যে ধরনের ই-মেইল ওপেন করা উচিত নয়

ডা. মোহাম্মদ সিয়াম মোয়াজ্জেম

তথ্যপ্রযুক্তি আমাদের প্রাত্যহিক জীবনযাত্রা ও আধুনিক যোগাযোগ ব্যবস্থাকে যেমন সহজ, সরল ও গতিময় করেছে; তেমনি করেছে উৎকণ্ঠাময়ও। ভাইরাস, স্প্যাম, স্ক্যাম প্রভৃতি আমাদের প্রাত্যহিক কমপিউটিং জীবনকে শুধু ব্যাহত করেনি, করেছে কলুষিত। এমনকি বিশ্বের সবচেয়ে দ্রুত, নিরাপদ, বিশ্বাসযোগ্য ও নির্ভরযোগ্য যোগাযোগ ব্যবস্থা ই-মেইলও আস্থাহীনতায় ভুগছে। কেননা, বিভিন্ন ধরনের ই-মেইল স্ক্যামের মাধ্যমে ব্যবহারকারীরা প্রতিনিয়তই আক্রান্ত হচ্ছেন। তাই ভাইরাস, স্ক্যাম প্রভৃতির ক্ষতিকর প্রভাব থেকে রক্ষা পাওয়ার জন্য সিকিউরিটি গবেষকেরা কঠোর পরিশ্রম করে যাচ্ছেন। সিকিউরিটি গবেষকদের প্রচেষ্টা থাকা সত্ত্বেও প্রতিদিনই বিপুলসংখ্যক লোক বিভিন্ন ধরনের ই-মেইল স্ক্যামের শিকার হচ্ছেন। হতে পারে তা বিশেষ কোনো কর্মপরিকল্পনা-সংশ্লিষ্ট যেমন– get rich quick অথবা সুকৌশলে ডিজাইন করা কোনো ই-মেইল, যা দেখে মনে হবে আপনার ক্রেডিট কার্ড প্রোভাইডারের বৈধ কমিউনিকেশন-সংশ্লিষ্ট, যা সত্য-মিথ্যা যাচাই করা কঠিন সাধারণ ব্যবহারকারীর। সিকিউরিটি বিশেষজ্ঞদের পরামর্শ, ই-মেইল স্ক্যামের বিরুদ্ধে প্রতিরোধ গড়ে তোলাই হলো সেরা নলেজ বা জ্ঞান। কী অনুসন্ধান করতে হবে আর কী এড়িয়ে যেতে হবে, তা ব্যবহারকারীদের বুঝতে হবে। যদিও আমাদের ইনবক্স স্প্যাম দিন দিন উন্নততর হচ্ছে। তার অর্থ এই নয়, আপনি সম্পূর্ণ নিরাপদ। শতভাগ নিরাপদ থাকার জন্য সিকিউরিটি বিশেষজ্ঞদেরকে এখনও অনেক কাজ করতে হবে। কেননা, সম্প্রতি এক প্রতিবেদনে উল্লেখ করা হয়, যুক্তরাষ্ট্রে বছরে সাইবার অপরাধের কারণে ক্ষতিগ্রস্ত হয় প্রায় ৮০০ মিলিয়ন ডলার। সুতরাং নিজেকে রক্ষা করার জন্য আমরা কী করতে পারি, তা-ই এখন এক বড় প্রশ্ন।

জেনে নিন লক্ষণগুলো

সিকিউরিটি ফার্ম জোন অ্যালার্ম ফিশিং ই-মেইল স্ক্যামের শিকার হওয়ার হাত থেকে রক্ষা পাওয়ার জন্য কিছু টুকিটাকি তথ্য তুলে ধরেছে। প্রথমেই খেয়াল করে দেখুন কোম্পানির নামের বানানে বা গ্রামারে ভুল আছে কি না। বৈধ কোম্পানি তাদের ই-মেইলকে স্পষ্টত প্রফেশনালভাবে উপস্থাপন করার জন্য সাধারণত বেশ কয়েকবার এডিট করে থাকে। স্ক্যামারের ক্ষেত্রে সাধারণত এমনটি হতে দেখা যায় না। এদের উদ্দেশ্য শুধু পার্সোনাল তথ্য হাতিয়ে নেয়া।

তাৎক্ষণিক অ্যাকশনের জন্য আপনাকে কোনো রিকোয়েস্ট করতে পারে, যা হলো আরেকটি লক্ষণীয় বিষয়। রিকোয়েস্টে আপনাকে বলতে পারে Open Immediately বা বলতে পারে Immediate Action Required। যদি কোনো কোম্পানি আপনার সাথে যোগাযোগ করতে চায়, তাহলে সংক্ষেপে বলা যায়, তারা কোনো ব্যক্তির মাধ্যমে বা ফোনের মাধ্যমে যোগাযোগ করবে।

জেনে নিন ধরন

ফিশিং ই-মেইলের বেসিক চিহ্ন ও বিভিন্ন ধরন জানাটাই হলো মূল বিষয়। সিকিউরিটি ম্যাট্রিক্স নামের সিকিউরিটি ফার্ম ই-মেইল ফিশিং স্ক্যামকে দশটি ভিন্ন ক্যাটাগরিতে ভাগ করেছে :

