

# Home Work 01

**Q1: How does an organization differentiate between a legitimate user and a malicious user?**

একটি প্রতিষ্ঠান কীভাবে বৈধ ব্যবহারকারী এবং ম্যালিশিয়াস ব্যবহারকারীকে আলাদা করে?

একটি প্রতিষ্ঠান লিগিটিমেট (বৈধ) ব্যবহারকারী এবং ম্যালিশিয়াস (ক্ষতিকর) ব্যবহারকারী চিহ্নিত করতে নিরাপত্তা নীতিমালা, অ্যানালিটিকস, এবং মনিটরিং সিস্টেম ব্যবহার করে। নিচে কিছু গুরুত্বপূর্ণ কৌশল ব্যাখ্যা করা হলো—

---

## ❶ পরিচয় যাচাই ও অটেনটিকেশন (Authentication & Identity Verification)

✓ বৈধ ব্যবহারকারী → সঠিক ইউজারনেম, পাসওয়ার্ড, **2FA (Two-Factor Authentication)** ব্যবহার করে লগইন করে।

✗ ম্যালিশিয়াস ব্যবহারকারী → ফিশিং, পাসওয়ার্ড গেসিং, ব্রুট-ফোর্স অ্যাটাকের মাধ্যমে প্রবেশ করতে চায়।

✓ প্রতিরোধ ব্যবস্থা:

- **Multi-Factor Authentication (MFA):** পাসওয়ার্ডের পাশাপাশি OTP, ফিঙ্গারপ্রিন্ট বা ফেস স্ক্যান ব্যবহার করা।

- **Biometric Authentication:** ব্যবহারকারীর ফিঙ্গারপ্রিন্ট বা আইরিস স্ক্যান ব্যবহার করে পরিচয় নিশ্চিত করা।
- 

## ❷ আচরণগত বিশ্লেষণ (User Behavior Analytics - UBA)

✓ বৈধ ব্যবহারকারী → সাধারণত একই সময়ে, নির্দিষ্ট ডিভাইস থেকে, স্বাভাবিক কাজ করে।

✗ ম্যালিশিয়াস ব্যবহারকারী → অস্বাভাবিক সময়ে লগইন করে, একই সঙ্গে বিভিন্ন স্থানে প্রবেশের চেষ্টা করে।

✓ প্রতিরোধ ব্যবস্থা:

- **AI & Machine Learning** ব্যবহার করে ব্যবহারকারীর স্বাভাবিক কার্যক্রম নিরীক্ষণ করা।
  - যদি কেউ অস্বাভাবিক কার্যকলাপ করে (যেমন: হঠাৎ প্রচুর ডাটা ডাউনলোড করা), তাহলে সতর্কতা পাঠানো হয় বা অ্যাক্সেস ব্লক করা হয়।
- 

## ❸ লগ ও মনিটরিং (Log Monitoring & SIEM - Security Information and Event Management)

✓ বৈধ ব্যবহারকারী → নির্দিষ্ট ডিভাইস ও নির্দিষ্ট আইপি থেকে স্বাভাবিক কার্যক্রম করে।

✗ ম্যালিশিয়াস ব্যবহারকারী → **VPN** বা **Tor** ব্যবহার করে লুকিয়ে প্রবেশের চেষ্টা করে, অথবা ব্যাকডোর খুলতে চায়।

✓ প্রতিরোধ ব্যবস্থা:

- **SIEM (Security Information and Event Management)** সিস্টেম ব্যবহার করে সন্দেহজনক লগ এবং সিস্টেম ইভেন্ট পর্যবেক্ষণ করা।
- অনুসন্ধান করা: কোন ব্যবহারকারী অনিয়মিত সময়ে অ্যাক্সেস করছে, অসংখ্যবার লগইন ফেইল করছে, বা ডাটা চুরি করছে কি না।

---

#### ❏ অনুমতি ও অ্যাক্সেস কন্ট্রোল (Role-Based Access Control - RBAC)

✓ বৈধ ব্যবহারকারী → শুধুমাত্র তার কাজের জন্য প্রয়োজনীয় ফাইল ও ডাটা অ্যাক্সেস করতে পারে।

✗ ম্যালিশিয়াস ব্যবহারকারী → অপ্রয়োজনীয় ফাইল ও সিস্টেম অ্যাক্সেস করার চেষ্টা করে।

✓ প্রতিরোধ ব্যবস্থা:

- **Zero Trust Security Model** অনুসরণ করা (কেউ বিশ্বাসযোগ্য নয়, সবাইকে যাচাই করতে হবে)।
- **Least Privilege Policy**: প্রতিটি ব্যবহারকারীকে শুধু তার প্রয়োজনীয় অ্যাক্সেস দেওয়া হবে।

---

#### ❏ অস্বাভাবিক নেটওয়ার্ক ট্রাফিক পর্যবেক্ষণ (Anomaly Detection in Network Traffic)

✓ বৈধ ব্যবহারকারী → নির্দিষ্ট IP ও নির্দিষ্ট জায়গা থেকে সাধারণ ট্রাফিক তৈরি করে।

✗ ম্যালিশিয়াস ব্যবহারকারী → VPN/Tor ব্যবহার করে একাধিক IP থেকে অনুপ্রবেশের চেষ্টা করে বা অস্বাভাবিকভাবে অনেক ডাটা ডাউনলোড করে।

✓ প্রতিরোধ ব্যবস্থা:

- **Intrusion Detection System (IDS) এবং Intrusion Prevention System (IPS)** ব্যবহার করে সন্দেহজনক ট্রাফিক ব্লক করা।
  - **Geo-Location Restrictions**: যদি কোনও অ্যাক্সেস অপ্রত্যাশিত দেশ বা লোকেশন থেকে আসে, তাহলে তা চিহ্নিত করে অ্যাক্সেস ব্লক করা।
-

## ❖ ডাটা এক্সফিলট্রেশন (Data Exfiltration) সনাক্তকরণ

✓ বৈধ ব্যবহারকারী → স্বাভাবিক পরিমাণে ডাটা ব্যবহার করে।

✗ ম্যালিশিয়াস ব্যবহারকারী → বিশাল পরিমাণে সংবেদনশীল তথ্য ডাউনলোড বা ট্রান্সফার করার চেষ্টা করে।

✓ প্রতিরোধ ব্যবস্থা:

- **DLP (Data Loss Prevention)** সিস্টেম ব্যবহার করে সংবেদনশীল তথ্যের অস্বাভাবিক স্থানান্তর সনাক্ত করা।
  - অস্বাভাবিক ডাউনলোড বা আপলোড হলে সিকিউরিটি টিমকে সতর্ক করা।
- 

## ❖ ডিভাইস ও ব্রাউজার ফিঙ্গারপ্রিন্টিং (Device & Browser Fingerprinting)

✓ বৈধ ব্যবহারকারী → নির্দিষ্ট ব্রাউজার, ডিভাইস, এবং অপারেটিং সিস্টেম ব্যবহার করে।

✗ ম্যালিশিয়াস ব্যবহারকারী → বারবার ডিভাইস বা ব্রাউজার পরিবর্তন করে, Incognito বা Tor ব্যবহার করে।

✓ প্রতিরোধ ব্যবস্থা:

- **Device & Browser Fingerprinting** টেকনোলজি ব্যবহার করে কোনো নতুন বা সন্দেহজনক ডিভাইস শনাক্ত করা।
- কোনো ব্যবহারকারী নতুন ডিভাইস থেকে লগইন করলে অতিরিক্ত যাচাই (2FA) বাধ্যতামূলক করা।

## Q2. What are some real-world examples of malicious user attacks?

ম্যালিশিয়াস ইউজারদের আক্রমণের বাস্তব উদাহরণ:

### ১. ইনসাইডার থ্রেট - টেসলা (২০২০)

- এক রাশিয়ান হ্যাকার টেসলার এক কর্মচারীকে \$১ মিলিয়ন অফার করেছিল, যেন সে কোম্পানির নেটওয়ার্কে ম্যালওয়্যার ইনস্টল করে।
- ম্যালওয়্যারটি সংবেদনশীল তথ্য চুরি ও নেটওয়ার্ক ধ্বংস করার জন্য ডিজাইন করা হয়েছিল।
- তবে সেই কর্মচারী টেসলা ও এফবিআই-কে জানায়, ফলে হ্যাকার গ্রেফতার হয়।

### ২. ফিশিং আক্রমণ - গুগল ও ফেসবুক (২০১৩-২০১৫)

- সাইবার অপরাধীরা গুগল ও ফেসবুকের কর্মচারীদের ফাঁদে ফেলে \$১০০ মিলিয়ন হাতিয়ে নেয়।
- তারা এক ভুয়া ভেন্ডর সেজে ফেক ইনভয়েস ও ইমেইল ব্যবহার করেছিল।
- দুই বছর পর এটি ধরা পড়ে।

