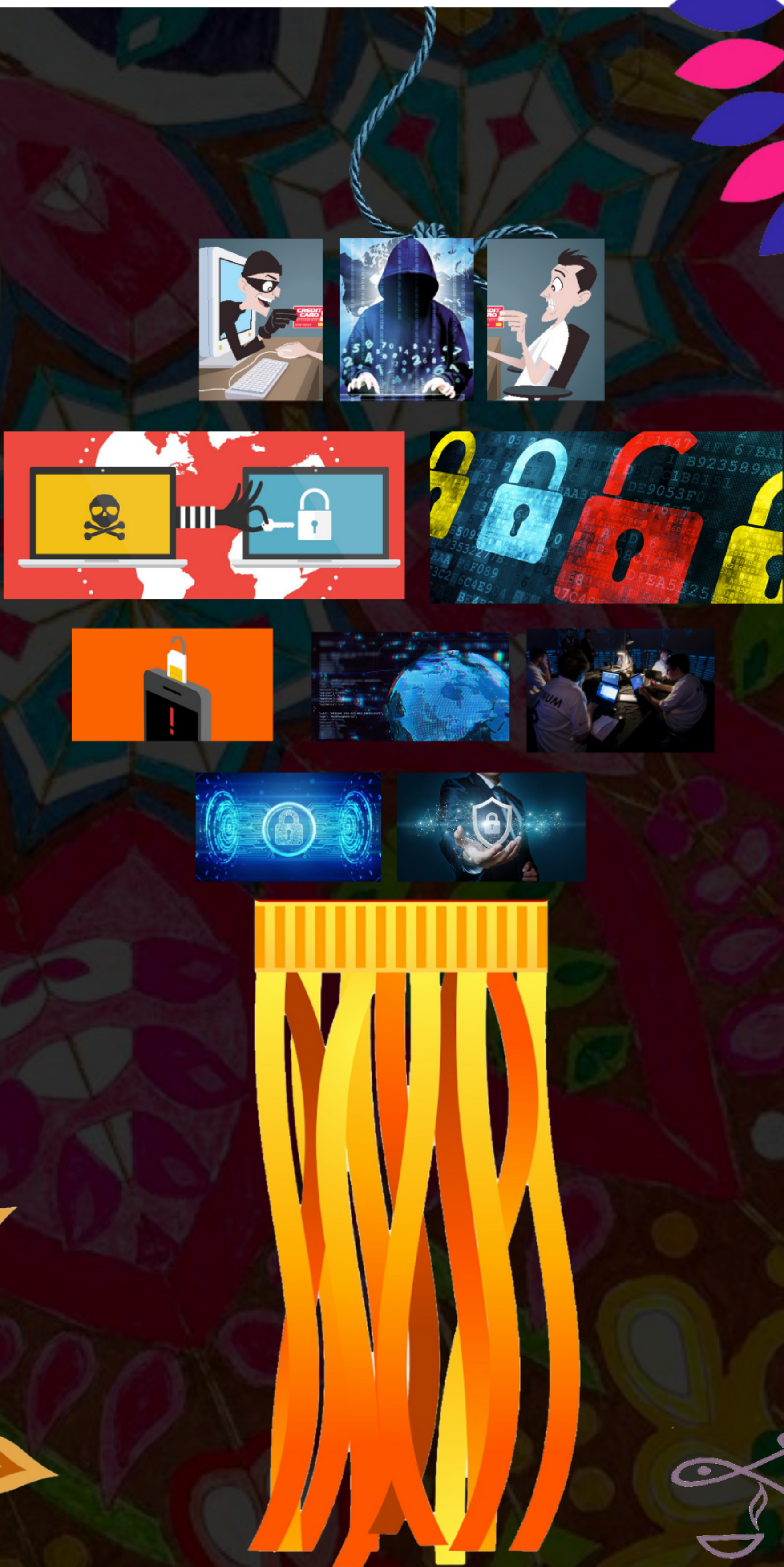
सायबरसाक्षर

Cyber Literate India

दिवाळी अंक २०१९ (वर्ष पहिले)



शुभ दिपावली

सायबर साक्षर - दिवाळी अंक २०१९

ऋणनिर्देश

या आगळ्यावेगळ्या पण गरज असलेल्या सायबर दिवाळी अंकासाठी अगदी नि:संकोच आणि दिलखुलासपणे मदत केल्या बद्दल सर्व लेखकांचे आभार. काहींनी अगदी शॉर्ट नोटीसवर लिहून दिल्याबद्दल दुप्पट आभार.

अक्षररचना, कल्पना, छायाचित्रे, रेखाटनं, मांडणी इत्यादी साठी मदत करणाऱ्या प्रत्येकाचे आभार मानावे तेवढे कमीच आहेत. अनेकजणांचे लेख यात सामील करून घेता आले नाहीत त्यांना क्षमस्व.

या दिवाळी अंकाची कल्पना दिल्याबाबदल माझ्या आईचा मी शतशः ऋणी आहे.

- ओंकार गंधे
संपादक, सायबर साक्षर

cybersakshar.com

सायबर साक्षर - दिवाळी अंक (वर्ष पहिले)

संपादक: प्रा. ओंकार गंधे

मुखपृष्ठ: प्रारब्ध ढवळे
अक्षररचना: श्रुती कोठावदे
भाषांतर: संयुक्ता सराफ
छायाचित्रे आणि मांडणी: प्रसाद मोरे, आशुतोष गायकवाड
प्रसिद्धी: अथर्व देव, कुणाल खडके
रेखाटन साहाय्य: अनिकेत गायकवाड, कृष्णा वडनेरे

प्रकाशन: ऑन वेब टेक्नॉलॉजिज
कार्यालयीन पत्ता: २३९०, ज्ञानेश्वर लेन,
संगमनेर जि. अ.नगर
४२२६०५
cybersakshar@gmail.com

© सर्व हक्क संपादकांकडे राखीव

या मासिकात लिहिलेले लेख आणि व्यक्त केलेली मते ही संबंधित लेखकांची आहेत, त्या मतांशी सायबर साक्षर मासिक किंवा संपादक, प्रकाशक सहमत असतीलच असे नाही. टंकलेखनात, अक्षर जुळवणीत किंवा भाषांतरात चुका आढळल्यास क्षमस्व.

अनुक्रमणिका

- **भेदिले सायबर मंडळे.!** - अरविंद व्यं. गोखले - ७
- **डिजीटल इंडियाची डिजीटल गुन्हेगारी** - ॲड. यज्ञेश कदम - १०
- **डिजिटल समाजसेवा** - सतीश भालेराव - १५
- **सोशल खाजगीपण** - विवेकराज ठाकूर - २५
- **टेक्नोसॅव्ही होतांना..** - अनिल सुमति बागुल - २६
- **आजची सायबर सुरक्षा** - प्रितेश आहिरे - २८
- **सायबर गुन्ह्यांविरूद्ध महिलांचे संरक्षण करण्यासाठी कायदे** - हर्षिता जाधव - ३३
- **स्पाय ॲप** - ओंकार गंधे - ३८
- **सावधान, तुम्हाला कुणीतरी पाहतंय..** - तेजस्विता खिडके - ४२
- **तुमची शाळा, तुमचे कॉलेज सायबर साक्षर आहे का?** - ४६
- **सिम स्वॅप आणि २० लाख गायब** - कविता गांगुर्डे - ४७
- **वेडे प्रेम** - प्रारब्ध ढवळे - ५०
- **व्यवसाय आणि तंत्रज्ञान** - प्रदीप मोकळ - ५३
- **सुरक्षित आर्थिक व्यवहारांसाठी..** - विहंग घाटे - ५९
- **थोडक्यात** - आर जे शोनाली - ६१
- **मनांत** - पराग आचलिया - ६२
- **महिला सुरक्षा ॲप्स** - तेजा दुर्वे - ६२
- **सायबर दोस्त** - मनीषा रतिलाल बागुल - ६३
- **जबाबदारी** - ज्योती वाकचौरे - ६५
- **सुरेल** - आनंद ओक - ६६
- **धक्कादायक अनुभव** - शलाका भेंडे - ६७
- **आम आदमीवाली सायबर सुरक्षा** - आर जे शुभी - ६९
- **PRO TIPS** - संतोष खडसरे - ७०
- **फेसबुक व धार्मिक भावना** - आवेज काझी - ७३
- **अर्थसाक्षर** - सीए अभिजित कोळपकर - ७५
- **माझ्या नजरेतून..** - अक्षय भाटकर - ७६
- **ई-कॉमर्स धोके** - निकिता कोल्हे - डोखे - ७८
- **सायबर प्रेम** - आर जे प्रथम - ७९

संपादकीय

दिवाळी आली की फराळ, फटाके, नवीन कपडे, खरेदी आणि सगळ्यात महत्वाचा तो म्हणजे दिवाळी अंक. दिवाळी येऊन ठेपली की दिवाळी अंकांची रेलचेल सुरु होते. विविध विषयांवर किंवा विषयांशिवायचं अनेक दिवाळी अंक निघतात. टेक्नॉलॉजी विषयावरही अनेक अंक प्रसिद्ध होतात, पण सायबर सुरक्षा विषयावर फारच कमी. त्यातल्या त्यात तर मराठी म्हणजे अगदीच बोटावर मोजण्याइतके.

सायबर सुरक्षा विषयात गेली अनेक वर्षे मी काम करत आहे. अनेक समस्या स्वतःच्या डोळ्यांनी पहिल्या, अनुभवल्या. अनेक जणांना, संस्थांना, पोलिसांना प्रत्यक्ष आणि अप्रत्यक्षरित्या छोटी-मोठी मदतही केली. पण समाजात सायबर सुरक्षेबाबत परिस्थिती दिवसेंदिवस बिकटच होत जात आहे. सायबर गुन्ह्यांमध्ये फासणारे कॉलेज तरुण तरुणी अधिक आहेत. त्यामुळे शाळा आणि कॉलेजला जाणाऱ्या विद्यार्थ्यांनाच सायबर साक्षर करणे जास्त गरजेचे आहे. सायबर साक्षरचा असा मानस आहे कि पुढील वर्षभरात किमान एक हजार शाळा आणि कॉलेजेस सायबर साक्षर होतील. या अंकाच्या शेवटी याबद्दल लिहिले आहेच.

सायबर साक्षरतेच्या मोठ्या कार्यात हा दिवाळी अंक नकीच काही भर पडेल अशी आशा आहे. तुम्हा सर्वांना हा दिवाळी अंक नक्की आवडेल आणि तुम्ही हा अंक जास्तीत जास्त लोकांपर्यंत शेयर कराल हि अपेक्षा आहे. सर्व वाचकांना दिवाळीच्या खूप खूप शुभेच्छा..!!

धन्यवाद..!

- ओंकार गंधे

भेदिले सायबर मंडळे.!

अरविंद व्यं. गोखले

सायबर सुरक्षा हा सध्याचा अत्यंत गुंतागुतीचा असलेला, पण सर्वार्थाने आपले विश्व व्यापणारा विषय ओंकार गंधे हे अतिशय सोप्या भाषेत आपल्याला गेल्या काही वर्षांपासून समजावून सांगत आहेत. ओंकार हे या विषयातले ज्येष्ठ तज्ञ आणि त्या विषयात प्रवीण असलेले संपादक आहेत. हा विषय मी अतिशय मनापासून वाचतो, याचे कारण मला या विषयाची आवड आहे. सध्याचा प्रश्न आहे तो सायबर सुरक्षेविषयी अधिक तपशील मिळवायचा आणि त्यासंबंधात काळजी करण्याचा. मी स्वत: पत्रकार आहे आणि मी ज्या वृत्तपत्रात काम करत होतो तिथे जेव्हा सुरुवातीला संगणक आले तेव्हा ते अचानक बंद पडायचे. ते होते एका प्रसिद्ध अमेरिकन कंपनीचे. त्या काळी घरगुतीरित्या (होममेड) बनवलेले संगणक बाजारात उपलब्धच नसत. त्यामुळे ते बंद पडले की, त्यावर बॉँबचे चित्र येत असे. आमचे ऑपरेटर्स 'आला बॉँब आला', म्हणून ओरडायचे. आता तो संगणक बंद करा, असे सांगत. तेव्हा तो एक प्रकारचा विषाणू (व्हायरस) असे, असा निष्कर्ष काढला जाई. तेव्हाच्या त्या काळात त्यावर जालीम उपाय सापडलेला नव्हता. मग सगळेच कपाळाला हात लावून बसत आणि तो विषाणू कधी माघारी जाईल, याची वाट पाहात. मग केव्हा तरी 'अरे गेला वाटते', असे म्हणून ते संगणक सुरु केले जात. तोपर्यंत त्यावर तयार केला गेलेला मजकूर हा गायब झालेला असे. मग पुन्हा पहिल्यापासून कित्ते गिरविणे यायचे. म्हणजे पहिल्यापासून तो मजकूर तयार करणे. त्यावेळी ऑपरेटर्स होते म्हणून हे लाड चालत, पण जेव्हा आमची संपादक मंडळी स्वत: मजकूर तयार करायला लागली तेव्हा त्यांना सक्त सूचना दिली जात असे की, तुम्ही तयार करत असलेला मजकूर हा एका वेगळ्या फाईलमध्ये जतन (सेव्ह) करून ठेवणे गरजेचे आहे हे त्यांना सांगितले जात असे. हे झाले वृत्तपत्रीय मजकुराचे.

