E-ISSN: 2583-9667
Indexed Journal
Peer Reviewed Journal
https://multiresearchjournal.theviews.in

Received: 02-10-2024
Accepted: 13-11-2024
Published: 05-01-2025

INTERNATIONAL JOURNAL OF ADVANCE RESEARCH IN MULTIDISCIPLINARY

Volume 3; Issue 1; 2025; Page No. 264-268

भारतीय बैंकिंग प्रणाली में साइबर खतरों की पहचान और वर्गीकरण करना

[1]Rakesh Kumar Rai, [2]Dr. Subhasish Basu and [3]Dr. Aiman Fatma

[1]Research Scholar, Department of Commerce, P.K. University, Shivpuri, Madhya Pradesh, India
[2]Supervisor, Department of Commerce, P.K. University, Shivpuri, Madhya Pradesh, India
[3]Associate Professor, Department of Commerce, P.K. University, Shivpuri, Madhya Pradesh, India

DOI: https://doi.org/10.5281/zenodo.18696295

Corresponding Author: Rakesh Kumar Rai

सारांश

साइबर अपराधी तेज़ी से कॉर्पोरेट के रूप में कार्य कर रहे हैं, नए उत्पाद विकास दल और कुछ संगठन उनकी सेवाएँ दे रहे हैं या उन्हें अन्य आपराधिक गिरोहों के साथ एकीकृत कर रहे हैं। साइबर अपराध अन्य अपराधों की तुलना में अधिक लाभदायक है, इसलिए बैंकों को इसके विरुद्ध सुरक्षा बनाने में बहुत अधिक संसाधनों का निवेश करना जारी रखना चाहिए।यदि कॉर्पोरेट ग्राहक जानते हैं कि बैंक धोखाधड़ी और साइबर हमलों को रोकने के लिए प्रतिबद्ध है, तो बैंक में विश्वास बढ़ेगा तथा अच्छे संबंध स्थापित होंगे। साइबर अपराध से निपटने के लिए बैंकों को सिस्टम और लोगों में भारी निवेश करना चाहिए।

मूल शब्दः साइबर, भारतीय बैंकिंग, कॉर्पोरेट, साइबर अपराध, खतरों।

प्रस्तावना

बैंकिंग क्षेत्र में प्रौद्योगिकी द्वारा पैदा किए गए अवसरों और संभावनाओं के बावजूद, यह बैंकिंग क्षेत्र और वित्तीय सेवा संस्थानों के लिए एक विशेष चुनौती भी प्रस्तुत करती है। हम सभी जानते हैं कि प्रौद्योगिकी के दुर्भावनापूर्ण उपयोग से बैंकों और वित्तीय सेवा संस्थानों के बुनियादी ढांचे में व्यवधान, सुरक्षा का उल्लंघन, ग्राहक विश्वास, वित्तीय स्थिरता को खतरे में डालना और अन्य साइबर अपराध होते हैं। सूचना सुरक्षा उल्लंघन कभी भी अचानक हो सकता है क्योंकि सब कुछ इंटरनेट के साथ एकीकृत है और साइबर अपराधी जो बैंकों और वित्तीय सेवा संस्थानों की इंटरनेट चीजों में हेरफेर कर रहे हैं, वे बैंकों के ग्राहक डेटा को हैक करने और वित्तीय संस्थानों के ग्राहकों के पैसे को डिजिटल रूप से चुराने में सक्षम हैं।

बैंकिंग क्षेत्र में प्रौद्योगिकी के महत्वपूर्ण विकास के साथ, प्रौद्योगिकी से जुड़े जोखिम भी बढ़ गए हैं। इसलिए, बैंकिंग क्षेत्र के संबंध में हर दिन कई प्रकार और रूप में साइबर सुरक्षा हमले/खतरे सामने आते हैं। साइबर सुरक्षा हमले पूरे वित्तीय तंत्र के लिए खतरा पैदा करते हैं, इस तथ्य की पुष्टि अंतर्राष्ट्रीय, क्षेत्रीय और स्थानीय स्तर पर इस संबंध में जारी रिपोर्टों से होती है। इस संदर्भ में, विश्व बैंक की रिपोर्ट बैंकिंग क्षेत्र और वित्तीय सेवा संस्थानों में साइबर सुरक्षा हमलों की एकाग्रता का संकेत देती है, जिसमें 2016 में साइबर सुरक्षा हमलों में 65% की उल्लेखनीय वृद्धि देखी गई, जो पिछले वर्ष की तुलना में 29% की वृद्धि को दर्शाता है। इसके अलावा, वैश्विक बैंक की रिपोर्ट बताती है कि मैलवेयर का उपयोग करके वित्तीय क्षेत्र के खिलाफ चोरी पिछले वर्ष की तुलना में 2015 में प्रति वर्ष 80% बढ़ी है, जबकि इन हमलों में 2015 में रिपोर्ट की गई घटनाओं का 38% हिस्सा था, जो 2014 में 23% था।

