

Cyber Security Syllabus

Unit 1: Introduction of Cyber Security

A Brief History of the Internet, Computer Crime, Defining Cyber Security and Cyberspace, Communication and web technology, Internet, World wide web, regulation of cyberspace, concept of cyber security, Issues and challenges of cyber security. Cyber security terminologies: Security, Attacks, risk, vulnerability, exploit, hacker, Computer Criminals, Cyber warfare, Security Services, Security Mechanisms, Case Studies.

Unit 2: Cyber crimes

Cyber crimes targeting Computer systems and Mobiles - spyware, logic bombs, DoS, virus, Trojans, ransomware, data breach, Online scams and frauds - email scams, Phishing, Online job fraud, Online sextortion, Debit/ credit card fraud, Online payment fraud, website defacement, Cyber espionage, Darknet - illegal trades, drug trafficking, human trafficking, Social Media Scams & Fraud impersonation, identity theft, misinformation, fake news, cyber crime against persons - cyber grooming, child pornography, cyber stalking, Cyber bullying, Social Engineering attacks, Crime reporting procedure, Case studies.

Unit 3: Digital Devices Security, Tools & Technologies for Cyber Security

End Point device and Mobile phone security, Password policy, Security management, Data backup, Downloading and management of third party software, Device security policy, Cyber Security best practices, Significance of host firewall and Ant-virus, Wi-Fi security, Configuration of basic security policy and permissions.

Unit 4: Cyber law and Investigation

Cyber crime and legal landscape around the world, IT Act, 2000 and its amendments. Limitations of IT Act, 2000. Cyber crime and punishments, Cyber Laws and Legal and ethical aspects related to new technologies- AI/ML, IoT, Blockchain, Darknet and Social media, Cyber Laws of other countries, Case Studies.

ইন্টারনেট, সাইবার ক্রাইম এবং সাইবার সিকিউরিটির একটি সংক্ষিপ্ত বিবরণ

ইন্টারনেটের সংক্ষিপ্ত ইতিহাস

- উৎপত্তি: ১৯৬০-এর দশকে সামরিক যোগাযোগ এবং গবেষণার জন্য ARPANET থেকে ইন্টারনেটের সূচনা হয়।
- উন্নয়ন: ১৯৮০-এর দশকে TCP/IP প্রোটোকল প্রবর্তনের মাধ্যমে বিশ্বব্যাপী নেটওয়ার্ক সংযোগ স্থাপিত হয়।
- আধুনিক ইন্টারনেট: ১৯৯০-এর দশকে ওয়ার্ল্ড ওয়াইড ওয়েব (WWW) ইন্টারনেটকে জনপ্রিয় করে তোলে।

কম্পিউটার অপরাধ (সাইবার ক্রাইম)

- সংজ্ঞা: কম্পিউটার বা নেটওয়ার্ক ব্যবহার করে অবৈধ কাজ, যেমন হ্যাকিং, ফিশিং, ম্যালওয়্যার আক্রমণ।
- উন্নয়ন: প্রাথমিকভাবে অনুমতি ছাড়া প্রবেশের উপর সীমাবদ্ধ ছিল; বর্তমানে পরিচয় চুরি, র‍্যাকসময়্যার এবং সাইবার সন্ত্রাসবাদ অন্তর্ভুক্ত।

সাইবার সিকিউরিটি এবং সাইবারস্পেসের সংজ্ঞা

- সাইবারস্পেস: ডিজিটাল প্রযুক্তি এবং নেটওয়ার্কের মাধ্যমে সংযুক্ত ভার্চুয়াল পরিবেশ।
- সাইবার সিকিউরিটি: সিস্টেম, নেটওয়ার্ক এবং ডেটাকে সাইবার আক্রমণ থেকে রক্ষা করার প্রক্রিয়া।

যোগাযোগ এবং ওয়েব প্রযুক্তি

- ইন্টারনেট: ডেটা বিনিময়ের জন্য সংযুক্ত কম্পিউটারগুলির একটি বৈশ্বিক নেটওয়ার্ক।
- ওয়ার্ল্ড ওয়াইড ওয়েব (**WWW**): ওয়েব পৃষ্ঠাগুলি ব্রাউজারের মাধ্যমে অ্যাক্সেস করার একটি সেবা।
- প্রযুক্তি: প্রোটোকল (যেমন FTP, SMTP), ব্রাউজার, ক্লাউড কম্পিউটিং এবং IoT অন্তর্ভুক্ত।