त्यानंतरच्या काळात जेव्हा इंटरनेट आले तेव्हा त्यास आंतरजाळे असा शब्दप्रयोग आम्ही रूढ केला. इंटरनेट म्हणायची लाज वाटत होती. कारण मराठीशिवाय अन्य भाषेचा वापर हा त्याज्य मानला जात असे. हे आंतरजाळे हे कोळ्याच्या जाळ्यासारखे वाटू लागले. कोळी आपल्या घरात जाळे विणतो आणि त्यात कीडे, मुंग्या यांना आकृष्ट करतो. ते त्या जाळ्याच्या आकर्षणाने तिथे जातात आणि अडकतात. तेव्हा त्यांचा फडशा पाडला जातो.

भेदिले सायबर मंडळे.!

इंटरनेटवर मग लोकांचे म्हणजेच आमच्या सहकाऱ्यांचे शोध सुरु झाले. त्यातून नवनवी माहिती गोळा केली जाऊ लागली. त्यातून आमचे ज्ञान वाढू लागले. ही ज्ञानाची आस मग अडचणीचीही ठरू लागली. आपल्याकडे विश्वामित्राचा तपोभंग एका देखण्या मेनकेने केल्याच्या कहाण्या ऐकवल्या गेल्या आहेत. त्या खऱ्याही असतील, पण समजा तुम्ही काही मजकुराचा शोध घेत आहात आणि तुमच्या समोर अशी एखादी अप्सरा येऊन उभी राहिली तर तुमचे लक्ष तिच्याकडे आकृष्ट होईल की नाही? मग काय होईल, तर ती तथाकथित अप्सरा तुमच्या संगणकात शिरेल आणि तिथे असलेली सर्व माहिती काढून घेऊन पसार होईल. पोटात शिरून माहिती काढण्याचा हा प्रकार जुन्या काळापासूनच आहे, फक्त तेव्हा इंटरनेट नव्हते इतकेच.

त्यानंतर संगणक अधांतरी (हँग) राहू लागले. म्हणजे काय तर ते पुढेही काम करेनासे झाले आणि जिथल्या तिथे अडकून राहू लागले. मग त्यावर उपाय काय? आमचे इंजिनिअर्स (आता या संगणकांच्या दुरुस्तीसाठी किंवा देखभालीसाठी आमच्याकडे अतिशय प्रशिक्षित असे इंजिनिअर आले.) अशावेळी यायचे आणि त्यावर उपाय सांगायचे. त्यांचा उपाय सोपा असायचा. ते म्हणायचे की तुमचा कॉँप्युटर बंद करा आणि मग तो सुरु करा. तेव्हा आम्ही गमतीत त्याला म्हणायचो देखील की तू ही कल्पना मालकांना सांगू नकोस. का? नाही तर 'बंद करून सुरु करायचे हे तंत्र' तो मालक वापरायला लागेल. म्हणजे आधी ते वृत्तपत्र बंद करेल आणि मग चालू करेल. तोपर्यंत आपण हाताची घडी घालून ते वृत्तपत्र कधी सुरु होते त्याची वाट पाहात बसायचे. ही झाली गंमत, पण एक लक्षात घ्या मित्रांनो, सायबर सुरक्षा हा आता गंमतीचा आणि चेष्टेचा विषय राहिलेला नाही. तो आपले लष्कर, नाविक दल किंवा हवाई दल यांच्या दृष्टीने काळजी घ्यायचा विषय आहे.

माझ्या माहितीनुसार एका मंत्र्याने एका ठिकाणचा हवाई दलाचा विमानतळ हलवून तो संपूर्ण नागरी करायचा प्रयत्न सुरु केला, तेव्हा संतापलेल्या एका माजी हवाई दल प्रमुखाने त्या मंत्र्याला किंवा त्यावेळच्या त्या नेत्याला माझ्यादेखत झापल्याचे उदाहरण मला माहिती आहे. त्याने या विमानतळावर देशाच्या सर्व सुरक्षेची तसेच सायबरसुरक्षेची व्यवस्था कशी आहे ते त्याला समजावून दिले आणि त्याच्या त्या मागणीला खो घातला. आता हा विमानतळ परदेशातला आणि तो मंत्रीही परदेशातला होता म्हणून ठीक आहे अन्यथा काही धडगत नव्हती. मोठ्या कॉर्पोरेट संस्था, आर्थिक संस्था, वैद्यकीय संस्था यांनाही हाच नियम लागू आहे. त्यांचीही बरीच माहिती ही शत्रूच्या किंवा अगदी दुसऱ्या व्यक्तीच्या हाती लागू नये याची काळजी घेतली जायला हवी. त्यांच्यासाठी स्वतंत्र सायबर सुरक्षेचे पाठ दिले जाऊ लागले. नासा किंवाा आपली इस्रोसारखी संस्था घ्या, तिथे केले जात असलेले सर्व प्रयोग हे गुप्त ठेवले जाण्याची आवश्यकता असते. ते जर कोणत्याही शत्रू राष्ट्राच्या हाती पडणार असतील तर मग त्या प्रयोगांचे काही खरे नाही, असे म्हणावे लागेल.

आता काही महत्वाचे प्रसंग डोळ्यासमोर आणू. समजा तुम्ही वापरत असलेला पेन ड्राइव्ह हा दुसऱ्या व्यक्तीकडून वापरून आला आहे आणि त्याच्या संगणकात कोणताही एक विषाणू असेल तर तो तुमचा संगणक उद्ध्वस्त करायला कारण ठरू शकतो. तेव्हा पेनड्राइव्ह देताना किंवा घेताना त्यासंबंधीची काळजी घ्यायला हवी की नको? तुमच्याकडे येणाऱ्या पेनड्राइव्हला जरत्यासारखे प्रशिक्षण दिले गेले असेल तर तुमच्या संगणकात दडलेली सर्व माहिती हा पेनड्राइव्ह चोरू शकतो हे लक्षात घ्या. हेच सीडीबाबतही खरे आहे. कोणत्याही लिंक उघडतानाही ही काळजी घेणे गरजेचे आहे. तुम्हाला माहिती आहे का, की पहिला क्रीपर विषाणू १९७१ मध्ये आढळला. तो पहिला ठरला. तुम्हाला हेही माहिती असायला हवे की, 'क्रिप्टोग्राफिक कम्युनिकेशन सिस्टीम्स अँड मेथड' मध्ये पहिले पेटंट हे अमेरिकेत बॉस्टनच्या 'मॅसॅच्युसेट्स इन्स्टिट्यूट ऑफ टेक्नॉलॉजी' म्हणजेच एमआयटीने १९८३ मध्ये मिळवले. ते जगातले पहिले सायबरसुरक्षा पेटंट आहे. म्हणजे पहिला विषाणू तयार झाल्यानंतर त्याविरोधातले पहिले पेटंट मिळवायला एक तप जावे लागले. असो, सांगायचा मुद्दा हा की तुम्ही सगळे ओंकार गंधे यांचे मार्गदर्शन तुमच्या या सायबर साक्षरतेतून घेत असता. ही माहिती चांगलीच असते, पण ती नुसती चांगली नाही, तर ती तुम्हाला घ्यायची काळजीही सांगते. तेव्हा सायबर सुरक्षेला दाद द्या आणि आपली माहिती जपून ठेवा. ती दुसऱ्याना चोरू देऊ नका. कारण ती अमूल्य आहे.

अरविंद व्यं. गोखले

लेखक पन्नास वर्षांहून अधिक काळ पत्रकारितेत आहेत. केसरी ते लोकसत्ता असा प्रवास. आजही ते अनेक वृत्तपत्रांतून लिहितात. पाकिस्तान आणि अन्य परराष्ट्रीय राजकारणाचे अभ्यासक. कलम ३७० + ३५ अ तसेच संघर्ष बलुचिस्तानचा या अलीकडील पुस्तकांचे लेखक. मंडालेचा राजबंदी या पुस्तकाचे लेखक. द प्रिझनर ऑफ मंडाले हे त्याचे भाषांतर प्रसिद्ध.

arvindgokhale@gmail.com

डिजीटल इंडियाची डिजीटल गुन्हेगारी

ॲड. यज्ञेश कदम

डिजीटल इंडिया डिजीटल इंडिया नारा जेव्हा आपले नेते पुढारी लावतात तेव्हा ते ऐकण्यासाठी फार मनोरंजक वाटत परंतु असा नारा देण्याआधी व त्याची जबरदस्ती जनतेवर लादण्याआधी आपण खरोखर त्यासाठी तंत्रज्ञानाच्या दुष्टिने सक्षमआहोत का याचा गहन विचार करणे आवश्यक आहे पुण्यात झालेल कॉसमॉस बॅक प्रकरण खरच डिजीटल इंडिया च्या संकल्पनेला सुरुंग लावल्यासारख आहे भारतातील मुख्य बँका जशा आरबीआय, एसबीआय, त्याचप्रमाणे मुंबई पोलीस यांच्या वेबसाईटसुद्धा हॅक करण्यात आल्या होत्या. रशियातील सिटी बँकेचे पासवर्ड, नेट बॅकिंग आयडी, हॅक करून रशियाच्या विविध सिटीबँकेच्या खात्यातील १० हजार लक्ष डॉलर्स विविध शाखांतून काढण्यात आले. एखाद्या देशाच्या अर्थव्यवस्थेबरोबरच सुरक्षाव्यवस्थेलाही मोठा धोका सायबर क्राईमद्वारे होऊ शकतो सायबर गुन्हा किंवा संगणकीय गुन्हा ही संज्ञा संगणक व इंटरनेटाशी संबंधित असणाऱ्या व प्रत्यक्ष गुन्ह्यात संगणकाचा प्रामुख्याने वापर असणाऱ्या गुन्ह्याला उद्देशून योजली जाते. सायबर गुन्हे विशेषकरून हॅकिंग, प्रताधिकारभंग, बाल लैंगिक चित्रण इत्यादी स्वरूपात घडताना दिसतात. याशिवाय खासगी किंवा गोपनीय माहिती चोरणे, फोडणे आदी प्रकारदेखील सायबर गुन्ह्यांमध्ये मोडतात. माहिती तंत्रज्ञानाच्या प्रसाराबरोबर सायबर गुन्ह्यांमध्ये लक्षणीय वाढ होताना आढळत आहे. पाकिस्तान सायबर आर्मीने इंडिअन वेब साईड हकेद करन्याचा प्रयत्न केला नवनवीन तंत्रज्ञानाच्या शोधाचा एक प्रमुख दुष्परिणाम म्हणून सायबर गुन्हेगारीकडे पहावे लागेल. आधुनिक काळात ही एक जागतिक समस्याच बनली आहे.

आजकाल आपण सायबर गुन्ह्यांबद्दल बरेच ऐकतो,वर्तमानपत्रात वाचतो परंतु सायबर गुन्हे म्हणजे काय ? त्याबद्दल कोणता कायदा आणि त्यात शिक्षेच्या कोणत्या तरतुदी हे बऱ्याच जणांना माहित नसते.म्हणून हा आजचा लेख.

संगणक, मोबाइल किंवा इंटरनेटसह इलेक्ट्रॉनिक व टेलिकम्युनिकेशन नेटवर्क्सचा गैरवापर करून एखादी व्यक्ती किंवा समूहाला शारीरिक, मानसिक हानी पोहचविण्यासाठी किंवा त्यांची बदनामी करण्यासाठी गुन्हेगारी उद्देशाने केलेले कृत्य म्हणजे सायबर गुन्हा.

यासाठी नियंत्रण करण्यासाठी 'इन्फॉरमेशन टेक्नॉलॉजी' (अमेंडमेंट) कायदा २००८ लागू करण्यात आला. संगणकीय क्षेत्रात सायबर क्राईमचा झालेला शिरकाव हा अनेक अनर्थ व संकटांना आमंत्रण देणारा आहे. साधारणत: सर्वसामान्य नागरिकांचा असा समज आहे की, सायबर क्राईमशी आपला काही संबंध नाही. या समजामुळे नागरिक सायबर क्राईमबाबत अनभिज्ञ आहेत. पण, जरा सूक्ष्मविचार करून पाहिलं तर आपल्याला रोजच या सायबर क्राईमचा सामना करावा लागतो. आपल्या ई-मेलवर स्पॅममेल येत असतात, मोबाईलवर अनावश्यक कॉल, मेसेजेस येतात, नेट बँकिंग अकाऊंट असेल तर त्याचा पासवर्ड, आय. डी. हॅक होतो. हे सर्व प्रकार सायबर गुन्हेगारीमध्ये मोडतात. संगणक, इंटरनेट यांच्या माध्यमातून एखाद्या व्यक्ती, संस्था आदींच्या संगणक प्रणालीमध्ये शिरून त्यातील माहिती हॅक करणे (चोरणे), त्याचा गैरवापर करणे, व्हायरस पाठविणे, मेलद्वारे फसवणूक, धमकी देणे, खंडणी मागणे अशा कारवायांना सायबर क्राईम म्हणता येईल. परंतु, सायबर क्राईमची व्याप्ती व तंत्र हे रोज बदलते असल्याने त्याला विशिष्ट अशा रचनेत वा संकल्पनेत बसविणे थोडे जिकिरीचे आहे.

