সাইবার-অপরাধ বলতে বোঝায় যে কোনো অপরাধ যা একটি কম্পিউটার এবং একটি নেটওয়ার্ক জড়িত। এটি সেই অপরাধমূলক কাজগুলিকে অন্তর্ভুক্ত করে যা কম্পিউটারের সাহায্যে সম্পাদিত হয়। এটিকে সংজ্ঞায়িত করা হয় ইন্টারনেটে সংঘটিত অপরাধ হিসাবে কম্পিউটার ব্যবহার করে একটি টুল বা একটি লক্ষ্যবস্তু শিকার হিসাবে। সাইবার-অপরাধ বলতে বোঝায় যেকোন অপরাধী বা অন্য অপরাধ যা ইলেকট্রনিক যোগাযোগ বা তথ্য ব্যবস্থার দ্বারা সহায়তা করে বা জড়িত থাকে, যার মধ্যে যেকোন ডিভাইস বা ইন্টারনেট বা যেকোন একটি বা একাধিক।

• দেবারতি হালদার এবং কে. জয়শঙ্কর সাইবার ক্রাইমকে এইভাবে সংজ্ঞায়িত করেছেন: "অপরাধ যেগুলি ব্যক্তি বা ব্যক্তিদের গোষ্ঠীর বিরুদ্ধে অপরাধমূলক উদ্দেশ্য নিয়ে সংঘটিত হয় যাতে শিকারের সুনামকে ইচ্ছাকৃতভাবে ক্ষতিগ্রস্ত করা হয় বা প্রত্যক্ষ বা পরোক্ষভাবে শিকারের শারীরিক বা মানসিক ক্ষতি বা ক্ষতি হয়। , ইন্টারনেট এবং মোবাইল ফোনের মতো আধুনিক টেলিকমিউনিকেশন নেটওয়ার্ক ব্যবহার করে "

• দুগ্গালের মতে: যেকোন অপরাধমূলক কার্যকলাপ যা কম্পিউটারকে একটি যন্ত্র, লক্ষ্য বা আরও অপরাধকে স্থায়ী করার উপায় হিসাবে ব্যবহার করে তা সাইবার-অপরাধের আওতার মধ্যে আসে।

সারা বিশ্বে সাইবার অপরাধের ব্যাপক বিস্তারের বেশ কিছু কারণ রয়েছে। কিছু উল্লেখযোগ্য কারণ হল-

• প্রযুক্তিতে অপরাধীদের দক্ষতা

• কম্পিউটার এবং তথ্য প্রযুক্তির উপর নির্ভরতা বৃদ্ধি
• ন্যূনতম ঝুঁকি
• অপরাধীর বিরুদ্ধে আইনি ব্যবস্থা নেওয়ার ক্ষেত্রে জটিলতা
• বিপুল আর্থিক লাভের সম্ভাবনা
• কম্পিউটার এবং ইন্টারনেট ব্যবহারকারীদের অসতর্কতা এবং অদক্ষ আচরণ
• অপরাধীদের শনাক্তকরণে সমস্যা
• সাইবার-অপরাধের শিকার ব্যক্তিদের আইনি ব্যবস্থা নিতে অনিচ্ছা
• অপরাধ সংঘটনের জন্য নতুন এবং অত্যাধুনিক উপায় অবলম্বন করা যা আইন প্রয়োগকারী কর্তৃপক্ষের সক্ষমতা অতিক্রম করে
• প্রতিশোধ
• অবহেলা

হ্যাকিং
হ্যাকিং সাধারণত একটি কম্পিউটার সিস্টেম এবং নেটওয়ার্কের অননুমোদিত অ্যাক্সেস হিসাবে বোঝা যায়।
যে ব্যক্তি ঘটাতে চায় বা জানে যে তার অন্যায়ভাবে ক্ষতি বা ক্ষতি হওয়ার সম্ভাবনা রয়েছে
জনসাধারণ বা কোনো ব্যক্তি, কম্পিউটারে থাকা কোনো তথ্য ধ্বংস বা মুছে বা পরিবর্তন করে
সম্পদ বা এর মান বা উপযোগিতা হ্রাস করে বা ক্ষতিকারকভাবে প্রভাবিত করে তাকে হ্যাকিং বলে।

