साइबर वॉर का खतरा

drishtiias.com/hindi/current-affairs-news-analysis-editorials/news-editorials/12-03-2019/print

संदर्भ

समय-समय पर मीडिया में यह चर्चा होती रहती है कि अमुक वेबसाइट हैक हो गई या फलाँ वेबसाइट पर चीन या पाकिस्तान के हैकर्स ने कब्ज़ा करके उसे कुछ समय के लिये निष्क्रिय कर दिया। अभी हाल ही में देश में सत्तारूढ़ दल भाजपा की वेबसाइट हैक होने की खबर आई थी...और ज़्यादा समय नहीं हुआ जब UPSC की वेबसाइट को भी हैक कर लिया गया था। भारत में इस तरह के साइबर हमले लगातार बढ़ रहे हैं।

हाल ही में पुलवामा आतंकी हमले के बाद एक भारतीय हैकर ग्रुप ने पाकिस्तान पर बड़ा साइबर हमला कर दिया। भारतीय हैकर ने 200 से अधिक पाकिस्तानी वेबसाइट्स को हैक कर दिया था। टीम आई-क्रू द्वारा हैक की गई इन वेबसाइट्स को खोलने पर वहाँ शहीदों को श्रद्धांजलि देने वाले संदेश और एक मोमबत्ती जलती हुई दिखाई दे रही थी। इससे पहले पुलवामा हमले के फौरन बाद खबर मिली कि पाकिस्तानी हैकरों ने भारत सरकार से जुड़ी कम-से-कम 90 वेबसाइट्स को हैक कर लिया। इनमें वित्तीय संचालन और पावर ग्रिड से संबंधित वेबसाइटें खासतौर से हैकरों के निशाने पर थीं।

क्या होता है साइबर अटैक?

'साइबर अटैक' वाक्यांश का इस्तेमाल आतंकवादी गतिविधियों में इंटरनेट के माध्यम से किये जाने वाले हमलों को बताने के लिये किया जाता है। इनमें कंप्यूटर वायरस जैसे साधनों के माध्यम से कंप्यूटर नेटवर्क में जान-बूझकर बड़े पैमाने पर किया गया व्यवधान शामिल है, विशेष रूप से इंटरनेट से जुड़े किसी निजी कंप्यूटर में। साइबर अटैक को किसी कंप्यूटर अपराध के रूप में और अधिक सामान्य तरीके से इस प्रकार परिभाषित किया जा सकता है...**वास्तविक दुनिया के बुनियादी ढाँचे, संपत्ति तथा किसी के जीवन को हानि पहुँचाए बिना किसी कंप्यूटर नेटवर्क को लक्षित कर उसे क्षति पहुँचाना। इसे हैकिंग भी कहा जाता है।**

क्या होती है हैकिंग?

हैकिंग एक ऐसी प्रक्रिया है जिसमें हैकिंग करने वाला किसी अन्य व्यक्ति की जानकारी को बिना उसकी इजाज़त के चोरी करता है। ऐसा करने के लिये वह उस व्यक्ति की निजी जानकारियों में सेंध लगाकर उन्हें हैक करता है। हैकिंग को गैरकानूनी माना गया है, लेकिन कई बार हैकिंग अच्छे काम के लिये भी की जाती है। इसके माध्यम से कई प्रकार के अपराध साइबर अपराधियों द्वारा किये जाते हैं।

कौन होता है हैकर?