पुण्यातील गणेश खिंड रस्त्यावरील कॉसमॉस बँकेच्या मुख्यालयातील एटीएम स्विच सर्व्हर हॅक करून अनेक खातेधारकांच्या डेबिट कार्ड आणि रुपी कार्डाची माहिती चोरल्याची घटना घडली आहे. याद्वारे तब्बल ८० कोटी रुपये हाँगकाँग येथील बँकेत ट्रान्सफर करण्यात आल्याची माहिती समोर आली आहे. बँकेने दिलेल्या माहितीनुसार, कॉसमॉस बँकेच्या डेबीट कार्डच्या माध्यमातून होणाऱ्या पेमेंट सिस्टमवर हॅकर्सनी हल्ला केला. शनिवारी दुपारी हा प्रकार बँकेच्या लक्षात आला. इंटरनॅशनल व्हिसा कार्डमधून नेहमीच्या व्यवहारांपेक्षा जास्त व्यवहार होत असल्याचे लक्षात आले. व्हिसा आणि रुपे कार्ड वापरुन एटीएम द्वारे सुमारे दोन तास हे व्यवहार चालू होते. यावर शंका आल्याने बँकेच्या वतीने तातडीने व्हिसा व रुपे डेबिट कार्ड यंत्रणा बंद करण्यात आली.हॅकर्सनी ७८ कोटी रुपयांची रक्कम २८ देशांमधील विविध एटीएममधून काढल्याचे समोर आले आहे. व्हिसाच्या सुमारे १२ हजार व्यवहारांची नोंद झाली असून भारताच्या एटीएममधून रुपे डेबिट कार्डाच्या आधारे अडीच कोटी रुपयांची रक्कम काढण्यात आली. यात सुमारे २, ८०० व्यवहारांची नोंद झाली.

हॅकिंग म्हणजे काय?

हॅकिंग म्हणजे कम्प्युटर यंत्रणा अथवा नेटवर्क यात बेकायदा शिरकाव करणं. हॅकर्स हे रेडिमेड कम्पुटर प्रोग्रामला लक्ष्य करण्यासाठी वापतात. काही हॅकर्स आर्थिक लाभासाठी गुन्हे करतात. क्रेडिट कार्डविषयक माहिती काढून घेणं, अनेक बँकांतील पैसे स्वत:च्या खात्यात वळवून घेणं. काहीवेळा असे हॅकर्स चोरलेल्या माहितीचा ब्लॅकमेल करण्यासाठी गैरवापर करतात.

हॅकर्संना शिक्षेची तरतूद -

या कायद्यात प्रामुख्याने हार्डवेअर आणि सॉफ्टवेअर यांची खरेदी आणि लायसन्स देणं, सिस्टिम सॉफ्टवेअर, दस्तऐवज सुरक्षा, कनेक्टिविटी, नेटवर्क ॲडमिनिस्ट्रेटर याबाबत नियमावली तयार करण्यात आली आहे. या कायद्याच्या कलम ६५ नुसार, कम्प्युटरचा माध्यम म्हणून वापर करण्यात ढवळाढवळ करणाऱ्यास शिक्षेची तरतूद आहे. अशा 'हॅकर'ला तीन वर्षं कारावास अथवा दोन लाख रुपयांचा दंड अथवा दोन्ही ठोठावण्याची तरतूद आहे.

ई-तिकिट गुन्हे -

'फेम ॲडलॅब' या थिएटरकडून मुंबईतील सायबर गुन्हे अन्वेषण खात्याकडे 'ई तिकिट' याबद्दल तक्रार आली होती. या प्रकरणात गुन्हेगारांनी मोबाईल फोन, इंटरनेट याद्वारे तिकिटं बुक करून ती थिएटरजवळ प्रेक्षकांना विकल्याचं आढळून आलं होतं.

ई-मेल, एसएमएस,चॉटिंग याव्दारे फसवणूक -

हो ही वस्तूस्थिती आहे. स्पॅम मेलचा हा प्रकार आहे. YOU HAVE WON 2500000 DOLLARS,KATRINA WANTS TO HAVE A DINNER WITH YOU, MAKE CHARITY. LOTTERY अशा प्रकारचे मेल किंवा एसएमएस आपल्याला वारंवार येतात. हा नायजेरियन सायबर फ्रॉड समजला जातो. यामध्ये संबंधितास लॉटरी किंवा मोठे बक्षिस मिळाल्याचे कळवून त्यापोटी प्रोसेसिंग फी किंवा नवीन अकाऊंट उघडण्यासाठी २५ हजार ते १ लाखापर्यंतची रक्कम संबंधिताकडून उकळली जाते. एवढय़ावर न थांबता संबंधिताच्या नेट बँकींग खात्यातून रक्कम काढणे किंवा मोठय़ा प्रमाणात खरेदीचे प्रकार घडले आहेत.

यावर प्रतिबंध -

इंटरनेट वापरताना आपला आयडी क्रमांक, नेट बँकींग अकाऊंट क्रमांक, आपला आयडी क्रमांक, पासवर्ड, क्रेडीट किंवा डेबीट पासवर्ड क्रमांक अथवा आपली वैयक्तिक माहिती उघड करताना सावधानता बाळगावी. ऑन लाईन खरेदी करताना सुरक्षिततेचे उपाय योजावेत.

आपली संगणक सिस्टीम ऍन्टी व्हायरस, फायर वॉलने सुरक्षित ठेवावी. स्पॅम मेल, फसवे मेल यावर डबल क्लिक करुन उघडण्याचा प्रयत्न करु नये. अशा मेल मधून व्हायरसची एक्झीक्युटेबल फाईल आपल्या नकळत डाऊन लोड होते. आपण जेव्हा संगणकावर काम करतो तेव्हा केलेल्या कामाची एक डुप्लीकेट फाईल तयार होऊन ती हार्ड डिक्सवर सेव्ह होते. जेव्हा आपण इंटरनेट चालू करतो तेव्हा अलगदपणे ही माहिती हॅकरला मेल व्दारे प्राप्त होते. त्यामुळे पुढील फसगत टाळण्यासाठी अशा प्रकारचे फसवे मेल डीलीट करणे हाच मोठा प्रतिबंधात्मक उपाय ठरतो.

सायबर हल्ल्याचे काही उदाहरण -

१. हॅकर्सनी अमेरिकेच्या सरकारी संगणकातील माहिती चोरली आहे. आताच्या व माजी अशा मिळून ४० लाख सरकारी कर्मचाऱ्यांची व्यक्तिगत माहिती चोरण्यात आली होती. आतापर्यंत अमेरिकी संगणकावर हॅकर्सनी केलेला हा सर्वात मोठा हल्ला आहे.

२. एखादा सायबर हल्ला क्षणार्धात ही गुप्तता धोक्यात आणत असल्याच्या घटनाही समोर येत असतात. अमेरिकेतील ऑफिस ऑफ पर्सनल मॅनेजमेंट (ओपीएम)वर झालेल्या सायबर हल्ल्यामध्ये तब्बल ५६ लाख जणांचे फिंगरप्रिन्ट्स चोरीला गेले होते.

३.पुण्यातील एका महाविद्यालयाची वेबसाईट काही दिवसांपूर्वी हॅकरनी हॅक केली होती.

४. चीन मधील प्रसिद्ध विद्यापीठाचीही वेबसाईट डॉन टू" या हॅकरनीच हॅक केली होती.

सायबर युद्धातील गुन्हेगार कसे शोधावे -

सायबर गुन्हे व गुन्हेगार शोधणे सोपं आहे. फ्रॉड मेल, धमकी देणारे मेल, किडनॉपिंग, फिशिंग, पोर्नोग्राफी आदींचे गुन्हे उघड करणे अतिशय सोपे आहे. यासाठी वापरात आलेल्या संगणक किंवा मेलवरुन गुन्हेगाराचा आयपी ऍड्रेस (इंटरनेट प्रोटोकॉल ऍड्रेस) शोधला जातो. असा मेल कोणत्या सर्व्हरवरुन आला हे शोधले जाते. आयपी ऍड्रेसवरुन वापरण्यात आलेल संगणक, त्याचा प्रकार, इंटरनेट स्पीड, सर्व्हरचे लोकेशन व सदरचा मेल कोठून आला हे उघड करुन गुन्हेगाराला शोधता येते.कोणताही सायबर ऍटॅक आयपी ऍड्रेसद्वारे शोधणे शक्य आहे. सुरक्षितता,सावधगिरी बाळगून इंटरनेटचा वापर करणे ही काळाची गरज आहे.

एथिकल हॅकिंग -

सायबर सुरक्षेमधील एक भाग म्हणजे एथिकल हॅकिंग. एखाद्या कंपनीने "आयएसओ 270001'ने प्रमाणित केल्याप्रमाणे सुरक्षा व्यवस्था साधली. ही व्यवस्था साधली आहे किंवा नाही हे तपासण्यासाठी एथिकल हॅकिंगचा वापर केला जातो. मी चोरी करण्याच्या उद्देशाने आलो, तर मला संगणक व्यवस्थेमध्ये प्रवेश मिळवता येतोय की नाही हे पाहण्यासाठी एथिकल हॅकिंग केले जाते. सायबर सुरक्षेची चाचणी यामुळे आपल्याला घेता येते. नेट बँकिंग, क्रेडिट कार्ड, एटीएम कार्ड असे आपले आर्थिक व्यवहार ज्या संगणकावरून करतो, ते व्यवहार सुरक्षित होताहेत किंवा नाही हे तपासायला हवे. अन्यथा आर्थिक सायबर गुन्हे वाढू शकतात.

आज जगतील प्रत्येक क्षेत्र, व्यवसाय, इंटरनेटने प्रभावित झालेला दिसतो. इंटरनेटच्या या मायाजालाचा हॅकर अतिशय क्लुप्तीने गैरवापर करतात. मध्यंतरी रशियाने जॉर्जियावर हल्ला करून हा देश आपल्या ताब्यात घेतला होता. मात्र, या हल्ल्याआधी रशियन इंटेलिजन्सच्या हॅकर्सने जॉर्जियाच्या संगणक प्रणाली, दूरसंचार यंत्रणा, प्रमुख सर्व्हर हॅक करून दळणवळण यंत्रणा या सायबर हल्ले करून आपल्या नियंत्रणाखाली आणल्यामुळे जॉर्जियावर प्रत्यक्ष हल्ला करणे रशियाला अगदी सोपे झाले. इराणची न्यूक्लियर वेपन सिस्टिममध्ये (क्षेपणास्त्र यंत्रणा) ‘स्टक्स नेट’ हा व्हायरस डाऊनलोड करण्याचा प्रयत्न झाला. अल कायदाच्या हॅकर्सचा यात हात असल्याचा संशय आहे तर अमेरिकेतील एका १२ वर्षीय मुलाने ‘नासा’ या अमेरिकेन अंतराळ संशोधन संस्थेतील न्यूक्लिअर वेपन्सची दिशा हॅकिंगद्वारे बदलली होती. व्यवसायावर सायबर हल्ला झाला तर त्याचा प्रतिकूल परिणाम अर्थव्यवस्थेवर होतो. म्हणूनच प्रत्येक आर्थिक संस्थेने अशा अडचणींवर मात करण्यासाठी सुसज्ज अशी सायबर यंत्रणा तयार ठेवून लगेचच कार्यवाही करावी.

ॲड. यज्ञेश कदम

CEO - चंद्रकांत कदम असोसीयेट

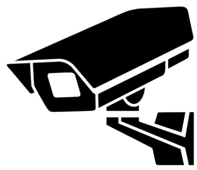
लेखक हे वसई व मुंबई न्यायालयात वकील म्हणुन कार्यरत आहेत व सायबर तज्ञ म्हणुन परिचीत आहेत.