ইমেল বোমা হামলা

এটি শিকারের কাছে প্রচুর সংখ্যক মেল প্রেরণকে বোঝায় এবং এর ফলে শেষ পর্যন্ত পরিণতি হয়
কম্পিউটার নেটওয়ার্ক সিস্টেম বিপর্যস্ত. ইন্টারনেট ব্যবহারে, একটি ইমেল বোমা হল নেট অপব্যবহারের একটি রূপ মেলবক্স উপচে পড়ার প্রয়াসে একটি ঠিকানায় বিপুল পরিমাণ ইমেল পাঠানোর সমন্বয়ে গঠিত অথবা মেল সার্ভার গুঁড়িয়ে দিন।
সিমলা কেস একটি ক্ষেত্রে, একজন বিদেশী যিনি প্রায় ত্রিশ বছর ধরে ভারতের সিমলায় বসবাস করতে চেয়েছিলেন
কম দামে জমি কেনার জন্য সিমলা হাউজিং বোর্ড কর্তৃক প্রবর্তিত একটি প্রকল্পের সুবিধা নিন। যখন সে
একটি আবেদন করেছেন, এটি প্রত্যাখ্যান করা হয়েছিল এই কারণে যে স্কিমগুলি শুধুমাত্র জন্য উপলব্ধ ছিল৷
ভারতের নাগরিক। তিনি তার প্রতিশোধ নেওয়ার সিদ্ধান্ত নেন। ফলস্বরূপ, তিনি হাজার হাজার মেইল পাঠান
সিমলা হাউজিং বোর্ড এবং তাদের সার্ভার ক্র্যাশ না হওয়া পর্যন্ত বারবার ই-মেইল পাঠাতে থাকে।

ই-মেইল স্পুফিং
এটি এক ধরণের ই-মেইল যা একটি উত্স থেকে উদ্ভূত বলে মনে হয় যদিও এটি আসলে পাঠানো হয়েছে
অন্য উৎস থেকে। কোনো ব্যক্তির মানহানির মতো কারণে বা কোনো কারণে এ ধরনের অপরাধ করা যেতে পারে
আর্থিক লাভ ইত্যাদি

ডেটা বিভ্রান্তি

ডেটা ডিডলিং (যাকে মিথ্যা ডেটা এন্ট্রিও বলা হয়) হল আগে বা চলাকালীন ডেটার অননুমোদিত পরিবর্তন
একটি কম্পিউটার সিস্টেমে তাদের ইনপুট। এটি একটি কম্পিউটার প্রক্রিয়া করার ঠিক আগে কাঁচা তথ্য পরিবর্তন জড়িত
এবং তারপর প্রক্রিয়াকরণ সম্পন্ন হওয়ার পরে এটিকে পরিবর্তন করুন।

লজিক বোমা
একটি লজিক বোমা হল কোডের একটি অংশ যা ইচ্ছাকৃতভাবে একটি সফ্টওয়্যার সিস্টেমে ঢোকানো হয় যা একটি সেট বন্ধ করবে
দূষিত ফাংশন যখন নির্দিষ্ট শর্ত পূরণ হয়.

উদাহরণস্বরূপ, একজন প্রোগ্রামার লুকিয়ে রাখতে পারে a
কোডের টুকরো যা ফাইল মুছে ফেলা শুরু করে। এটি একটি ইভেন্ট নির্ভর প্রোগ্রাম, যত তাড়াতাড়ি মনোনীত হয়
ঘটনা ঘটে, এটি কম্পিউটার ক্র্যাশ করে, একটি ভাইরাস বা অন্য কোন ক্ষতিকারক সম্ভাবনা ছেড়ে দেয়। কিছু
ভাইরাসগুলিকে লজিক বোমা বলা যেতে পারে কারণ তারা সারা বছর সুপ্ত থাকে এবং পরিণত হয়
শুধুমাত্র একটি নির্দিষ্ট তারিখে সক্রিয়, যেমন চেরনোবিল ভাইরাস।