अधिकांश लोगों को यह पता नहीं होता कि हैकर कौन है और वह क्या करता है...कैसे करता है। दरअसल...हैकिंग शुरू करते समय ज़्यादातर हैकर्स इसे शौकिया रूप में करते हैं, हर समय इसके पीछे पैसा उद्देश्य नहीं होता। अन्य हैकर्स के बीच पहचान बनाने की इच्छा या खुद को दूसरों से बेहतर बताने की होड़ के चक्कर में भी हैकिंग के लालच में यहीं के होकर रह जाते हैं। तकनीक की ताकत को अपने बस में करने की वजह से भी हैकिंग शुरू होती है। हैकर को हालांकि सबकुछ पता होता है कि क्या सही है और क्या गलत, बावजूद इसके वे इस काम में लगे होते हैं। सामाजिक रूप से स्वीकार्यता नहीं होना या किसी वज़ह से कमज़ोर दिखने के कारण भी युवा हैकिंग के क्षेत्र में कदम बढ़ाते हैं।

तीन प्रकार के हैकर

व्हाइट हैट हैकर: इस श्रेणी में आने वाले हैकर अच्छे काम करते हैं यानी इन्हें लोगों की सुरक्षा के लिये नियुक्त किया जाता है। इन्हें सरकार के द्वारा या किसी भी संस्था के द्वारा रखा जाता है इन्हें **एथिकल हैकर** के रूप में भी जाना जाता है।

ब्लैक हैट हैकर: इन हैकर्स को **क्रैकर्स** भी कहा जाता है। यह अपनी दक्षता का गलत इस्तेमाल करके गैरकानूनी काम करते हैं। जैसे- किसी की निजी जानकारियाँ चुराना, किसी के एकाउंट को हैक करना और उन जानकारियों का ऑनलाइन इस्तेमाल पैसा कमाने में करना।

ग्रे हैट हैकर: इस श्रेणी के हैकर ब्लैक और वाइट का सम्मिश्रण होते हैं, जो कुछ समय के लिये अच्छा काम करते हैं और कभी-कभी गैरकानूनी काम भी करते हैं।

फिशिंग (Phishing) क्या है?

इसे हिंदी में ऑनलाइन जालसाज़ी की संज्ञा दी गई है। इसके तहत अपराधी फिशिंग के माध्यम से नकली ई-मेल या संदेश भेजते हैं, जो किसी प्रतिष्ठित कंपनी, आपके बैंक, क्रेडिट कार्ड, ऑनलाइन शॉपिंग की तरह मिलते-जुलते होते हैं। अगर सतर्कता नहीं बरती जाए तो इनके फंदे में फंसना तय है। इन जाली ई-मेल या संदेशों का उद्देश्य लोगों की निजी पहचान से जुड़ी जानकारियों (Personally Identifiable Information) को चुराना है। इसके तहत किसी व्यक्ति की निजी जानकारियॉ आती हैं, जिनमें नाम, ई-मेल. यूज़र ID, पासवर्ड, मोबाइल नंबर, पता, बैंक खाता संख्या, ATM/डेबिट या क्रेडिट कार्ड नंबर और इनका पिन नंबर तथा जन्मतिथि आदि शामिल हैं।

रैनसमवेयर क्या है?

रैनसमवेयर एक प्रकार का फिरौती मांगने वाला सॉफ्टवेयर है। इसे इस तरह से बनाया जाता है कि वह किसी भी कंप्यूटर सिस्टम की सभी फाइलों को एनक्रिप्ट कर देता है। यह सॉफ्टवेयर द्वारा इन फाइलों को एनक्रिप्ट करते ही फिरौती मांगने लगता है और धमकी देता है कि यदि अमुक राशि नहीं चुकाई तो वह उस कंप्यूटर की सभी फाइलों को करप्ट कर देगा। इसके बाद इन फाइलों तक कंप्यूटर उपयोगकर्त्ता की तब तक पहुँच नहीं हो पाती, जब तक वह फिरौती में मांगी गई राशि का भुगतान नहीं कर देता। इस तरह के वायरस को किसी संदिग्ध स्थान से कोई फाइल डाउनलोड करके पहुँचाया जा सकता है।