डिजिटल समाजसेवा

सतीश भालेराव

"आई SS आई अग मला ग्राउंडवर सोडतेस ना?" अशी जेव्हा दुसरी हाक आरोह मोठ्या आवाजात मारत होता तेव्हा कुठे अरुंधती भानावर आली. हात हलवून तिने त्याला येते म्हणून सांगितले आणि तिने आवरायला घेतले. आठ वर्षाचा काळ तिच्या डोळ्यासमोरून भरकन पुढे निघून गेला. हाच आरोह तेव्हा लहान होता. आई हे एकच पालकत्व घेऊन त्याला मोठं करणं ही अरुंधतीची जबाबदारी होती कारण अर्णव बरोबरचे ते थोडेसेच मिळालेले सुगंधी क्षण आणि त्याचा तो आनंद या सर्वांचा आरोह हा प्रतीक होता. अर्णव आणि अरुंधती जोडा अगदी लक्ष्मीनारायणाचा शोभतो - असे सगळेजण कौतुक करत करत तो विवाह सोहळा संपन्न झाला. अर्णव आणि अरुंधती दोघेही हनिमूनला निघाली. "आई येतेस ना", पुन्हा हाक ऐकल्यावर मात्र अरुंधती पटकन खाली उतरली आणि आरोहला घेऊन गाडीवरून निघाली. त्याला ग्राउंड वर सोडून परत येताना मात्र मनातले विचार तिची पाठ सोडत नव्हते. नेहमीच्याच रस्ता होता, गाडी चालवण्याकडे तिचे लक्ष नव्हते, पण काळाच्या मनात काही वेगळेच होते. त्याच वळणाच्या चौकावर एकाएकी दुसऱ्या एका भरधाव येणाऱ्या वाहनाने अरुंधतीला धडक दिली. मोठा आवाज झाला आणि काय होते आहे ते समजायच्या आतच तिची शुद्ध हरपली. मागून येणाऱ्या एका तरुणाने ताबडतोब तिला उचलले. तिची गाडी बाजूला लावली. पाठीमागून येणाऱ्या एका रिकाम्या रिक्षामध्ये तिला कसेबसे बसवले आणि त्याने रिक्षा हॉस्पिटलला घ्यायला सांगितली. आपल्या सॅकमधून पाण्याची बाटली काढून अरुंधतीच्या तोंडावर त्याने पाणी शिंपडले पण तिला शुद्ध आली नाही. तेव्हा सर्वप्रथम त्याने त्या रिक्षाचा नंबर आरटीओच्या ट्रॅफिक हेल्पलाइनला कळवला आणि आपल्या मोबाईल मधून लोकेशन पण आरटीओ ला कनेक्ट केले. पुढील दोन मिनिटाच्या आत वायरलेस वरून सर्व चौकामध्ये ग्रीन झोन देण्यात आला आणि पाच ते सात मिनिटात त्याची रिक्षा अपघाता करता खास राखीव असलेल्या त्या हॉस्पिटलमध्ये पोहोचली. हे करत असताना त्याने त्या अपघाताच्या राखीव इस्पितळाला आपल्या मोबाईल फोनवरून पेशंटचे डिटेल्स पाठवले. हे त्याला शक्य झाले झाले कारण आपल्याजवळील स्मार्ट बेल्ट त्याने अरुंधतीच्या मनगटाला लावला आणि त्याचे कलेक्शन त्याने हॉस्पिटलच्या हेल्पलाइनला जोडले. पेशंट हॉस्पिटलमध्ये येईपर्यंत डॉक्टरांना पेशंट ची सर्व हिस्ट्री आणि आवश्यक ती पूर्ण माहिती मिळाली.

ताबडतोब उपचार सुरू झाले दरम्यानच्या काळात त्या तरुणाने पेशंटचे रजिस्ट्रेशन केले अरुंधतीच्या पर्समध्ये तिथे आधार कार्ड मिळाले. त्यावरून सर्व माहिती हॉस्पिटलच्या प्रशासनाला मिळाली आणि त्या तरुणाने आपली माहिती म्हणजे नाव संग्राम सरपोतदार, फोन नंबर इत्यादी नोंद केली, अरुंधतीच्या आधार कार्ड वरून लिंक असलेल्या तिच्या राष्ट्र माहिती कोषामधून इतर नातेवाईकांचे दूरध्वनी क्रमांक आले. संग्रामने ताबडतोब त्यांच्याशी संपर्क साधला आणि तासाभराच्या आत अरुंधतीचे सासू सासरे दवाखान्यात दाखल झाले. काही वेळातच डॉक्टरांनी अरुंधतीला शुद्ध येत असल्याचे सांगितले. बघता बघता संध्याकाळ झाली. अरुंधतीच्या आई-बाबांचा निरोप घेऊन संग्राम जायला निघाला. तेव्हा अरुंधतीने त्याचे सर्व संपर्काचे दूरध्वनी क्रमांक बाबांकडे लिंक करायला सांगितले व आपल्याही मोबाईल मध्ये ते लिंक करून घेतले. काही दिवसांनी अरुंधती घरी आली पण इतकी तातडीची मदत आपल्याला देणार संग्राम याचे तिला आभार मानायचे होते. कारणही तसेच होते संग्रामने केवळ हॉस्पिटल पुरतीच मदत केली नाही तर परत येताना त्यांनी तिची गाडी योग्य प्रकारे पोलिसांच्या हवाली केली. गाडीमधील पेपर्स बघून त्याने स्वतःच्याच मोबाईलवरून गाडीचे फोटो पाठवून इन्शुरन्स क्लेम पण केला. आरटीओ ऑफिस मध्ये त्याचा मोबाईल लिंक झालेलाच होता. तेव्हा त्यांनी सीसीटीव्ही फुटेज ची रिक्वेस्ट टाकली.



अपघाताच्या क्षणाचे सर्व फोटो त्याने नजीकच्या सर्व पोलीस स्टेशनला पाठवले. त्यामध्ये ज्या वाहनाने धडक दिली त्या वाहना चा रजिस्ट्रेशन क्रमांकही मिळाला. रात्री बऱ्याच उशिरा पर्यंत त्या वाहनाचा मालक मिळाला नाही पण पण शेवटी त्याच्याशी भेट झालीच परिसरचा तक्रार पंचनामा करून संग्राम आवश्यकते सर्व कागदपत्र घेऊन घरी गेला दुसऱ्या दिवशी त्याने अरुंधती ची गाडी पोलीस स्टेशन मधून सोडवून दुरुस्ती करता जमाही केली आणि तो नुकसान भरपाईचे मिळालेले पैसे देण्याकरता अरुंधती च्या घरी गेला. अरुंधतीला नुकताच घरी येण्याचा परवाना मिळाला होता त्यामुळे तिलाही बरे वाटले. मनापासून संग्रामचे आभार मानले संग्रामने डिजिटल स्वरूपात व डिजिटल डिझास्टर मॅनेजमेंट चा वापर करून ही परिस्थिती व्यवस्थितपणे हाताळली.

याचेही अरुंधतीला कौतुक वाटले पण तिच्या बाबांनी व अरुंधतीने ते पैसे घेण्यास मात्र नकार दिला व जेव्हा गाडी दुरुस्त होईल तेव्हा ती आणून देण्याची फक्त विनंती केली. संग्राम याला ते पैसे म्हणजे एक ओझेच झाले होते सध्यातरी एकूणच अरुंधती च्या घरची परिस्थिती पाहून संग्रामने तात्पुरते ते पैसे आपल्याकडेच ठेवले पण त्याला त्याचे मन शांत बसू देत नव्हते.

एक-दोन दिवसातच संग्रामने अरुंधतीचे नाव बदलून ही सर्व हकीगत एका ब्लॉग वर टाकली. नंतर दोन-तीन दिवस असेच गेले. काही दिवसांनी तो ब्लॉग वाचून संग्रामची जुनी मैत्रीण समीरा त्याला भेटायला आली. तिने तो सर्व घटनाक्रम लक्षात घेतला. सायकॉलॉजी ची विद्यार्थिनी असलेली समीरा यातून काहीतरी वेगळं शोधत होती. कारण समीराने घटनास्थळाचे रेकॉर्ड केलेले फुटेज पुन्हा पाहिले. अरुंधतीचा चेहरा क्लोज-अप मध्ये पण पाहिला. आणि तिला जाणवले ते म्हणजे अरुंधतीचा मानसिक ताण आणि यावर तिने संग्रामशी चर्चा केली. अरुंधतीला पुन्हा भेटण्याचे ठरवले. पण यावेळी मात्र संग्राम, समीरा आणि अरुंधती घरी न भेटता एका छान निसर्गरम्य ठिकाणी भेटली तेव्हा हळूहळू अरुंधती बोलायला लागली. काही वेळातच अरुंधती चा बांध फुटला आणि ती रडू लागले समीराने तिला शांत केले. तिथे मनमोकळं बोलणे होण्यासाठी तिने अरुंधतीला मोजकेच प्रश्न विचारले.अरुंधतीने आठ वर्षांपूर्वीचा तो घटनाक्रम पुन्हा एकदा जागा केला. लग्नानंतरचे ते कोवळे दिवस आणि हनिमूनच्या दिवसातली ती बेधुंद वागणूक सारं काही मनात साठवून हनिमूनच्या शेवटच्या दिवशी परत घरी येण्याकरता अरुंधती व अर्णव निघाले. पण काळ वेगळ्याच ठिकाणी अर्णवला घेऊन जात होता. एका सुंदर मनमोहक स्पॉटवर आपला सेल्फी काढायचा राहून गेला हे जाणवल्यावर अरुंधतीला घेऊन अर्णव त्या कड्यापाशी गेला. आपल्या मागील सुंदर निसर्गाच्या सौंदर्यावर आपला सेल्फी आपण किती छानपणे अपलोड करू व आपल्याला भरपूर लाईक मिळतील या विचारात अर्णव जास्तीत जास्त निसर्ग आपल्या सेल्फीच्या चौकटीत आणण्याचा प्रयत्न करत होता. अर्णव जास्तच धोकादायक परिस्थितीत कड्याच्या जवळ होता. अरुंधती त्याला ओरडून सांगत होती पण अर्णव सेल्फी क्लिक करण्याच्या नादात किंचित मागे गेला. सेल्फी क्लिक झाली पण अखेर त्याचा पाय घसरला आणि तो मागे असलेल्या प्रचंड खोल दरीत जाऊन कोसळला. होत्याचे नव्हते झाले. अरुंधती ओरडून ओरडून दमली. दरीतून काही आवाज येत नव्हता. पोलिस, फायर ब्रिगेड सर्व प्रकार प्रकार झाले. अरुंधतीचे बाबा सर्वजण येऊन तिला घेऊन गेली आणि कायद्याप्रमाणे पोलिसांनी काही विशिष्ट कालावधीनंतर अर्णवला मृत घोषित केले. अर्णव आपली आठवण मागे ठेवून गेला. अरुंधतीला दिवस गेले आणि नंतर आरोह चा जन्म झाला. हेच सारे अरुंधतीला आठवत होते. त्या नादातच तिला गाडीवरून परत येताना अपघात झाला.

हे सर्व ऐकून संग्राम आणि समीरा सुन्न होऊन झाली संग्रामच्या धाडसी वृत्तीला आणि समीराच्या दुसऱ्याच्या मनाचा ठाव घेणाऱ्या वृत्तीला जणूकाही हे एक प्रकारचे आव्हानच होते. दोघांनाही आठ वर्षापूर्वी काय घडले असावे, याची उत्सुकता शांत बसू देत नाही. एकीकडे अरुंधती व इतरांनी नाकारलेले पैसे हातात होते आणि पोलिसांनी केवळ कायद्याचा आधार घेऊन अर्णवला मृत घोषित केले होते केले होते. सारेच काही मनाला क्लेशदायक आणि न पटणारे होते. काही दिवसांनी आपल्या कामांमधून थोडीशी सवलत घेऊन संग्राम व समीरा आठ वर्षांपूर्वीच्या त्या हनिमूनचे ठिकाण आणि त्याच स्पॉटवर जाऊन पोहोचले. खरोखरीच काळजाचा ठाव घेणारी जीवघेणी ती दरी होती. माणूस त्यात पडल्यानंतर जिवंत सापडणं केवळ अशक्य होते. पण तरीही कुठेतरी मनामध्ये एक छोटासा आशेचा किरण होता म्हणून संग्राम आणि समीरा त्या छोट्याशा गावामध्ये वेगवेगळ्या वेळी अनेक ठिकाणी अनेक माणसांना सहज म्हणून गप्पा मारत भेटत होते. या सगळ्यात महत्त्वाचा दुवा होता तो म्हणजे त्या हॉटेलचा जुना सेवक आणि त्यावेळी माहिती सांगणारा त्या निसर्गरम्य ठिकाणाचा तो गाईड या दोघांना कसे बोलते करावे हाच एक प्रश्न समीर आणि संग्राम यांना भेडसावत होता एक-दोन दिवस राहिल्यानंतर असे समजले कि तो जुना गाईड आता खूप वयस्कर झाला आहे आणि त्याच गावात एका छोट्याशा घरातो. संग्राम आणि समीराने त्याची भेट घेतली व त्याला आत्तापर्यंत घडलेल्या सर्व घटनां सविस्तर सांगितल्या . त्याने पण त्या खोल दरीमध्ये कसे जाता येईल व कसा शोध घेता येईल याचा थोडासा सल्ला त्या दोघांना दिला पण केवळ जीवावर उदार होऊनच हे काम तुम्हाला करावे लागेल असा धोक्याचा इशाराही त्यांनी दिला. आता प्रश्न होता हॉटेलच्या त्या जुन्या नोकराचा कारण तो एकच व्यक्ती असा होता कि ज्याला सर्व दऱ्याखोऱ्यांची पूर्ण माहिती होती. संग्राम व समीराचे वास्तव्य त्याच हॉटेलमध्ये असल्याने हळूहळू त्या जुन्या सेवकाची त्यांच्याशी मैत्री झाली. त्या दरीच्या खोल खोल भागात एक आदिवासी जमात राहते असे त्याने सांगितले पण तिथे जाणे व त्या जमातीशी संबंध जोडणे फार अवघड होते. तरीदेखील त्यावेळचा तो जुना गाईड, हॉटेलचा सेवक, संग्राम आणि समीरा यांनी एका भल्या पहाटे त्या दरीमध्ये उतरण्याचा प्रयत्न सुरू केला.