### ৩. ক্রেডেনশিয়াল স্টাফিং - জুম (২০২০)

- হ্যাকাররা পুরোনো ডাটা ব্রিচ থেকে পাওয়া ৫ লাখ জুম অ্যাকাউন্টের লগইন তথ্য ব্যবহার করে অনুপ্রবেশ করে।
- এসব অ্যাকাউন্ট ডার্ক ওয়েবে বিক্রি করা হয়, ফলে অনেক মিটিং অননুমোদিত ব্যবহারকারীরা অ্যাক্সেস করে।

### ৪. সোশ্যাল ইঞ্জিনিয়ারিং - টুইটার (২০২০)

- হ্যাকাররা টুইটারের কিছু কর্মচারীকে প্রতারিত করে অভ্যন্তরীণ টুলের অ্যাক্সেস পায়।

- তারা ইলন মাস্ক, বারাক ওবামা, জেফ বেজোসসহ অনেকের অ্যাকাউন্ট হাইজ্যাক করে বিটকয়েন স্ক্যাম চালায়।
- ব্যবহারকারীদের কাছ থেকে \$১,২০,০০০ মূল্যের বিটকয়েন হাতিয়ে নেওয়া হয়।

#### ৫. র‍্যানসমওয়ার আক্রমণ - কলোনিয়াল পাইপলাইন (২০২১)

- DarkSide নামক হ্যাকার গ্রুপ ফাঁস হওয়া পাসওয়ার্ডের মাধ্যমে কলোনিয়াল পাইপলাইনের নেটওয়ার্কে প্রবেশ করে।
- এই আক্রমণে যুক্তরাষ্ট্রের পূর্ব উপকূলে জ্বালানি সরবরাহ বন্ধ হয়ে যায়।
- কোম্পানিটি হ্যাকারদের \$৪.৪ মিলিয়ন মুক্তিপণ দেয়।

#### ৬. ইনসাইডার ডাটা চুরি - মর্গান স্ট্যানলি (২০১৬ ও ২০২১)

- এক প্রাক্তন কর্মচারী গোপন কাস্টমার ডেটা চুরি করে এবং তা প্রতারণার কাজে ব্যবহার করতে চায়।
- ২০২১ সালে সংস্থার ভুলভাবে নিষ্ক্রিয় করা সার্ভার থেকে ডেটা ফাঁস হয়ে যায়।

#### ৭. সাপ্লাই চেইন আক্রমণ - সোলারওয়িন্ডস (২০২০)

- হ্যাকাররা সোলারওয়িন্ডসের সফটওয়্যার আপডেটে ব্যাকডোর ইনস্টল করে।
- এতে মার্কিন সরকারি সংস্থা ও ফরুচন ৫০০ কোম্পানিগুলো আক্রান্ত হয়।
- কয়েক মাস পরে এই গুপ্তচরবৃত্তিমূলক আক্রমণ ধরা পড়ে।

#### ৮. অননুমোদিত অ্যাক্সেস - ম্যারিয়ট ডাটা ব্রিচ (২০১৮)

- হ্যাকাররা চার বছর ধরে ম্যারিয়ট হোটেলের সিস্টেমে লুকিয়ে ছিল।
- এতে ৫০ কোটি অতিথির ব্যক্তিগত তথ্য ফাঁস হয়, যার মধ্যে পাসপোর্ট নম্বর, ক্রেডিট কার্ড ডিটেইলস অন্তর্ভুক্ত ছিল।

এই ঘটনা প্রমাণ করে যে ম্যালিশিয়াস ইউজাররা ফিশিং, সোশ্যাল ইঞ্জিনিয়ারিং, পাসওয়ার্ড চুরি, ইনসাইডার থ্রেট ব্যবহার করে বড় বড় প্রতিষ্ঠানের ক্ষতি করতে পারে।

### Q3 What types of malicious users exist (e.g., insider threats, external attackers)?

ম্যালিশিয়াস ইউজারের ধরন (ইনসাইডার থ্রেট, এক্সটার্নাল অ্যাটাকার )

#### ১. ইনসাইডার থ্রেট (সংস্থার অভ্যন্তরীণ হামলাকারী)

এই ধরনের আক্রমণকারী সাধারণত কর্মচারী, কন্ট্রাক্টর বা পার্টনার হয়ে থাকে, যারা নিজেদের অ্যাক্সেসের অপব্যবহার করে ক্ষতি করে।

- অসন্তুষ্ট কর্মচারী → ব্যক্তিগত ক্ষোভ থেকে ডাটা চুরি বা ধ্বংস করে।
- অবহেলামূলক কর্মচারী → অজান্তে ডাটা ফাঁস করে বা ফিশিং আক্রমণের শিকার হয়।
- দুষ্টু অভ্যন্তরীণ ব্যক্তি → ইচ্ছাকৃতভাবে সংস্থার গোপন তথ্য বিক্রি করে বা হ্যাকারদের সহায়তা করে।
- তৃতীয় পক্ষের কন্ট্রাক্টর → সংস্থার অ্যাক্সেস পেয়ে অপব্যবহার করতে পারে।

#### ◆ উদাহরণ:

- এক আইটি অ্যাডমিন চাকরি ছাড়ার আগে সংস্থার গুরুত্বপূর্ণ ফাইল মুছে ফেলে।

---

#### ২. এক্সটার্নাল অ্যাটাকার (বাইরের সাইবার অপরাধী)

এরা হ্যাকার বা সাইবার ক্রিমিনাল যারা নিরাপত্তা ভেঙে সংস্থার ডাটা চুরি বা ধ্বংস করার চেষ্টা করে।

##### A. সাইবার অপরাধী (আর্থিক লাভের উদ্দেশ্যে আক্রমণ করে)

- ভাড়াটে হ্যাকার → টাকার বিনিময়ে আক্রমণ চালায়।
- র‍্যানসমওয়্যার অপরাধী → ডাটা এনক্রিপ্ট করে মুক্তিপণ দাবি করে।

- ফিশার → প্রতারণামূলক ইমেইল বা ওয়েবসাইটের মাধ্যমে পাসওয়ার্ড ও আর্থিক তথ্য চুরি করে।

#### B. হ্যাকটিভিস্ট (রাজনৈতিক বা সামাজিক কারণে আক্রমণ করে)

- সরকার বা সংস্থার বিরুদ্ধে প্রতিবাদ করার জন্য সাইবার হামলা চালায়।
- DDoS, ওয়েবসাইট ডিফেসিং বা তথ্য ফাঁস করতে পারে।
- উদাহরণ: "Anonymous" হ্যাকিং গ্রুপ।

#### C. রাষ্ট্র-সমর্থিত হ্যাকার (APT - Advanced Persistent Threats)

- গোয়েন্দাবৃত্তি বা ধ্বংসাত্মক উদ্দেশ্যে সরকার-সমর্থিত হ্যাকাররা কাজ করে।
- উদাহরণ: SolarWinds হ্যাক (২০২০), যেখানে রাশিয়ার সন্দেহভাজন হ্যাকাররা মার্কিন সংস্থাগুলোর তথ্য চুরি করেছিল।

#### D. স্ক্রিপ্ট কিডিজ (অল্প দক্ষতাসম্পন্ন হ্যাকার)

- পূর্বনির্ধারিত হ্যাকিং টুল ব্যবহার করে, নিজেরা বেশি কিছু জানে না।
- মজার জন্য বা ছোটখাটো অর্থনৈতিক লাভের জন্য আক্রমণ চালায়।

---

### ৩. সাপ্লাই চেইন অ্যাটাকার

- ভেন্ডর বা তৃতীয় পক্ষের সফটওয়্যার আক্রমণ করে মূল সংস্থায় প্রবেশ করার চেষ্টা করে।
- উদাহরণ: SolarWinds হামলা, যেখানে একটি সফটওয়্যার আপডেট হ্যাক করে হাজার হাজার সংস্থা আক্রান্ত হয়েছিল।

---

### ৪. সোশ্যাল ইঞ্জিনিয়ার

- মানুষকে প্রতারণা করে সংবেদনশীল তথ্য বের করে।
- কৌশল: ফিশিং, বেইটিং, ইম্পারসোনেশন, প্রিটেক্সটিং।
- উদাহরণ: Twitter হ্যাক (২০২০) → হ্যাকাররা কর্মচারীদের ঠকিয়ে টুলের অ্যাক্সেস নিয়েছিল।



---

#### ৫. বট এবং স্বয়ংক্রিয় আক্রমণকারী

- বটনেট: হাজার হাজার সংক্রমিত ডিভাইস একসঙ্গে ব্যবহার করে বড়সড় সাইবার হামলা চালায়।
- ক্রেডেনশিয়াল স্টাফিং বট: ফাঁস হওয়া পাসওয়ার্ড ব্যবহার করে বিভিন্ন অ্যাকাউন্টে অনুপ্রবেশের চেষ্টা করে।
- উদাহরণ: Mirai Botnet (২০১৬) → বিশাল DDoS আক্রমণ চালিয়ে ইন্টারনেট পরিষেবা ব্যাহত করেছিল।

### Q4: How do social engineering techniques help malicious users gain access?

সোশ্যাল ইঞ্জিনিয়ারিং কীভাবে ম্যালিশিয়াস ইউজারদের প্রবেশাধিকার পেতে সহায়তা করে?