সালামি আক্রমণ
এই ধরনের অপরাধ সাধারণত আর্থিক প্রতিষ্ঠানে বা উদ্দেশ্যের জন্য প্রচলিত
আর্থিক অপরাধ করছে। এই ধরনের অপরাধের একটি গুরুত্বপূর্ণ বৈশিষ্ট্য হল পরিবর্তন
এত ছোট যে এটি সাধারণত অলক্ষিত হবে। যেমন জিগলার কেস, যেখানে একটি লজিক বোমা ছিল
ব্যাঙ্ক ব্যবস্থায় চালু করা হয়েছে, যা প্রতিটি অ্যাকাউন্ট থেকে 10 সেন্ট কেটে একটি তে জমা করে
বিশেষ অ্যাকাউন্ট।
জিগলার কেস
মার্কিন যুক্তরাষ্ট্রে একটি ব্যাংকের একজন কর্মচারীর চাকরি বন্ধ হয়ে গেছে। অনুমিত দ্বারা ক্ষুব্ধ
তার নিয়োগকর্তাদের দ্বারা দুর্ব্যবহার, লোকটি ব্যাঙ্কের সার্ভারে একটি লজিক বোমা প্রবর্তন করেছিল। যুক্তিটা
ব্যাঙ্কে নিবন্ধিত সমস্ত অ্যাকাউন্ট থেকে দশ সেন্ট ডেবিট এবং স্থানান্তর করার জন্য বোমা প্রোগ্রাম করা হয়েছিল
সেগুলি সেই ব্যক্তির অ্যাকাউন্টে যাঁর নাম বর্ণানুক্রমিকভাবে ব্যাঙ্কের রেকর্ডে শেষ ছিল।
পরে তিনি জিগলারের নামে একটি অ্যাকাউন্ট খুলেছিলেন। স্থানান্তরিত পরিমাণ এত কম ছিল যে

কেউ দোষ লক্ষ্য করেনি। তবে বিষয়টি প্রকাশ্যে আনা হলে ওই নামে এক ব্যক্তি মো
জাইগলার একই ব্যাংকে তার অ্যাকাউন্ট খোলেন। বিপুল পরিমাণ অর্থ পেয়ে তিনি বিস্মিত হন
প্রতি সপ্তাহে তার অ্যাকাউন্টে স্থানান্তর করা হচ্ছে। তিনি ব্যাঙ্ক এবং প্রাক্তনকে 'ভুল' জানিয়েছেন
কর্মচারীর বিরুদ্ধে মামলা করা হয়েছে।

ওয়েব জ্যাকিং
এই শব্দটি হাই জ্যাকিং শব্দ থেকে উদ্ভূত হয়েছে। এই ধরনের অপরাধে, হ্যাকার অ্যাক্সেস লাভ করে
এবং অন্যের ওয়েব সাইটের উপর নিয়ন্ত্রণ। এমনকি তিনি সাইটের তথ্য পরিবর্তন করতে পারেন।
এটি ঘটে যখন কেউ পাসওয়ার্ড ক্র্যাক করে এবং পরে জোর করে একটি ওয়েবসাইটের নিয়ন্ত্রণ নেয়
এটা পরিবর্তন ওয়েবসাইটের প্রকৃত মালিকের আর কোন নিয়ন্ত্রণ নেই যা প্রদর্শিত হবে
যে ওয়েবসাইট.