सर्व प्रकारच्या इलेक्ट्रॉनिक्स माध्यमांचा त्यांनी वापर केला. दरीमध्ये उतरण्याच्या आधीच अत्याधुनिक अशी जीपीएस ची साधने त्यांनी दरीमध्ये खोल सोडली होती. त्यामधून त्यांना चांगलेच सिग्नल्स मिळत होते आणि हे सर्व करताना त्यांनी ही सर्व माहिती तेथील स्थानिक पुढाऱ्यांना, प्रशासनाला आणि पोलिसांना पण दिली होती. त्यामुळे घाबरण्याचे तसे काहीच कारण नव्हते पण शेवटी एका अस्थिर आणि आणि अनभिज्ञ कामाकरता ते निघाले. दरी खोल असल्यामुळे साधारणपणे दुपारच्या तीन साडेतीनच्या वेळीच तेथे अंधार जमा होत असे.

सर्व प्रकारची शस्त्रे स्वतः जवळ घेऊन घेऊन अतिशय सुरक्षितपणे त्यांनी ती रात्र त्याच दरीमध्ये कशीबशी काढली. दुसऱ्या दिवशी दिवस उजाडताच ते आणखीन खाली उतरू लागले. त्याच वेळी आदिवासी जमातीची मोठी आरडाओरड त्यांना ऐकू आली. त्यावरून हॉटेलच्या सेवकाने त्यांना समजून सांगितले की त्या जमातीला आपण हल्ला करण्यास येत आहोत आहोत असा संशय आलेला आहे त्यामुळे त्यांनी आरडाओरड केली आहे. आदिवासींच्या इंटरनेटवर केलेल्या सर्व जमातीच्या भाषेच्या अभ्यासावरून संग्रामने त्यांना आपण शिक्षण व आरोग्य या विषयावर मदत करण्यास येत आहोत असे त्यांच्याच भाषेत लिहून ते कागद कसेबसे त्यांच्यापर्यंत फेकले. समीराने तिच्या मानसशास्त्रीय भाषेमध्ये मित्रत्वाची जी काही सर्व स्केचेस तिला काढता आली ती काढून तिने ती स्केचेस आदिवासींच्या जमातीकडे फेकली. तेव्हा कमीत कमी विरोध आणि आरडाओरड त्या जमाती कडून संपला व एक लहान मुलगा पांढरी फुले घेऊन समोर आला त्या वेळी अक्षरशः सगळ्यांच्या डोळ्यातून आनंदाश्रू वाहिले कारण पांढरी फुले ही मैत्रीचे प्रतीक सांगतात. प्रत्युत्तरादाखल पुन्हा संग्रामने काही लिहून आणि समीराने चित्र काढून त्यांच्याकडे पाठवली. आता मात्र सर्व आदिवासी जमातीची लोक त्यांना पटापट मदत करण्याकरता पुढे आली. त्यांनी त्यांचा दरी उतरण्याचा खडतर प्रवास अतिशय सुलभ केला. सहज म्हणून समीर आणि संग्रामने वरती पाहिले तर आकाशही दिसत नव्हते. याचा अर्थ आपण जगापासून किती दूर आलो आहोत हे त्यांना जाणवले. त्याचवेळी संग्राम अतिशय काळजीपूर्वकपणे सर्व जीपीएस यंत्रणेला आपण सुरक्षित असल्याचे व आदिवासींची मदत मिळत असल्याचे योग्य संदेश पाठवत होता आणि त्यामुळे दरीच्या वरच्या बाजूस असणाऱ्या सर्व यंत्रणेला दिलासा मिळाला. कधीही न घडलेला असा हा प्रसंग तिथे सर्वजण अनुभवत होते. त्या संध्याकाळी रात्री समीरा व इतर आदिवासींच्या जमातीत राहिले. दुसऱ्या दिवशी सकाळी त्यांची भाषा समजून घेणे हे सगळ्यात महत्त्वाचं काम संग्रामने जीपीएस व इंटरनेटचा वापर करून सुरू केले. इतक्या खोल दरीमध्ये कोणत्याही प्रकारची रेंज मिळणे अशक्य होते पण जीपीएस मध्ये घडलेल्या नवीन तंत्राचा वापर केल्यामुळे व स्थानिक प्रशासनाने त्यांच्या शासकीय सेवेचा पण वापर करून दिल्यामुळे हे सर्व शक्य झाले. एक दिवसातच आदिवासींना सर्व प्रकार समजला अजूनही आपण कोणाला शोधायला आलो आहोत हे समीर, संग्रामने त्यांना सांगितले नाही. त्यांना आरोग्य आणि शिक्षणाची जास्तीत जास्त जास्त चांगली माहिती देण्याचा प्रयत्न केला त्या चौघांची शोधक नजर कोणी अनोळखी माणूस तिथे दिसतोय का हेच शोधत होती साधारणपणे दुपारच्या जेवणाच्या वेळी एक लहान मुलगा जेवणाची थाळी घेऊन काहीस दूर जाताना दिसला हॉटेलच्या सेवकाने आदिवासींच्या भाषेमध्ये त्याच्याशी गप्पा मारत तो जेथे जात आहे तेथ पर्यंत गेला आणि काय आश्चर्य तेथे ज्या माणसाला तो छोटा मुलगा जेवण देत होता, तोच माणूस आठ वर्षापूर्वी दरीत कोसळला होता, हॉटेल मधून निघताना अर्णवचे मिळालेले

सर्व फोटो खिशातनं काढून त्याने त्याची खातरजमा पण केलीपण इतक्यात हे सर्व अर्णवला कसे सांगावे हे न समजल्यामुळे त्या छोट्या मुलाबरोबरतो परत आला आणि शांतपणे समीरा, संग्राम यांना त्यांनी ही माहिती दिली आता हळूहळू त्यांनी अर्णवला ज्या बाजूला ठेवले होते त्या बाजूला आपला मुक्काम हलवला. आणखीन एक दिवसात त्यांनी आपली काहीही ओळख न देता त्या अर्णवशी मैत्री केलीआणि हे करताना अर्णवचे त्यांनी फोटोही काढले. संग्राम ने ते फोटो ताबडतोब इंटरनेटवरून पोलीस यंत्रणेला पाठवले आठ वर्षांपूर्वीचे सर्व रेकॉर्ड पोलिसांनी संगणकामध्ये आधीच तयार ठेवले होते त्यांनी डोळ्याच्या बाहुल्या, चेहऱ्याचा आकार संगणकातील रेकॉर्ड बरोबर खात्री करून घेतले आणि ही तीच व्यक्ती आहे याचा संदेशही संग्राम कडे पाठवला पण प्रश्न असा होता की आता हे सर्व अर्णवला विचारायचे कसे तेव्हा समीराने तिच्या मानसशास्त्रीय अभ्यासाचा कस लावून अर्णवला त्याच्या पूर्व आयुष्यामध्ये घडलेल्या घटनांचा आढावा घेण्यास उद्युक्त केले. तरीदेखील त्यांना हवी असलेली माहिती मिळत नव्हती. तेव्हा संग्रामने डिजिटल डिझास्टर मॅनेजमेंट मधील एक अतिशय प्रगत असा स्मार्ट बेल्ट अर्णवच्या मनगटाला एक खेळणं आहे असं सांगून बांधला व त्याचा संपर्क त्याने अर्णवच्या हॉस्पिटलच्या सेंट्रल रेकॉर्ड सिस्टिमशी जोडला. तेथील डॉक्टरांशी संपर्क साधून त्याने अर्णवची सध्याची शारीरिक परिस्थिती जाणून घेतली. त्याला धक्काच बसला कारण अर्णवला काहीही म्हणजे काहीही आठवतच नव्हते. अर्णव सापडला तर खरा पण अर्णवला तु अर्णव आहेस हे कसे पटवून द्यायचे आणि आदिवासींची परवानगी काढून अर्णवला या जमातीच्या बाहेर कसे न्यायचे हा एक मोठा प्रश्न सगळ्यांसमोर आता उभा राहिला राहिला तेव्हा समीराने ही सर्व केस न्यू जर्सीमध्ये संशोधन करत असलेल्या तिच्या जेनी नावाच्या मैत्रिणीला इंटरनेटवरून पाठवली. तिच्याकडून मिळालेल्या माहितीच्या आधारे तिने आदिवासींच्या मानसशास्त्र प्रमाणे काही ठराविक लोकांना शिक्षण व आरोग्याचे आणखीन काही नवीन शिक्षण घेण्याकरता सर्वसाधारण जगामध्ये जावे लागेल असे सुचवले ते आदिवासींच्या प्रमुखाला पण पटले त्यांनी आदिवासींच्या काही तरुणांचा, मुलींचा व इतरांचा एक ग्रुप बनवला अर्थातच समीर आणि संग्रामने त्या ग्रुपमध्ये अर्णवला सामील करण्याची विनंती केली. त्यांचा अंदाज खरा ठरला आदिवासी जमातीच्या प्रमुखाने लगेचच " अहो त्याला कशाला घेऊन जात आहे , तो तर इथं पडला होता मरता मरता वाचला , त्याचा काय उपयोग आहे आम्हाला, तो तर आमची भाषा पण समजत नाही, त्यामुळे त्याला घेऊन जाऊ नका, त्याच्याऐवजी आमच्यातल्या एका एका तरुण मुलाला घेऊन जा, म्हणजे तो नवीन काहीतरी शिकून येथे मदत करेल, हाच संदर्भ वापरून समीर आणि संग्रामने आठ वर्षांपूर्वीची सर्व घटना त्यांच्याकडंन समजून घेतली . घडलं होतं ते सारे धक्कादायकच होतं अर्णव जेव्हा पडला तेव्हा तो खोल दरीत पडला पण तो चक्क जमिनीवर पडला नव्हता तर दोन-तीन झाडांच्या फांद्या जेथे एकत्र आल्या होत्या तेथे अलगत गादीवर झोपावे तसा येऊन पडला होता