সোশ্যাল ইঞ্জিনিয়ারিং এমন একটি প্রতারণামূলক কৌশল যেখানে হ্যাকাররা মানুষের মনস্তাত্ত্বিক দুর্বলতাকে কাজে লাগিয়ে গোপন তথ্য বের করে বা সিস্টেমে প্রবেশ করে। এখানে প্রযুক্তিগত হ্যাকিংয়ের তুলনায় মানুষকে ঠকানোই প্রধান অস্ত্র।

---

#### প্রধান সোশ্যাল ইঞ্জিনিয়ারিং কৌশল

ফিশিং (Phishing) – ভুয়া ইমেইল, লিংক ও ওয়েবসাইট ব্যবহার

- কীভাবে কাজ করে?
  - হ্যাকাররা বিশ্বস্ত সংস্থার নামে ইমেইল পাঠায় এবং ব্যবহারকারীকে ভুয়া লগইন পেজে ক্লিক করায়।
  - ব্যবহারকারী তার ইউজারনেম ও পাসওয়ার্ড দিলে, তা হ্যাকারদের হাতে চলে যায়।

- উদাহরণ:

- আপনি একটি ইমেইল পেলেন যেখানে লেখা, "আপনার **Gmail** অ্যাকাউন্ট ব্লক হয়ে গেছে! লগইন করুন।"
- আপনি ভুয়া লিংকে ক্লিক করে পাসওয়ার্ড দিলে, হ্যাকার আপনার অ্যাকাউন্ট নিয়ন্ত্রণ নেয়।

✓ প্রতিরোধ: সন্দেহজনক ইমেইল এড়িয়ে চলুন, লিংক ক্লিক করার আগে যাচাই করুন।

---

স্পিয়ার ফিশিং (**Spear Phishing**) – নির্দিষ্ট ব্যক্তিকে লক্ষ্য করে আক্রমণ

- কীভাবে কাজ করে?

- হ্যাকাররা একজন নির্দিষ্ট ব্যক্তিকে টার্গেট করে এবং তার সম্পর্কে তথ্য সংগ্রহ করে।
- তারপর বিশেষভাবে তৈরি ইমেইল বা মেসেজ পাঠায় যা ব্যক্তিটি বিশ্বাস করতে বাধ্য হয়।

- উদাহরণ:

- এক CEO-এর কাছে একটি ইমেইল আসে "আপনার ব্যাংকের লেনদেন চেক করুন" বলে।
- CEO ইমেইলে থাকা লিংকে ক্লিক করে ব্যাংকের পাসওয়ার্ড দিলে, হ্যাকার তা নিয়ে অর্থ চুরি করে।

✓ প্রতিরোধ: অনির্ভরযোগ্য ইমেইল ও ফাইল ওপেন করার আগে যাচাই করুন।

---

③ ভিশিং (**Vishing**) – ফোন কল ব্যবহার করে প্রতারণা

- কীভাবে কাজ করে?

- হ্যাকাররা ব্যাংক, সরকারি সংস্থা, বা আইটি সাপোর্ট কর্মী সেজে ফোন করে।
- ব্যবহারকারীকে **OTP**, পাসওয়ার্ড, বা ক্রেডিট কার্ড তথ্য দিতে বাধ্য করে।

- উদাহরণ:

- একজন ফোন করে বলে, "আপনার ব্যাংক অ্যাকাউন্ট হ্যাক হয়েছে, এখনই আপনার **OTP** বলুন!"

- ব্যবহারকারী আতঙ্কিত হয়ে OTP দিলে, হ্যাকার তার অ্যাকাউন্ট থেকে টাকা তুলে ফেলে।

✓ প্রতিরোধ: ব্যাঙ্ক বা সরকারি সংস্থার নাম করে কেউ ফোন করলে আগে যাচাই করুন।

---

#### 4] বেইটিং (Baiting) – লোভ দেখিয়ে প্রতারণা করা

- কীভাবে কাজ করে?
  - হ্যাকাররা ব্যবহারকারীকে ফ্রি সফটওয়্যার, ফ্রি গিফট, বা চাকরির অফার দেখিয়ে প্রতারণা করে।
  - এতে থাকা ম্যালওয়্যার ব্যবহারকারীর ডিভাইসে ইনস্টল হয়ে যায়।
- উদাহরণ:
  - কেউ আপনাকে বলে "ফ্রি **Netflix** সাবস্ক্রিপশন ডাউনলোড করুন" এবং আপনাকে একটি ফাইল দেয়।
  - আপনি এটি ইনস্টল করলে, আপনার কম্পিউটার হ্যাক হয়ে যায়।

✓ প্রতিরোধ: সন্দেহজনক লোভনীয় অফার এড়িয়ে চলুন।

---

#### 5] প্রিটেক্সটিং (Pretexting) – পরিচয় ভেঙে বিশ্বাস অর্জন করা

- কীভাবে কাজ করে?
  - হ্যাকাররা নিজেকে ব্যাংক অফিসার, আইটি সাপোর্ট, বা সরকারি কর্মকর্তা হিসেবে পরিচয় দেয়।
  - এরপর ব্যবহারকারীর বিশ্বাস অর্জন করে ব্যক্তিগত তথ্য চেয়ে নেয়।
- উদাহরণ:
  - একজন হ্যাকার বলে, "আমি আপনার কোম্পানির **HR** থেকে বলছি, আপনার নতুন বেতন কার্ডামো চেক করতে আপনার লগইন দরকার!"
  - আপনি লগইন দিলে, হ্যাকার আপনার অফিস অ্যাকাউন্টের নিয়ন্ত্রণ নিয়ে নেয়।

✓ প্রতিরোধ: পরিচয় যাচাই না করে কারও কথায় তথ্য শেয়ার করবেন না।

---

## 6 টেলিটেলি (Tailgating) – নিরাপত্তা ব্যবস্থা ফাঁকি দেওয়া


- কীভাবে কাজ করে?
  - হ্যাকাররা ভুয়া আইডি কার্ড ব্যবহার করে বা কোনো কর্মচারীর সঙ্গে ঢুকে পড়ে।
- উদাহরণ:
  - একজন হ্যাকার "আমি ইন্টার্ন" বলে কোম্পানির গেটে ঢোকে এবং কম্পিউটারে ম্যালওয়্যার ইনস্টল করে।

✓ প্রতিরোধ: অপরিচিত ব্যক্তিদের বিনা যাচাইয়ে অফিসে প্রবেশ করতে দেবেন না।

---

## কীভাবে ম্যালিশিয়াস ইউজাররা সোশ্যাল ইঞ্জিনিয়ারিং ব্যবহার করে প্রবেশ করে?

- ✓ মানুষের মনস্তাত্ত্বিক দুর্বলতা কাজে লাগিয়ে তারা সংবেদনশীল তথ্য বের করে।
- ✓ আতঙ্ক সৃষ্টি করে দ্রুত সিদ্ধান্ত নিতে বাধ্য করে (যেমন: "তুরন্ত আপনার অ্যাকাউন্ট ব্লক হয়ে যাবে!")।
- ✓ বিশ্বাসযোগ্য পরিচয় তৈরি করে ভুয়া পরিচয়ে আক্রমণ চালায়।
- ✓ ফ্রি অফার বা গুরুত্বপূর্ণ ফাইলের লোভ দেখায় যাতে মানুষ সহজেই ক্লিক করে।

 কীভাবে সোশ্যাল ইঞ্জিনিয়ারিং থেকে নিজেকে রক্ষা করবেন?

- ✓ অপরিচিত লিংক ও ইমেইল ওপেন করবেন না।
- ✓ কোনো সংস্থা বা ব্যাংক ফোন করলে আগে যাচাই করুন।
- ✓ নিজের ব্যক্তিগত তথ্য কাউকে বলবেন না।
- ✓ সন্দেহজনক সফটওয়্যার বা অফার থেকে দূরে থাকুন।

**Q5. How can role-based access control (RBAC) help mitigate risks from malicious users?**

Role-Based Access Control (RBAC) কীভাবে ম্যালিশিয়াস ব্যবহারকারীদের ঝুঁকি কমাতে সাহায্য করে?

