अक्टूबर, 2024

केंद्रीय रिज़र्व पुलिस बल

साइबर बाइट

विशेष संस्करण

सरकार द्वारा दर्जनों अवैध सट्टेबाजी ऐप पर प्रतिबंध लगाया

एक नया घोटाला, जिसे "डिजिटल अरेस्ट" के नाम से जाना जाता है

हैकर्स उपकरणों को मैलवेयर से संक्रमित करने के लिए **AI-** जनरेटेड कोड का उपयोग करते हैं

1.साइबर गीक्स समाचार

क) सरकार ने दर्जनों अवैध सट्टेबाजी ऐप पर प्रतिबंध लगाया:-

सरकार ने प्रवर्तन निदेशालय (ईडी) की जांच के बाद दो दर्जन से अधिक वेबसाइटों पर प्रतिबंध लगा दिया है, जो कथित तौर पर अवैध विदेशी सट्टेबाजी एप्लीकेशनों से धन शोधन कर रही थीं, जो ई-कॉमर्स और विदेशी मुद्रा व्यापार पोर्टल के रूप में कार्यरत थीं।

इनमें ऑक्टाएफएक्स, फेयरप्ले, मैजिकविन, महादेव ऑनलाइन बुक और 30 अन्य शामिल हैं, जिनका संचालन स्पेन, दुबई, रूस और पाकिस्तान में स्थित प्रमोटरों द्वारा किया जाता है। इस अपराध से होने वाली आय ₹10,000 करोड़ आंकी गई है।

ईडी की जांच में पाया गया कि फर्जी ई-कॉमर्स वेबसाइट के नाम पर कई कंपनियां बनाई गईं और इन फर्जी शेल कंपनियों के नाम पर चालू खाते खोले गए। इस अपराध की आय को ठिकाने लगाने के उद्देश्य से फॉरेक्स ट्रेडिंग वेबसाइट भी शुरू कीगईं।

सुझाव:-

- किसी भी सट्टेबाजी सॉफ्टवेयर को डाउनलोड करने से पहले, गहन शोध के माध्यम से इसकी विश्वसनीयता और भरोसेमंदता को सुनिश्चित करना महत्वपूर्ण है।

- यह सत्यापित करना आवश्यक है कि जिस सट्टेबाजी एप्लिकेशन पर आप विचार कर रहे हैं वह आपके अधिकार क्षेत्र में एक प्रतिष्ठित शासी निकाय द्वारा अधिकृत और विनियमित ऐप्प है।

- जब भी आपको सट्टेबाजी ऐप्स का प्रचार करने वाले या यह दावा करने वाले कि आपने पुरस्कार जीता है, अनचाहे टेक्स्ट, ईमेल या सोशल मीडिया संदेश प्राप्त हों तो सावधानी बरतें।

- किसी सट्टेबाजी ऐप को खरीदने से पहले, प्लेटफॉर्म द्वारा प्रदान किए गए नियमों और शर्तों की अच्छी तरह से समीक्षा करना आवश्यक है।

ख)"डिजिटल गिरफ्तारी"

डिजिटल (घर में) गिरफ्तारी, व्यक्तियों की आभासी नियंत्रण है, यह एक ऐसी युक्ति है जिसका उपयोग साइबर अपराधी पीड़ितों को उनके घरों में फंसाने और उन्हें ठगने के लिए करते हैं। घोटालेबाज कानून प्रवर्तन अधिकारियों का रूप धारण करने के लिए AI-जनरेटेड वॉयस या वीडियो कॉल का उपयोग करते हैं, पीड़ितों पर गलत काम करने का झूठा आरोप लगाकर डर पैदा करते हैं, जो आम तौर पर उनके आधार या फोन नंबर से संबंधित होता है। वे मामले को बंद करने के बदले में पैसे की मांग करते हैं, अक्सर पीड़ित को धमकी देते हैं कि अगर वे ऐसा नहीं करते हैं तो उन्हें गिरफ्तार कर लिया जाएगा। पीड़ितों को तब तक वीडियो कॉल पर रहना पड़ता है जब तक वे उनकी मांगें पूरी नहीं कर देते।

कुछ मामलों में, अपराधी दावा करते हैं कि पीड़ित ने ड्रग्स या नकली पासपोर्ट जैसे अवैध पार्सल प्राप्त किए हैं या भेजे हैं। वे पीड़ित के रिश्तेदारों या दोस्तों को इसमें फंसाने की धमकी भी दे सकते हैं।