महत्त्वपूर्ण सरकारी वेबसाइट्स की हैकिंग

आज से लगभग 6 साल पहले एक आँकड़ा एडवर्ड स्नोडेन ने मुहैया कराया था। इसमें बताया गया था कि बाहर बैठे सेंधमारों ने भारतीयों की 6.3 अरब खुफिया सूचनाओं तक पहुँच बना ली थी। आज हालत यह है कि हमारे प्रधानमंत्री कार्यालय से लेकर रक्षा व विदेश मंत्रालय, भारतीय दूतावासों, मिसाइल प्रणालियों, NIC, CBI के कंप्यूटरों पर भी साइबर हमले हो चुके हैं। भारत के सरकारी संस्थान साइबर हमलों से सुरक्षित नहीं हैं। दरअसल, सरकार और कॉरपोरेट जगत को हैकर्स द्वारा अपनाए जा रहे

खतरनाक तरीकों के बारे में कोई विशेष जानकारी ही नहीं है। एंटी वायरस और फायरवॉल सॉफ्टवेयर लोड करने के बाद भारत में ज़्यादातर विभाग और कॉरपोरेट कंपनियाँ यह मान लेती हैं कि उन्होंने अपने सिस्टम और नेटवर्क को साइबर हमलों से सुरक्षित कर लिया है।

राष्ट्रीय साइबर सुरक्षा नीति

साइबर खतरों को भाँपते हुए भारत सरकार ने छह साल पहले 2013 में **राष्ट्रीय साइबर सुरक्षा नीति** जारी की थी, जिसमें देश के साइबर सुरक्षा के बुनियादी ढाँचे की रक्षा के लिये प्रमुख रणनीतियों को अपनाने की बात कही गई थी। इन नीतियों के तहत देश में 24 घंटे काम करने वाले एक **नेशनल क्रिटिकल इन्फॉर्मेशन प्रोटेक्शन सेंटर** (NCEIPC) की स्थापना शामिल है, जो देश में महत्त्वपूर्ण सूचना तंत्र के बुनियादी ढाँचे सुरक्षा के लिये एक नोडल एजेंसी के रूप में काम कर सके। फिलहाल देश में साइबर सुरक्षा पर कोई संयुक्त कार्यकारी समूह नहीं है और साइबर सुरक्षा पर किसी स्वायत्त निकाय का गठन भी नहीं किया गया है।

मुख्य विशेषताएँ

- इलेक्ट्रॉनिक लेनदेन का सुरक्षित माहौल तैयार करना, विश्वास और भरोसा कायम करना तथा साइबर जगत की सुरक्षा के लिये हितधारकों के कार्यों में मार्गदर्शन करना।
- देश में सभी स्तरों पर साइबर सुरक्षा के मुद्दों से निपटने के लिये व्यापक, सहयोगात्मक और सामूहिक कार्रवाई हेतु रूपरेखा तैयार की गई है।
- इस नीति में ऐसे उद्देश्यों और रणनीतियों की आवश्यकता को मान्यता दी गई है जिन्हें राष्ट्रीय और अंतर्राष्ट्रीय स्तर पर अपनाए जाने की आवश्यकता है।
- इस नीति का विज़न और मिशन नागरिकों, व्यवसायियों और सरकार के लिये साइबर जगत को सुरक्षित और लचीला बनाना है।
- साइबर हमलों से राष्ट्र को सुरक्षित बनाने और खामियाँ दूर करने का लक्ष्य तय करना।
- देश के अंदर सभी हितधारकों के बीच सहयोग और समन्वय बढ़ाना।
- राष्ट्रीय साइबर सुरक्षा विज़न और मिशन के समर्थन में उद्देश्य एवं रणनीति तय करना।
- ऐसी रूपरेखा और पहल तैयार की गई हैं जो सरकार के स्तर, क्षेत्र स्तर पर और सरकारी-निजी भागीदारी के माध्यम से आगे बढ़ाई जा सकती हैं।
- इससे साइबर सुरक्षा अनुपालन, साइबर हमलों, साइबर अपराध और साइबर बुनियादी ढाँचे जैसे रुझानों की राष्ट्रीय स्तर पर निगरानी की जा सकेगी।