वित्तीय संस्थानों के सामने आने वाले साइबर अपराध पर चर्चा करने के लिए ग्रुप आईबी विशेषज्ञों के आकलन के आधार पर, वित्तीय संस्थानों के सामने आने वाले लगभग 99% साइबर अपराध पैसे की चोरी हैं, जिसने 2017 में कई कंपनियों को बर्बाद कर दिया, जैसे कि MDLZ और DLA Piper, पहचान की चोरी के अलावा, और इक्विफैक्स उन पीड़ितों में से एक था जहाँ साइबर अपराधी संवेदनशील व्यक्तिगत जानकारी का उपयोग करते हैं और इसका उपयोग पहचान की चोरी के लिए करते हैं। 2018 में, विश्व आर्थिक मंच ने धोखाधड़ी और वित्तीय अपराधों पर ध्यान दिया, जिनकी राशि इस वर्ष एक ट्रिलियन डॉलर थी, जिसने निजी कंपनियों को 2017 में धन शोधन अपराधों से निपटने पर लगभग 8.2 बिलियन डॉलर खर्च करने के लिए प्रेरित किया।

साइबर सुरक्षा का उल्लंघन इस उद्योग के लिए सबसे गंभीर खतरों

में से एक बन गया है। साइबर अपराध और सुरक्षा सर्वेक्षण रिपोर्ट के अनुसार, मैलवेयर, फ़िशिंग, कंप्यूटर चोरी और बॉट हमले साइबर हमलों के लिए प्रचलित रणनीति हैं। तंजानिया ने कई साइबर अपराध घटनाओं के परिणामस्वरूप $6 मिलियन का नुकसान उठाया है, जिससे देश को CCU और CERT बनाने के लिए मजबूर होना पड़ा है। आभासी दुनिया में गोपनीयता की रक्षा के लिए, नए सुरक्षा उपायों की आवश्यकता है। वांग एट अल., (2020) चार घटकों के माध्यम से साइबरनेटिक रक्षात्मक चक्र को प्राप्त करने के लिए साइबर-हमला प्रबंधन समाधान प्रदान करता है। साइबर हमले और जोखिम चिंता का एक प्रमुख स्रोत बन गए हैं। महत्वपूर्ण खोज यह थी कि चाहे कोई भी मजबूत हमला हो, इराकी निजी बैंक एक निश्चित स्तर की सुरक्षा बनाए रखते हैं।

साहित्य समीक्षा

अकेलो (2023)समकालीन नेटवर्क और डेटा-केंद्रित वातावरण में संगठनात्मक सूचना सुरक्षा एक महत्वपूर्ण मुद्दा है। जैसे-जैसे साइबर हमले अधिक लगातार और परिष्कृत होते जा रहे हैं, फर्मों को अपने संवेदनशील डेटा की गोपनीयता, अखंडता और उपलब्धता के लिए पर्याप्त जोखिम का सामना करना पड़ रहा है। यह दस्तावेज़ कॉर्पोरेट सूचना सुरक्षा से जुड़ी प्रमुख विशेषताओं और मुद्दों का अवलोकन प्रस्तुत करता है। यह बाहरी हमलों से बचाव के लिए फायरवॉल, घुसपैठ का पता लगाने वाली प्रणाली, एन्क्रिप्शन तकनीक और सुरक्षित कोडिंग पद्धतियों सहित कड़े सुरक्षा प्रोटोकॉल स्थापित करने की आवश्यकता को रेखांकित करता है। यह सुरक्षा घटनाओं की कुशलतापूर्वक पहचान करने और उनका समाधान करने के लिए निरंतर निगरानी, खतरे की खुफिया जानकारी के प्रसार और घटना प्रतिक्रिया क्षमताओं की आवश्यकता को रेखांकित करता है। य

अहमद (2024)कंपनी परिवर्तन में बढ़े हुए डिजिटलीकरण ने पर्याप्त लाभ दिए हैं, साथ ही सूचना सुरक्षा के लिए नई समस्याएं भी पेश की हैं। यह अध्ययन डिजिटल परिवर्तन अवधि के दौरान सामने आई साइबर सुरक्षा चिंताओं की जांच करना चाहता है, जो सूचना प्रणालियों पर केंद्रित है। उपयोग की गई शोध तकनीक इन कठिनाइयों की गहन समझ प्राप्त करने के लिए साहित्य और केस स्टडीज की गहन समीक्षा है। यह अध्ययन डिजिटल परिवर्तन के कार्यान्वयन में साइबर सुरक्षा से जुड़े कई महत्वपूर्ण मुद्दों की पहचान करता है, जिसमें मैलवेयर हमले, फ़िशिंग, अपर्याप्त नेटवर्क सुरक्षा और गोपनीयता उल्लंघन शामिल हैं। कारण विश्लेषण से पता चला कि अपर्याप्त प्रशिक्षण और सुरक्षा जागरूकता, सूचना प्रणालियों में खराब डिज़ाइन के साथ, प्राथमिक जोखिम कारक थे।