সাইবারস্পেসের নিয়ন্ত্রণ

- নিয়ন্ত্রণের প্রয়োজন: নিরাপদ এবং সুরক্ষিত ডিজিটাল পরিবেশ নিশ্চিত করা।
- পদ্ধতি: GDPR-এর মতো আইন, সাইবারক্রাইম চুক্তি এবং জাতীয় সাইবার নীতি।

সাইবার সিকিউরিটির ধারণা

- উদ্দেশ্য: ডিজিটাল সম্পদের গোপনীয়তা, অখণ্ডতা এবং প্রাপ্যতা নিশ্চিত করা।
- স্তরসমূহ: নেটওয়ার্ক সুরক্ষা, অ্যাপ্লিকেশন সুরক্ষা, তথ্য সুরক্ষা, এবং অপারেশনাল সুরক্ষা।

সাইবার সিকিউরিটির সমস্যা ও চ্যালেঞ্জ

- চ্যালেঞ্জ:
 - দ্রুত পরিবর্তনশীল সাইবার হুমকি (যেমন AI-চালিত ম্যালওয়্যার)।
 - দক্ষ পেশাদারের অভাব।
 - অভ্যন্তরীণ হুমকি।

- গোপনীয়তা এবং সুরক্ষার মধ্যে ভারসাম্য রক্ষা।
- সমাধান: ঝুঁকি ব্যবস্থাপনা, ব্যবহারকারীদের সচেতনতা বৃদ্ধি, এবং আন্তর্জাতিক সহযোগিতা।

সাইবার সিকিউরিটির টার্মিনোলজিসমূহ

1. সুরক্ষা: সিস্টেমকে ক্ষতি থেকে রক্ষার ব্যবস্থা।
2. আক্রমণ: সিস্টেমে অবৈধ প্রবেশ বা ক্ষতির প্রচেষ্টা (যেমন DoS, ফিশিং)।
3. ঝুঁকি: ক্ষতি বা হুমকির সম্ভাবনা।
4. দুর্বলতা: সিস্টেমের এমন দুর্বল অংশ যা কাজে লাগানো যেতে পারে।
5. এক্সপ্লয়েট: দুর্বলতাকে কাজে লাগানোর একটি পদ্ধতি।
6. হ্যাকার: প্রতিরক্ষা ভেদ করার পদ্ধতি অনুসন্ধানকারী।
7. কম্পিউটার অপরাধী: সাইবার অপরাধে যুক্ত ব্যক্তি।
8. সাইবার যুদ্ধ: রাষ্ট্রের স্পন্দনে পরিচালিত আক্রমণ।
9. নিরাপত্তা পরিষেবা: নিরাপত্তার লক্ষ্য অর্জনের জন্য কার্যাবলি (যেমন প্রমাণীকরণ, এনক্রিপশন)।
10. নিরাপত্তা প্রক্রিয়া: নিরাপত্তা নীতি কার্যকর করার সরঞ্জাম বা কৌশল।

কেস স্টাডি

- স্ট্রাসনেট ওয়ার্ম (২০১০): ইরানের পারমাণবিক সুবিধাগুলিতে আক্রমণ, যা সাইবার যুদ্ধের ক্ষমতা দেখিয়েছে।
- টার্গেট ডেটা ব্রিচ (২০১৩): তৃতীয় পক্ষের দুর্বলতার কারণে গ্রাহকের তথ্য চুরি।
- সোলারউইন্ডস হ্যাক (২০২০): একটি সরবরাহ চেইন আক্রমণ যা বিশ্বব্যাপী বহু সংস্থাকে প্রভাবিত করেছে।