০১. দি গভর্নমেন্ট স্ক্যাম : এ ধরনের ই-মেইলগুলো এমনভাবে তৈরি করা হয়েছে, দেখে মনে হবে এগুলো এসেছে সরকারি এজেন্সি থেকে। যেমন– আইআরএস, এফবিআই বা সিআইএ। বিশ্বাস রাখবেন, যদি এরা আপনাকে ধরতে চায়, তাহলে আর যাই হোক ই-মেইল করে ধরতে চাইবে না।

০২. দি লং লস্ট ফ্রেন্ডস : এই স্ক্যামার আপনাকে ভাবাতে চেষ্টা করে আপনি যেকোনোভাবে তাদেরকে চেনেন। হতে পারে তা আপনার কোনো কন্টাক্ট, যা হ্যাক হয়েছিল। যদি আপনি টাকার জন্য কোনো ভুতুড়ে রিকোয়েস্ট পান এবং তাদেরকে প্রথমে কল দেন।

০৩. দি বিলিং ইস্যু : টিপিক্যালি দেখতে বৈধ কমিউনিকেশন থেকে এই ই-মেইলগুলো আসে। এগুলোর মধ্যে কোনো একটি যদি বুঝতে পারেন তাহলে ওয়েবসাইটে আপনার মেম্বার অ্যাকাউন্টে লগইন করুন অথবা কলসেন্টারে কল করুন। গুরুত্বপূর্ণ কোনো তথ্য ই-মেইলের মাধ্যমে সেন্ড করবেন না।

০৪. দি এক্সপাইরেশন ডেট : একটি কোম্পানি দাবি করল আপনার যে আকাউন্ট আছে তার মেয়াদ প্রায় শেষ। আপনার ডাটা রাখার জন্য সাইন করতে হবে। ই-মেইলের একটি লিঙ্কে ক্লিক করার পরিবর্তে সরাসরি মেম্বার ওয়েবসাইটে সাইন করুন।

০৫. ইউআর ইনফেক্টেড : একটি মেসেজ দাবি করে যে আপনি ভাইরাসে আক্রান্ত হয়েছেন। সুতরাং এখানে তা ফিক্স করুন। এ জন্য শুধু অ্যান্টিভাইরাস রান করে চেক করুন।

০৬. ইউ হ্যাভ ওউন : এতে দাবি করা হয় যে আপনি একটি প্রতিযোগিতায় জিতেছেন, যেখানে কখনই অংশ নেননি। যেহেতু আপনি তেমন কোনো সৌভাগ্যবান ব্যক্তি নন, তাই এ ই-মেইল মেসেজটি ডিলিট করে দিতে পারবেন নিশ্চিন্তে।

০৭. দি ব্যাংক নোটিফিকেশন : একটি ই-মেইলে কয়েক ধরনের ডিপোজিট বা উইথড্রলের দাবি করা হয়। যদি তেমনভাবে এমনটি ঘটে থাকে, তাহলে এটি হবে আপনার ব্যাংকের জন্য এক উচ্চাকাঙ্ক্ষী প্রচেষ্টা। সুতরাং কোনো কিছু করার আগে আপনার ব্যাংকের সাথে যোগাযোগ করাটা হবে সবচেয়ে নিরাপদ উপায়।

০৮. প্লেয়িং দ্য ভিকটিম : এ ধরনের মেইল আপনাকে খারাপ লোকে পরিণত করবে এবং দাবি করবে আপনি কোনোভাবে তাদেরকে আঘাত করেছেন। যদিও এটি বিশ্বাস করা কঠিন, তারা কোনো বৈধ উপায়ে বা অন্য কোনো ব্যক্তির মাধ্যমে এর সমাধান করে নিতে চায়।

০৯. দি ট্যাক্সম্যান : এই ই-মেইল আচরণ করে আইআরএস হিসেব এবং দাবি করে আপনি আর্থিক কষ্টে আছেন। এ ইস্যুতে আইআরএস আপনার সাথে ই-মেইলের মাধ্যমে যোগাযোগ করবে না। এগুলো ডিলিট করে দিয়ে সরে যান।

১০. দি সিকিউরিটি চেক : এটি খুব সাধারণ একটি ফিশিং স্ক্যাম। এর মাধ্যমে কোম্পানি শুধু আপনার অ্যাকাউন্ট নম্বর ভেরিফাই করতে চায়। কোনো কোম্পানিই ই-মেইলের মাধ্যমে অ্যাকাউন্ট নম্বর চাইবে না। সুতরাং এর বৈধতা যাচাই করার জন্য কোম্পানির ওয়েবসাইটে অ্যাক্সেস করুন।

নিজেকে রক্ষা করবেন যেভাবে

নিজেকে রক্ষা করার সবচেয়ে সহজ উপায় হলো সন্দেহজনক ই-মেইল ওপেন না করা। সবাই জানি, এ কাজটি করার চেয়ে বলা অনেক সহজ। কেননা, ভুল হয়ে থাকে আমাদের অজান্তেই। সিকিউরিটি সফটওয়্যার প্রোভাইডার নর্টনের ভাষ্যমতে, আত্মরক্ষার সবচেয়ে সেরা উপায় হলো ই-মেইলের মাধ্যমে কাউকে পার্সোনাল ইনফরমেশন না দেয়া এবং সাধারণ তথ্যের জন্য যেসব রিকোয়েস্ট আসে সে ব্যাপারে সচেতন থাকা কজ

ফিডব্যাক : siam.moazzem@gmail.com