केस स्टडी 1 - नोएडा में रहने वाली एक डॉक्टर ने डिजिटल अरेस्ट स्कैम में 60 लाख रुपये गंवा दिए। डॉक्टर को ट्राई के अधिकारी बनकर जालसाजों ने फोन किया और कहा कि उनके फोन नंबर का इस्तेमाल अवैध अश्लील वीडियो प्रसारित करने के लिए किया जा रहा है। जब तक वह उनकी मांगें पूरी नहीं कर सकीं, तब तक उन्हें धमकाया जाता रहा। इससे पहले, जालसाजों ने पुलिस कर्मियों के रूप में खुद को पेश किया और दक्षिण दिल्ली के सी.आर. पार्क में रहने वाली एक 72 वर्षीय महिला से 83 लाख रुपये की ठगी की।

केस स्टडी 2 -

सीबीआई अधिकारी बनकर ठगी करने वालों के एक समूह ने लखनऊ के एक लेखक-कवि को निशाना बनाया और उनको छह घंटे तक डिजिटल रूप से हिरासत में रखा। पीड़ित को 7 जुलाई को एक व्यक्ति का वीडियो कॉल आया जिसने खुद को सीबीआई इंस्पेक्टर रोहन शर्मा बताया। ठग ने पीड़ित से कहा कि वह मनी लॉन्ड्रिंग के मामले में जांच के दायरे में हैं और उनको गिरफ्तार करने की धमकी दी। ठगी करने वाले के पहनावे से पीड़ित को यकीन हो गया कि वह असली पुलिस अधिकारी है। छह घंटे तक उसे डिजिटल रूप से हिरासत में रखने के दौरान ठगी करने वालों ने पीड़ित से मशहूर शायर मिर्जा गालिब और फैज अहमद फैज के दोहे सुनाने को कहा। ठगी करने वाले ने उसे 24 घंटे के भीतर रिहा करने का वादा किया और कहा कि वह उनकी मांगें मानकर जेल जाने से बच सकता है।

डिजिटल धोखाधड़ी का शिकार होने से कैसे बचें?

- अज्ञात नंबरों या कानून प्रवर्तन या सरकारी अधिकारी होने का दावा करने वाले व्यक्तियों से आने वाली अप्रत्याशित कॉल या संदेशों से सावधान रहें।
- कभी भी व्यक्तिगत जानकारी या भुगतान विवरण अप्रमाणित लोगों के साथ साझा न करें।
- कभी भी घबराएं नहीं या आवेगपूर्ण तरीके से कार्य न करें, भले ही आपको गिरफ्तारी या कानूनी कार्रवाई की धमकी दी जाए।
- संदिग्ध कॉल या संदेश की सूचना तुरंत अधिकारियों को दें।
- इन घटनाओं की रिपोर्ट साइबर क्राइम पोर्टल (https://www.cybercrime.gov.in) पर करें या हेल्पलाइन नंबर - 1930 डायल करें।

ग) हैकर्स डिवाइस को मैलवेयर से संक्रमित करने के लिए AI-जनरेटेड कोड का उपयोग करते हैं

आज के जनरेटिव आर्टिफिशियल इंटलीजेंस मॉडल के लिए सबसे मजबूत उपयोग संबंधी मामलों में से एक उनका प्रयोग कुछ ही मिनटों में कोड की सैकड़ों लाइनें लिखने के लिए करना है। हालांकि, मंगलवार, 24 सितंबर को प्रकाशित नए शोध के अनुसार, हैकर्स कथित तौर पर दुर्भावनापूर्ण कोड

बनाने के लिए इन उपकरणों का दुरुपयोग कर रहे हैं। HP के सुरक्षा शोधकर्ताओं ने पाया कि हैकर्स ने फ्रेंच बोलने वालों को लक्षित करके एक दुर्भावनापूर्ण अभियान शुरू किया। अभियान के हिस्से के रूप में, कुख्यात हैकर्स पीड़ितों के उपकरणों को **AsyncRAT नामक मैलवेयर से संक्रमित करके** उनके स्क्रीन और कीस्ट्रोक्स तक पहुँचकर और उन्हें रिकॉर्ड करने की कोशिश करते हैं ।