১. কম্পিউটার ও মোবাইল সিস্টেমকে লক্ষ্য করে সাইবার অপরাধ

ক. ক্ষতিকারক সফটওয়্যার

- স্পাইওয়্যার: গোপনে ব্যক্তিগত তথ্য সংগ্রহ করে।
- লজিক বোম্ব: নির্দিষ্ট শর্তে সক্রিয় হয় এমন ক্ষতিকারক কোড।
- ডিনায়াল অব সার্ভিস (DoS) আক্রমণ: সিস্টেম অকার্যকর করে দেয়।
- ভাইরাস: ফাইল সংক্রমিত করে ক্ষতি করে।
- ট্রোজান: বৈধ সফটওয়্যার হিসেবে ছদ্মবেশে কাজ করে।
- র‍্যানসমওয়্যার: সিস্টেম বা ডেটা লক করে মুক্তিপণ দাবি করে।

খ. ডেটা চুরি

- অনুমতি ছাড়াই সংবেদনশীল তথ্য চুরি।

২. অনলাইন প্রতারণা ও জালিয়াতি

ক. প্রতারণা

- ইমেইল প্রতারণা: বিশ্বাসযোগ্য সংস্থার নাম ব্যবহার করে জাল ইমেইল।
- ফিশিং: ভুয়া বার্তার মাধ্যমে লগইন তথ্য বা ব্যক্তিগত তথ্য চুরি।
- অনলাইন চাকরি প্রতারণা: ভুয়া চাকরির বিজ্ঞাপন দিয়ে টাকা বা তথ্য চুরি।
- সেক্সটর্শন: ব্যক্তিগত ছবি বা ভিডিও প্রকাশের হুমকি দিয়ে অর্থ দাবি।

খ. আর্থিক জালিয়াতি

- ডেবিট/ক্রেডিট কার্ড প্রতারণা: কার্ডের তথ্য চুরি করে টাকা লেনদেন।
- অনলাইন পেমেন্ট প্রতারণা: পেমেন্ট গেটওয়ে ব্যবহার করে জালিয়াতি।

গ. ওয়েবসাইট বিকৃতকরণ

- ওয়েবসাইটের চেহারা বা বিষয়বস্তু পরিবর্তন করা।

ঘ. সাইবার গুপ্তচরবৃত্তি

- রাজনৈতিক বা অর্থনৈতিক সুবিধার জন্য গোপন তথ্য চুরি।

৩. ডার্কনেট কার্যক্রম

- অবৈধ ব্যবসা: নিষিদ্ধ পণ্য ও পরিষেবার বাণিজ্য।
- ড্রাগ পাচার: মাদকদ্রব্য ক্রয়-বিক্রয়।
- মানব পাচার: ব্যক্তিদের শোষণের জন্য কেনা-বেচা।

৪. সামাজিক মাধ্যমের প্রতারণা

ক. ছদ্মবেশ ও পরিচয় চুরি

- অন্যের পরিচয় ব্যবহার করে প্রতারণা।

খ. ভুল তথ্য ও ভুয়া খবর

- জনমত প্রভাবিত বা বিভ্রান্ত করার জন্য ভুয়া খবর প্রচার।

৫. ব্যক্তিদের বিরুদ্ধে সাইবার অপরাধ

ক. হয়রানি ও শোষণ

- সাইবার গ্রুমিং: আস্তা তৈরি করে শোষণ।
- শিশু পর্নোগ্রাফি: শিশুদের অবৈধ কনটেন্ট তৈরি বা প্রচার।
- সাইবার স্টকিং: অনলাইনে বিরক্তিকর মনোযোগ।
- সাইবার বুলিং: অনলাইনে হুমকি বা অপমান।

খ. সামাজিক প্রকৌশল আক্রমণ

- ব্যক্তিগত তথ্য পেতে প্রতারণা।

৬. সাইবার অপরাধ রিপোর্টিং পদ্ধতি

- সরকারি বা আইন প্রয়োগকারী সংস্থার নির্দেশিকা অনুসরণ করা।
- সাইবার অপরাধ সেলের সাথে যোগাযোগ করা বা জাতীয় পোর্টালে রিপোর্ট করা।