शुकुर (2023)रोजमर्रा की गतिविधियों में इंटरनेट ऑफ थिंग्स (IoT) के तेजी से विस्तार ने संभावित साइबर सुरक्षा कमजोरियों के बारे में महत्वपूर्ण चिंताएँ पैदा की हैं। नतीजतन, सक्रिय और सक्रिय प्रतिक्रियाओं की वास्तविक आवश्यकता है। यह पत्र विभिन्न IoT उपकरणों से जुड़े वर्तमान साइबर सुरक्षा चिंताओं और खतरों का व्यापक साहित्य मूल्यांकन करता है। इसके अतिरिक्त, यह संरचनात्मक रूपरेखाओं के साथ-साथ प्रस्तावित उपाय भी प्रस्तुत करता है। इसके अलावा, यह विभिन्न तरीकों से संभावित जोखिमों का पता लगाने और उनकी पहचान करने में सहायता करता है। इसके अलावा, यह IoT से संबंधित औद्योगिक और आर्थिक क्षेत्रों में शोध की कमियों को उजागर करके योगदान देता है। हमारे परिणाम संकेत देते हैं कि IoT प्रणालियों में प्राथमिक चिंताएँ साइबर अपराध और गोपनीयता की समस्याएँ हैं।

पेत्रु-क्रिस्टियन (2023)इस अध्ययन का उद्देश्य विकासशील जटिलता को स्पष्ट करना है, समकालीन साइबर युद्धों और उनके कई प्रभावों के बारे में पूरी जानकारी की तत्काल आवश्यकता पर प्रकाश डालना है। यह विश्लेषणात्मक उपकरणों की एक सरणी के साथ ऐसा करने का प्रयास करता है। 2011 से 2020 के दशक में, 50 उल्लेखनीय साइबर घटनाएँ साइबर जोखिम और सुरक्षा के क्षेत्र में महत्वपूर्ण केस स्टडी रही हैं। इन केस स्टडीज़ का विश्लेषण साइबर सुरक्षा के व्यापक प्रभावों और कठिनाइयों को समझने के लिए एक अलग दृष्टिकोण प्रदान करता है। इसके अतिरिक्त, 2011 से 2020 तक के 50 केस स्टडीज़ में से प्रत्येक अलग-अलग कठिनाइयाँ, परिणाम और अंतर्दृष्टि प्रस्तुत करता है। इकबाल (2024)अध्ययन लेख का सारांश दें, साइबर सुरक्षा में नए रुझानों और संभावित मुद्दों को समझने के महत्व पर जोर दें। उद्देश्यों, दृष्टिकोण और प्रमुख परिणामों की जांच करें। उभरते साइबर खतरों से निपटने और डिजिटल बुनियादी ढांचे की सुरक्षा के लिए सक्रिय रणनीतियों की आवश्यकता पर प्रकाश डालें।

साइबर सुरक्षा

बैंकिंग में साइबर सुरक्षा उपायों का अवलोकन

साइबर हमलों के विभिन्न प्रकारों को कई श्रेणियों में वर्गीकृत करके विस्तृत रूप से समझाया गया है। विभिन्न प्रकार के साइबर हमलों में SQL इंजेक्शन, सोशल इंजीनियरिंग, साइबरस्टॉकिंग, डेनियल ऑफ सर्विस अटैक, डिस्ट्रिब्यूटेड डेनियल ऑफ सर्विस अटैक, क्रॉस-साइट स्क्रिप्टिंग, एटीएम क्लोनिंग, पाइरेसी, मैन इन द मिडल अटैक, बर्थडे अटैक, रैनसमवेयर अटैक, बॉटनेट अटैक, ब्रूट फोर्स अटैक शामिल हैं। आईटी एक्ट के अनुसार, 2014 से 2016 तक 29 भारतीय राज्यों में से 10 में साइबर अपराधों में वृद्धि हुई है।

डिजिटल बैंकिंग में प्रमुख साइबर सुरक्षा खतरों को कई कारकों द्वारा सुव्यवस्थित किया जा सकता है, जैसे, अनएन्क्रिप्टेड डेटा, मैलवेयर, थर्ड-पार्टी सेवाएँ, स्पूफिंग, फ़िशिंग, आदि। कोविड के बाद के वर्षों में, दुनिया भर में साइबर खतरे बढ़ गए हैं, जिसमें प्रमुख बैंकिंग सर्वर हैकर्स द्वारा अपहृत किए जा रहे हैं। प्रमाणीकरण, गोपनीयता और डेटा अखंडता सहित कथित सुरक्षा कारक, इंटरनेट बैंकिंग सेवाओं का उपयोग जारी रखने के लिए ग्राहकों की इच्छा को महत्वपूर्ण रूप से प्रभावित करते हैं। यह सूचना सुरक्षा के मुख्य स्तंभों- गोपनीयता, अखंडता और उपलब्धता के महत्व को उजागर करता है - जो साइबर सुरक्षा खतरों से जुड़ी व्यापक चिंताओं के साथ संरेखित है।

पाकिस्तान के बैंकिंग क्षेत्र में साइबर अपराध के मामलों के विश्लेषण से पता चला है कि साइबर अपराध सीधे संगठनात्मक प्रदर्शन को प्रभावित करते हैं, जैसा कि पाकिस्तानी बैंकिंग क्षेत्र के भीतर अनुसंधान द्वारा उजागर किया गया है। अध्ययन प्रदर्शन पर साइबर अपराध की घटनाओं के पर्याप्त नकारात्मक प्रभाव की पहचान करता है, जो साइबर सुरक्षा खतरों से जुड़े हानिकारक परिणामों की व्यापक कथा को पुष्ट करता है।

