ফিশিং

সহজ কিন্তু ভয়াবহ সাইবার হামলা

মোহাম্মদ জাবেদ মোর্শেদ চৌধুরী

নাজিয়া কাজ করে একটি মাল্টিন্যাশনাল কোম্পানিতে। সব কাজে নিজেকে এগিয়ে রাখতে ও সময় বাঁচাতে বরাবর তথ্যপ্রযুক্তির ওপর নির্ভর করে। মাস গেলে তার বেতনও সরাসরি চলে যায় নিজের ব্যাংক অ্যাকাউন্টে। নিজের ল্যাপটপে বসে খুব সহজেই অনলাইন ব্যাংকিংয়ের মাধ্যমে বিদ্যুৎ বিল, ওয়াসার বিল, মোবাইল রিফিল করা, এমনকি ছোট মেয়ের স্কুলের বেতনও দিয়ে থাকে। এতে তার জীবন বেশ স্বাচ্ছন্দ্যময়। অনেক সময়ও বাঁচে নিজের ও পরিবারের সাথে কাটানোর জন্য। কিন্তু গত মাসে নিজের অনলাইন ব্যাংক অ্যাকাউন্টে লগইন করে তো নাজিয়া হতভম্ব। তার অ্যাকাউন্ট থেকে ৫০ হাজার টাকা গায়েব। নাজিয়া কোনোমতেই মনে করতে পারে না কীভাবে এই টাকা তার অ্যাকাউন্ট থেকে গায়েব হলো। সে নিজে তথ্যপ্রযুক্তির একজন সাধারণ ব্যবহারকারী। তাই সে চিন্তা করলে তার আইটি এক্সপার্ট কলিগের সাথে ব্যাপারটা শেয়ার করবে। তাদের আলোচনায়ই বের হয়ে আসে, কিছুদিন আগে ব্যাংক থেকে পাওয়া ঠিকানা চেঞ্জের ই-মেইল আসে। কিন্তু ইউজারনেম ও পাসওয়ার্ড দেয়ার পরও সে নিজের ঠিকানা পরিবর্তন করতে পারেনি। সাথে সাথে সবাই বুঝে যায় নাজিয়া আসলে বহুল প্রচলিত হ্যাকিং পদ্ধতি 'ফিশিং' অ্যাটাকের শিকার।

যারা প্রতিনিয়ত ইন্টারনেট ব্যবহার করছেন, তাদের কাছে অতিপরিচিত একটি সাইবার ক্রাইমের নাম ফিশিং। এর নাম শুনেছেন অনেকেই, কিন্তু সঠিক ধারণা আছে ফিশিং নিয়ে এমন ব্যবহারকারীর সংখ্যা বেশ কম, যার প্রমাণ আমরা ফেসবুকে ভাইরাল স্প্যাম লিঙ্ক ছড়ানোর সময় প্রতিনিয়ত পাচ্ছি। চলুন দেখা যাক ফিশিং কত ধরনের ও কী কী এবং কীভাবে এর হাত থেকে রক্ষা পাবেন।

ফিশিং : ফিশিং হচ্ছে এমন কার্যক্রম, যাতে ইলেকট্রনিক যোগাযোগ ব্যবস্থায় তথ্যাদি সংগ্রহের জন্য কোনো বিশ্বস্ত মাধ্যমের ছদ্মবেশ ধারণ করা। সাধারণত জনপ্রিয় সামাজিক যোগাযোগমাধ্যম, ব্যাংক, আইটি অ্যাডমিনিস্ট্রেটরদের ওয়েবসাইট প্রভৃতির মাধ্যমে জনসাধারণকে প্রলোভিত করে ফিশিং সাইটের লিঙ্কগুলো সাধারণত ই-মেইল বা ইনস্ট্যান্ট ম্যাসেজিংয়ের মাধ্যমে পাঠানো হয়। ই-মেইলে কোনো ফেক ওয়েবসাইটের লিঙ্ক দেয়া হয়, যাতে ক্লিক করলেই ইউজারকে নকল ফিশিং ওয়েবসাইটটিতে নিয়ে যায়, যা দেখতে আসল অফিশিয়াল ওয়েবসাইটটির মতোই মনে হয়। ফিশিংয়ের মাধ্যমে বর্তমান ইন্টারনেট পরিস্থিতির দুর্বল নিরাপত্তা ব্যবস্থাকে অবৈধভাবে নিজের কাজে ব্যবহার করা হয়।