৭. কেস স্টাডি

- বাস্তব ঘটনা বিশ্লেষণ করে অপরাধের কৌশল ও প্রভাব বোঝা।

১. এন্ড-পয়েন্ট ডিভাইস এবং মোবাইল ফোন সুরক্ষা

- সংজ্ঞা: কম্পিউটার, ল্যাপটপ, এবং মোবাইল ফোনের মতো ডিভাইসগুলোকে অননুমোদিত প্রবেশ ও হুমকি থেকে রক্ষা করার ব্যবস্থা।
- পদ্ধতি:
 - সংবেদনশীল তথ্য এনক্রিপশন করুন।
 - নিয়মিত আপডেট ও প্যাচ ইনস্টল করুন।
 - প্রশাসনিক প্রিভিলেজ সীমিত রাখুন।
 - মোবাইল ডিভাইস ব্যবস্থাপনা (MDM) সফটওয়্যার ব্যবহার করুন।

২. পাসওয়ার্ড নীতি

- গুরুত্ব:
 - অ্যাকাউন্ট এবং সিস্টেমকে অননুমোদিত প্রবেশ থেকে সুরক্ষিত করে।
 - নিরাপদ ব্যবহারকারীর প্রমাণীকরণ নিশ্চিত করে।
- সেরা পদ্ধতি:
 - জটিল এবং দীর্ঘ পাসওয়ার্ড ব্যবহার করুন।
 - মাল্টি-ফ্যাক্টর অথেন্টিকেশন (MFA) চালু করুন।
 - নিয়মিত পাসওয়ার্ড পরিবর্তন করুন এবং সাধারণ পাসওয়ার্ড এড়িয়ে চলুন।

৩. সুরক্ষা ব্যবস্থাপনা

- উপাদান:
 - সাইবার আক্রমণের ক্ষেত্রে প্রতিক্রিয়া পরিকল্পনা।
 - নিয়মিত সুরক্ষা নিরীক্ষা।
 - ভূমিকা-ভিত্তিক অ্যাক্সেস নিয়ন্ত্রণ।
 - কর্মীদের সুরক্ষা সচেতনতা প্রশিক্ষণ।

৪. ডেটা ব্যাকআপ

- গুরুত্ব:
 - হার্ডওয়্যার ব্যর্থতা, সাইবার আক্রমণ, বা দুর্ঘটনাজনিত ডেটা মুছে ফেলা থেকে রক্ষা করে।
- পদ্ধতি:
 - স্বয়ংক্রিয় এবং ইনক্রিমেন্টাল ব্যাকআপ ব্যবহার করুন।
 - একাধিক নিরাপদ স্থানে ব্যাকআপ সংরক্ষণ করুন।
 - ব্যাকআপ ফাইল এনক্রিপ্ট করুন।

৫. থার্ড-পার্টি সফটওয়্যার ডাউনলোড এবং ব্যবস্থাপনা

- ঝুঁকি:
 - অবিশ্বস্ত সফটওয়্যারে ম্যালওয়্যার বা স্পাইওয়্যারের উপস্থিতি।
 - দুর্বলতা ব্যবহারের ঝুঁকি।
- সেবা পদ্ধতি:
 - শুধুমাত্র নির্ভরযোগ্য উত্স থেকে সফটওয়্যার ডাউনলোড করুন।
 - সফটওয়্যার সুরক্ষা মানের জন্য পরীক্ষা করুন।
 - নিয়মিত আপডেট করুন।

৬. ডিভাইস সুরক্ষা নীতি

- উদ্দেশ্য:
 - ডিভাইস ব্যবহারের জন্য গ্রহণযোগ্য নীতি ও সুরক্ষা ব্যবস্থা সংজ্ঞায়িত করা।
- উপাদান:
 - সফটওয়্যার ইনস্টলেশনের নির্দেশিকা।
 - হারিয়ে যাওয়া বা চুরি হওয়া ডিভাইস রিপোর্টিং প্রক্রিয়া।
 - পুরনো ডিভাইস নিরাপদে নিষ্পত্তি করার পদ্ধতি।

৭. সাইবার নিরাপত্তার সেবা পদ্ধতি

- প্রস্তাবনা:
 - নিয়মিত ঝুঁকি মূল্যায়ন করুন।
 - ব্যবহারকারীর অনুমতিগুলি ভূমিকা অনুযায়ী সীমাবদ্ধ করুন।
 - অনুপ্রবেশ সনাক্তকরণ এবং প্রতিরোধ ব্যবস্থা ব্যবহার করুন।
 - সাইবার নিরাপত্তা সম্পর্কে সচেতনতার পরিবেশ তৈরি করুন।