आणि त्याची शुद्ध गेली होती जेव्हा अर्णवला जाग आली तेव्हा तो ओरडू लागला त्याचे ओरडणे ऐकून खालच्या आदिवासी जमातीतीलकाही लोकांनी त्याला त्यांच्याकडे आणून झोपवले अनेक दिवस पूर्ण झोपूनच होता आणिनंतर जेव्हा त्याला पूर्ण जाग आली आली तेव्हा त्याची स्मृती गेलेली होती.तेव्हापासून त्या आदिवासी जमातींना त्याचा सांभाळ केला होता हे सर्व समजल्यावर आताकाय करावे खरे सांगावे की नाही सांगावे अशा द्विधा मनस्थितीत संग्राम आणि समीराअसताना त्यांनी त्यांच्याजवळील संग्राम चे पूर्वीचे फोटो त्या जमातीतील सर्वांनादाखवले त्यांना पण ते सगळे आश्चर्यकारक होते. एका चांगल्या कामाकरता हे लोकइतक्या खोल आलेले आहेत यावर त्यांचा विश्वास बसला आणि त्यांनी त्यांच्या दहाजणांच्या ग्रुप बरोबर या आठ वर्षापूर्वी सापडलेल्या व्यक्तीला म्हणजे अर्णवला परत घेऊन जाण्याची परवानगी दिली.त्यानंतर सर्व घटना अर्थातच तंत्रज्ञानाचा वापर करून अतिशय वेगाने घडल्या. आदिवासींना शासनाच्या सर्व सेवा-सुविधांचा तेथील स्थानिक शासनाने पूर्णपणे फायदा करून दिला व त्या जमातीचे खालच्या दरीतून सर्वसाधारण जगामध्ये प्रस्थापन केले हे सर्व करत असताना आता अर्णवला आपण कोठे जात आहोत हे कसे सांगायचे हे एक नवीन कोडे त्याच्यासमोर पडले. पुन्हा एकदा संग्रामचे तंत्रज्ञान आणि समीराचे मानसशास्त्र यांनी एकमेकांची साथ दिली व आपण पण आदिवासींकरता आणखीन काय करता येईल हे वरिष्ठ शासनाकडून समजून घेण्यासाठी शहरांमध्ये जात आहोत असे कसे बसे अर्णवला सांगून ते अर्णवला घेऊन त्याच्या घरी आले अर्णवला पाहून अरुंधतीच्या आनंदाला तर पारावारच उरला नाही पण तो आनंद काही काळच टिकला कारण पुढच्याच क्षणाला अर्णव कोणालाच ओळखत नाही हा धक्का अरुंधतीला सहन करावा लागलाअर्णवला पण हळूहळू समीराने त्याच्या मनाचा अभ्यास करत करत त्याला याच घरात इतरां बरोबर राहणे योग्य व सुरक्षित आहे हे समजले. त्याच वेळी अरुंधती आणि आरोह यांनी आपल्या सर्व पूर्वीच्या आयुष्याची दृश्य चित्रे आणि इतर संदर्भ अर्णवला दाखवली आपलेच फोटो या सगळ्या व्यक्तींबरोबर दिसत असल्यामुळे अर्णव पण काहीसा त्यांच्या मध्ये समरसून गेला काही दिवसांनी अर्णव सोडून इतर सर्वांनी, काही तज्ञ डॉक्टरांनी यावर सविस्तर चर्चाही केली
व्हिडिओ कॉन्फरन्सिंगद्वारे इतरांशी पण सल्लामसलत केली, यावरून एक गोष्ट निश्चित झाली की पुन्हा एकदा अर्णवला घेऊन त्याच गावांमध्ये जाऊन राहणे आवश्यक होते. त्याप्रमाणे अरुंधती अर्णव समीरा संग्राम सगळेजण पुन्हा त्याच गावांमध्ये जाऊन राहिले एक-दोन दिवसांनी अर्णवला काहीही कल्पना न देता अरुंधती पुन्हा त्याच ठिकाणी सेल्फी काढण्याकरता ती दोघे आली हे करत असताना सर्व काही आठ वर्षापूर्वीची आहे हे भासवण्याचा पूर्णपणे प्रयत्न झाला. इतकेच काय पण अरुंधतीने त्याचवेळीची साडी तेव्हा नेसली होती आणि अर्णव, अर्णव पडशील असे जोरात ओरडून अरुंधतीने अर्णवला पुन्हा

एकदा भानावर आणले. त्याचा परिणाम योग्य तोच झाला हळूहळू अर्णवला डोक्यामध्ये मुंग्या आल्यासारखे झाले त्याला थोडे थोडे पूर्वीचे आठवू लागले लागले सर्वप्रथमत्या ने ओळखले ते त्या हॉटेलच्या नोकराला कारण तो एकच चेहरा अरुंधती व्यतिरिक्त त्याने शेवटचा पाहिलेला होता आणि नंतर शास्त्रीय संकल्पना, औषधे इंटरनेट तंत्रज्ञान या सर्वांचा वापर करून अवघ्या दहा दिवसातच अर्णवला त्याचेपूर्वीचे आयुष्य पुन्हा मिळाले. हे सगळे शक्य झाले ते केवळ संग्राम आणि समीराच्या अथक प्रयत्नामुळे. त्यांनी योग्य प्रकारे वापरलेले विज्ञान आणि तंत्रज्ञान यांच्या संयुक्त प्रयत्नातूनच हे यशमिळाले. प्रश्न येथे संपत नव्हते, आठ वर्षाचा कालावधी फार मोठा होता, अर्णवला सध्या त्याच्या मेंदूला पटकन कोणतेही नवीन काम घेणे व ताण देणे शक्य होत नव्हते यावरही पुन्हा एकदा संग्रामने मदत केली त्याच्या जवळ असलेले पैसे एक ओझे म्हणून राहिलेले होते त्यातून संग्रामने शासनाच्या आदिवासी विभागाशी संपर्क साधून " अर्णव फाउंडेशन" ही संस्था त्यागावात स्थापन केली . त्याचे सर्व अधिकार अर्णव आणि अरुंधतीला देऊन टाकले त्या गावाच्या दहा किलोमीटरच्या परिसरात असलेल्या सर्व आदिवासी जमातींना शिक्षण व आरोग्य मोफत देण्याकरता हे फाउंडेशन कटिबद्ध आहे हे त्यांनी शासनाला व स्थानिक गावकऱ्यांना समजून सांगितले संग्रामने तर कमालच केली अर्णव फाउंडेशन च्या वेबसाईटवर त्याने अर्णव फाऊंडेशनच्या जन्माची ही कथा अतिशय बोलक्या आणि भावनिक शब्दात मांडली अर्थातच त्याला जोड होती समीरच्या मानसशास्त्रीय संकल्पनांची.

या सर्वांना प्रतिसाद सगळीकडून मिळाला मदतीचा ओघ आला आणि थोड्याच दिवसात अर्णव फाउंडेशनचा हा वटवृक्ष फार मोठ्या स्वरूपात सर्व आदिवासी जमातींना एक आधारस्तंभ बनून राहिला कोठे सुरुवात झाली आणि कोठे शेवट झाला. अर्णव फाउंडेशनची वाटचाल खूपच प्रगतशील झाली दहावर्षे कशी निघून गेली हे कोणालाच कळले नाही दरम्यानच्या काळात संग्राम आणि समीराच्या या धडाडीच्या आयुष्यात विवाहबंधन झाले आणि एका धडाकेबाज छोट्या बाळाचे आगमन पण घडले सर्वजण आज अर्णव फाऊंडेशनच्या दहाव्या वर्धापन दिनानिमित्त एकत्र जमले होते तेथील स्थानिक प्रशासनाने, गावकऱ्यांनी व सर्व आदिवासी बांधवांनी एक छान समारंभ तेथे योजला होता.त्या परिसराचे पालकमंत्रीही आवर्जून त्या कार्यक्रमास उपस्थित होते. सर्व कार्यक्रमसंपत येताना पालकमंत्र्यांनी एक छानशी भेट सर्वांना दिली. त्यांनी डिजिटल डिझास्टर मॅनेजमेंट या संस्थेची स्थापना याच गावात समीरा आणि संग्रामच्या अधिपत्याखाली होईल अशी घोषणाही केली. त्या दोघांना डिजिटल कपल म्हणून त्यांचा सन्मान केला. हे सर्व पाहत असताना अरुंधती आणि अर्णव यांना अश्रूंना काय चव असते हे कळलं कारण येणारे अश्रू हे खारट असते तरी ते आनंदाचे होते. ती गोड दोन मुले - आरोह आणि समीरा, संग्राम चा अद्वैत- हे दोघेही त्यांच्या समोर एक पुढील भविष्य म्हणून उभे होते. पुन्हा आरोह म्हणत होता," आई अग समारंभ संपला निघायचं " त्याच्या त्या हाक मारण्यामुळे अरुंधती भानावर आली व ती गाडीत जाऊन बसली आठवणींचा पटल हळूहळू दूर गेला पण पण माणसं मात्र जवळ आली त्यांच्या सर्वांबरोबर भावी आयुष्यात अर्णव फाऊंडेशनची अशीच वाटचाल करण्याकरता त्यांनी मनोमन देवाची प्रार्थना केली.

सतीश भालेराव (नाशिक)

satishvbhalerao@gmail.com

दिवाळीच्या
हार्दीक शुभेच्छा
Shruti Kothawade

सोशल खाजगीपण

विवेकराज ठाकूर

फेसबुक, व्हॉट्सॲप व इतर माध्यमांतून आपण जगाशी जोडले गेलो आहोत. आपले रोजचे जगणेच इंटरनेटशी जोडले गेले आहे. आर्थिक व्यवहारांसाठी मोबाईल बँकींग, नेट बँकींगचा आपण वापर करत आहोत. पण त्यातून धोकेही तितक्याच मोठ्या प्रमाणावर निर्माण होत आहेत. याची अनेक उदाहरणे आपल्यासमोर घडत आहेत. ‘सायबर गुन्हेगारी’ या नव्या डोकेदुखीने सर्वांनाच चक्रावून टाकले आहे. आपल्या मोबाईल, फेसबुकवरील डेटावर विशिष्ट व्यक्तींचे लक्ष आहे आणि तो पळवून गैरवापर करणे सुरू आहे. आपल्या खाजगीपणांवर यामुळे गदा आली आहे.

‘डेटा मायनिंग’ हा नवीन धोका सर्वांना भेडसावत आहे. सोशल माध्यमांवरील आपल्या व्यक्तिमत्त्वाचे वैशिष्ठ शोधून त्याचा गैरवापर केला जातो. हे ‘केम्ब्रिज ॲनालॅटीका’ संस्थेच्या कारभारावरून जगाला लक्षात आले आहे. ह्या संदर्भात NETFLIX वरील THE GREAT HACK ही फिल्म नक्की बघावी. ती सायबर सिक्युरीटी आणि डेटाब्रिच याविषयी डोळ्यात अंजन घालणारी आहे.

यासाठी भारताने ‘डेटा प्रोटेक्शन लॉ’ची अंमलबजावणी करणे तातडीणे गरजेचे आहे. तरच हे रोखण्यास मदत होईल. त्याचबरोबर सोशल माध्यमे काळजीपूर्वक हाताळण्याची गरज आहे व त्याबाबत जनप्रबोधन करण्याची आवश्यकता आहे. शेवटी खाजगीपण हा देखील तुमचा मुलभूत हक्क आहे असे मला वाटते.

विवेकराज ठाकूर

अध्यक्ष, सामुदायिक रेडिओ संघटना
(पश्चिम विभाग - महाराष्ट्र, गुजरात, राजस्थान आणि गोवा)

टेक्नोसॅव्ही होतांना ...

अनिल सुमति बागुल

नव्वदीच्या वा नंतरच्या काळात जन्मलेल्या पिढीचं मस्त चालू असतं, नवनवीन 'गॅझेट्स' हाताळणं. नवनवीन ऍप वापरणं, नवीन टेक्नॉलॉजिशी जमवून घेणं. इ- कॉमर्सचे व्यवहार सफाईने करणं. पेटीएम, पे-फोन, गुगल-पे, ओला, उबर, स्वीग्गी, अमेझॉन इ. साऱ्या ठिकाणी डिजिटल मनी अगदी 'इझ'मध्ये फिरवत असतात. नेट बँकिंग, ऑन लाईन बिल भरणे, मनी ट्रान्स्फर इ. बँकेच्या माध्यमातून होणारे व्यवहार म्हणजे त्यांच्या दृष्टीने डाव्या हाताचा मळ !

आताची 'जनरेशन' जन्माला आल्यावर, पीसी, लॅपि, पीडी, किंडल असे सारे शब्द अंगाईगीतासारखे ऐकत असते. त्यांच्या आयांना म्हणा, कुठलं अंगाईगीत यायला. पण ह्याच साऱ्या गोष्टी, सत्तरीच्या, ऐंशीच्या दशकात जन्मलेल्या पिढीच्या दृष्टीने 'टफ टास्क'. वयाच्या पंचविशीत पहिल्यांदा कोंपुटर पाहिलेला. तो ही भला मोठा डेस्कटॉप. त्यापूर्वी कधीच कॉम्पुटरशी संबंध आलेला नाही. त्यानंतर आला 'पेजर'. नवीन जनरेशनला हा प्रकार, बहुधा माहिती नसणार ! मग ते ते फ्लॅट स्क्रीन मॉनिटर, टीव्ही आले. पूर्वीचे साधे मोबाईल, 'नोकिया' कंपनीचे, ह्या जनरेशनने मात्र पहिल्यांदा हाताळले. त्याचा उपयोग फक्त कॉल करणे व स्वीकारणे इतकाच. रेंजची फारच बोंब असायची. मग खूप वर्षांनी ते 'नोकिया' कंपनीचे हँडसेट जाऊन, आधुनिक 'अन्ड्रॉईड' तंत्रज्ञानाचे 'सॅमसंग' वगैरे कंपनीचे हँडसेट बाजारात आले. आणि नोकीया कंपनी हे नवीन तंत्रज्ञान वापरात नसल्याने इतर कंपन्यांच्या स्पर्धेत बरीच मागे पडली, मार्केटमध्ये आऊटडेटेड तंत्रज्ञान वापरल्याने. जगण्याच्या मार्केटमध्ये आऊटडेटेड होऊन गायब व्हायचं नसेल तर, नवीन तंत्रज्ञान आत्मसात करावेच लागेल. त्याला आपलंसं करावंच लागेल, 'टेक्नोसॅव्ही' व्हावं लागेल, हाच ह्या जुन्या जनरेशन करता धडा.