रिपोर्ट के अनुसार, इस मैलवेयर में ऐसा कोड था जो जनरेटिव एआई टूल्स की मदद से वीबीस्क्रिप्ट और जावास्क्रिप्ट प्रोग्रामिंग भाषाओं में लिखा गया था ।

एचपी की जोखिम सुरक्षा टीम की रिपोर्ट महत्वपूर्ण है, क्योंकि यह दर्शाती है कि हैकर्स फिशिंग हमलों के माध्यम से पीड़ितों को लुभाने के लिए जनरेटिव एआई का उपयोग करने से आगे बढ़ रहे हैं।

एआई-आधारित साइबर हमलों से बचाव

हालाँकि एआई-आधारित साइबर हमले एक बड़ा खतरा उत्पन्न करते हैं, लेकिन उनसे बचाव के लिए कुछ कदम उठाए जा सकते हैं। इस संबंध में नीचे कुछ प्रमुख रणनीतियाँ दी गई हैं:-

स्तरीकृत सुरक्षा दृष्टिकोण अपनाएं :

इसमें आपके नेटवर्क के विभिन्न बिंदुओं पर कई सुरक्षा समाधान उपलब्ध करना शामिल है ताकि आप खुद को विभिन्न प्रकार के खतरों से बचा सकें। इसमें **मल्टी-फैक्टर प्रमाणीकरण सक्षम करना, स्थिरता और पारगमन में डेटा पर एन्क्रिप्शन और फ़ायरवॉल लागू करना आदि** शामिल हैं।

सशक्त प्रमाणीकरण और प्राधिकरण नियंत्रण लागू करें:

इससे आपके सिस्टम और डेटा तक अनधिकृत पहुंच को रोकने में मदद मिलेगी।

अपने कर्मचारियों को शिक्षित करें:

जागरूकता प्रशिक्षण से कर्मचारियों को फ़िशिंग हमलों और अन्य सोशल इंजीनियरिंग तकनीकों की पहचान करने और उनसे बचने में मदद मिल सकती है।

नवीनतम खतरों के बारे में अद्यतन जानकारी रखें:

अपने सॉफ्टवेयर और सिस्टम को नवीनतम पैच और सुरक्षा अपडेट के साथ अद्यतन रखना सुनिश्चित करें।

एक व्यापक घटना प्रतिक्रिया योजना को विकसित करें:

इससे आपको साइबर हमलों का त्वरित और प्रभावी ढंग से जवाब देने में मदद मिलेगी।

2.साइबर धोखाधड़ी

क) नवी मुंबई के साइबर घोटाले:-

फर्जी पुलिस व्यवस्था, भावनात्मक हेरफेर, पीड़ितों को ठगने के लिए ठग भय का फायदा उठाते हैं।

जबरन वसूली की रणनीति अधिक परिष्कृत हो गई है, साइबर अपराधी फर्जी आरोपों के लिए "डिजिटल गिरफ्तारी" की धमकी देने के लिए कानून प्रवर्तन अधिकारियों का रूप धारण करते हैं, साइबर विशेषज्ञ और ब्यूरो आईडी के विकास प्रमुख - एक ट्रस्ट नेटवर्क जो नए युग के व्यवसायों के लिए शुरू-से-अंत तक पहचान सत्यापन, अनुपालन और धोखाधड़ी की रोकथाम की सुविधा प्रदान करता है।

गृह मंत्रालय और भारतीय साइबर अपराध समन्वय केंद्र (I4C) ने इस तरह के घोटालों में वृद्धि की ओर संकेत किया है। एक मामले में, एक साइबर गिरोह ने नवी मुंबई के घनसोली निवासी से यह दावा करते हुए कि उसका नाम आतंकवादियों से जुड़ा हुआ है, 26.52 लाख रुपये की उगाही की। गिरोह ने उसे देशद्रोह के आरोप में गिरफ्तार करने की धमकी दी। साइबर अपराधियों ने पूरे देश में कहर बरपाया है, नवी मुंबई में प्रतिदिन 2 करोड़ रुपये से अधिक की साइबर धोखाधड़ी की रिपोर्ट आ रही है। स्थानीय अधिकारियों के अनुसार, पिछले साल 200 से अधिक मामले दर्ज किए गए हैं, जिसमें 200 करोड़ रुपये से अधिक का नुकसान हुआ है।