हालाँकि, सूचना सुरक्षा जागरूकता एक महत्वपूर्ण शमन कारक के रूप में उभरती है, जो संगठनात्मक प्रदर्शन पर साइबर अपराधों के प्रतिकूल प्रभावों को कम करने में महत्वपूर्ण भूमिका निभाती है। अध्ययन में यह भी पाया गया कि साइबर अपराधों का संगठनात्मक प्रदर्शन पर प्रभाव सूचना सुरक्षा जागरूकता के स्तर के आधार पर भिन्न होता है। साइबर सुरक्षा जागरूकता बढ़ाना और वित्तीय संस्थानों के बीच सहयोग बढ़ाना डिजिटल बैंकिंग को अपनाने को बढ़ावा देने के लिए महत्वपूर्ण उपाय हैं, साथ ही

डिजिटल युग में वित्तीय लेनदेन की सुरक्षा और अखंडता सुनिश्चित करना भी महत्वपूर्ण है।

भारतीय बैंकिंग क्षेत्र और साइबर सुरक्षा

भारतीय बैंकिंग क्षेत्र में साइबर हमलों और बचाव रणनीतियों का विस्तृत विश्लेषण प्रस्तुत किया। अध्ययन में बैंकों द्वारा सामना किए जाने वाले विभिन्न साइबर खतरों पर प्रकाश डाला गया है, जिसमें 60% अधिकारियों ने ऑनलाइन पहचान चोरी की घटनाओं की रिपोर्ट की है, और सेवा से वंचित (DoS) हमलों, फ़िशिंग, विशिंग और स्पूफिंग पर महत्वपूर्ण चिंता व्यक्त की है, बाद वाले की पुष्टि 76% उत्तरदाताओं ने की है। अन्य कमजोरियों में दुर्भावनापूर्ण कोड, SQL इंजेक्शन और ब्रूट-फोर्स हमले शामिल हैं, जिसमें पहचान धोखा 80% अधिकारियों द्वारा बताई गई एक प्रमुख रणनीति है।

एन्क्रिप्शन, अद्वितीय लॉगिन, बायोमेट्रिक्स और नियमित एंटीवायरस अपडेट सहित मजबूत सुरक्षा उपायों को अपनाने के बावजूद, डेटा ग्रैन्युलैरिटी, उपयोगकर्ता पहुँच नीतियाँ और लॉगिंग गतिविधियों जैसे क्षेत्रों पर अधिक ध्यान देने की आवश्यकता है। अध्ययन सक्रिय उपायों के महत्व को रेखांकित करता है, जैसे घुसपैठ का पता लगाने वाले उपकरण, लगातार नीति समीक्षा और संदिग्ध गतिविधियों के लिए उपयोगकर्ता अलर्ट। इसके अलावा, हैकिंग, फ़िशिंग और पहचान की चोरी जैसे खतरों को कम करने के लिए साइबर सुरक्षा और सुरक्षित प्रथाओं के बारे में ग्राहकों को शिक्षित करने के लिए सरकारों और निजी संस्थाओं के साथ सहयोग करना आवश्यक है। मुंधे एट अल. (2024) द्वारा किए गए एक अन्य अध्ययन ने यह निष्कर्ष निकाला कि भारतीय बैंकिंग क्षेत्र का डिजिटल परिवर्तन महत्वपूर्ण साइबर सुरक्षा चुनौतियों के साथ-साथ महत्वपूर्ण अवसर भी लाता है। जैसे-जैसे बैंक तेजी से डिजिटल चैनल अपना रहे हैं, डेटा उल्लंघन और सिस्टम कमजोरियों सहित साइबर सुरक्षा जोखिम प्रमुख चिंता का विषय बन गए हैं।

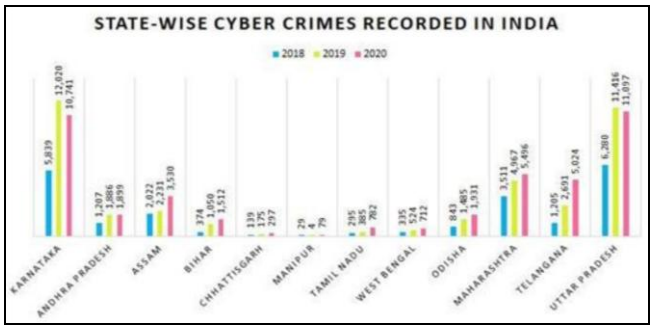
डिजिटल संचालन की सुरक्षा के लिए AI, मशीन लर्निंग और ब्लॉकचेन जैसी उन्नत तकनीकों जैसे साइबर सुरक्षा उपायों में मजबूत निवेश आवश्यक है। विश्वास और परिचालन अखंडता बनाए रखने के लिए विकसित नियामक आवश्यकताओं का अनुपालन भी उतना ही महत्वपूर्ण है। फिनटेक फर्मों और प्रौद्योगिकी प्रदाताओं के साथ सहयोग सुरक्षा ढांचे और उभरते खतरों के लिए अनुकूलनशीलता को और बढ़ा सकता है। इसके अतिरिक्त, डिजिटल उपकरणों को प्रभावी ढंग से लागू करने और प्रबंधित करने के लिए कार्यबल का निरंतर कौशल विकास महत्वपूर्ण है, जिससे एक सुरक्षित और लचीला बैंकिंग पारिस्थितिकी तंत्र सुनिश्चित होता है।

