রগতির জন্য অনলাইন স্টোরেজে Girl Scout কুকিজ লিস্ট থেকে শুরু করে গোপন পরিকল্পনা পর্যন্ত সবকিছু পাওয়া যায়। একইভাবে স্ট্রিমিং মিডিয়াতে লগইন ক্যাপচারে খুব বেশি আয়ের সম্ভাবনা নেই। তবে সেই অ্যাকাউন্টে অ্যাক্সেসের ফলে একই ক্রেডেন্সিয়ালের সাথে আরও কিছু গুরুত্বপূর্ণ অ্যাকাউন্টে আপস করা হতে পারে। ৩নং চিত্রের অ্যাড্রেস বারটি খেয়াল করুন। এমনকি আপনি যদি একজন নির্বোধ বন্ধুর কাছ থেকে স্ক্যামিং ক্রেডেন্সিয়ালের মাধ্যমে নেটফ্লিক্সে লগইন করেন, তাহলে আপনি অবশ্যই ইউআরএলে "idiotfriend" দেখতে পাবেন না।



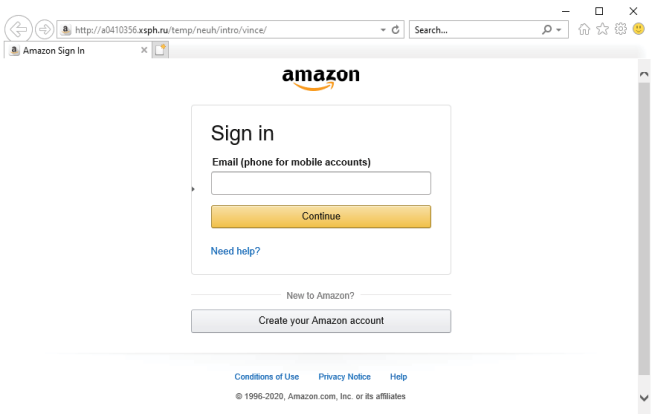
চিত্র-৪ : সিকিউরিটি অ্যালার্ট

স্পষ্টতই ইউআরএল উপস্থাপন করে না Xfinity অথবা Comcast অথবা সংশ্লিষ্ট যেকোনো ব্র্যান্ড। এছাড়া ব্রাউজার একটি বড় লাল পতাকা তরঙ্গায়িত করে। এটি নির্দেশ করে যে সাইটের সিকিউরিটি সার্টিফিকেট বাতিল করা হয়েছে। বৈধ সাইটের জন্য ওয়েবমাস্টার মাঝেমধ্যে স্ক্রুআপ করে এবং তাদের সার্টিফিকেট ফাঁস হতে দেয়। তবে এ পেজটি স্পষ্টতই প্রতারণামূলক।

লক অনুসন্ধান করা

বেসিক ইন্টারনেট যোগাযোগের জন্য ব্যবহৃত হাইপার টেক্সট ট্রান্সফার প্রটোকল (HTTP) কমিউনিকেশন সিস্টেম বিশ্বব্যাপী ওয়ার্ল্ড ওয়াইড ওয়েবের প্রথম দিন থেকেই ধারণ করে আসছে। এটি সুরক্ষিত নয়। কেননা ইন্টারনেটে অন্যরা খারাপ কাজ করতে পারে কেউ কল্পনা করতে পারে না। খারাপ লোক বিশ্বের সব জায়গায় রয়েছে। সুতরাং ইন্টারনেট সংযোগের একমাত্র বুদ্ধিমান উপায় হলো নিরাপদ HTTPS প্রটোকল ব্যবহার করা। HTTPS পেজের জন্য ওয়েব ব্রাউজার প্রদর্শন করে একটি লক আইকন। ক্রোম একধাপ এগিয়ে গেছে এবং HTTP সাইটকে সক্রিয়ভাবে চিহ্নিত করেছে Not secure হিসেবে। সুতরাং এমন কোনো সাইটে কখনোই লগইন করা উচিত নয় যেটি HTTPS ব্যবহার করে না।

এইচটিটিপিএস যুগে কোনো অজুহাত গ্রহণযোগ্য নয়। কোনো কোনো সাইট আছে যেগুলো চায় আপনি লগইন করবেন HTTPS ব্যবহার না করে। এটি যদি কোনো জালিয়াতি না করে, তাহলেও এই সাইটকে বৈধ বলে গণ্য করা যায় না।