सरकार द्वारा उठाए गए कदम

- सूचना प्रौद्योगिकी अधिनियम 2000 की धाराएँ 43, 43ए, 66, 66बी, 66 सी, 66डी, 66ई, 66एफ, 67, 67ए, 67बी, 70, 72, 72ए तथा 74 हैकिंग और साइबर अपराधों से संबंधित हैं।
- सरकार ने साइबर सुरक्षा से संबंधित फ्रेमवर्क का अनुमोदन किया है। इसके लिये **राष्ट्रीय सुरक्षा परिषद सचिवालय** को नोडल एजेंसी बनाया गया है।
- राष्ट्रीय विशिष्ट अवसंरचना और विशिष्ट क्षेत्रों में साइबर सुरक्षा के लिये **राष्ट्रीय प्रौद्योगिकी अनुसंधान संगठन** को नोडल एजेंसी बनाया गया है।
- साइबर सुरक्षा के खतरों के विश्लेषण करने, अनुमान लगाने और चेतावनी देने के लिये भारत **कंप्यूटरर आपात प्रतिक्रिया टीम** (CERT-IN) को नोडल एजेंसी बनाया गया।
- साइबर अपराधों को लेकर गृह मंत्रालय ने राज्यों/केंद्रशासित प्रदेशों के लिये दिशा-निर्देश जारी किये हैं।
- महिलाओं और बच्चों के लिये गृह मंत्रालय '**महिला व बच्चों के खिलाफ होने वाले साइबर अपराधों की रोकथाम**' कार्यक्रम चला रहा है।

- फोन पर होने वाले धोखाधड़ी से निपटने के लिये गृह मंत्रालय ने **अंतर-मंत्रालय समिति** का गठन किया है। इसके अलावा, राज्यों/केंद्रशासित प्रदेशों के लिये दिशा-निर्देश भी जारी किये हैं।

साइबर क्राइम एक अवैध कार्य है, जहाँ कंप्यूटर को साधन या लक्ष्य या दोनों ही तरीके से इस्तेमाल किया जाता है। कह सकते हैं कि यह एक व्यापक अवधारणा है जिसमें कंप्यूटर या कंप्यूटर नेटवर्क को साधन, लक्ष्य या आपराधिक गतिविधि के स्थान की तरह इस्तेमाल किया जाता है।

आज साइबर स्पेस के खतरों की बात काल्पनिक नहीं रह गई है। वर्चुअल आतंकवाद, सेंधमारी और सैन्य व आर्थिक महत्त्व की सूचनाओं के लीक होने जैसी घटनाओं ने साबित कर दिया है कि सूचनाओं के इलेक्ट्रॉनिक नेटवर्क में घुसपैठ की रोकथाम के पुख्ता प्रबंध नहीं करने का खमियाज़ा दुनिया में कई देशों को उठाना पड़ सकता है।

साइबर कहें या वर्चुअल (आभासी) वॉर, अब इसका खतरा वास्तविक है। इसमें संदेह नहीं रह गया है कि भविष्य की सबसे बड़ी चुनौती साइबर वॉर होगी। साइबर वॉर यानी इंटरनेट के जरिये संचालित की जाने वाली वे आपराधिक और आतंकी गतिविधियाँ जिनसे कोई व्यक्ति या संगठन देश-दुनिया और समाज को नुकसान पहुँचाने की कोशिश करता है।

आज सूचनाओं और जानकारियों का सारा संचालन इंटरनेट के जरिये ही हो रहा है। ऐसी स्थिति में विजेता वही होगा जो दुश्मन के कंप्यूटर नेटवर्क में सेंध लगाने में सक्षम होगा और हैकरों द्वारा इंटरनेट पर संचालित किये जाने वाले हमलों से निपट सकेगा।