Role-Based Access Control (RBAC) হল একটি সিকিউরিটি মডেল, যেখানে ব্যবহারকারীদের নির্দিষ্ট ভূমিকা (Role) অনুযায়ী সীমিত অ্যাক্সেস দেওয়া হয়। এটি নিশ্চিত করে যে কেউ তার কাজের জন্য যতটুকু প্রয়োজন, ততটুকুই অ্যাক্সেস পাবে—অতিরিক্ত কিছু নয়।

---

✓ RBAC কীভাবে ম্যালিশিয়াস ব্যবহারকারীদের ঝুঁকি কমায়?

#### ① সীমিত অ্যাক্সেস – Least Privilege Implementation

✓ কীভাবে কাজ করে?

- প্রতিটি ব্যবহারকারী শুধুমাত্র তার নির্দিষ্ট Role-এর জন্য অনুমোদিত ডাটা ও রিসোর্স অ্যাক্সেস করতে পারবে।
- অপ্রয়োজনীয় অ্যাক্সেস বন্ধ থাকলে, ইনসাইডার থ্রেট ও এক্সটার্নাল হ্যাকারের ক্ষতি করার সুযোগ কমে।

✗ যদি RBAC না থাকে?

- একজন সাধারণ কর্মচারী ভুলবশত বা ইচ্ছাকৃতভাবে সংবেদনশীল তথ্য মুছে ফেলতে পারে।
- হ্যাকার যদি একবার কম্প্রোমাইজড অ্যাকাউন্ট পায়, তবে সে সকল ডাটায় অ্যাক্সেস পেয়ে যেতে পারে।

✓ RBAC থাকার ফলে:

- ✓ অপ্রয়োজনীয় সিস্টেম ও ফাইল অ্যাক্সেস বন্ধ থাকে।
  - ✓ হ্যাকারের আক্রমণ সফল হওয়ার সম্ভাবনা কমে।
-

## 2] ইনসাইডার থ্রেট প্রতিরোধ

### ✓ কীভাবে কাজ করে?

- একজন কর্মচারী যদি অবৈধভাবে ডাটা কপি করতে চায় বা সিস্টেম পরিবর্তন করতে চায়, তাহলে তার RBAC অনুমতি না থাকলে সে তা করতে পারবে না।

### ✗ যদি RBAC না থাকে?

- একজন সাধারণ কর্মচারী বড় ডাটা ডাউনলোড করতে পারে, ব্যাকডোর ইনস্টল করতে পারে, বা কোম্পানির গোপন ফাইল চুরি করতে পারে।

### ✓ RBAC থাকার ফলে:

- ✓ শুধুমাত্র অনুমোদিত ব্যক্তিরাই সংবেদনশীল তথ্য ব্যবহার করতে পারে।
  - ✓ কোনও কর্মচারী সন্দেহজনক কিছু করলে তা সহজেই শনাক্ত করা যায়।
- 

## 3] অটোমেটেড অ্যাক্সেস কন্ট্রোল – কম প্রশাসনিক ঝামেলা

### ✓ কীভাবে কাজ করে?

- RBAC সিস্টেম নতুন কর্মচারী যোগ হলে বা কেউ পদোন্নতি পেলে স্বয়ংক্রিয়ভাবে অনুমতি আপডেট করতে পারে।
- ম্যানুয়ালি প্রতিটি কর্মচারীর অ্যাক্সেস পরিবর্তনের দরকার হয় না।

### ✗ যদি RBAC না থাকে?

- একজন কর্মচারী কোম্পানি ছেড়ে যাওয়ার পরও যদি তার অ্যাকাউন্ট সক্রিয় থাকে, তাহলে সে সিস্টেমে ঢুকে ক্ষতি করতে পারে।

### ✓ RBAC থাকার ফলে:

- ✓ ব্যবহারকারীর অনুমতি সহজে নিয়ন্ত্রণ করা যায়।
  - ✓ পুরাতন কর্মচারীদের অ্যাক্সেস স্বয়ংক্রিয়ভাবে বাতিল করা হয়।
- 

## 4] হ্যাকারদের ল্যাটারাল মুভমেন্ট রোধ

### ✓ কীভাবে কাজ করে?

- হ্যাকার যদি একটি অ্যাকাউন্ট হ্যাক করেও, তবে সে শুধুমাত্র সেই নির্দিষ্ট Role-এর রিসোর্সই অ্যাক্সেস করতে পারবে।
- অন্যান্য গুরুত্বপূর্ণ ডাটা ও অ্যাডমিন প্যানেলে প্রবেশ করতে পারবে না।

### ✗ যদি RBAC না থাকে?

- হ্যাকার একটি সাধারণ অ্যাকাউন্ট পেলে তা ব্যবহার করে পুরো সিস্টেমের নিয়ন্ত্রণ নিতে পারে।

### ✓ RBAC থাকার ফলে:

- ✓ একটি কম্প্রোমাইজড অ্যাকাউন্ট পুরো নেটওয়ার্ককে ক্ষতিগ্রস্ত করতে পারবে না।
- ✓ হ্যাকারদের আক্রমণ সীমিত থাকবে।

---

## 5) নিরীক্ষণ ও অডিট ট্রেইল (Monitoring & Audit Logs)

### ✓ কীভাবে কাজ করে?

- প্রতিটি ব্যবহারকারীর কোন ফাইল বা সিস্টেমে অ্যাক্সেস করেছে তা লগ করে রাখা হয়।
- কোনও সন্দেহজনক কাজ ঘটলে, তা সহজে তদন্ত করা যায়।

### ✗ যদি RBAC না থাকে?

- কোনও কর্মচারী যদি ডাটা মুছে ফেলে বা পরিবর্তন করে, তাহলে কার দায়িত্ব ছিল তা বের করা কঠিন হবে।

### ✓ RBAC থাকার ফলে:

- ✓ সকল অ্যাক্সেস ও পরিবর্তনের রেকর্ড সংরক্ষণ করা হয়।
- ✓ অস্বাভাবিক কার্যকলাপ দ্রুত শনাক্ত করা যায়।

---

## 🔍 বাস্তব জীবনের উদাহরণ

### ✓ Google ও Microsoft-এর RBAC ব্যবহারের উদাহরণ:

- Google এবং Microsoft-এর মত বড় কোম্পানিগুলো RBAC ব্যবহার করে নিশ্চিত করে যে সাধারণ কর্মচারীরা সংবেদনশীল ডাটাবেস বা সার্ভারে প্রবেশ করতে না পারে।
- শুধুমাত্র সাইবার সিকিউরিটি টিম ও আইটি অ্যাডমিনরা গুরুত্বপূর্ণ ডাটা অ্যাক্সেস করতে পারে।
- যদি কেউ বিনা অনুমতিতে কিছু করার চেষ্টা করে, তাৎক্ষণিকভাবে এলার্ট পাঠানো হয়।

## Q6. What are the consequences of insider threats in cybersecurity?

ইনসাইডার থ্রেটের পরিণতি সাইবার নিরাপত্তায় কী হতে পারে?

ইনসাইডার থ্রেট (**Insider Threat**) হল এমন একটি সাইবার নিরাপত্তা ঝুঁকি যেখানে প্রতিষ্ঠানের অভ্যন্তরীণ ব্যক্তি (যেমন: কর্মচারী, ঠিকাদার, বা অংশীদার) ইচ্ছাকৃতভাবে বা অনিচ্ছাকৃতভাবে সিস্টেমের ক্ষতি করে বা ডাটা ফাঁস করে।

ইনসাইডার থ্রেটের পরিণতি অত্যন্ত বিপজ্জনক, কারণ ভিতরের কেউ সাধারণত অনুমোদিত অ্যাক্সেস পেয়ে থাকে, যা বহিরাগত হ্যাকারদের তুলনায় তাদের আরও মারাত্মক করে তোলে।

---

### ● ইনসাইডার থ্রেটের প্রধান পরিণতি:

① সংবেদনশীল ডাটা ফাঁস (**Data Breach & Leakage**)

✓ কীভাবে ঘটে?



