ফিশিং অ্যাটাক | ই-কমার্সের নিরাপত্তা হুমকি

মোহাম্মদ জাবেদ মোর্শেদ চৌধুরী

দিন দিন জনপ্রিয় হয়ে উঠছে অনলাইন শপিং। ওয়েবসাইট কিংবা ফেসবুক ফ্যানপেজের মাধ্যমে উদ্যোক্তারা পণ্য বিক্রি করছেন। শুধু নতুন পণ্যই নয়, পুরনো পণ্য বাসায় বা অফিসে বসে সহজেই কিনতে পারছেন ক্রেতারা। সংশ্লিষ্টরা বলছেন, সবকিছু ছাপিয়ে অনলাইনের এই কেনাকাটা জীবনযাত্রাকে যেমন সহজ করেছে, তেমনি তরুণ উদ্যোক্তা শ্রেণীও গড়ে উঠছে এর মাধ্যমে। এসব ওয়েবসাইট অ্যাক্সেস করার জন্য একজন ব্যবহারকারীকে তার ক্রেডিট কার্ড বা ডেবিড কার্ড ব্যবহার করতে হয়। এখন যদি কেউ তার ফিন্যান্সিয়াল তথ্য চুরি করতে পারেন তবে তিনি সেই তথ্য ব্যবহার করে নিজের জন্য কোনো পণ্যও কিনতে পারেন। এ ধরনের তথ্য চুরির জন্য সবচেয়ে বড় প্রচলিত ও ভয়ঙ্কর নিরাপত্তা আক্রমণ হলো ফিশিং অ্যাটাক।

মাছকে ধোঁকা দিয়েই আমরা মাছ ধরি অর্থাৎ আমাদের বড়শিতে গেঁথে দেয়া খাদ্য মাছ খেতে আসে। তারপর সে নিজেই আমাদের খাদ্যে পরিণত হয়ে যায়। এই ফিশিংয়ের মতো আপনিও Phisher/Hacker-দের ফিশিং জালে আটকা পড়ে যেতে পারেন। ফিশিং ব্যাপারটি এমনই। কমপিউটার ব্যবহারকারীকে ধোঁকা দিয়ে ব্যবহারকারীর সব তথ্য ফিশার নিয়ে নেবে। কীভাবে ঘটতে পারে ব্যাপারটি?

০১. ব্যবহারকারী যেসব ওয়েবসাইট ব্যবহার করেন সে ধরনের কোনো একটি ওয়েবসাইটের হুবহু একটি লগইন পেজ পাঠানো হয় ব্যবহারকারীকে। সাধারণত এটি ই-মেইলের মাধ্যমে হয়ে থাকে।

০২. ই-মেইলের মাধ্যমে একজন হ্যাকার একটি ফেক লিঙ্ক দিয়ে থাকে। ব্যবহারকারী সেই লিঙ্কে ক্লিক করলে সেই ফেক ওয়েবসাইটে যাবে। এখন যদি ব্যবহারকারী সেখানে তার ইউজারনেম, পাসওয়ার্ড ও ক্রেডিট কার্ডের তথ্য দেন তবে তা ওই সাইটে না গিয়ে সেই ফেক ওয়েবসাইটের মাধ্যমে হ্যাকারের কাছে চলে যাবে।

০৩. তারপর হ্যাকার ব্যবহারকারীকে জানায় যে তার দেয়া তথ্যগুলো ভুল। কিন্তু প্রকৃতপক্ষে সে ব্যবহারকারীর এসব গোপনীয় তথ্য নিজের কমপিউটার বা সার্ভারে কপি করে রাখে এবং পরে তা ব্যবহার করে।

যেভাবে নিজেকে নিরাপদ রাখবেন

এই টিপগুলো আপনাকে যথেষ্ট নিরাপদে রাখবে ঠিকই, তবে মনে রাখতে হবে, সাইবার অপরাধীরাও তাদের প্রতারণায় সফল হতে নতুন নতুন উপায় বের করতে সচেষ্ট আছে, যাতে আপনি সহজেই তাদের ভুয়া সাইট ও ফিশিং ই-মেইলে প্রলুব্ধ হন। আপনি যেসব বিষয়ের প্রতি সতর্ক দৃষ্টি রাখতে পারবেন বা মনে রাখতে পারবেন এই টিপগুলো শুধু সেগুলোই, যা কোনো সাইটের বৈধতা সম্পর্কে আপনার মনে প্রশ্ন জাগাতে সাহায্য করতে পারে। নিচে এ ধরনের কিছু উপায় উল্লেখ করা হলো, যা সাইবার অপরাধীদের নেটওয়ার্কে ধরা না পড়তে আপনাকে সাহায্য করবে :

০১. নিজেকে শিক্ষিত করা : সর্বশেষ প্রতারণার ঘটনাগুলো পড়ুন ও জানুন। সর্বাধুনিক ফিশিংগুলোর চেহারা কেমন তা দেখুন, যাতে সহজ প্রতারণার কৌশলগুলো আপনি নিজেই ধরতে পারেন।

০২. সাধারণ জ্ঞানের ব্যবহার : সতর্কতার সাথে আপনার মেইলগুলো পড়ুন। প্রথমে দেখতে হবে প্রেরককে চেনা যাচ্ছে কি না। যেকোনো মেইল, যাতে আপনার ব্যক্তিগত গোপনীয় ও অর্থ সংক্রান্ত তথ্যগুলোর বিষয় উল্লেখ করা থাকে, সেগুলোর ব্যাপারে অবশ্যই সন্দেহ পোষণ করুন। কোনো প্রেরককে না চিনলে বা বিশ্বস্ত মনে না হলে তার পাঠানো এটাচমেন্টগুলো বা ফাইলগুলো খোলার ক্ষেত্রে সর্বোচ্চ সতর্কতা অবলম্বন করুন।