पण हे टेक्नोसॅव्ही होतांना ... थोडं काळजीपूर्व, थोडं सावधपणे. सोशल अकाउंट हॅक होणं, बँकेच्या अकाउंट मधून पैसे काढून घेतले जाणं, असे प्रकार आजूबाजूला घडतांना आढळतात. मागच्यास ठेच, पुढचा शहाणा ह्या न्यायाने काही गोष्टीत सजग असणं खूप आवश्यक. 'डूज आणि डोन्ट डूज' ह्यातली नियमावली नेमकेपणाने 'फॉलो' करणे हा पहिला नियम! जस की आपला ई-मेल अकाउंटचा ‘पासवर्ड’ कुणाशी शेअर न करणं. ‘एटीएम पिन’ कुणालाही नं सांगणं. मोबाईल सेट वऱ अपरिचित ‘ॲप’ डाउनलोड न करणं. इ. गोष्टी प्राथमिक गरजेच्या. शेवटी एकचं सांगणं, टेक्नोसॅव्ही होतांना ...

सावध हरणी सावध गं
करील कुणीतरी पारध गं

हे आपणाला सर्वांना परिचित असलेलं गाणं लक्षात असू द्या, म्हणजे झालं.

अनिल सुमति बागुल

प्राचार्य, धन्वंतरी इन्स्टिटयूट ऑफ डिझाईन अँड टेक्नॉलॉजी
नाशिक

anilbagul1968@gmail.com

आजची सायबर सुरक्षा

प्रितेश आहिरे

तंत्रज्ञानाच्या प्रगतीमुळे माणूस त्याच्या सर्व गरजा पूर्ण करण्यासाठी इंटरनेटवर अवलंबून आहे. एक ठिकाणी बसून इंटरनेटने माणसाला प्रत्येक गोष्ट सहज शक्य करून दिली आहे. सोशल नेटवर्किंग, ऑनलाईन शॉपिंग, गेमिंग,बँकेचे व्यवहार , ऑनलाइन अभ्यास, ऑनलाइन नोकरी, माणूस विचार करू शकणारी प्रत्येक गोष्ट इंटरनेटच्या माध्यमातून करता येते. इंटरनेट जवळजवळ प्रत्येक क्षेत्रात वापरली जाते. इंटरनेटच्या विकासासह आणि त्याच्या संबंधित फायद्यांमुळे सायबर गुन्ह्यांची संख्या पण वाढली आहे. सायबर गुन्हे वेगवेगळ्या स्वरूपात केले जातात. सायबर गुन्हे घडण्याचे प्रमाणही दिवसेंदिवस वाढत आहे. तरुण पिढीचा कल हा हॅकिंग क्षेत्रात जास्त वाढतो कारण त्यांना ते जास्त आकर्षित होत.सायबर गुन्ह्यांसाठी अटक केलेले जास्तीत जास्त गुन्हेगार 18-30 वयोगटातील होते.सायबर गुन्ह्यांना बेकायदेशीर कृत्य असं म्हटले जाते.ज्यामध्ये फिशिंग, क्रेडिट कार्ड घोटाळे, बँक दरोडा, अवैध डाउनलोडिंग, अश्लीलता प्रसारित करणे, सायबर दहशतवाद, व्हायरस, स्पॅम इत्यादी गुन्ह्यांचा समावेश आहे. या सर्व गुन्ह्यांना आळा घालण्यासाठी सायबर सेक्युरिटी हि अत्यंत महत्वाची आहे. सायबर सेक्युरिटी म्हणजे ह्या सर्व सायबर गुन्ह्यांवर नियंत्रण आणि त्यांचे व्यवस्थापन. जर आपण सायबर सेक्युरिटी बाळगली नाही तर याचा त्रास आपल्याला तर होईलच त्याचप्रमाणे आपल्या आजूबाजूच्या लोकांना देखील याचा त्रास होऊ शकतो.

सध्याच्या काळात सर्वात जास्त धोका आहे तो म्हणजे थर्ड पार्टी ॲप्स. जे प्लेस्टोर वर उपलब्ध नाही ते ॲप्स मोठ्या प्रमाणात धोकादायक असतात .कारण ते एखाद्या वेबसाईटवरून आपण डाउनलोड करत असतो आणि त्या वेबसाईट ला भरपूर अश्या निरुपयोगी वेबसाईट नकळत जोडल्या गेल्या असतात आणि त्या वेबसाईट द्वारे व्हायरस आपल्या मोबाईल मध्ये प्रवेश करत असतात. आत्ताच कॅम स्कॅनर नावाच्या ॲप चा घोटाळा बाहेर आला. त्या ॲप कडून त्या ॲप वर असलेला सर्व लोकांचा डेटा हा चोरीला गेला किंवा लीक झाला.यात आपला तर काही दोष नाही.तरी पण याचा त्रास आपल्याला होऊ शकतो. काही ॲप्स प्लेस्टोर वर पैसे देऊन मग आपण त्यांचा वापर करू शकतो. पण तेच ॲप्स एखाद्या अनाधिकृत वेबसाईट वर निशुल्क उपलब्ध असतात आणि भारतामध्ये निशुल्क

गोष्टींना मोठ्या प्रमाणात प्राधान्य दिलं जात.पण तेच आपल्याला घातक ठरत. आपण कोणतेही ॲप एखाद्या वेबसाईट वरून डाउनलोड करायच्या आधी ते ॲप किंवा ती वेबसाईट आपल्याकडून आपल्या मोबाईल चे संपर्क, फोटोस, आणि आपल्या मोबाईल च्या डाटा ची परवानगी मागत असतो आणि ती परवानगी आपण बहुतेक वेळा न वाचता देऊन पण टाकतो आणि याचा पण त्रास आपल्याला नकळत पुढे होत असतो .आपण तेव्हा विचार करतो की असे कसे झाले परंतु हे सगळं आपल्याच निष्काळजी पणा मुळे होत असत.

इंटरनेट हे एक साधन आहे जे आपण दररोज खरेदी करण्यासाठी, बँकेचे व्यवहार करण्यासाठी, ईमेल करण्यासाठी आणि अजून भरपूर कामांसाठी वापरतो. आणि, कोणत्याही साधनांप्रमाणेच, आपण काळजीपूर्वक त्याचा वापर करणे आवश्यक आहे. इंटरनेट आपल्यासाठी आपले दररोजचे जीवन व्यवस्थापित करणे सुलभ करते, परंतु हे आपल्या वैयक्तिक माहिती - मौल्यवान संकेतशब्द, बँकिंग तपशील, ईमेल, फोटो आणि बरेच काही सुलभतेने सायबर गुन्हेगार देखील प्रदान करते. डेस्कटॉप पीसी आणि लॅपटॉपप्रमाणेच, इंटरनेटशी कनेक्ट असलेल्या सर्व मोबाइल डिव्हाइसला मालवेयर आणि इतर हल्ल्यांपासून संरक्षण करण्यासाठी सॉफ्टवेअर संरक्षणाची आवश्यकता आहे.जर आपण इंटरनेट वापरतो तर आपल्या मोबाईल ला धोका हा असणारच कारण ह्या माहितीच्या अथांग सागरामध्ये कुठली वेबसाईट कुठे जोडलेली असेल हे आपल्याला सांगता येणार नाही. म्हणून कोणत्याही
वेबसाईट ला भेट देण्याआधी त्याबद्दल थोडी माहिती जाणून घेणे फार गरजेचे असते.आपण काही वेळेला ऑनलाइन ऑफर्स ला बळी पडतो आपण त्या ऑफर्स ला आकर्षित होऊन आपला मोबाइल नंबर, ई-मेल किंवा आपल्या दुसऱ्या अजून काही संपर्क माहिती देत असतो.त्या ऑफर चा आपल्याला काही फायदा तर होत नाही परंतु त्याचा तोटा आपल्याला नकळत होत असतो.

नोटबंदी झाल्यापासून, डिजिटल इंडिया ची घोषणा झाल्यापासून आणि इंटरनेट चे दर कमी झाल्यापासून इंटरनेट वापरकर्त्यांची संख्या मोठ्या प्रमाणात वाढली आहे आणि तेव्हापासून डिजिटल व्यवहार पण लोक जास्त प्रमाणात करायला लागलेआहेत हे तर आनंदाची बातमी आहे यात काही शंका नाही.पण आपण जेव्हा एखादा व्यवहार ऑनलाइन करत असतो तेव्हा आपल्या मोबाईल च्या आयपी ऍ‍ड्रेस पासून तर आपल्या एटीएम कार्ड च्या नंबर पर्यन्त सर्व माहिती त्या त्या वेबसाईट ला किंवा अँप मिळत असते.जर ते अँप अधिकृत असेल तर काही प्रॉब्लेम नाही. परंतु सध्या च्या काळात सायबरगुन्हे करणारे अश्या अँप्स ला पण हॅक करून त्याचा डेटा चोरी करतात आणि त्याचात्रास आपल्याला होत असतो म्हणून सायबर सुरक्षा बाळगणे अत्यंत महत्वाचे आहे.   म्हणून आपण यापुढे जेव्हा पण अश्या काही अँप्स चा वापर करू सुरक्षा बाळगली पाहिजे. कोणते पण अँप डाउनलोड करायच्या आधी दहा वेळा विचार करायचा.आणि आपल्याला जेवढं शक्य होईल तेवढी सायबर सुरक्षा बाबत जनजागृती करायची जेणेकरून सायबर गुन्हे घडण्याचा प्रमाण कमी होईल, आपल्याला त्रास होणार नाही आणि जे करतात त्यांना शिक्षा होईल.

प्रितेश आहिरे (नाशिक)

priteshma270@gmail.com

नमस्कार सर, मी नॅशनल बॅंकेतून मॅनेजर बोलतो आहे. तुमचे बॅंक अकाऊंट बंद होणार आहे, आणि तुम्ही या पुढे रक्कम काढू शकणार नाही.पुन्हा अकाऊंट चालू करण्यासाठी मला लगेच तुमचा कार्ड नंबर आणि त्यावर असलेला सिव्हिव्हि नंबर सांगा.
तसेच ५ मिनिटात तुम्हाला एक ओटीपी येईल तो सांगा, तुमचे अकाउंट पुन्हा सुरू होउन जाईल.
HAcker

खरं तर अहो, मी आत्ता बॅंकेतच बसलो आहे. तुम्ही कुठे बसले आहात सांगा, मी येतो तिथे लगेच.
NATIONAL BANK
MANAGER

अश्या अवैध कॉल्स पासुन सावध रहा !

"कुठलीही बँक तुम्हाला, तुमच्या स्वतःच्या खात्याविषयक माहिती विचारत नाही."

संकल्पना - कृष्णा वडनेरे

रेखाटन - अनिकेत गायकवाड

सायबर गुन्ह्यांविरूद्ध महिलांचे संरक्षण करण्यासाठी कायदे

हर्षिता जाधव

माहिती तंत्रज्ञान ही आजच्या जागतिक आणि तंत्रज्ञानाच्या विकासाची धुरा बनली आहे. इंटरनेटच्या प्रगतीमुळे हे साधन वापरणारे गुन्हेही वाढू लागले आहेत. सायबर क्राइममुळे बळी पडलेल्यांपैकी 90 टक्के व्यक्ती या विशेषत: महिला आहेत. प्रत्येक सेकंदाला, भारतातील एका महिलेला सायबर गुन्ह्यांचा बळी पडून फसवले जाते आणि आता ऑनलाइन प्लॅटफॉर्म हे एक नवीन व्यासपीठ आहे जिथे प्रत्येक क्षणी स्त्रीची प्रतिष्ठा, गोपनीयता आणि सुरक्षिततेला आव्हान दिले जात आहे. फेसबुक, ट्विटर आणि इतर सोशल मीडिया प्लॅटफॉर्मवर तयार केलेल्या बनावट आयडीच्या माध्यमातून सायबर क्राइम घडत जातो, कारण या प्लॅटफॉर्मद्वारे मेसेज व ईमेलद्वारे ब्लॅकमेलिंग, धमकी देणे, गुंडगिरी करणे किंवा फसवणूक करणे गुन्हेगारांकडून केले जाते.

भारतात स्त्रियांना तोंड द्यावा लागणारा सर्वात निंदनीय सायबर क्राइम आणि शोध प्रक्रियेतील आव्हाने:

१) सायबर स्टॉकिंग

“एखाद्या पुरुषाने महिलेच्या ओढणीला खेचले तर आयपीसीच्या 35 354 (बी) चे उल्लंघन करण्याचा प्रयत्न केल्याबद्दल त्याला पोलिस ठाण्यात ओढले जाऊ शकते." सायबर स्टॉकिंग ही अशी वागणूक आहे ज्यात एखादी व्यक्ती, व्यक्तींचा किंवा संघटनेचा एक किंवा अधिक व्यक्तींना त्रास देण्यासाठी माहिती आणि संप्रेषण तंत्रज्ञानाचा वापर केला जातो. सायबर स्टॉकिंग हा ऑनलाईन धोका आहे आणि पीडित आणि सायबर स्टॉकर यांच्यात थेट संबंध नाही. असे मानले जाते की पीडितांमध्ये 75% पेक्षा जास्त महिला आहेत. लैंगिक छळ, प्रेम, सूड आणि द्वेष आणि अहंकार यामागील हेतू आहेत. गुन्हा रोखण्यासाठी शिक्षा वाढविणे आवश्यक आहे. यू / एस 4 354 डी आयपीसी स्टॉकिंग हा एक मोठा गुन्हा असून त्याला ३ वर्षांपर्यंतची शिक्षा आणि दंड ठोठावला जाऊ शकतो.