ফিশিং পদ্ধতির বিভিন্ন ধরন রয়েছে। নিচে এসব ধরনের মধ্যে কিছু উপস্থিত হলো :

স্পেয়ার ফিশিং : যেখানে কিছু ব্যক্তি মিলে বা একটি কোম্পানি কোনো বিশেষ ব্যক্তির সম্পর্কে তথ্য জোগাড় করে সম্ভাব্য সাফল্যের জন্য।

কোলন ফিশিং : আগে প্রেরিত কোনো ই-মেইলের ক্লোন করে এর কনটেন্টগুলো বা লিঙ্কগুলো পরিবর্তনের পর অন্য ই-মেইল অ্যাড্রেস থেকে পাঠানো হয়। যেমন মনে হয়, এটি প্রকৃত অ্যাড্রেস থেকে প্রেরিত। আগে আক্রান্ত কোনো কমপিউটার থেকে এ ধরনের মেইল পাঠানো যায়।

লিঙ্ক ম্যানিপুলেশন : এর মাধ্যমে আক্রান্ত কোনো ম্যালিশাস ওয়েবসাইটে রিডিরেক্ট হতে পারে। ফিশার সাধারণত ভুল অথবা অন্য লিঙ্ক অথবা সাব ডোমেইনগুলো ব্যবহার করে থাকে।

ফিল্টার ইভেশন : ফিশারেরা টেক্সটের বদলে ইমেজ লিঙ্ক হিসেবে ব্যবহার করতে শুরু করে যেন অ্যান্টি ফিশিং ফিল্টারের কাছে ধরা না পড়ে।

ওয়েবসাইট ফরগ্রেরে : একবার ফিশিং ওয়েবসাইট ভিজিট করার পরই এর চাতুরী শেষ নয়। ফিশারেরা জাভা স্ক্রিপ্ট ব্যবহার করতে পারে অ্যাড্রেস বার পরিবর্তনের জন্য। এ ছাড়া কোনো সত্যিকারের ওয়েবসাইটের কোনো ফটো অ্যাড্রেস বারে স্থাপনের মাধ্যমে। আরও কিছু ট্রিক ব্যবহার হয়, যা ধরতে হলে আরও বেশি জ্ঞানী হতে হবে। এ ছাড়া ফ্ল্যাশ টেকনোলজির মাধ্যমে এর ওপর নির্ভরশীল ওয়েবসাইটে ফ্ল্যাশ ফিশিং ব্যবহার করা হয় অ্যান্টি ফিশিং পদ্ধতিগুলোকে ধোঁকা দিতে।

ফোন ফিশিং : এটি প্রমাণ করে যে সব ফিশিংয়ের জন্য ওয়েবসাইটের প্রয়োজন হয় না। এ ক্ষেত্রে কোনো ব্যক্তির ফোন নাম্বার সংগ্রহের পর তাকে ফোন করে বিভিন্ন তথ্য বলতে বা ডায়াল করে দিতে প্ররোচিত করে। এ ছাড়া ফিশিংয়ের আরও টেকনিক রয়েছে। আপনি খুব সহজে কোডিং না জেনেও কোনো জনপ্রিয় ওয়েবসাইটের কপি করে কোনো ফ্রি বা পেইড সার্ভারে আপলোড করে ফিশিং করতে পারেন।

যেভাবে নিজেকে নিরাপদ রাখবেন

এই টিপগুলো আপনাকে অনেকদূর পর্যন্ত নিরাপদে রাখবে ঠিকই, কিন্তু মনে রাখতে হবে, সাইবার অপরাধীরাও তাদের প্রতারণায় সফল হতে নতুন নতুন উপায় বের করতে সচেষ্ট আছে, যাতে আপনি সহজেই তাদের ভুয়া সাইট এবং 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 করতে পারে :