- একজন অসন্তুষ্ট কর্মচারী বা সাবেক কর্মচারী ইচ্ছাকৃতভাবে গোপন ডাটা (যেমন: গ্রাহকের তথ্য, আর্থিক তথ্য, গোপন প্রকল্প) বাইরে ফাঁস করতে পারে।
- অনেক সময় কর্মচারীরা ডাটা ভুলভাবে সংরক্ষণ করে বা নিরাপত্তাহীনভাবে শেয়ার করে, যা হ্যাকারদের হাতে চলে যেতে পারে।

### ❌ পরিণতি:

- গ্রাহকদের তথ্য ফাঁস হলে বিশ্বাস হারাতে পারে এবং বিশাল জরিমানা গুণতে হতে পারে।
- **Facebook, Yahoo, Equifax** এর মতো বড় কোম্পানিগুলো এমন ডাটা লিকের কারণে কোটি কোটি ডলার ক্ষতির সম্মুখীন হয়েছে।

### ✅ প্রতিরোধ:

- ✓ **Data Loss Prevention (DLP)** সিস্টেম ব্যবহার করা।
  - ✓ কর্মচারীদের শুধুমাত্র প্রয়োজনীয় ডাটা অ্যাক্সেস দেওয়া।
- 

## ❷ আর্থিক ক্ষতি (Financial Loss & Fraud)

### ✓ কীভাবে ঘটে?

- একজন ইনসাইডার সংস্থার ব্যাংক অ্যাকাউন্ট, ট্রানজেকশন, বা পেমেন্ট সিস্টেমে অনুপ্রবেশ করে আর্থিক ক্ষতি করতে পারে।
- কেউ যদি অতিরিক্ত অর্থ তোলার অনুমতি পেয়ে যায় বা কৌশলে টাকা চুরি করে, তাহলে প্রতিষ্ঠান বড় ধরনের লোকসানে পড়তে পারে।

### ❌ পরিণতি:

- প্রতিষ্ঠানের দেউলিয়া হওয়ার ঝুঁকি তৈরি হয়।
- **2016** সালে সুইফট ব্যাংক হ্যাকিং-এ বাংলাদেশ ব্যাংক থেকে **\$81** মিলিয়ন ডলার চুরি করা হয়েছিল, যা ইনসাইডার সহযোগিতার সম্ভাবনা দেখায়।

### ✅ প্রতিরোধ:

- ✓ ফিন্যান্সিয়াল সিকিউরিটি মনিটরিং এবং অটোমেটেড অ্যালার্ট ব্যবস্থা থাকতে হবে।

✓ প্রতিটি লেনদেন দ্বৈত যাচাই (**Dual Authorization**) পদ্ধতিতে অনুমোদিত হতে হবে।

---

### ③ ব্যবসার খ্যাতির ক্ষতি (**Reputation Damage**)

✓ কীভাবে ঘটে?

- সংস্থার অভ্যন্তরীণ কেউ যদি গ্রাহকদের ব্যক্তিগত তথ্য চুরি বা বিক্রি করে, তাহলে কোম্পানির প্রতি বিশ্বাস নষ্ট হয়।
- যদি কোন বড় প্রতিষ্ঠান গ্রাহকের গোপন তথ্য সুরক্ষিত রাখতে ব্যর্থ হয়, তাহলে লোকেরা আর সেই কোম্পানির পরিষেবার উপর আস্থা রাখবে না।

✗ পরিণতি:

- স্টক মার্কেটে শেয়ারের দাম কমে যেতে পারে।
- নতুন গ্রাহকরা পরিষেবাগ্রহণে অনাগ্রহী হয়ে উঠতে পারে।
- **Uber** ও **Facebook**-এর ডাটা লিক কেলেঙ্কারির পর তাদের গ্রাহক সংখ্যা হ্রাস পেয়েছিল।

✓ প্রতিরোধ:

- ✓ কর্মচারীদের ডাটা প্রোটেকশন প্রশিক্ষণ দেওয়া।
  - ✓ **Zero Trust Security Model** ব্যবহার করা।
- 

### ④ আইনি সমস্যা ও জরিমানা (**Legal Issues & Regulatory Fines**)

✓ কীভাবে ঘটে?

- যদি কোনও প্রতিষ্ঠান গ্রাহকের ব্যক্তিগত তথ্য রক্ষা করতে ব্যর্থ হয়, তাহলে স্থানীয় ও আন্তর্জাতিক আইনের অধীনে শাস্তির সম্মুখীন হতে পারে।
- **GDPR (General Data Protection Regulation)** এবং **CCPA (California Consumer Privacy Act)** এর মতো কঠোর ডাটা সুরক্ষা আইন রয়েছে।

### ❌ পরিণতি:

- বড় অংকের জরিমানা দিতে হতে পারে।
- কোম্পানির বিরুদ্ধে মামলা দায়ের হতে পারে।

### ✅ প্রতিরোধ:

- ✓ ডাটা এনক্রিপশন ও অ্যাক্সেস কন্ট্রোল নীতি কার্যকর করা।
  - ✓ নিয়মিত নিরাপত্তা অডিট পরিচালনা করা।
- 

## 5 গুরুত্বপূর্ণ সিস্টেমের ধ্বংস বা ব্যাকডোর তৈরি (System Sabotage & Backdoor)

### ✓ কীভাবে ঘটে?

- একজন অসন্তুষ্ট কর্মচারী সিস্টেমে ব্যাকডোর ইনস্টল করতে পারে, যা ভবিষ্যতে আক্রমণের সুযোগ তৈরি করে।
- কেউ গুরুত্বপূর্ণ ফাইল বা সার্ভার মুছে ফেলতে পারে, যাতে প্রতিষ্ঠান বড় ক্ষতির সম্মুখীন হয়।

### ❌ পরিণতি:

- কোম্পানির সার্ভার বা ক্লাউড ডাটা সম্পূর্ণ মুছে যেতে পারে।
- প্রতিষ্ঠানের কাজ থেমে যেতে পারে বা ডাটা পুনরুদ্ধার করা অসম্ভব হয়ে পড়তে পারে।

### ✅ প্রতিরোধ:

- ✓ SIEM (Security Information & Event Management) ব্যবহার করে লগ মনিটর করা।
  - ✓ এক্স-এমপ্লয়ীদের অ্যাক্সেস তৎক্ষণাৎ বন্ধ করা।
- 

## 6 মালওয়ার ইনজেকশন ও সাইবার আক্রমণ সহযোগিতা

### ✓ কীভাবে ঘটে?

- ইনসাইডাররা ম্যালওয়্যার বা র‍্যানসমওয়্যার ইনস্টল করে কোম্পানির ফাইল এনক্রিপ্ট করতে পারে।
- অনেক ক্ষেত্রে হ্যাকাররা ইনসাইডারদের ঘুষ দিয়ে সহযোগিতা করে।

#### ❌ পরিণতি:

- প্রতিষ্ঠানের গুরুত্বপূর্ণ ফাইল লুক হয়ে যেতে পারে।
- বিপুল অংকের মুক্তিপণ দাবি করা হতে পারে (যেমন: WannaCry র‍্যানসমওয়্যার)।

#### ✅ প্রতিরোধ:

- ✓ **Endpoint Detection & Response (EDR)** ব্যবহার করা।
- ✓ সন্দেহজনক কার্যকলাপ শনাক্ত করতে **AI**-বেইসড অ্যানালাইটিক্স ব্যবহার করা।

## Q7. What security policies can be enforced to prevent insider threats?

### ইনসাইডার থ্রেট প্রতিরোধে কার্যকরী নিরাপত্তা নীতি

ইনসাইডার থ্রেট প্রতিরোধে সঠিক নিরাপত্তা নীতিমালা (**Security Policies**) প্রয়োগ করা অত্যন্ত গুরুত্বপূর্ণ। অনেক সময়, প্রতিষ্ঠানের কর্মচারী, ঠিকাদার, বা পার্টনাররা অনিচ্ছাকৃতভাবে বা ইচ্ছাকৃতভাবে সংস্থার গোপন তথ্য ফাঁস করতে পারে, যা বড় ধরনের সাইবার নিরাপত্তা ঝুঁকি তৈরি করে।

নিম্নলিখিত গুরুত্বপূর্ণ নিরাপত্তা নীতিগুলো কার্যকরভাবে ইনসাইডার থ্রেট প্রতিরোধ করতে পারে 👉

---

#### ❶ **Role-Based Access Control (RBAC)** প্রয়োগ করা

- ◆ কেন দরকার?

RBAC সিস্টেমে প্রতিটি ব্যবহারকারীর জন্য নির্দিষ্ট ভূমিকা (**Role**) ও অনুমতি (**Permission**) নির্ধারণ করা হয়।

- ◆ কীভাবে কাজ করে?

- শুধুমাত্র প্রয়োজনীয় তথ্য ও সিস্টেমের অ্যাক্সেস নির্দিষ্ট ব্যক্তিদের দেওয়া হবে।
- কর্মচারীরা নিজেদের কাজের বাইরের তথ্য দেখতে বা পরিবর্তন করতে পারবে না।

✓ প্রতিরোধ:

✓ ইনসাইডাররা অতিরিক্ত অনুমতি পাবে না, ফলে ডাটা চুরি বা পরিবর্তন করতে পারবে না।

✓ সিস্টেমে কম অ্যাক্সেস থাকলে ঝুঁকি কমে যায়।

---

## 2 Zero Trust Security Model বাস্তবায়ন

- ◆ কেন দরকার?