घनसोली के पीड़ित, एक डॉक्टर, से गिरोह ने 26 अगस्त को पुलिस अधिकारी बनकर संपर्क किया। उन्होंने एक वीडियो कॉल किया, जिसमें एक नकली पुलिस सेटअप दिखाया गया और उसे विश्वास दिलाया कि मामला राष्ट्रीय सुरक्षा का मुद्दा है। गिरोह ने आरोप लगाया कि पीड़ित का अकाउंट आतंकवादी याकूब मेमन और ड्रग तस्करी से जुड़ा हुआ है।
दबाव में आकर पीड़ित ने विभिन्न खातों में 26.52 लाख रुपये ट्रांसफर कर दिए, लेकिन बाद में उसे पता चला कि यह एक धोखाधड़ी है और उसने नेरुल साइबर पुलिस में शिकायत दर्ज कराई। मामले की जांच की जा रही है।

भावनात्मक हैकिंग से सुरक्षा

घोटालेबाज मानवीय भावनाओं का फायदा उठाकर सुरक्षा को दरकिनार कर देते हैं। जबकि टू-फैक्टर प्रमाणीकरण और फ़ोन सत्यापन सुरक्षा में मदद करते हैं, वे वीडियो-आधारित जबरन वसूली जैसे सोशल इंजीनियरिंग घोटालों के खिलाफ कम प्रभावी हैं। जॉइस सटीक पहचान की जांच, डायनेमिक लेनदेन सीमा और वास्तविक समय(रियल टाइम) धोखाधड़ी अलर्ट सहित मजबूत लेनदेन-स्तर की सुरक्षा का सुझाव देते हैं। वित्तीय संस्थानों को धोखाधड़ी का पता लगाने वाली प्रणालियों को बढ़ाना चाहिए और ऐसे घोटालों को बेहतर ढंग से रोकने के लिए संवेदनशील कार्यों के लिए जोखिम-आधारित पहचान सत्यापन को लागू करना चाहिए।

ख) 1.15 करोड़ रुपये की ठगी करने के आरोप में कोयंबटूर से तीन लोग गिरफ्तार

तमिलनाडु पुलिस की साइबर अपराध शाखा ने गुरुवार (26 सितंबर, 2024) को कोयंबटूर से तीन लोगों को गिरफ्तार किया, जिन पर साइबर धोखाधड़ी मामले में मुख्य आरोपी होने का संदेह है, जिसमें चेन्नई में एक व्यक्ति से कथित तौर पर ₹1.15 करोड़ की ठगी की गई थी।
चेन्नई निवासी को 24 अगस्त को एक अज्ञात व्यक्ति ने व्हाट्सएप पर कॉल किया, जिसमें दावा किया गया कि उसके पास मुंबई उच्च न्यायालय से एक सम्मन है। कॉल करने वाले ने पीड़ित को आगे की जानकारी के लिए '0' दबाने को कहा। ऐसा करने पर, एक अन्य जालसाज ने कॉल उठाया, जिसने आरोप लगाया कि शिकायतकर्ता मुंबई ईस्ट, अंधेरी शाखा में उसके नाम पर एक आईसीआईसीआई बैंक खाते के माध्यम से अवैध मनी लॉन्ड्रिंग गतिविधियों में शामिल था, और उसे मुंबई साइबर अपराध विभाग से बात करनी होगी।

शिकायतकर्ता ने अपनी सुरक्षा के डर से अपने दो बैंक खातों से पांच लेन-देन में आरटीजीएस के माध्यम से कुल 1.15 करोड़ रुपये स्थानांतरित कर दिए।

तमिलनाडु पुलिस की साइबर क्राइम विंग में उनकी शिकायत के बाद मामला दर्ज किया गया। साइबर क्राइम विंग के अतिरिक्त पुलिस महानिदेशक संदीप मित्तल ने कहा, "हमारी जांच से पता चला है कि शिकायतकर्ता की खोई हुई रकम विन पावर एनर्जी सॉल्यूशंस प्राइवेट लिमिटेड के लाभार्थी बैंक खाते (भारतीय स्टेट बैंक का खाता) में ट्रांसफर की गई थी। अपराध में शामिल आरोपियों को पकड़ने और खोई हुई रकम वापस पाने के लिए एक विशेष टीम बनाई गई थी। विशेष टीम ने आरोपियों को गिरफ्तार करके त्वरित कार्रवाई की है।"