৮. হোস্ট ফায়ারওয়াল এবং অ্যান্টি-ভাইরাসের গুরুত্ব

- হোস্ট ফায়ারওয়াল:
 - নিরাপত্তা নীতিমালার ভিত্তিতে নেটওয়ার্ক ট্রাফিক ফিল্টার করে।
 - ডিভাইসে অননুমোদিত প্রবেশ রোধ করে।
- অ্যান্টি-ভাইরাস:
 - ম্যালওয়্যার শনাক্ত, কোয়ারেন্টাইন এবং অপসারণ করে।
 - ক্রমবর্ধমান হুমকির বিরুদ্ধে রিয়েল-টাইম সুরক্ষা প্রদান করে।

৯. ওয়াই-ফাই সুরক্ষা

- ঝুঁকি:
 - অননুমোদিত প্রবেশ এবং ডেটা চুরি।
- সেরা পদ্ধতি:
 - WPA3 এনক্রিপশন ব্যবহার করুন।
 - রাউটারের ফার্মওয়্যার নিয়মিত আপডেট করুন।
 - ভিজিটরদের জন্য একটি আলাদা গেস্ট নেটওয়ার্ক সেট করুন।

১০. মৌলিক সুরক্ষা নীতি এবং অনুমতি কনফিগারেশন

- প্রয়োগ:
 - ব্যবহারকারী এবং অ্যাপ্লিকেশনের জন্য অ্যাক্সেস স্তর সংজ্ঞায়িত করুন।

- লিস্ট প্রিভিলেজ নীতি বাস্তবায়ন করুন।
- অননুমোদিত প্রবেশ প্রচেষ্টার জন্য অ্যালার্ট সেট আপ করুন।

সাইবার অপরাধ ও আইনি কাঠামো: বিশ্ব ও ভারতের প্রেক্ষাপট

১. সাইবার অপরাধ এবং বিশ্বব্যাপী আইনি কাঠামো

সাইবার অপরাধ হলো ডিজিটাল সিস্টেম বা ইন্টারনেটের মাধ্যমে সংঘটিত বেআইনি কার্যকলাপ। এ ধরনের অপরাধের মধ্যে রয়েছে:

- হ্যাকিং,
- পরিচয় চুরি,
- ফিশিং,
- সাইবার বুলিং,
- র‍্যানসমওয়্যার আক্রমণ।

আন্তর্জাতিক প্রচেষ্টা:

- বুদাপেস্ট কনভেনশন: সাইবার অপরাধের বিরুদ্ধে প্রথম আন্তর্জাতিক চুক্তি।
- ইউরোপিয়ান ইউনিয়নের **GDPR**: তথ্যের গোপনীয়তা ও সুরক্ষার ওপর জোর দেয়।
- যুক্তরাষ্ট্র: **CFAA (Computer Fraud and Abuse Act)** এবং **DMCA (Digital Millennium Copyright Act)** দ্বারা সাইবার অপরাধ নিয়ন্ত্রণ করা হয়।

২. তথ্যপ্রযুক্তি আইন, ২০০০ এবং সংশোধনী

ভারতের তথ্যপ্রযুক্তি আইন, ২০০০ সাইবার অপরাধ এবং ই-কমার্সের জন্য একটি আইনি কাঠামো প্রদান করে।

প্রধান বৈশিষ্ট্যসমূহ:

1. ডিজিটাল স্বাক্ষর এবং ইলেকট্রনিক নথি স্বীকৃতি।
2. সাইবার অপরাধ শাস্তি: হ্যাকিং, পরিচয় চুরি, এবং সাইবার সন্ত্রাসবাদের মতো অপরাধের জন্য শাস্তির ব্যবস্থা।
3. ইন্টারমিডিয়েরি দায়িত্ব: সোশ্যাল মিডিয়া প্ল্যাটফর্ম এবং ইন্টারনেট পরিষেবা প্রদানকারীদের নিয়ন্ত্রণ।