"**Trust No One**" ধারণার উপর ভিত্তি করে **Zero Trust Model** কাজ করে। এর মানে হলো, কেউ অটোমেটিকভাবে বিশ্বাসযোগ্য নয় – সবাইকে প্রতিবার যাচাই করতে হবে।

- ◆ কীভাবে কাজ করে?

- প্রতিটি অনুরোধ নতুনভাবে যাচাই করা হবে (Verify Every Access Request)।
- **Multi-Factor Authentication (MFA)** বাধ্যতামূলক করা হবে।
- কর্মচারীদের ব্যক্তিগত ডিভাইস থেকে সংবেদনশীল সিস্টেমে প্রবেশ নিষিদ্ধ করা হবে।

✓ প্রতিরোধ:

✓ একজন ইনসাইডার যদি পাসওয়ার্ড পেয়েও যায়, তারপরও **MFA** ছাড়া অ্যাক্সেস পাবে না।

✓ হ্যাকারের হাতে অ্যাকাউন্ট চলে গেলেও, তারা লগইন করতে পারবে না।

---

### 3 Data Loss Prevention (DLP) নীতি কার্যকর করা

#### ◆ কেন দরকার?

DLP সিস্টেমের মাধ্যমে কোনো ব্যবহারকারী সংবেদনশীল তথ্য শেয়ার, কপি, বা এক্সপোর্ট করছে কিনা তা স্বয়ংক্রিয়ভাবে সনাক্ত করা যায়।

#### ◆ কীভাবে কাজ করে?

- কর্মচারীরা গোপন তথ্য অননুমোদিতভাবে ক্লাউড বা **USB**-তে সংরক্ষণ করতে পারবে না।
- ইমেইল বা মেসেজিং সিস্টেমে সংবেদনশীল তথ্য শেয়ার করলে অ্যালার্ট পাঠানো হবে।

#### ✓ প্রতিরোধ:

- ✓ গোপন ফাইল বাইরে পাঠানো, কপি করা বা ডাউনলোড করা কঠিন হয়ে যাবে।
  - ✓ ইনসাইডাররা ভুলবশত গুরুত্বপূর্ণ তথ্য ফাঁস করলেও, সিস্টেম তা ব্লক করবে।
- 

### 4 SIEM এবং UBA টুলস ব্যবহার করা

#### ◆ কেন দরকার?

SIEM (Security Information and Event Management) এবং UBA (User Behavior Analytics) টুলস ব্যবহার করে কর্মচারীদের কার্যক্রম পর্যবেক্ষণ করা যায় এবং সন্দেহজনক কার্যকলাপ শনাক্ত করা সম্ভব।

#### ◆ কীভাবে কাজ করে?

- অস্বাভাবিক লগইন (যেমন: রাত ৩টায় লগইন, বিভিন্ন লোকেশন থেকে লগইন) শনাক্ত করা যায়।
- যদি কেউ অনেক বড় ডাটা কপি করে বা অননুমোদিত সফটওয়্যার চালায়, তবে সতর্কবার্তা পাঠানো হবে।

#### ✓ প্রতিরোধ:

- ✓ ইনসাইডার হুমকি আগে থেকেই শনাক্ত করা সম্ভব।
- ✓ কর্মচারী অস্বাভাবিক কিছু করলে, সিকিউরিটি টিম সাথে সাথে পদক্ষেপ নিতে পারবে।

---

## 5 কর্মচারীদের সাইবার নিরাপত্তা প্রশিক্ষণ (Cybersecurity Awareness Training)

### ♦ কেন দরকার?

বেশিরভাগ ইনসাইডার থ্রেট অজ্ঞতা বা ভুল সিদ্ধান্তের কারণে ঘটে। তাই সঠিক প্রশিক্ষণ দিলে এই ঝুঁকি কমানো সম্ভব।

### ♦ কীভাবে কাজ করে?

- সন্দেহজনক ইমেইল ও ফিশিং আক্রমণ চিনতে শেখানো হবে।
- প্রযুক্তিগত ঝুঁকি সম্পর্কে কর্মচারীদের সচেতন করা হবে।

### ✓ প্রতিরোধ:

- ✓ কর্মচারীরা ভুল করে ক্ষতি করার সম্ভাবনা কমে যাবে।
  - ✓ সাইবার অপরাধীরা সহজে কর্মচারীদের ফাঁদে ফেলতে পারবে না।
- 

## 6 এক্স-এমপ্লয়ীদের (Ex-Employees) অ্যাক্সেস দ্রুত বন্ধ করা

### ♦ কেন দরকার?

অনেক সময় প্রাক্তন কর্মচারীদের অ্যাকাউন্ট সক্রিয় থাকে, যা সিস্টেমের জন্য বড় ঝুঁকি হতে পারে।

### ♦ কীভাবে কাজ করে?

- কেউ চাকরি ছাড়ার সাথে সাথেই তার অ্যাকাউন্ট ডিয়াক্টিভেট করা হবে।
- **Ex-Employee Access Audit** চালিয়ে পুরনো অ্যাকাউন্ট ডিলিট করা হবে।

### ✓ প্রতিরোধ:

- ✓ এক্স-কর্মচারীরা প্রতিষ্ঠানের তথ্যের অ্যাক্সেস পাবে না।
  - ✓ কোনো অসন্তুষ্ট সাবেক কর্মী প্রতিশোধ নিতে পারবে না।
-

## 7 স্ট্রিক্ট Bring Your Own Device (BYOD) নীতি প্রয়োগ করা

### ♦ কেন দরকার?

কর্মচারীরা যদি নিজের ল্যাপটপ বা মোবাইল ব্যবহার করে সংস্থার নেটওয়ার্কে কাজ করে, তাহলে গোপন তথ্য ফাঁস হওয়ার ঝুঁকি থাকে।

### ♦ কীভাবে কাজ করে?

- ব্যক্তিগত ডিভাইসে সংস্থার গুরুত্বপূর্ণ ডাটা অ্যাক্সেস নিষিদ্ধ করা হবে।
- শুধুমাত্র এন্টারপ্রাইজ-ম্যানেজড ডিভাইস ব্যবহার করতে বলা হবে।

### ✓ প্রতিরোধ:

✓ একজন ইনসাইডার তার ব্যক্তিগত ল্যাপটপ বা ফোন থেকে তথ্য কপি করতে পারবে না।

✓ প্রতিষ্ঠানের ডাটা সুরক্ষিত থাকবে।

## Q8. What is an Account Takeover Attack (ATO), and how does it affect users?

অ্যাকাউন্ট টেকওভার আক্রমণ (**Account Takeover Attack - ATO**) কি এবং এটি ব্যবহারকারীদের কীভাবে প্রভাবিত করে?

অ্যাকাউন্ট টেকওভার আক্রমণ (ATO) কি?

**Account Takeover Attack (ATO)** এমন একটি সাইবার আক্রমণ যেখানে একজন হ্যাকার বা ম্যালিশিয়াস ব্যবহারকারী অন্য কারও অনলাইন অ্যাকাউন্টের নিয়ন্ত্রণ নিয়ে নেয়।

📌 এটি সাধারণত ফিশিং, ক্রেডেনশিয়াল স্টাফিং, ব্রুট ফোর্স আক্রমণ, বা সোশ্যাল ইঞ্জিনিয়ারিং-এর মাধ্যমে ঘটে।



♦ টার্গেট করা অ্যাকাউন্টগুলোর ধরন:

- ✓ ব্যাংকিং অ্যাকাউন্ট (ফিন্যান্সিয়াল লসের জন্য)
  - ✓ ইমেইল অ্যাকাউন্ট (ফিশিং ও তথ্য চুরির জন্য)
  - ✓ সোশ্যাল মিডিয়া অ্যাকাউন্ট (প্রতারণা বা ব্ল্যাকমেইলের জন্য)
  - ✓ ই-কমার্স ও পেমেন্ট অ্যাকাউন্ট (অনলাইন কেনাকাটায় প্রতারণার জন্য)
- 

🔴 অ্যাকাউন্ট টেকওভার আক্রমণ কীভাবে ঘটে?