০৩. স্মার্ট সার্ফিং অনুশীলন : আপনি যখনই কোনো ওয়েবসাইট ভিজিট করবেন ও কোনো তথ্য দেবেন, তার আগে অবশ্যই লক্ষ রাখবেন সাইটটি নিরাপদ কি না। যদি সন্দেহ হয়, তাহলে একটি ভুয়া পাসওয়ার্ড ব্যবহার করুন এবং ফিশিং সাইট হলে এই ভুয়া পাসওয়ার্ডই এটি গ্রহণ করবে। অধিকতর নিরাপদ থাকার জন্য আপনি এমন সার্চ ইঞ্জিন ব্যবহার করুন, যা ভুল বানান ধরতে পারে ও ভুয়া সাইটে আপনার তথ্য দেয়া থেকে বিরত রাখতে পারে। এছাড়া সার্চ টুল যেমন : ম্যাকাফি, সাইটঅ্যাডভাইজর ইত্যাদি ব্যবহার করতে পারেন, যেগুলো সার্চ রেজাল্টে এটিও দেখাবে যে সাইটগুলো নিরাপদ কি না।

০৪. নিরাপত্তাপ্রযুক্তি ব্যবহার করা : এন্টিফিশিংসহ ব্যাপকভিত্তিক নিরাপত্তা সম্পন্ন সফটওয়্যার ব্যবহার করা যেতে পারে, যা আপনাকে নিরাপদ রাখতে পারে। আপনি নিশ্চিত হয়ে নিন, আপনার সফটওয়্যারটি সর্বাধুনিক ভার্সন এবং এতে অটোআপডেট অপশন বা কন্ট্রোল প্যানেলে আপডেট অপশন আছে কি না।

০৫. সবসময় সতর্ক থাকুন : আপনি যখন অফলাইনে থাকবেন তখনও সতর্ক থাকুন এবং নিয়মিত মনিটর করুন আপনার ব্যাংক ও ক্রেডিট কার্ডের অ্যাকাউন্টে কোন ধরনের সন্দেহজনক লেনদেন (চার্জ বা ট্রান্সফার) হয়েছে কি না। পাসওয়ার্ডটি নিয়মিত পরিবর্তন করুন। আপনি নিশ্চিত হোন, পাসওয়ার্ডটি যেনো যথেষ্ট শক্তিশালী হয় এবং এতে নাম্বার, লেটার ও বিশেষ চিহ্নের সমন্বয়ে হয়। পাসওয়ার্ডে কোনোভাবেই নিকনেম বা জন্ম তারিখ বা এ ধরনের কোনো ব্যক্তিগত তথ্য দেয়া যাবে না, যা অন্য কেউ জানতে পারে।

০৬. সন্দেহজনক কিছু হলেই রিপোর্ট করুন : আপনার কাছে যদি সন্দেহজনক কোনো কিছু মনে হয়, তবে তা সাথে সাথে সংশ্লিষ্ট ব্যাংক বা কোম্পানিতে রিপোর্ট করুন। যদিও ফিশিং খুবই সাধারণ বিষয়, কিন্তু সচেতনতা ও সঠিক পূর্বসতর্কতা আপনাকে অনেকদূর পর্যন্ত নিরাপত্তা দিতে পারে।

ভুয়া ওয়েবসাইট চেনার উপায়

আপনি কোনো ভুয়া সাইট ব্যবহার করছেন নাকি ফিশিং ই-মেইলে তথ্য দিচ্ছেন, তা নিম্ন উপায়ে শনাক্ত করা যাবে :

০১. অশুদ্ধ ইউআরএল ব্যবহার : যদি আপনার ব্যাংক অ্যাকাউন্টে একটি নিয়মিত অ্যাড্রেসের মাধ্যমে প্রবেশ করে থাকেন এবং যদি কখনও দেখেন অ্যাড্রেসটি মিলছে না, তাহলে নিশ্চিত হতে পারেন ওয়েবসাইটটি ভুয়া। সবসময় অন্তত দুইবার চেক করুন যে সাইটটি সঠিক, ভুয়া নয়।

ই-মেইলটির সত্যতা যাচাইয়ের জন্য ই-মেইলের লিঙ্কে আপনার মাউস পয়েন্টারটি রেখে দেখতে পারেন লিঙ্কটি এবং ই-মেইলটি একই সাইট থেকে এসেছে কি না।

০২. ব্যাংকিং তথ্য জিজ্ঞেস করা : ব্যাংক কখনও আপনার ব্যাংক অ্যাকাউন্ট তথ্য, যেমন : ডেবিট কার্ড ও পিন নাম্বার ই-মেইলে চাইবে না। ওই সব ই-মেইল ও সাইট থেকে সতর্ক থাকুন, যেগুলো আপনার গোপনীয় তথ্য (যেমন : সোশ্যাল সিকিউরিটি নাম্বার) চাইবে, যা স্ট্যান্ডার্ড লগইনের পরিপন্থী।

০৩. পাবলিক ইন্টারনেট অ্যাকাউন্ট ব্যবহার করা : যেকোনো লিঙ্কে ক্লিক করার আগে প্রেরকের ই-মেইল অ্যাড্রেসটি দেখে নিন।

(বাকি অংশ ৬৮ পৃষ্ঠায়)