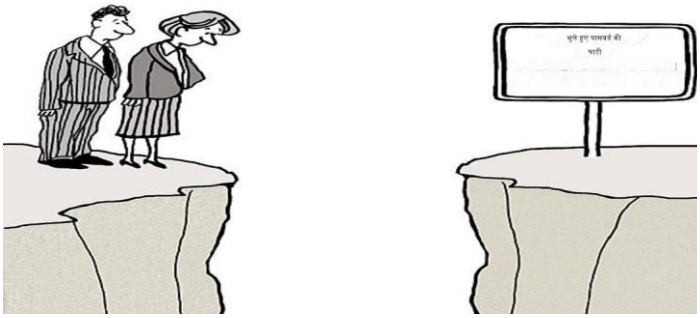
तीनों आरोपियों को न्यायिक हिरासत में भेज दिया गया तथा अपराध में शामिल अन्य लोगों की गिरफ्तारी के लिए आगे की जांच जारी है।

3. इस माह की टिप

क)सुरक्षित ऑनलाइन लेनदेन के लिए सुझाव

- **पासवर्ड नियमित रूप से बदलें**

पहली बार अपने इंटरनेट बैंकिंग खाते में लॉग इन करते समय आपको बैंक द्वारा दिया गया पासवर्ड इस्तेमाल करना होगा। हालाँकि, अपने खाते को सुरक्षित रखने के लिए आपको यह पासवर्ड बदलना होगा।



इसके अलावा, नियमित अंतराल पर अपना पासवर्ड बदलते रहें। सबसे महत्वपूर्ण बात यह है कि पासवर्ड को हमेशा गोपनीय रखें।

- **लॉग इन करने के लिए सार्वजनिक कंप्यूटर का उपयोग न करें**

साइबर कैफे या लाइब्रेरी में आम कंप्यूटर पर अपने बैंक खाते में लॉग इन करने से बचें। ये भीड़-भाड़ वाली जगहें हैं, और आपके पासवर्ड का पता लगने या दूसरों द्वारा देखे जाने की संभावना अधिक होती है। अगर आपको ऐसी जगहों से लॉग इन करना है, तो सुनिश्चित करें कि आपने कैश और ब्राउज़िंग हिस्ट्री साफ़ कर दी है, और कंप्यूटर से सभी अस्थायी फ़ाइलें हटा दी हैं। साथ ही, ब्राउज़र को कभी भी अपना आईडी और पासवर्ड याद रखने की अनुमति न दें।

- **अपना विवरण किसी के साथ साझा न करें**

आपका बैंक कभी भी फ़ोन या ईमेल के ज़रिए आपकी गोपनीय जानकारी नहीं मांगेगा। इसलिए, चाहे आपको बैंक से कोई फ़ोन कॉल आए या कोई ईमेल जिसमें आपकी जानकारी मांगी गई हो, अपनी लॉगिन जानकारी न दें। अपने लॉगिन आईडी और पासवर्ड का इस्तेमाल सिर्फ़ बैंक के आधिकारिक लॉगिन पेज पर करें, जो एक सुरक्षित वेबसाइट होनी चाहिए। लॉग इन करते समय URL में 'https://' देखें; इसका मतलब है कि वेबसाइट सुरक्षित है।

- **बचत खाते की नियमित जांच करते र**

ऑनलाइन कोई भी ट्रांजेक्शन करने के बाद अप खाते की जांच करें। सुनिश्चित करें कि आपके खाते सही राशि कटी है या नहीं। अगर आपको राशि में को अंतर नज़र आए तो तुरंत बैंक को सूचित करें।

- **हमेशा लाइसेंस प्राप्त एंटी-वायरस सॉफ़्टवेयर का उपयोगकरें।**

अपने कंप्यूटर को नए वायरस से बचाने के लिए, सुनिश्चित करें कि आप हमेशा लाइसेंस प्राप्त एंटी-वायरस सॉफ़्टवेयर का उपयोग करें। एंटी-वायरस सॉफ़्टवेयर के पायरेटेड संस्करण मुफ़्त में उपलब्ध हो सकते हैं, लेकिन वे आपके कंप्यूटर को ऑनलाइन दुनिया में प्रचलित नए वायरस से बचाने में विफल हो सकते हैं। इसके अलावा, आपको समय-समय पर सॉफ़्टवेयर में अपडेट के लिए सूचनाएँ मिलेंगी। सुनिश्चित करें कि आप अपने एंटी-वायरस को अपडेट रखें, ताकि आपकी गोपनीय जानकारी हमेशा सुरक्षित रहे।