একজন আক্রমণকারী ATO চালানোর জন্য বিভিন্ন কৌশল ব্যবহার করতে পারে, যেমন:

❶ ফিশিং (Phishing)

হ্যাকার একটি ভুয়া ইমেইল, লিংক বা ওয়েবসাইট তৈরি করে, যা দেখতে আসল ওয়েবসাইটের মতো লাগে। ব্যবহারকারী ভুল করে তার লগইন তথ্য দিয়ে দিলে, হ্যাকার তা সংগ্রহ করে অ্যাকাউন্ট নিয়ন্ত্রণ নিয়ে নেয়।

♦ উদাহরণ: "আপনার ব্যাংক অ্যাকাউন্ট ব্লক হয়ে গেছে, লগইন করুন পুনরায় চালু করতে" – এই ধরনের ইমেইল পাঠানো হয়।

❷ ক্রেডেনশিয়াল স্টাফিং (Credential Stuffing)

হ্যাকাররা লিক হওয়া পাসওয়ার্ড ও ইমেইল ব্যবহার করে বিভিন্ন ওয়েবসাইটে লগইন করার চেষ্টা করে।

♦ উদাহরণ: ব্যবহারকারী যদি একই পাসওয়ার্ড **Facebook**, **Gmail**, এবং **PayPal**-এ ব্যবহার করে, তাহলে একটিতে হ্যাক হলে বাকি সবও হ্যাক হওয়ার ঝুঁকি থাকে।

❸ ব্রুট ফোর্স অ্যাটাক (Brute Force Attack)

হ্যাকার স্বয়ংক্রিয় সফটওয়্যার ব্যবহার করে হাজার হাজার পাসওয়ার্ড চেষ্টা করে অ্যাকাউন্ট হ্যাক করতে পারে।

♦ উদাহরণ: কেউ যদি খুব দুর্বল পাসওয়ার্ড ("123456" বা "password") ব্যবহার করে, তাহলে সহজেই তার অ্যাকাউন্ট হ্যাক করা সম্ভব।

❹ কীলগার এবং ম্যালওয়্যার (Keylogger & Malware)

হ্যাকাররা স্পাইওয়্যার বা কীলগার ইনস্টল করে ব্যবহারকারীর টাইপ করা পাসওয়ার্ড চুরি করতে পারে।

- ◆ উদাহরণ: কেউ যদি সন্দেহজনক সফটওয়্যার বা ম্যালিশিয়াস লিংক ডাউনলোড করে, তাহলে তার পাসওয়ার্ড লিক হতে পারে।

---

### ⚠ ATO আক্রমণের প্রভাব

- ✓ আর্থিক ক্ষতি: হ্যাকার ব্যাংক অ্যাকাউন্ট হ্যাক করে টাকা সরিয়ে নিতে পারে।
  - ✓ পরিচয় চুরি (**Identity Theft**): ব্যক্তিগত তথ্য ফাঁস হলে হ্যাকার তা খারাপ কাজে ব্যবহার করতে পারে।
  - ✓ সোশ্যাল মিডিয়া প্রতারণা: হ্যাক হওয়া অ্যাকাউন্ট থেকে স্প্যাম বা প্রতারণামূলক মেসেজ পাঠানো হতে পারে।
  - ✓ গোপনীয়তা লঙ্ঘন: ইমেইল বা ক্লাউড স্টোরেজ অ্যাক্সেস পেলে হ্যাকার গুরুত্বপূর্ণ ডকুমেন্ট চুরি করতে পারে।
- 

### 🛡 কীভাবে অ্যাকাউন্ট টেকওভার প্রতিরোধ করা যায়?

- ◆ ❶ শক্তিশালী ও ইউনিক পাসওয়ার্ড ব্যবহার করুন
  - ✓ "123456" বা "password" এর মতো দুর্বল পাসওয়ার্ড ব্যবহার করবেন না।
  - ✓ একই পাসওয়ার্ড বারবার ব্যবহার করবেন না।
- ◆ ❷ মাল্টি-ফ্যাক্টর অথেনটিকেশন (**MFA**) চালু করুন
  - ✓ **OTP, Google Authenticator**, বা হার্ডওয়্যার টোকেন ব্যবহার করুন।
- ◆ ❸ ফিশিং ইমেইল বা সন্দেহজনক লিংকে ক্লিক করবেন না
  - ✓ অজানা ইমেইল, ম্যাসেজ বা লিংক এড়িয়ে চলুন।
- ◆ ❹ পাসওয়ার্ড ম্যানেজার ব্যবহার করুন
  - ✓ **Dashlane, LastPass** বা **Bitwarden**-এর মতো টুল ব্যবহার করুন।
- ◆ ❺ নিয়মিতভাবে অ্যাকাউন্ট মনিটর করুন ও লগইন হিস্টোরি চেক করুন
  - ✓ অপরিচিত ডিভাইস থেকে লগইন হলে সাথে সাথে পাসওয়ার্ড পরিবর্তন করুন।

## Q9. How can multi-factor authentication (MFA) help prevent malicious user activities?

মাল্টি-ফ্যাক্টর অথেনটিকেশন (MFA) কীভাবে ম্যালিশিয়াস ব্যবহারকারীদের কার্যকলাপ প্রতিরোধ করতে সাহায্য করে?

মাল্টি-ফ্যাক্টর অথেনটিকেশন (MFA) কী?

মাল্টি-ফ্যাক্টর অথেনটিকেশন (MFA) হল একটি নিরাপত্তা ব্যবস্থা যেখানে ব্যবহারকারীর পরিচয় নিশ্চিত করতে একাধিক স্তরের যাচাই (authentication) ব্যবহার করা হয়।

✓ সাধারণত, MFA তিনটি ফ্যাক্টরের উপর ভিত্তি করে গঠিত হতে পারে:

- ❶ কিছু আপনি জানেন – যেমন পাসওয়ার্ড বা পিন।
- ❷ কিছু আপনার কাছে আছে – যেমন OTP (One-Time Password), হার্ডওয়্যার টোকেন, বা Google Authenticator কোড।
- ❸ কিছু যা আপনার নিজস্ব – যেমন ফিঙ্গারপ্রিন্ট, ফেস স্ক্যান, বা ভয়েস রিকগনিশন।

♦ উদাহরণ:

➡ আপনি ব্যাংকের ওয়েবসাইটে লগইন করলে প্রথমে পাসওয়ার্ড দিতে হয় (কিছু আপনি জানেন), এরপর মোবাইলে **OTP** আসে (কিছু আপনার কাছে আছে), যা প্রবেশ করলে অ্যাকাউন্টে ঢোকা যায়।

---

🔴 **MFA** কীভাবে ম্যালিশিয়াস ব্যবহারকারীদের প্রতিরোধ করে?

- ❶ পাসওয়ার্ড হ্যাক করলেও অ্যাকাউন্ট সুরক্ষিত থাকে

হ্যাকার যদি ফিশিং, ব্রুট ফোর্স, বা ডেটারিচের মাধ্যমে পাসওয়ার্ড চুরি করে, তবুও তারা অ্যাকাউন্টে প্রবেশ করতে পারবে না কারণ **OTP** বা বায়োমেট্রিক অথেনটিকেশন লাগবে।

- ♦ উদাহরণ:

একজন হ্যাকার আপনার ফেসবুক পাসওয়ার্ড পেয়ে গেলেও, যদি **MFA** চালু থাকে, তাহলে লগইনের সময় **OTP** লাগবে, যা কেবল আপনার মোবাইলেই আসবে।

---

## ❷ ফিশিং আক্রমণ প্রতিরোধ করে

হ্যাকাররা ভুয়া ওয়েবসাইট বানিয়ে পাসওয়ার্ড হাতিয়ে নেয়ার চেষ্টা করতে পারে। কিন্তু যদি **MFA** চালু থাকে, তাহলে শুধু পাসওয়ার্ড দিলেই হবে না, বরং **OTP** বা বায়োমেট্রিক যাচাইও লাগবে, যা হ্যাকারদের পক্ষে সংগ্রহ করা কঠিন।

- ♦ উদাহরণ:

আপনি যদি ভুলবশত ভুয়া ব্যাংক ওয়েবসাইটে পাসওয়ার্ড দিয়ে দেন, তারপরও **OTP** ছাড়া লগইন সম্ভব হবে না।

---

## ❸ বট ও স্ক্রিপ্ট-ভিত্তিক আক্রমণ ঠেকায়

অনেক হ্যাকার বট বা স্ক্রিপ্ট ব্যবহার করে অটোমেটেডভাবে পাসওয়ার্ড অনুমান করার চেষ্টা করে (**Brute Force Attack**)। কিন্তু **MFA** চালু থাকলে **OTP** বা বায়োমেট্রিক ভেরিফিকেশন লাগবে, যা বট দ্বারা অনুমান করা সম্ভব নয়।

---

## ❹ অ্যাকাউন্ট টেকওভার (ATO) প্রতিরোধ করে

**ATO** বা অ্যাকাউন্ট টেকওভার আক্রমণে হ্যাকাররা বিভিন্ন কৌশলে অ্যাকাউন্টের নিয়ন্ত্রণ নেয়। কিন্তু **MFA** চালু থাকলে, পাসওয়ার্ড ফাঁস হলেও অ্যাকাউন্ট সুরক্ষিত থাকে।

- ♦ উদাহরণ:

হ্যাকার যদি ডার্ক ওয়েব থেকে আপনার পাসওয়ার্ড পায়, তারপরও **OTP** কোড ছাড়া লগইন করতে পারবে না।

---

🛡️ কীভাবে **MFA** সেটআপ করবেন?