UPI, इंटरनेट बैंकिंग, मोबाइल बैंकिंग, मोबाइल वॉलेट और QR कोड जैसी विभिन्न डिजिटल तकनीकों को अपनाने के साथ भारत में डिजिटल बैंकिंग में उल्लेखनीय प्रगति हुई है। डिजिटल बैंकिंग की प्रगति ने बैंकिंग और वित्तीय क्षेत्र में सुविधा, वैयक्तिकरण, दक्षता, पारदर्शिता और नवाचार को बढ़ाया है। हालाँकि, डिजिटल बैंकिंग सुरक्षा, डेटा गोपनीयता और तेजी से विकसित हो रहे प्रौद्योगिकी रुझानों के साथ तालमेल बनाए रखने के लिए निरंतर अनुकूलन की आवश्यकता से संबंधित चुनौतियाँ भी प्रस्तुत करती है।

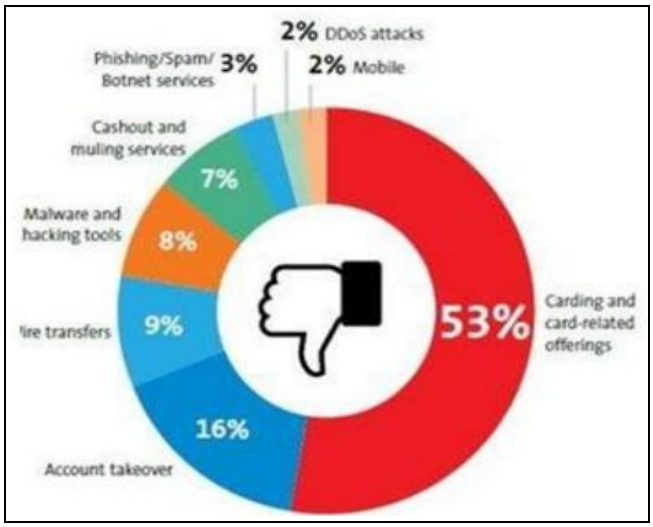
बैंकिंग उद्योग में साइबर अपराध

साइबर अपराध कोई भी अवैध गतिविधि है जो ऑनलाइन या कंप्यूटर के माध्यम से होती है। दूसरे शब्दों में कहें तो डिजिटल कदाचार को साइबर अपराध भी कहा जाता है, जब कोई अपराधी कंप्यूटर या किसी अन्य इलेक्ट्रॉनिक डिवाइस और इंटरनेट का उपयोग करके कई तरह के अपराध करता है, जिसमें अनधिकृत पहुँच के माध्यम से धन हस्तांतरण और निकासी शामिल है।

आज की वैश्वीकृत दुनिया में, बैंकिंग उद्योग अपने ग्राहकों को क्रेडिट कार्ड सेवाओं और इंटरनेट बैंकिंग सहित कई तरह की सेवाएँ प्रदान करता है। "डेबिट कार्ड से ऑनलाइन भुगतान करना" उपभोक्ताओं को सभी बैंक सेवाओं तक चौबीसों घंटे पहुँच मिलती है, और वे अपने फ़ोन और इंटरनेट का उपयोग करके दुनिया के किसी भी स्थान से सुविधाजनक रूप से व्यवसाय कर सकते हैं और अपने खातों का प्रबंधन कर सकते हैं।" हालाँकि ये सेवाएँ उपयोगकर्ताओं के लिए मददगार हैं, जैसा कि हम सभी जानते हैं, इनका एक नकारात्मक पहलू भी है जिसमें डकैती और हैकर शामिल हैं।



बैंकिंग क्षेत्र से जुड़े साइबर अपराध के प्रकार



हैकिंग

हैकिंग एक प्रकार का साइबर अपराध है, जिसमें कोई व्यक्ति बैंकिंग वेबसाइट या ग्राहक खातों में सेंध लगाकर सुरक्षा उपायों को भंग करने का प्रयास करता है, या सिस्टम तक अनधिकृत पहुंच प्राप्त कर लेता है।

वायरस

यह एक प्रकार का स्व-प्रतिकृति सॉफ़्टवेयर है जो संक्रमित करने के लिए दस्तावेज़ों या निष्पादन योग्य कोड में अपनी प्रतियाँ सम्मिलित करता है। एक निष्पादन योग्य फ़ाइल जिसे किसी

प्रोग्राम द्वारा संक्रमित किया गया है जो इसे अजीब तरह से व्यवहार करता है उसे वायरस कहा जाता है। यह ऑपरेटिंग सिस्टम और प्रोग्राम फ़ाइलों सहित निष्पादन योग्य फ़ाइलों से खुद को जोड़कर फैलता है। निष्पादन योग्य फ़ाइल लोड करने की प्रक्रिया वायरस को खुद को दोहराने का कारण बन सकती है। दूसरी ओर, वर्म्स ऐसे प्रोग्राम होते हैं जो पीड़ित के कंप्यूटर से खुद को कॉपी करने और अन्य कंप्यूटरों को प्रतियां भेजने की क्षमता रखते हैं। वर्म्स बिना किसी फ़ाइल को बदले या हटाए उपयोगकर्ता के कंप्यूटर से खुद की प्रतियों को दूसरे कंप्यूटरों में कॉपी और ट्रांसफर करते हैं।