চিত্র-৫ : অ্যামাজনে সাইন ইন করা

যদি আপনি .ru ডোমেইনটি লক্ষ না করেন, তাহলে এই পেজটি একটি বৈধ অ্যামাজন লগইন পেজের মতো দেখাবে। লক্ষণীয়, যদিও এ পেজে কোনো লক নেই এবং অ্যাড্রেস শুরু হয়েছে http: দিয়ে, https: দিয়ে নয়। এমন পেজ এড়িয়ে চলুন, কেননা এটি একটি খারাপ সাইট।

কখনো কখনো আপনি শুধু ডোমেইন নেমে তাকিয়ে বলতে পারেন না। কমনওয়েলথ ব্যাংক ওয়েবসাইটের অনলাইন ব্যাংকিং সিস্টেমকে Netbank বলে। সুতরাং উপরে প্রদর্শিত netbank.com সুরক্ষিত পেজটি বৈধ বলে মনে হয়। যদি আপনি নিশ্চিত হতে না পারেন, তাহলে ডোমেইনের জন্য whois ডাটা সম্পর্কে তাৎক্ষণিকভাবে নজর দিতে পারেন, যা দ্রুত সিদ্ধান্ত নেয়ার ক্ষেত্রে সহায়তা করতে পারে। প্রকৃত কমনওয়েলথ ব্যাংকের সাইটটি CrazyDomains.com সাইটের সাথে পার্ক করবে তার সম্ভাবনা কম।

সোর্স বিবেচনা করা

আপনার অপরিচিত কোনো ব্যক্তির কাছ থেকে আসা ই-মেইল মেসেজ লিঙ্কে ক্লিক করবেন না। আপনার অপরিচিত কোনো ব্যক্তির কাছ থেকে আসা মেসেজ লিঙ্কে ক্লিক করবেন না। কেননা তারা হ্যাক হয়ে থাকতে পারে। এটি একটি ভালো উপদেশ। র‍্যান্ডম লিঙ্ক তথা এলোমেলো লিঙ্কে ক্লিক করলে আপনাকে কোনো ম্যালওয়্যার-হোস্টিং সাইটে অথবা প্রতারক সাইটে নিয়ে যেতে পারে। লিঙ্কটি যখন আপনাকে কোনো লগইন পেজে নিয়ে যাবে, তখন আপনাকে বিশেষভাবে বিবেচনা করতে হবে এর সোর্সকে।

আপনার ব্যাংক থেকে ই-মেইল মেসেজ পেতে পারেন, যেহেতু অনেক ব্যাংক এভাবে যোগাযোগ রক্ষা করে থাকে। যদি সম্পর্কযুক্ত নয় এমন কোনো সাইটের লিঙ্কে ক্লিক করেন এবং ব্যাংক অব আমেরিকার লগইনে ক্ষতবিক্ষত হন, তাহলে এটি ফেইক হওয়ার সম্ভাবনা বেশি।

যদি আপনার ব্যাংক অথবা আইআরএস অথবা পেপাল আপনার অ্যাকাউন্টে কোনো সমস্যা সম্পর্কে আপনাকে ধরে রাখার চেষ্টা করবে? এর সমাধান খুব সাধারণ। এ ক্ষেত্রে লিঙ্কটি এড়িয়ে যান এবং সরাসরি সার্ভিসগুলোতে লগইন করুন সাধারণত আপনি যেভাবে করে থাকেন।

ফিশিং থেকে নিজেকে রক্ষা করা

আপনার অতি প্রয়োজনীয় ক্যাশ স্ক্যামে শিকার হওয়ার যন্ত্রণা এড়াতে চাইলে অথবা প্রতারকদের হাতে সংবেদনশীল ডাটা তুলে দিয়ে বিব্রতকর অবস্থায় পড়া এড়াতে চাইলে আপনার অ্যান্টিভাইরাসে পাসওয়ার্ড ম্যানেজার এবং ফিশিং-ডিটেকশন সিস্টেম রিসোর্স ব্যবহার করা নিশ্চিত করুন। তবে নিজের চোখ খোলা রাখুন যেকোনো ধরনের প্রতারণা চিহ্নিত করার জন্য। যদি কোনো পেজ সন্দেহজনক লিঙ্ক থেকে আসে, যদি অ্যাড্রেস বারে কোনো HTTPS লক না থাকে, যদি এটি কোনো উপায়ে ভুল দেখায়, তবে এটি স্পর্শ করবেন না। আপনার ভিজিল্যান্স বন্ধ হয়ে যাবে কজ

ফিডব্যাক : mahmood_sw@yahoo.com