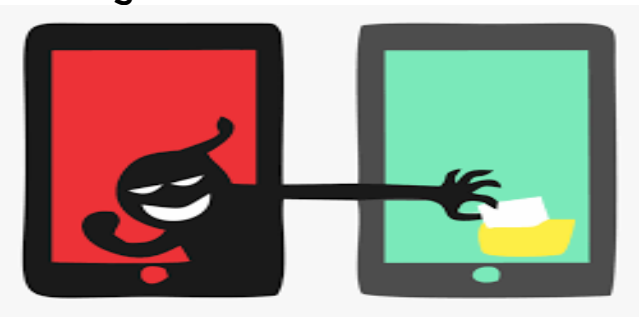
- **उपयोग में न होने पर इंटरनेट कनेक्शन डिस्कनेक्ट करें**

अधिकांश ब्रॉडबैंड उपयोगकर्ता अपने कंप्यूटर पर इंटरनेट कनेक्शन को डिस्कनेक्ट नहीं करते हैं जब वे इसका उपयोग नहीं कर रहे होते हैं। दुर्भावनापूर्ण हैकर्स इंटरनेट कनेक्शन के माध्यम से आपके कंप्यूटर तक पहुंच सकते हैं और आपकी गोपनीय बैंकिंग जानकारी चुरा सकते हैं। अपने डेटा को सुरक्षित रखने के लिए, सुनिश्चित करें कि जब आपको इसकी आवश्यकता न हो तो आप इंटरनेट को डिस्कनेक्ट कर दें ।

- **अपना इंटरनेट बैंकिंग यूआरएल टाइप करें**

ईमेल में दिए गए लिंक पर क्लिक करने की तुलना में ब्राउज़र के एड्रेस बार में अपने बैंक का यूआरएल टाइप करना ज़्यादा सुरक्षित है। धोखेबाज़ों द्वारा धोखाधड़ी वाली वेबसाइट लिंक के साथ ईमेल भेजने के कई उदाहरण हैं जो बिल्कुल बैंक की मूल वेबसाइट की तरह डिज़ाइन किए गए हैं। एक बार जब आप ऐसी वेबसाइट पर अपना लॉगिन विवरण दर्ज करते हैं, तो उनका उपयोग आपके खाते तक पहुँचने और आपके पैसे चुराने के लिए किया जा सकता है। लॉग इन करते समय, URL में 'https://' की जाँच करें और सुनिश्चित करें कि यह आपके बैंक की प्रामाणिक वेबसाइट है।

ख)मोबाइल सुरक्षा टिप्स



1. सॉफ्टवेयर को अपडेट रखें

सॉफ़्टवेयर अपडेट न केवल नई सुविधाएँ और प्रदर्शन सुधार पेश करते हैं, बल्कि ज्ञात सुरक्षा कमज़ोरियों को भी ठीक करते हैं। इसलिए, इन अपडेट को अनदेखा करने से आपके डिवाइस साइबर हमलों के प्रति कमज़ोर हो सकते हैं। संभावित खतरों से अधिकतम सुरक्षा सुनिश्चित करने के लिए ऑपरेटिंग सिस्टम और इंस्टॉल किए गए एप्लिकेशन दोनों को हमेशा अपडेट रखना एक आवश्यक उपाय है।

2. मजबूत पासवर्ड का उपयोग करें

मजबूत पासवर्ड आपके डिवाइस और आपके डेटा तक अनधिकृत पहुंच के खिलाफ़ सुरक्षा की पहली पंक्ति है। अनुमान लगाने में आसान पासवर्ड, जैसे कि “123456” या “पासवर्ड” का उपयोग करने से बचें, साथ ही स्पष्ट और आसानी से खोजी जा सकने वाली व्यक्तिगत तिथियों, जैसे कि उपयोगकर्ता का जन्मदिन का उपयोग न करें। सबसे अच्छा विकल्प लंबे और अद्वितीय पासवर्ड चुनना है जो अक्षरों, संख्याओं और विशेष वर्णों को जोड़ते हैं ताकि डिक्रिप्शन को और अधिक कठिन बनाया जा सके।

3. ऑटो-लॉक सक्रिय करें

स्वचालित डिवाइस लॉकिंग एक आवश्यक सुरक्षा उपाय है जो खो जाने या फोन को बिना देखे छोड़ दिए