০১. নিজেকে শিক্ষিত করা : সর্বাধুনিক প্রতারণার ঘটনাগুলো পড়ুন এবং জানুন। সর্বাধুনিক ফিশিংগুলোর চেহারা কেমন তা দেখুন, যাতে সহজে 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, যেখানে আপনার ব্যক্তিগত গোপনীয় এবং অর্থ সংক্রান্ত তথ্যগুলোর বিষয় উল্লেখ করা থাকে, সেগুলোর ব্যাপারে অবশ্যই সন্দেহ পোষণ করুন। কোনো প্রেরককে না চিনলে বা বিশ্বস্ত মনে না হলে, তার পাঠানো অ্যাটাচমেন্টগুলো বা ফাইলগুলো খোলার ক্ষেত্রে সর্বোচ্চ সতর্কতা অবলম্বন করুন।

০৩. স্মার্ট সার্ফিং অনুশীলন : আপনি যখনই কোনো ওয়েবসাইট ভিজিট করবেন এবং 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 এবং ভুয়া সাইটে আপনার তথ্য দেয়া থেকে বিরত রাখতে পারে। এছাড়া সার্চ টুল যেমন– ম্যাকাফি, সাইট অ্যাডভাইজর ইত্যাদি ব্যবহার করতে পারেন, যার সার্চ রেজাল্টে এটিও দেখাবে, সাইটগুলো নিরাপদ কি না।

০৪. নিরাপত্তার জন্য টেকনোলজি ব্যবহার করা : অ্যান্টিফিশিংসহ ব্যাপকভিত্তিক নিরাপত্তাসম্পন্ন সফটওয়্যার ব্যবহার করা যেতে পারে, যা আপনাকে নিরাপদ রাখতে পারে। আপনি নিশ্চিত হয়ে নিন, আপনার সফটওয়্যারটি সর্বাধুনিক ভার্সন এবং এতে অটো আপডেট অপশন বা কন্ট্রোল প্যানেলে আপডেট অপশন আছে কি না।

০৫. সর্বদা সতর্ক থাকুন : যখন অফলাইনে থাকবেন তখনও সতর্ক থাকুন এবং নিয়মিত মনিটর করুন আপনার ব্যাংক ও ক্রেডিট কার্ডের অ্যাকাউন্টে কোনো ধরনের সন্দেহজনক লেনদেন (চার্জ বা ট্রান্সফার) হয়েছে কি না। পাসওয়ার্ডটি নিয়মিত পরিবর্তন করুন। আপনি নিশ্চিত হোন,

(বাকি অংশ ৬৬ পৃষ্ঠায়)

ফিশিং

(৬৪ পৃষ্ঠার পর)

পাসওয়ার্ডটি যেন যথেষ্ট শক্তিশালী হয় এবং নাম্বার, লেটার ও বিশেষ চিহ্নের সমন্বয়ে হয়। পাসওয়ার্ডে কোনোভাবেই নিকনেম বা জন্মতারিখ বা এ ধরনের কোনো ব্যক্তিগত তথ্য দেয়া যাবে না, যা অন্য কেউ জানতে পারে।

০৬. সন্দেহজনক মনে হলে 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 এবং সঠিক পূর্বসতর্কতা আপনাকে অনেক দূর পর্যন্ত নিরাপত্তা দিতে পারে।

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

০১. অশুদ্ধ ইউআরএল ব্যবহার : যদি আপনি ব্যাংক অ্যাড্রেসে একটি নিয়মিত অ্যাড্রেসের মাধ্যমে প্রবেশ করে থাকেন এবং যদি কখনও দেখেন যে, অ্যাড্রেসটি মিলছে না, তাহলে আপনি নিশ্চিত হন, ওয়েবসাইটটি ভুয়া। সব সময় অন্তত দুইবার চেক করুন সাইটটি সঠিক না ভুয়া।