स्पाइवेयर

ऑनलाइन बैंकिंग क्रेडेंशियल्स लेने और उन्हें धोखाधड़ी से इस्तेमाल करने का सबसे लोकप्रिय तरीका स्पाइवेयर है। स्पाइवेयर द्वारा कंप्यूटर और वेबसाइटों के बीच जानकारी एकत्र की जाती है या भेजी जाती है। अधिकतर, इसे झूठे "पॉप अप" विज्ञापनों द्वारा इंस्टॉल किया जाता है जो सॉफ़्टवेयर डाउनलोड करने का अनुरोध करते हैं। इस तरह के सॉफ़्टवेयर को उद्योग-मानक एंटीवायरस प्रोग्राम द्वारा खोजा और समाप्त किया जाता है, ज्यादातर कंप्यूटर को संक्रमित करने से पहले प्रोग्राम के डाउनलोड और इंस्टॉलेशन को रोककर।

फ़िशिंग

फ़िशिंग एक प्रकार का घोटाला है जिसमें प्रतिष्ठित स्रोतों से आने वाले ईमेल का उपयोग ग्राहक आईडी, आईपिन, सीवीवी नंबर, डेबिट/क्रेडिट कार्ड नंबर और समाप्ति तिथि जैसी व्यक्तिगत जानकारी चुराने के लिए किया जाता है। ईमेल स्पूफिंग और इंस्टेंट मैसेजिंग फ़िशिंग में इस्तेमाल की जाने वाली दो विधियाँ हैं।

इस तरह की धोखाधड़ी में, जालसाज बैंक कर्मचारियों के रूप में खुद को पेश करते हैं और एक सीधा लिंक बनाते हैं जो इच्छित शिकार के ब्राउज़र को एक नकली वेबपेज पर ले जाता है जो वास्तविक बैंक वेबसाइट की नकल करता है। ग्राहक के खाते पर, प्राप्त गोपनीय जानकारी का उपयोग करके बाद में धोखाधड़ी वाले लेनदेन किए जाते हैं। इन दिनों, फ़िशर्स अपने अपराधों को अंजाम देने के लिए मोबाइल (वॉयस फ़िशिंग) और एसएमएस (स्मैशिंग) तकनीकों का भी उपयोग करते हैं।

फ़ार्मिंग

इंटरनेट का इस्तेमाल औषधीय कार्यों के लिए किया जाता है। हैकर्स यूआरएल में हेरफेर करते हैं ताकि जब कोई उपभोक्ता बैंक की वेबसाइट पर जाए, तो उसे एक नकली वेबसाइट पर ले जाया जाए जो बैंक की मूल वेबसाइट की नकल करती है।

ATMSKIMMIN गैंड बिक्री अपराध बिंदु

मशीन कीपैड के ऊपर स्कीमिंग डिवाइस लगाना ताकि यह असली कीपैड जैसा लगे या कार्ड रीडर से जुड़ा कोई उपकरण लगाना ताकि यह मशीन का ही एक घटक लगे, एटीएम या पॉइंट-ऑफ-सेल (POS) सिस्टम में घुसने का एक तरीका है। इन डिवाइस पर सीधे क्रेडिट कार्ड की जानकारी चुराने वाले मैलवेयर भी इंस्टॉल किए जा सकते हैं। कार्ड नंबर और व्यक्तिगत पहचान संख्या (पिन) उन एटीएम से प्राप्त किए जा सकते हैं जिनमें स्किमर सफलतापूर्वक इंस्टॉल किए गए हैं। फिर इन विवरणों की नकल की जाती है और धोखाधड़ी वाले लेनदेन में उनका उपयोग किया जाता है।

DNS कैशपॉइज़निंग

किसी संगठन के नेटवर्क में, DNS सर्वर का उपयोग कैश में पहले से प्राप्त क्वेरी परिणामों को संग्रहीत करके समाधान प्रतिक्रिया समय को तेज़ करने के लिए किया जाता है। DNS सॉफ़्टवेयर में भेद्यता का लाभ उठाकर, DNS सर्वर के विरुद्ध ज़हर भरे हमले किए जाते हैं। सर्वर उन सभी उपयोगकर्ताओं को गलत प्रविष्टियाँ प्रदान करेगा जो इसके स्थानीय कैश से समान अनुरोध करते हैं। बैंक क्लाइंट को आपराधिक-नियंत्रित सर्वर पर पुनर्निर्देशित किया जा सकता है, जहाँ मैलवेयर परोसा जा सकता है या उन्हें धोखाधड़ी वाली वेबसाइट के लिए अपनी लॉगिन जानकारी दर्ज करने के लिए धोखा दिया जा सकता है। IP स्पूफ़िंग एक ऐसी तकनीक है जिसका उपयोग क्लाइंट पर नियंत्रण पाने के लिए किया जाता है। इसमें बैंक की वेबसाइट के DNS रिकॉर्ड को एक DNS सर्वर से दूसरे DNS सर्वर में बदलना शामिल है, जिसमें उनके स्वामित्व वाले सर्वर का IP पता इस्तेमाल किया जाता है।