जाने की स्थिति में अनधिकृत पहुँच को रोकता है। डिवाइस को निष्क्रियता की एक छोटी अवधि के बाद स्वचालित रूप से लॉक करने के लिए कॉन्फ़िगर करें और अपनी गोपनीयता और डिवाइस में मौजूद सभी व्यक्तिगत डेटा की सुरक्षा के लिए एक अतिरिक्त अवरोध के रूप में इसे अनलॉक करने के लिए पासवर्ड या सुरक्षित अनलॉकिंग विधि सेट करें।

4. सार्वजनिक नेटवर्क का उपयोग करने से बचें

सार्वजनिक वाई-फाई नेटवर्क आपके डिवाइस के लिए सुरक्षित स्थान नहीं हैं, क्योंकि उनमें अक्सर आपकी जानकारी की सुरक्षा के लिए आवश्यक सुरक्षा उपायों की कमी होती है। असुरक्षित वाई-फाई नेटवर्क से कनेक्ट होने से बचना उचित है, जैसे कि कैफे या हवाई अड्डों में पाए जाने वाले, और इंटरनेट का उपयोग करते समय अपने डेटा को एन्क्रिप्ट करने और अपनी गोपनीयता की रक्षा करने के लिए वर्चुअल प्राइवेट नेटवर्क (वीपीएन) का उपयोग करने पर भी विचार करें।

5. केवल विश्वसनीय स्रोतों से ही ऐप्स डाउनलोड करें

अनधिकृत या अविश्वसनीय स्रोतों से एप्लिकेशन इंस्टॉल करने से आपको सुरक्षा जोखिम हो सकते हैं, जैसे मैलवेयर इंस्टॉलेशन या व्यक्तिगत डेटा का नुकसान। नए एप्लिकेशन की तलाश करते समय, सबसे सुरक्षित विकल्प उन्हें केवल आधिकारिक ऐप स्टोर से डाउनलोड करना है, जैसे कि गूगल प्ले स्टोर या ऐप स्टोर जहाँ जोखिम की संभावना कम होती है क्योंकि पब्लिश होने से पहले एप्लिकेशन को स्कैन और सत्यापित किया जाता है।

6. ऐप अनुमतियों की समीक्षा करें

किसी डिवाइस पर नया एप्लिकेशन इंस्टॉल करने से पहले, उस एप्लिकेशन द्वारा मांगी गई अनुमतियों की सावधानीपूर्वक समीक्षा करना महत्वपूर्ण है। किसी भी अतिरिक्त अनुमति को अक्षम करना उचित है जो एप्लिकेशन के संचालन के लिए बहुत आवश्यक नहीं है और उन एप्लिकेशन को हटाने पर विचार करें जो आपके व्यक्तिगत डेटा तक अत्यधिक पहुंच का अनुरोध करते हैं। ऐप अनुमतियों को सीमित करने से आपकी गोपनीयता और ऑनलाइन सुरक्षा की रक्षा करने में मदद मिल सकती है।

7. अपने डेटा का नियमित बैकअप लें

फ़ोटो, वीडियो और अन्य दस्तावेज़ों जैसे महत्वपूर्ण डेटा का नियमित बैकअप लेते रहे और यह आपके डिवाइस के खोने या चोरी होने की संभावना पर डेटा को बचाने के लिए ज़रूरी है। इन बैकअप को बचाने के लिए, आप गूगल ड्राइव या आई-क्लाउड जैसी क्लाउड सेवाओं या बाहरी स्टोरेज डिवाइस का इस्तेमाल करके अपने डेटा का नियमित रूप से बैकअप ले सकते हैं और सुनिश्चित कर सकते हैं कि आपातकालीन स्थिति में वे सुरक्षित रहें।

8. सुरक्षा ऐप्स का उपयोग करें

डिवाइस की सुरक्षा बढ़ाने के लिए, आप एंटीवायरस और एंटी-मालवेयर जैसे विश्वसनीय सुरक्षा एप्लिकेशन इंस्टॉल कर सकते हैं, ताकि वायरस, मालवेयर और फ़िशिंग जैसे ज्ञात खतरों से डिवाइस की सुरक्षा हो सके।

इस प्रकार के ऐप्स उपकरणों को दुर्भावनापूर्ण सॉफ़्टवेयर से बचने के लिए स्कैन कर सकते हैं तथा दुर्भावनापूर्ण वेबसाइटों और संभावित खतरनाक डाउनलोडों के विरुद्ध वास्तविक समय में सुरक्षा प्रदान कर सकते हैं।