পিরানহা কেস
মার্কিন যুক্তরাষ্ট্রে প্রকাশিত একটি সাম্প্রতিক ঘটনায় শিশুদের জন্য একটি শখের ওয়েবসাইটের মালিক একটি ইমেল পেয়েছেন যাতে তাকে জানানো হয় যে একদল হ্যাকার তার ওয়েবসাইটের নিয়ন্ত্রণ অর্জন করেছে। তাদের দাবি ছিল ক
তার কাছ থেকে 1 মিলিয়ন ডলার মুক্তিপণ। মালিক, একজন স্কুল শিক্ষক, হুমকিটিকে গুরুত্বের সাথে নেননি।

তিনি অনুভব করেছিলেন যে এটি কেবল একটি ভীতিকর কৌশল এবং ই-মেইল উপেক্ষা করে। তিনদিন পর মেয়েটা এলো
সারা দেশ থেকে অনেক টেলিফোন কলের পর জানতে, হ্যাকাররা ওয়েব জ্যাক করেছে
তার ওয়েবসাইট। পরবর্তীকালে, তারা ওয়েবসাইটের একটি অংশ
পরিবর্তন করেছিল যার শিরোনাম ছিল 'কীভাবে
গোল্ডফিশের সাথে মজা করুন। যে সমস্ত জায়গায় এটি উল্লেখ করা হয়েছিল, সেখানে তারা শব্দটি প্রতিস্থাপন করেছিল
'গোল্ডফিশ' শব্দের সাথে 'পিরানহাস'। পিরানহা ছোট কিন্তু অত্যন্ত বিপজ্জনক মাংস খাওয়া মাছ।
অনেক শিশু জনপ্রিয় ওয়েবসাইট পরিদর্শন করেছিল এবং ওয়েবসাইটের বিষয়বস্তু কী তা বিশ্বাস করেছিল
প্রস্তাবিত এই হতভাগ্য শিশুরা নির্দেশ অনুসরণ করে, পিরানহাদের সাথে খেলার চেষ্টা করেছিল, যা
তারা পোষা দোকান থেকে কেনা, এবং খুব গুরুতর আহত হয়.

সাইবার পর্নোগ্রাফি
সাইবার পর্নোগ্রাফির মধ্যে পর্নোগ্রাফিক ওয়েবসাইট পরিচালনা করা অন্তর্ভুক্ত; পর্নোগ্রাফিক প্রকাশ এবং মুদ্রণ
কম্পিউটার এবং ইন্টারনেট ব্যবহার করে ম্যাগাজিন, পর্নোগ্রাফিক ছবি ডাউনলোড এবং প্রেরণ করা,
ফটো; লেখা ইত্যাদি

জালিয়াতি
জাল নোট, ডাক ও রাজস্ব স্ট্যাম্প, মার্কশিট, সার্টিফিকেট ইত্যাদি জাল হতে পারে
অত্যাধুনিক কম্পিউটার, প্রিন্টার এবং স্ক্যানার ব্যবহার করে। এগুলি কম্পিউটার এবং উচ্চমানের স্ক্যানার এবং প্রিন্টার ব্যবহার করে তৈরি করা হয়। এটি এখন একটি ক্রমবর্ধমান ব্যবসা হয়ে উঠছে।

পরিষেবা আক্রমণ অস্বীকার
পরিষেবা অস্বীকারের ক্ষেত্রে লক্ষ্যযুক্ত কম্পিউটারটি এতগুলি অনুরোধ পেয়েছে যা এটি করতে পারে না
হাতল. এটি কম্পিউটার সংস্থান ক্র্যাশ করে। ফলস্বরূপ, কম্পিউটার
সম্পদ প্রদান অস্বীকার
অনুমোদিত ব্যবহারকারীর যথাযথ সেবা।

সাইবার মানহানি
কম্পিউটার বা ইন্টারনেটের সাহায্যে মানহানি ঘটলে এটি ঘটে। উদাহরণ স্বরূপ,
কেউ একটি ওয়েবসাইটে কারও সম্পর্কে মানহানিকর বিষয় প্রকাশ করে বা তার বন্ধুদের ই-মেইল পাঠায়
মানহানিকর তথ্য ধারণকারী।