बैंकों पर साइबर अपराध का प्रभाव

दैनिक जीवन में मोबाइल नेटवर्क के प्रसार और सूचना एवं प्रौद्योगिकी (आईटी) की उन्नति ने वित्तीय सेवाओं को व्यापक दर्शकों के लिए अधिक सुलभ बना दिया है। लेकिन जहाँ तकनीकी प्रगति ने बैंकिंग सेवाओं को अधिक सुलभ और किफ़ायती बना दिया है, वहीं इसने साइबर हमलों का लक्ष्य बनने के जोखिम को भी बढ़ा दिया है।

साइबर अपराधियों द्वारा पैसे चुराने, कंपनियों की जासूसी करने और निजी कंपनी की जानकारी तक पहुँचने के लिए इस्तेमाल किए जाने वाले सरल तरीकों का बैंक के वित्त पर अप्रत्यक्ष प्रभाव पड़ता है। इन साइबर अपराधों का मुकाबला करने के लिए, बैंकिंग उद्योग को नियंत्रण प्रतिमान बनाने के लिए सरकारी अधिकारियों और निगरानी समूहों के साथ मिलकर काम करना चाहिए।

इस मामले में मुख्य रुचि का विषय बैंकिंग क्षेत्र में एक प्रभावी संकलन सेवा का अभाव है, जो साइबर अपराध के पैटर्न की पहचान करने तथा उनके आधार पर एक मॉडल तैयार करने में सक्षम हो।

भारतीय बैंकिंग प्रणाली

बैंकिंग का अर्थ

बैंकिंग दूसरों के लिए पैसे की सुरक्षा का व्यवसाय है। बैंक इस पैसे को उधार देते हैं, जिससे ब्याज मिलता है जो बैंक और उसके ग्राहकों के लिए मुनाफ़ा पैदा करता है।

बैंक एक वित्तीय संस्था है जिसे जमा स्वीकार करने और ऋण देने का लाइसेंस दिया गया है। लेकिन वे अन्य वित्तीय सेवाएँ भी प्रदान कर सकते हैं।

वित्तीय लेनदेन का अर्थ

वित्तीय लेनदेन एक समझौता या संचार है, जो खरीदार और विक्रेता के बीच भुगतान के लिए वस्तुओं, सेवाओं या परिसंपत्तियों का आदान-प्रदान करने के लिए होता है। किसी भी लेनदेन में दो या अधिक व्यवसायों या व्यक्तियों के वित्त की स्थिति में बदलाव शामिल होता है। एक वित्तीय लेनदेन में हमेशा एक या अधिक वित्तीय परिसंपत्तियाँ शामिल होती हैं, सबसे आम तौर पर पैसा या कोई अन्य मूल्यवान वस्तु जैसे सोना या चाँदी।

वित्तीय लेन-देन के कई प्रकार हैं। सबसे आम प्रकार, खरीद, तब होती है जब कोई वस्तु, सेवा या अन्य वस्तु पैसे के बदले उपभोक्ता

को बेची जाती है। ज़्यादातर खरीद नकद भुगतान के साथ की जाती है, जिसमें भौतिक मुद्रा, डेबिट कार्ड या चेक शामिल हैं। भुगतान का दूसरा मुख्य रूप क्रेडिट है, जो बाद की तारीख में पुनर्भुगतान के बदले में धन तक तत्काल पहुँच प्रदान करता है।

भारत में बैंकों का वर्गीकरण

भारत में बैंकिंग प्रणाली का हिस्सा बनने वाले बैंकों को दो श्रेणियों में विभाजित किया जा सकता है - अनुसूचित बैंक और गैर-अनुसूचित बैंक।

अनुसूचित बैंक

भारत में बैंकिंग प्रणाली के अंतर्गत अनुसूचित बैंकों से तात्पर्य उन वित्तीय संस्थाओं से है जो भारतीय रिज़र्व बैंक अधिनियम, 1934 की दूसरी अनुसूची में सूचीबद्ध हैं। इस समावेशन का अर्थ है कि वे आरबीआई द्वारा निर्धारित विशिष्ट मानदंडों को पूरा करते हैं और इसके सख्त नियमों के अधीन हैं।

गैर-अनुसूचित बैंक

भारत में बैंकिंग प्रणाली के अंतर्गत गैर-अनुसूचित बैंक उन वित्तीय संस्थाओं को कहा जाता है, जो भारतीय रिज़र्व बैंक अधिनियम, 1934 की दूसरी अनुसूची में शामिल किए जाने के मानदंडों को पूरा नहीं करते हैं। अनुसूची से बाहर रखे जाने का अर्थ है कि वे अनुसूचित बैंकों की तुलना में अलग नियमों के तहत काम करते हैं।

निष्कर्ष

साइबर सुरक्षा को अलग-अलग तरीकों से तैयार किया जा सकता है, जिसका लोगों पर अलग-अलग प्रभाव पड़ता है। साइबर सुरक्षा एक जटिल और बहुआयामी क्षेत्र है जिसका कोई स्पष्ट नायक या अपराधी नहीं है। साइबर सुरक्षा को तैयार करने में असमर्थता ने उचित कार्रवाई करना और पर्याप्त नीतियाँ विकसित करना असंभव बना दिया है। किसी कंपनी की सुरक्षा के लिए प्रत्येक कर्मचारी के समर्थन की आवश्यकता होगी। अधिकतम प्रभावशीलता के लिए अनुकूलित चल रहे सुरक्षा जागरूकता कार्यक्रम के साथ, एक संगठन सभी कर्मियों द्वारा समर्थित साइबर सुरक्षा संस्कृति बना सकता है। जबकि कई उपयोगकर्ता ऑनलाइन वित्तीय और गैर-वित्तीय लेनदेन का उपयोग करते हैं, वे साइबर सुरक्षा नियमों से अनजान हैं।