✓ ১. **Google Authenticator / Microsoft Authenticator** ব্যবহার করুন  
→ Facebook, Gmail, GitHub-এর মতো সার্ভিসে **Google Authenticator** বা **Microsoft Authenticator** সেটআপ করতে পারেন।

✓ ২. **SMS / Email-based OTP** চালু করুন  
→ অনেক ব্যাংক এবং ওয়েবসাইটে লগইনের সময় OTP পাঠানোর অপশন থাকে, এটি চালু করে রাখুন।

✓ ৩. হার্ডওয়্যার টোকেন ব্যবহার করুন  
→ নিরাপত্তা আরও শক্তিশালী করতে **YubiKey** বা **Titan Security Key** ব্যবহার করতে পারেন।

✓ ৪. বায়োমেট্রিক অথেনটিকেশন চালু করুন  
→ মোবাইল এবং ল্যাপটপে **Fingerprint**, **Face ID** বা **Windows Hello** চালু রাখুন।

---

## Q10. What tools are used to detect and block malicious users in a network?

নেটওয়ার্কে ম্যালিশিয়াস ব্যবহারকারী সনাক্ত ও ব্লক করার জন্য ব্যবহৃত টুলস

নেটওয়ার্কের নিরাপত্তা নিশ্চিত করতে বিভিন্ন সিকিউরিটি টুলস ও প্রযুক্তি ব্যবহার করা হয়, যা ম্যালিশিয়াস ব্যবহারকারীদের চিহ্নিত ও ব্লক করতে সাহায্য করে। নিচে সেরা কিছু টুলস ও প্রযুক্তি আলোচনা করা হলো:

---

🔴 ❶ **Intrusion Detection System (IDS)** – অনুপ্রবেশ শনাক্তকরণ ব্যবস্থা

**IDS** এমন একটি টুল যা নেটওয়ার্ক ট্রাফিক পর্যবেক্ষণ করে সন্দেহজনক কার্যকলাপ শনাক্ত করে। এটি সাধারণত অ্যালার্ট পাঠায় কিন্তু স্বয়ংক্রিয়ভাবে ব্লক করে না।

✓ বিখ্যাত **IDS** টুলস:

- ◆ **Snort** – ওপেন সোর্স, শক্তিশালী নেটওয়ার্ক-ভিত্তিক IDS।
- ◆ **Suricata** – মাল্টি-থ্রেডেড IDS যা দ্রুত কাজ করতে পারে।
- ◆ **Bro (Zeek)** – উন্নত ট্রাফিক বিশ্লেষণের জন্য ব্যবহৃত IDS।

✓ কীভাবে কাজ করে?

📌 যদি কোনো ব্যবহারকারী অস্বাভাবিক পোর্ট স্ক্যানিং, ম্যালওয়্যার ট্রাফিক, বা ব্রুট ফোর্স আক্রমণ চালায়, তাহলে IDS এটি শনাক্ত করতে পারে।

---

● ② **Intrusion Prevention System (IPS)** – অনুপ্রবেশ প্রতিরোধ ব্যবস্থা

**IPS** **IDS**-এর মতোই কাজ করে, তবে এটি শুধু শনাক্তই করে না, বরং সন্দেহজনক ট্রাফিক স্বয়ংক্রিয়ভাবে ব্লকও করতে পারে।

✓ বিখ্যাত **IPS** টুলস:

- ◆ **Snort (IPS Mode)** – Snort-কে IPS মোডে চালানো সম্ভব।
- ◆ **Suricata (IDS/IPS)** – এটি IDS ও IPS উভয় হিসেবে কাজ করতে পারে।
- ◆ **Cisco Firepower** – এন্টারপ্রাইজ লেভেলের IPS।

✓ কীভাবে কাজ করে?

📌 যদি কোনো ব্যবহারকারী **SQL Injection** বা **Brute Force Attack** করার চেষ্টা করে, তাহলে IPS স্বয়ংক্রিয়ভাবে সেই ব্যবহারকারীর **IP** ব্লক করে দেবে।

---

● ③ **Security Information and Event Management (SIEM)** – সিকিউরিটি বিশ্লেষণ ও পর্যবেক্ষণ

**SIEM** টুলস বিভিন্ন নিরাপত্তা লগ সংগ্রহ ও বিশ্লেষণ করে, এবং ম্যালিশিয়াস কার্যকলাপ শনাক্ত করতে সাহায্য করে।

✓ বিখ্যাত **SIEM** টুলস:

- ◆ **Splunk** – বড় পরিসরের ডাটা বিশ্লেষণের জন্য জনপ্রিয়।
- ◆ **ELK Stack (Elasticsearch, Logstash, Kibana)** – ওপেন সোর্স SIEM সমাধান।
- ◆ **IBM QRadar** – এন্টারপ্রাইজ লেভেলের SIEM টুল।

✓ কীভাবে কাজ করে?

📌 যদি কেউ একই সময়ে বিভিন্ন দেশ থেকে লগইন করতে চায় বা একটি সার্ভার থেকে হঠাৎ করে অনেক ডাটা বের করতে চায়, তাহলে SIEM টুল অ্যালার্ট পাঠাবে।

---

🔴 4 **Firewalls** – ফায়ারওয়াল (নেটওয়ার্ক সুরক্ষার জন্য বাধা)

ফায়ারওয়াল ইনকামিং ও আউটগোয়িং ট্রাফিক ফিল্টার করে, এবং সন্দেহজনক ব্যবহারকারীদের ব্লক করতে পারে।

✓ বিখ্যাত **Firewall** টুলস:

- ◆ **pfSense** – ওপেন সোর্স ফায়ারওয়াল।
- ◆ **Cisco ASA (Adaptive Security Appliance)** – এন্টারপ্রাইজ লেভেল ফায়ারওয়াল।
- ◆ **FortiGate** – উন্নত AI-ভিত্তিক ফায়ারওয়াল।
- ◆ **iptables (Linux)** – লিনাক্স সিস্টেমের বিল্ট-ইন ফায়ারওয়াল।

✓ কীভাবে কাজ করে?

📌 যদি কোনো ব্যবহারকারী অবৈধ পোর্টে প্রবেশের চেষ্টা করে, তাহলে ফায়ারওয়াল সেই ট্রাফিক ব্লক করে দেবে।

---

🔴 5 **Endpoint Detection and Response (EDR)** – এন্ডপয়েন্ট সুরক্ষা

**EDR** সফটওয়্যার বিভিন্ন এন্ডপয়েন্ট (ল্যাপটপ, ডেস্কটপ, মোবাইল) পর্যবেক্ষণ করে এবং সন্দেহজনক কার্যকলাপ শনাক্ত করে।

✓ বিখ্যাত EDR টুলস:

- ◆ **CrowdStrike Falcon** – AI-ভিত্তিক এন্ডপয়েন্ট সুরক্ষা।
- ◆ **Microsoft Defender for Endpoint** – উইন্ডোজ এন্ডপয়েন্ট সুরক্ষার জন্য কার্যকরী।
- ◆ **SentinelOne** – উন্নত EDR টুল যা ম্যালওয়্যার ব্লক করতে পারে।

✓ কীভাবে কাজ করে?

📌 যদি কোনো ব্যবহারকারী একটি ম্যালওয়্যার চালানোর চেষ্টা করে, তাহলে EDR সেই ফাইলটি ব্লক করে দেবে এবং প্রশাসককে সতর্ক করবে।

---

🔴 6 Honeypots – হানিপট (ফাঁদ) ব্যবহার করে আক্রমণকারীদের ধরার ব্যবস্থা

হানিপট এমন একটি নিরাপত্তা ব্যবস্থা যা হ্যাকারদের আকৃষ্ট করে, যাতে তাদের কার্যকলাপ বিশ্লেষণ করা যায়।

✓ বিখ্যাত Honeypot টুলস:

- ◆ **Kippo** – SSH-ভিত্তিক হানিপট।
- ◆ **Dionaea** – ম্যালওয়্যার ক্যাপচার করার জন্য ব্যবহৃত হয়।
- ◆ **Cowrie** – উন্নত SSH ও Telnet হানিপট।

✓ কীভাবে কাজ করে?

📌 যদি কোনো হ্যাকার নেটওয়ার্কে প্রবেশের চেষ্টা করে, তাহলে হানিপট সেটি শনাক্ত করে এবং তার কার্যকলাপ লোগ করে।