সংশোধনী আইন, ২০০৮:

1. সাইবার সন্ত্রাসবাদের জন্য শাস্তির ব্যবস্থা।
2. ডেটা সুরক্ষা আইন শক্তিশালীকরণ।

3. ইন্টারমিডিয়োরিদের জন্য শর্ত শিথিল।

আইনের সীমাবদ্ধতা:

1. নতুন প্রযুক্তি (AI, IoT, Blockchain) সম্পর্কিত অপরাধ অন্তর্ভুক্ত নয়।
2. সাইবার বুলিং এবং সামাজিক মাধ্যমের অপরাধগুলো অপরাধভাবে কাভার করা হয়েছে।
3. আন্তর্জাতিক আইনি সহায়তা: আইনে সীমিত নির্দেশিকা।

৩. সাইবার অপরাধ ও শাস্তি

- হ্যাকিং: ৩ বছর পর্যন্ত কারাদণ্ড বা ₹৫ লক্ষ টাকা জরিমানা (ভারত)।
- পরিচয় চুরি: ৩ বছর পর্যন্ত কারাদণ্ড।
- সাইবার সন্ত্রাসবাদ: যাবজ্জীবন কারাদণ্ড।

৪. নতুন প্রযুক্তি ও সাইবার আইন

কৃত্রিম বুদ্ধিমত্তা (AI) এবং মেশিন লার্নিং (ML):

- নৈতিক বিষয়: অ্যালগরিদমে পক্ষপাতিত্ব, মুখের চিহ্নিতকরণ অপব্যবহার।
- আইনি চ্যালেঞ্জ: AI-এর সিদ্ধান্তের জন্য দায়িত্ব কার?

ইন্টারনেট অফ থিংস (IoT):

- গোপনীয়তার ঝুঁকি: সংযুক্ত ডিভাইসের দুর্বলতা।
- আইনের অভাব: ডেটা সুরক্ষার জন্য মানসম্মত আইন নেই।

ব্লকচেইন:

- স্মার্ট চুক্তি: প্রচলিত আইনের সাথে মানানসই নয়।
- ক্রিপ্টোকারেন্সি: বৈধতা এবং নিয়ন্ত্রণ নিয়ে অস্পষ্টতা।

ডার্কনেট:

- চ্যালেঞ্জ: বেআইনি বাণিজ্য পর্যবেক্ষণ।

- আইনি পদক্ষেপ: মার্কেটপ্লেস অপারেটরদের (যেমন: সিন্ধু রোড) আটক।

সোশ্যাল মিডিয়া:

- ভুয়া থবর: অ্যালগরিদম দ্বারা ছড়িয়ে পড়া।
- সাইবার বুলিং: ব্যবহারকারীদের জবাবদিহিতা নিশ্চিত করার অভাব।

৫. অন্যান্য দেশের সাইবার আইন

- যুক্তরাষ্ট্র: CFAA, DMCA, এবং CCPA-এর মতো আইনি কাঠামো।
- ইউরোপ: GDPR এবং ই-প্রাইভেসি ডিরেকটিভ।
- চীন: কঠোর সাইবার নিরাপত্তা আইন।
- অস্ট্রেলিয়া: ডেটা লঙ্ঘন এবং জরিমানার জন্য কঠোর আইন।

৬. কেস স্টাডি

১. ওয়ানাক্রাই র‍্যানসমওয়্যার আক্রমণ (২০১৭):

- পুরনো সিস্টেমের দুর্বলতা প্রকাশ করে।
- আন্তর্জাতিক সাইবার নিরাপত্তা সহযোগিতার প্রয়োজনীয়তা বাড়ায়।

২. ক্যামব্রিজ অ্যানালিটিকা স্ক্যান্ডাল (২০১৮):

- ডেটার অপব্যবহার এবং গোপনীয়তা লঙ্ঘন।
- বিশ্বজুড়ে কড়া ডেটা সুরক্ষা আইন চালু হয়।

৩. ভারতের आधार তথ্য ফাঁস:

- বায়োমেট্রিক ডেটা চুরির কারণে ডিজিটাল পরিচয়ের নিরাপত্তা নিয়ে প্রশ্ন উঠেছে।