ট্রোজান আক্রমণ
এটি একটি অননুমোদিত প্রোগ্রাম, যা প্যাসিভভাবে অন্যের সিস্টেমের উপর নিয়ন্ত্রণ লাভ করে
একটি অনুমোদিত প্রোগ্রাম হিসাবে নিজেকে প্রতিনিধিত্ব. এটি আসলে যা করছে তা গোপন করছে।
লেডি ডিরেক্টর কেস
মার্কিন যুক্তরাষ্ট্রে চ্যাট করার সময় একজন মহিলা চলচ্চিত্র পরিচালকের কম্পিউটারে একটি ট্রোজান ইনস্টল করা হয়েছিল। সাইবার অপরাধী কম্পিউটারে বসানো ওয়েব ক্যামের মাধ্যমে তার নগ্ন ছবি প্রাপ্ত করে। তিনি আরও
এই মহিলাকে হয়রানি করেছে।

প্রতারণা ও প্রতারণা
অনলাইন জালিয়াতি এবং প্রতারণা হল সবচেয়ে লাভজনক ব্যবসাগুলির মধ্যে একটি যা আজকের দিনে বাড়ছে
সাইবার স্পেস এটা বিভিন্ন ফর্ম অনুমান করতে পারে. অনলাইনে কিছু প্রতারণা ও প্রতারণার ঘটনাও ঘটেছে
ক্রেডিট কার্ডের অপরাধ, চুক্তিভিত্তিক অপরাধ, চাকরির প্রস্তাব ইত্যাদির সাথে সম্পর্কিত বিষয়গুলি প্রকাশ্যে এসেছে।
আজিমের প্রতারণার মামলা
সম্প্রতি দিল্লির মেট্রোপলিটন ম্যাজিস্ট্রেট আদালত ২৪ বছর বয়সী ইঞ্জিনিয়ার আজিমকে দোষী সাব্যস্ত করেছেন।
প্রতারণামূলকভাবে গ্রাহকদের ক্রেডিট কার্ডের বিবরণ লাভ।
মেট্রোপলিটন ম্যাজিস্ট্রেট গুলশান কুমার

আজিমকে প্রতারণার দায়ে দোষী সাব্যস্ত করলেও তাকে কারাগারে পাঠাননি। পরিবর্তে, আজিমকে ক
20,000 টাকার ব্যক্তিগত বন্ড এবং এক বছরের পরীক্ষায় মুক্তি দেওয়া হয়েছিল।

সাইবার বুলিং
কেমব্রিজ অভিধান অনুসারে, সাইবার বুলিং মানে ইন্টারনেট ব্যবহার করার কার্যকলাপ
অন্য ব্যক্তির ক্ষতি বা ভয় দেখান, বিশেষ করে তাদের অপ্রীতিকর বার্তা পাঠিয়ে।
সাইবার বুলিং এসএমএস, টেক্সট এবং অ্যাপের মাধ্যমে বা অনলাইনে সোশ্যাল মিডিয়া, ফোরাম বা
গেমিং যেখানে লোকেরা দেখতে, অংশগ্রহণ করতে বা সামগ্রী ভাগ করতে পারে। সাইবার বুলিং এর মধ্যে রয়েছে পাঠানো,
অন্য কারো সম্পর্কে নেতিবাচক, ক্ষতিকর, মিথ্যা সামগ্রী পোস্ট করা বা শেয়ার করা। এটা শেয়ারিং অন্তর্ভুক্ত করতে পারে
অন্য কারো সম্পর্কে ব্যক্তিগত বা ব্যক্তিগত তথ্য যা বিব্রত বা অপমান সৃষ্টি করে।

হিন্দুজা সাইবার বুলিংকে "কম্পিউটার, সেল ব্যবহারের মাধ্যমে ইচ্ছাকৃত এবং বারবার ক্ষতি" হিসাবে সংজ্ঞায়িত করেছেন
ফোন বা অন্যান্য ইলেকট্রনিক ডিভাইস।''
এই উপাদানগুলির মধ্যে নিম্নলিখিতগুলি অন্তর্ভুক্ত রয়েছে:

ইচ্ছাকৃত: আচরণটি ইচ্ছাকৃত হতে হবে, আকস্মিক নয়।
বারবার: ধমকানো আচরণের একটি প্যাটার্ন প্রতিফলিত করে, শুধুমাত্র একটি বিচ্ছিন্ন ঘটনা নয়।
ক্ষতি: লক্ষ্য অবশ্যই বুঝতে হবে যে ক্ষতি হয়েছে।
কম্পিউটার, সেল ফোন এবং অন্যান্য ইলেকট্রনিক ডিভাইস: এটি অবশ্যই পার্থক্য করে
ঐতিহ্যগত গুন্ডামি থেকে সাইবার বুলিং।

সবচেয়ে সাধারণ জায়গা যেখানে সাইবার বুলিং হয়:

- সোশ্যাল মিডিয়া, যেমন- Facebook, Instagram, WhatsApp, Imo, Viber, Tiktok, Twitter ইত্যাদি।
- এসএমএস (শর্ট মেসেজ সার্ভিস) ডিভাইসের মাধ্যমে পাঠানো টেক্সট মেসেজ নামেও পরিচিত
- তাত্ক্ষণিক বার্তা (ডিভাইস, ইমেল প্রদানকারী পরিষেবা, অ্যাপস এবং সোশ্যাল মিডিয়া মেসেজিংয়ের মাধ্যমে
বৈশিষ্ট্য)
- ইমেইল

2010 চু জার্নাল বিভাগে উল্লেখ করা হয়েছে, পৃষ্ঠা 349 এ, ড. আর.সি. মিশ্র, আইপিএস, তাঁর বইতে
"সাইবার-অপরাধ: নতুন সহস্রাব্দে প্রভাব" সাইবার অপরাধ প্রতিরোধের জন্য নির্দিষ্ট প্রযুক্তি সম্পর্কে বলা হয়েছে।

ক) ফায়ারওয়াল: নিরাপদ মানের সাথে প্রয়োগ করা ফায়ারওয়াল কোন অনুপ্রবেশকারীকে প্রবেশের অনুমতি দেবে না পদ্ধতি.

খ) এনক্রিপ্ট করা টানেলিং: একটি এনক্রিপ্ট করা টানেল ইন্টারনেট জুড়ে নিরাপদ যোগাযোগের অনুমতি দেয়।
এতে ইন্টারনেটে ডেটা প্যাকেটগুলি এনক্রিপ্ট করা হয় এবং তারপরে শুরুতে আইপিতে মোড়ানো হয়
টানেলের বিন্দু। এনক্রিপ্ট করা প্যাকেট তারপর ইন্টারনেটের মাধ্যমে প্রেরণ করা যাবে যখন
প্যাকেটগুলি টানেলের অন্য প্রান্তে এসেছে, সেগুলি মোড়ানো এবং ডিক্রিপ্ট করা হয়েছে।

গ) সিকিউর সকেট লেয়ার (SSL) এবং সিকিউর HTTP: এটি একটি এনক্রিপ্ট করা TCP/IP প্রদান করে
ইন্টারনেট SSL-এ দুটি হোস্টের মধ্যে পাথওয়েগুলি যেকোনো TCP প্রোটোকল এনক্রিপ্ট করতে ব্যবহার করা যেতে পারে
HTTP এনক্রিপ্ট করতে।
সাইবার অপরাধ প্রতিরোধের জন্য প্রযুক্তি

ঘ) সিকিউর ইলেকট্রিক ট্রান্সফর্ম (SET): এই প্রযুক্তিতে ক্রিপ্টোগ্রাফিক অ্যালগরিদম জড়িত

ক্রেডিট কার্ড নম্বর এনক্রিপ্ট করুন, তাই এটি ইন্টারনেটে দেখা যাবে না।

ঙ) ডিজিটাল স্বাক্ষর: ক্রিপ্টোগ্রাফিক কৌশল ব্যবহার করা হয় যাতে শুধুমাত্র অনুমোদিত প্রমাণীকৃত হয়
ব্যক্তি সিস্টেমে প্রবেশ করতে পারেন।

চ) কর্মচারী প্রশিক্ষণ