संदर्भ

1. सेले एनएन, क्वेंडा एस. क्या साइबर सुरक्षा के खतरे और जोखिम डिजिटल बैंकिंग को अपनाने पर प्रभाव डालते हैं? एक व्यवस्थित साहित्य समीक्षा. जर्नल ऑफ फाइनेंशियल क्राइम. 2024.
2. बामारा ए, सिंह जी, भट्ट एम. भारत में साइबर हमले और बचाव रणनीतियाँ: बैंकिंग क्षेत्र का एक अनुभवजन्य मूल्यांकन. एसएसआरएन इलेक्ट्रॉनिक जर्नल. 2013.
3. मुंधे ई. भारतीय बैंकिंग क्षेत्र में डिजिटल परिवर्तन: अवसर और चुनौतियाँ. विभिन्न विषयों में ज्ञान का विकास-समकालीन रुझान और अग्रगामी नवाचार. 2024:103.
4. प्रभाकर एस. भारत में डिजिटल बैंकिंग के रुझान, अवसर और चुनौतियाँ: एक समीक्षा.
5. अल-दोसारी के, फ़ैतैस एन, कुकुकवर एम. बैंकिंग उद्योग के लिए आर्टिफिशियल इंटेलिजेंस और साइबर डिफेंस सिस्टम: एआई अनुप्रयोगों और चुनौतियों का एक गुणात्मक अध्ययन. साइबरनेटिक्स एंड सिस्टम्स. 2022;55(2):302–330.
6. फराजी एमआर, शिकदर एफ, हसन एमएच, इस्लाम एमएम, अक्तर यूके. साइबर सुरक्षा में कृत्रिम बुद्धिमत्ता की भूमिका की जांच: वित्तीय लेनदेन में संभावित समाधानों को रोकने के लिए एक व्यवस्थित समीक्षा. इंटरनेशनल जर्नल. 2024;5(10):4766–4782.
7. आचार्य एस, जोशी एस. भारत में बैंकिंग संस्थानों पर साइबर हमलों का प्रभाव: सुरक्षा तंत्र और निवारक उपायों का एक अध्ययन. पलार्च जर्नल ऑफ आर्कियोलॉजी ऑफ इजिप्ट/इजिप्टोलॉजी. 2020;17(6). आईएसएसएन 1567-214.
8. बुख्त टीएफएन, रज़ा एमए, अवान जेएच, अहमद आर. पाकिस्तान के बैंकों और उनके समाधानों पर लक्षित साइबर हमलों का विश्लेषण. इंटरनेशनल जर्नल ऑफ कंप्यूटर साइंस एंड नेटवर्क सिक्योरिटी. 2020;20(2).
9. जोवेदा एन, खान एमटी, पाठक ए. साइबर लॉन्ड्रिंग: बांग्लादेश में बैंकिंग उद्योगों के लिए खतरा-प्रभावी कानूनी ढांचे और वित्तीय जानकारी की साइबर सुरक्षा की तलाश में. इंटरनेशनल जर्नल ऑफ इकोनॉमिक्स एंड फाइनेंस. 2019;11(10).
10. बाउवेरेट ए. वित्तीय क्षेत्र के लिए साइबर जोखिम: मात्रात्मक मूल्यांकन के लिए एक रूपरेखा. अंतर्राष्ट्रीय मुद्रा कोष वर्किंग पेपर, रणनीति, नीति और समीक्षा विभाग. 2019 मई 27.
11. साइबर सुरक्षा: खतरे, कारण, चुनौतियाँ, कार्यप्रणाली और औद्योगिक अनुप्रयोगों के लिए अत्याधुनिक समाधान. स्कूल ऑफ इलेक्ट्रिकल इंजीनियरिंग एंड कंप्यूटर साइंस, नेशनल यूनिवर्सिटी ऑफ साइंसेज एंड टेक्नोलॉजी. 2019.
12. चिगाडा जे, मैडज़िंगा आर. कोविड-19 के दौरान साइबर हमले और खतरे: एक व्यवस्थित साहित्य समीक्षा. साउथ अफ्रीकन जर्नल ऑफ इंफॉर्मेशन मैनेजमेंट.
13. क्रिसैंटो जेसी, प्रेनियो जे. बैंकों के साइबर-सुरक्षा ढांचे को बढ़ाने के लिए नियामक दृष्टिकोण. फाइनेंशियल स्टेबिलिटी इंस्टीट्यूट. 2017 अगस्त. आईएसबीएन: 978-92-9259-080-2.
14. अंतर्राष्ट्रीय मुद्रा कोष. एक ऐसा संकट जैसा कोई और नहीं, एक अनिश्चित रिकवरी. वर्ल्ड इकोनॉमिक आउटलुक अपडेट. 2020 जून.
15. चेक प्वाइंट सॉफ्टवेयर टेक्नोलॉजीज लिमिटेड. चेक प्वाइंट रिसर्च: क्षेत्रवार साइबर हमले की श्रेणियाँ एच1 2020. 2020.