9. रिमोट वाइप सुविधा सक्षम करें

अपने डिवाइस पर रिमोट वाइप सुविधा को सक्रिय करने से आप डिवाइस के खो जाने या चोरी हो जाने की स्थिति में अपने व्यक्तिगत डेटा को दूर से भी से मिटा सकते हैं। यह आपकी गोपनीय जानकारी की सुरक्षा करने और आपके डिवाइस के गलत हाथों में पड़ जाने की स्थिति में आपके डेटा तक अनधिकृत पहुँच को रोकने में मदद कर सकता है।

ग)ऑनलाइन गेमिंग धोखाधड़ी :

ऑनलाइन गेमिंग उद्योग ने हाल के वर्षों में धंधे में जबरदस्त वृद्धि का अनुभव किया है, जिसमें लाखों खिलाड़ी इमर्सिव वर्चुअल दुनिया और प्रतिस्पर्धी गेमप्ले में शामिल हैं। दुर्भाग्य से, लोकप्रियता में इस उछाल ने ऑनलाइन गेमिंग धोखाधड़ी में भी वृद्धि की है। बेईमान व्यक्तियों ने धोखाधड़ी गतिविधियों के माध्यम से उद्योग का शोषण करने की कोशिश की है, जिससे गेमिंग विक्रेताओं के लिए वित्तीय नुकसान और प्रतिष्ठा को नुकसान पहुंचा है।

ऑनलाइन गेमिंग धोखाधड़ी वाले ऐप्स में आमतौर पर दुर्भावनापूर्ण सॉफ़्टवेयर या स्कैम शामिल होते हैं जो गेमर्स को निशाना बनाते हैं, उनके व्यक्तिगत डेटा, वित्तीय जानकारी या इन-गेम संपत्तियों से समझौता करते हैं। ऑनलाइन गेमिंग धोखाधड़ी वाले कुछ सामान्य प्रकार के ऐप्स में शामिल हैं:

1. **फ़िशिंग ऐप्स:** लॉगिन क्रेडेंशियल चुराने के लिए लोकप्रिय गेम या प्लेटफ़ॉर्म की नकल करते हैं।
2. **मैलवेयर-संक्रमित:** ऐप्स: मैलवेयर छिपाते हैं, डिवाइस को नुकसान पहुंचाते हैं या संवेदनशील जानकारी चुराते हैं।
3. **नकली गेम मॉडस या धोखाधड़ी:** लाभ का वादा करते हैं लेकिन उनमें मैलवेयर होता है या डेटा चुराते हैं।
4. **स्कैम ऐप्स:** पुरस्कार या इन-गेम मुद्रा का वादा करते हैं, लेकिन भुगतान या व्यक्तिगत जानकारी की मांग करते हैं।
5. **कीलॉगर्स:** लॉगिन क्रेडेंशियल चुराने के लिए की-स्ट्रोक्स रिकॉर्ड करते हैं।
6. **रैनसमवेयर:** डिवाइस या खातों को लॉक करना, भुगतान की मांग करना।
7. **सोशल इंजीनियरिंग:** गेमर्स से संवेदनशील जानकारी उजागर करवाना।
8. **इन-गेम आइटम घोटाले**: दुर्लभ या मूल्यवान वस्तुओं के लिए फेक ऑफर।
9. **खाता अधिग्रहण :** गेमर अकाउंट को चुराना या हाईजैक करना।
10. **फर्जी गेमिंग प्लेटफॉर्म:** दुर्भावनापूर्ण गेम वितरित करने वाले अनौपचारिक प्लेटफॉर्म।

शिकार बनने से बचने के लिए सुझाव:

1. आधिकारिक स्टोर से गेम डाउनलोड करें।
2. ऐप अनुमतियों को सत्यापित करें।
3. संदिग्ध लिंक या ईमेल से सावधान रहें।
4. मजबूत पासवर्ड और दो-कारक प्रमाणीकरण का उपयोग करें।
5. खाता गतिविधि पर नज़र रखें।
6. डिवाइस और सॉफ्टवेयर को अद्यतन रखें।
7. प्रतिष्ठित एंटीवायरस सॉफ़्टवेयर का उपयोग करें।
8. गेम और डेवलपर्स पर शोध कर