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

০২. ব্যাংকিং তথ্য জিজ্ঞেস করা : ব্যাংক কখনও আপনার ব্যাংক অ্যাকাউন্ট তথ্য, যেমন– ডেবিট কার্ড এবং পিন নাম্বার ই-মেইলে চাইবে না। ওইসব 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 লিঙ্ক ক্লিক করার আগে প্রেরকের ই-মেইল অ্যাড্রেসটি একটু দেখে নিন। ই-মেইলটি কোনো পাবলিক অ্যাকাউন্ট থেকে আসা সত্ত্বেও দাবি করে যে, এটি আপনার ব্যাংক বা অন্য ব্যবসায় প্রতিষ্ঠান থেকেই এসেছে, তাহলে তা কখনও বিশ্বাস করবেন না। এছাড়া কোনো ই-মেইল বা ওয়েবসাইট কখনও বিশ্বাস করবেন না, যা আপনার গোপনীয় তথ্য দিয়ে কনফার্ম করতে বলবে। কারণ, এগুলো নিশ্চিতভাবেই প্রতারণা।

তাছাড়া ব্যাংক বা অন্য ব্যবসায় প্রতিষ্ঠানের পাঠানো ই-মেইলে অবশ্যই আপনার নাম উল্লেখ করে সম্বোধন করা থাকবে প্রতিষ্ঠানটির সাথে আপনার সম্পর্ক বোঝানোর জন্য। যেমন– লেখা থাকবে 'প্রিয় মি. আবির', 'প্রিয় কাস্টমার' কখনই নয়। 'প্রিয় কাস্টমার' হিসেবে সম্বোধন করলে সেই ই-মেইলের ব্যাপারে সতর্কতা অবলম্বন করুন।

০৪. ভুল বানান লেখা থাকলে : যদি কোনো ব্যাংক আপনার অ্যাকাউন্ট এই ধরনের ভুল বানানে লিখে থাকে 'acccount', তাহলে আপনি নিশ্চিতভাবেই ধরে নিতে পারেন এটি একটি ফিশিং ই-মেইল বা ভুয়া ওয়েবসাইট। প্রকৃত কোম্পানিতে পর্যাপ্ত স্টাফ থাকে এই ধরনের বানান ভুল পরীক্ষা করার জন্য। যদি আপনি এই ধরনের বানান ভুল বা কোম্পানির নামের বানান ভুল দেখতে পান, তাহলে আর ক্লু খোঁজেন। নিশ্চিত না হয়ে আপনার ব্যাংক অ্যাকাউন্ট সংক্রান্ত কোনো গোপনীয় তথ্য দেবেন না।

০৫. সিকিউর সাইট যদি না হয় : বৈধ ই-কমার্স সাইটে আপনার পেমেন্ট সংক্রান্ত যাবতীয় তথ্য নিরাপদ রাখার জন্য এনক্রিপশন বা স্ক্র্যাম্বলিং ব্যবহার করা হয়। ব্রাউজার উইন্ডো তো লক সিম্বল দেখেই বোঝা যাবে সাইটটিতে এনক্রিপশন ব্যবহার করা হয়েছে কি না। এই লক সিম্বলে ক্লিক করলে এটি আপনাকে ভেরিফাইয়ের অনুমোদন দেবে, সাইটটির জন্য কোনো সিকিউরিটি সার্টিফিকেট ইস্যু করা হয়েছে কি না, যা প্রমাণ করে এটি একটি বৈধ ও বিশ্বস্ত সাইট। আমাদেরকে আরও চেক করতে হবে, অ্যাড্রেসটি শুরু হয়েছে https:// দিয়ে, শুধু http:// দিয়ে নয়। কোনো সাইটের নিরাপত্তা নিশ্চিত না হয়ে কোনো ধরনের পেমেন্ট তথ্য দেয়া যাবে না।

০৬. খুব নিম্নমানের রেজ্যুলেশন ইমেজ প্রদর্শন : প্রতারকেরা সাধারণত অতি দ্রুত ভুয়া সাইট তৈরি করে। ফলে এগুলো হয় নিম্নমানের। যদি লোগো বা টেক্সট নিম্ন রেজ্যুলেশনের হয়, তাহলে সাইটটি ভুয়া হওয়ার সম্ভাবনা বাড়িয়ে দেয় কজ

ফিডব্যাক : jabedmorshed@yahoo.com