२) सायबर पोर्नोग्राफी

सायबर पोर्नोग्राफीमध्ये अश्लील वेबसाइट्सचा समावेश असतो. संगणकांचा वापर करून तयार केलेली अश्लील मासिके एक अपवादात्मक प्रकरण मानली जाते. याला आयटी कायदा २००० च्या कलमानुसार शिक्षा पाचवर्षांपर्यंत आणि दंड आहे. आयटी कायद्यासह गुन्हेगारास आयपीसीच्या विविधकलमांनुसार, सार्वजनिक उपद्रव केल्याबद्दल कलम २९०, अश्लील पुस्तकांच्याविक्रीसाठी कलम २९२ आणि कलम २९२ अ, अत्यंत अश्लील किंवा गुंतागुंतीचे विषय किंवा ब्लॅकमेल करण्याच्या हेतूने छापील किंवा प्रकाशित करण्यासाठी कलम २९३ तरुणांना अश्लील वस्तूंच्या विक्रीसाठी व नंतर कलम २९४ अन्वये अश्लील गाणी लिहिणे, लिहणे इ.

३) सायबर गुंडगिरी

“एखाद्या मुलीने आपल्याला फेसबुकवर फ्रेंड रिक्वेस्ट पाठवली याचा अर्थ असा नाही की तिला आपल्यात रस आहे.”

सायबर गुंडगिरी ही संगणक,मोबाईल आणि इंटरनेटचा वापर करून इलेक्ट्रॉनिक पद्धतीने संपर्क साधून धमकी देणे किंवा छळ करणे आहे. आयपीसीच्या कलम ५०६ नुसार दंडनीय आहे. यात दोन वर्षांची शिक्षा होऊ शकते. जर मृत्यू किंवा गंभीर दुखापत होण्याची धमकी देत असेल तर त्यास सात वर्षांची शिक्षा होऊ शकते. २०१४ मध्ये झालेल्या इप्सॉस सर्वेक्षणात, सायबर गुंडगिरीसाठी २५४ देशांच्या यादीत भारत अव्वल स्थानावर आहे. ब्लु व्हेल चॅलेंजसारखी इतर आव्हाने ही सायबर गुंडगिरीचे सर्वात क्रूर प्रकार आहेत.

४) लैंगिक बदनामी

काही वेळा संगणक आणि इंटरनेटच्या मदतीने बदनामी होते. उदा. एखादी वेबसाइटवर एखाद्याबद्दल बदनामीकारक गोष्टी प्रकाशित करते किंवा इतरांना बदनामीकारक मजकूर असलेला ई-मेल पाठवते. इंटरनेटमुळे सामान्य माणसाचे आयुष्य खूप बदलले आहे. लैंगिक बदनामी झाल्यास 2 वर्षांची शिक्षा आणि दंड ठोठावला आहे.

५) ईमेलद्वारे त्रास देणे

ईमेलद्वारे ब्लॅकमेलिंग, धमकी देणे, गुंडगिरी करणे आणि ईमेलद्वारे फसवणूक करणे हे यात समाविष्ट आहे. ईमेल स्पूफिंग हि फिशिंग आणि स्पॅम मोहिमांमध्ये वापरली जाणारी एक युक्ती आहे कारण जेव्हा एखादा ई-मेल अधिकृत स्त्रोताद्वारे पाठविला गेला आहे असे त्यांना वाटते

तेव्हा ई-मेल उघडण्याची अधिक शक्यता असते. यू / एस 67अ ई-मेलद्वारे छळासाठी ५ वर्षांपर्यंतची शिक्षा ठोठावली आहे.

६) ट्रोलिंग

"एखाद्या मुलीला' हाय, हॅलो, तू कशी आहेस?' असे संदेश एखाद्या अज्ञात नंबरवरून मिळाल्यास आणि जर तिने संदेशांचे स्क्रीनशॉट घेतले तर ती व्यक्ती छळासाठी जबाबदार आहे."

ट्रोलने इंटरनेटवर विरोधाभास पसरविणे, पीडित व्यक्तीला भावनिक, त्रास देण्याच्या हेतूने एखाद्या ऑनलाइन समुदायामध्ये दाहक संदेश पोस्ट करणे. ट्रोल हे सोशल मीडियावर बनावट आयडी तयार करुन केले जातात.

तक्रार दाखल कुठे करणार:

सायबर बदनामीमुळे त्रस्त व्यक्ती सायबर गुन्हे अन्वेषण कक्षाकडे तक्रार देऊ शकते. सायबर गुन्हे अन्वेषण कक्ष संगणक, संगणक नेटवर्क, संगणकीय स्त्रोत, संगणक प्रणाली, संगणक उपकरणे आणि इंटरनेट यासंदर्भातील गुन्ह्यांचा सामना करतात. इतर हाय-टेक गुन्ह्यांचा छडा लावण्याचीही त्यांची ताकद आहे. याव्यतिरिक्त, बऱ्याच राज्यात आता 'ई-एफआयआर' दाखल करण्याची तरतूद करण्यात आली आहे.

स्वतःचे सायबर रक्षण कसे करावे यावर मुख्य मुद्दे

१) पासवर्ड इतरांना देऊ नये.
२) वैयक्तिक माहिती उघड करू नये.
३) ऑनलाईन लोकांना भेटणे टाळा.
४) वेबकॅम काळजीपूर्वक वापरायला हवे.
५) प्रायव्हसी अटी वाचल्या पाहिजेत.
६) फ्री डाऊनलोडिंग साइट टाळा कारण त्यांच्या फाइल्समध्ये ट्रोजन्स असू शकतात.

कायदेशीर उपाययोजना

भारतीय दंड संहितेसह माहिती तंत्रज्ञान कायदा २००० मध्ये प्रचलित सायबर गुन्हेगारीबाबत योग्य तरतुदी आहेत. हे सायबर गुन्ह्याच्या प्रकारानुसार दोन वर्षांपासून जन्मठेपेपर्यंत आणि दंड / दंडाची शिक्षा ठोठावते. तथापि, सायबर गुन्हेगारीच्या घटना रोखण्यासाठी सरकारने अनेक कायदेशीर, तांत्रिक आणि प्रशासकीय उपाययोजना केल्या आहेत.

१. सायबर गुन्हेगारीच्या खटल्यांच्या अहवाल आणि तपासणीसाठी प्रत्येक राज्यात सायबर पोलिस स्टेशन आणि सायबर क्राइम सेल्सची स्थापना केली गेली आहे.

२. इलेक्ट्रॉनिक्स आणि माहिती तंत्रज्ञान मंत्रालयाने (एमइआयटीवाय) सायबर गुन्हे अन्वेषण व संग्रहण, इलेक्ट्रॉनिक पुरावा जपणे, जपणे आणि जप्त करणे यासाठी राज्य पोलिस अधिकारी आणि न्यायपालिकेला प्रशिक्षित करण्यासाठी ईशान्येकडील राज्ये आणि मुंबई, पुणे, कोलकाता आणि बेंगळुरूसारख्या शहरांमध्ये सायबर फॉरेन्सिक्स प्रशिक्षण प्रयोगशाळेची स्थापना केली आहे.

३. सायबर क्राइमशी संबंधित गृह मंत्रालय, एमइआयटीवाय (मीटी) आणि राज्य शासनाने विविध राष्ट्रीय व राज्य पोलीस अकादमी / न्यायिक अकादमी व इतर संस्थांद्वारे सायबर गुन्हेगारी रोखण्यासाठी व नियंत्रणासाठी ज्ञान आणि कौशल्यांसह पोलिस कर्मचार्यांना सुसज्ज करण्यासाठी आधुनिक तंत्रज्ञानाची आणि विविध प्रकारच्या पावले उचलली आहेत.

४. इलेक्ट्रॉनिक्स आणि माहिती तंत्रज्ञान मंत्रालयाने माहिती तंत्रज्ञान अधिनियम, २००० अन्वये १६ जून २०१६ रोजी मॅट्रिमोनिअल वेबसाइटच्या कामकाजाबद्दल एक आदेश जारी केला आहे आणि त्यानुसार या वेबसाइट्सचा वापर करणाऱ्या लोकांची फसवणूक होऊ नये यासाठी वेबसाइट्सना सुरक्षितता अंगीकारण्याचे निर्देश देण्यात आले आहेत.
५. वेबसाइटवर बनावट प्रोफाइल किंवा गैरवापर / चुकीची माहिती शोधणे, सायबर-हल्ले रोखण्यासाठी, शोधून काढण्यासाठी आणि उपाययोजना करण्याबाबत सरकारने सर्व मंत्रालय / विभागांना संगणकसुरक्षा धोरण व मार्गदर्शक सूचना दिल्या आहेत.
६. लोकांना सायबर क्राइमच्या तक्रारी नोंदविता याव्यात यासाठी गृह मंत्रालयाने www.cybercrime.gov.in नावाचे पोर्टल तयार केले आहे.

हर्षिता जाधव (नाशिक)

nilharshita174@gmail.com

स्पाय ॲप

ओंकार गंधे

आपल्या मोबाईल मध्ये अनेक वर्षांचे मेसेजेस, इ-मेल्स, फोटोज, व्हिडीओज अशा अनेक खाजगी गोष्टी असतात, काही व्यावसायिक दृष्ट्या गोपनीय माहिती साठवलेल्या असतात. आपले पासवर्ड, नोट्स, इंटरनेट ची हिस्टरी इत्यादी अनेक गोष्टी कळत नकळत आपल्या मोबाईल मध्ये असतातच.

आता विचार करा हि सगळी माहिती जर कोणाला मिळाली, तर काय होईल? तुमचा जोडीदार तुमच्या प्रत्येक हालचालीवर लक्ष ठेऊ शकतोय का? तुमच्या मोबाईल मधली सगळी माहिती एका क्लिक वर लांब बसलेल्या एखाद्या माणसाला सहज मिळू शकते.. कसे ते आपण बघूया. मोबाईल मधील आपले सर्व मेसेज, कॉल्स, फोटोस, व्हिडीओज, आणि इतर डेटा सहज एका ॲप च्या साहाय्याने दूर असलेला एखादा माणूस बघू शकतो, वाचू शकतो. अशा ॲप ना 'स्पाय ॲप' म्हणतात.

स्पाय ॲप कसे काम करतात?

स्पाय ॲप डाउनलोड करून मोबाईल मध्ये इन्स्टॉल करायचे. बाकी सगळं काम 'स्पाय ॲप' कडून केले जाते. ज्याच्या मोबाईल ची गुप्तहेरी करायची आहे त्याचा मोबाईल आधी मिळवणे गरजेचे असते. कारण मोबाईल मध्ये हे ॲप इन्स्टॉल केल्या शिवाय पुढे जाता येत नाही.
स्पाय ॲप प्रकारामध्ये मध्ये अनेक वेगवेगळ्या कंपन्यांचे ॲप उपलब्ध आहेत. पण प्रामुख्याने ॲप इन्स्टॉल केल्यावर त्या मध्ये साइन इन करावे लागते. हे साइन इन 'तो' हेरगिरी करणारा व्यक्ती करतो, आणि तुमचा मोबाईल परत ठेऊन देतो.
या स्पाय ॲप ना अँड्रॉइड किंवा IOS दोन्ही मध्ये प्रवेश करता येतो. त्या साठी इंस्टाल करताना मोबाइलकडून काही परवानग्या आवश्यक असतात, त्या मान्य केल्या जातात. त्यामुळे तुमच्या मोबाईल मधील सर्व डेटा, कॉल्स, मेसेजेस, फोटोज, इत्यादी गुप्तहेरी करणाऱ्याला दिसू लागतात. गुप्तहेरी करणारा त्याच्या घरी स्वतःच्या मोबाईल किंवा कॉम्पुटर वर बसून हे सर्व सहज बघू शकतो आणि वाचू शकतो.

स्पाय ॲप काय काय करू शकतात?

स्पाय ॲप जर व्यवस्थित इन्स्टॉल केलं असेल, सर्व परवानग्या मोबाईल कडून मान्य करवून घेतल्या असतील तर पुढील गोष्टी सहज मिळवता येतात -मोबाईल मध्ये असलेले सर्व कॉल रेकॉर्डस् , मेसेजेस, फोटोज, व्हिडीओज, इमेल्स, व्हाट्सॲप मेसेजेस, इंटरनेट ब्राउजिंग ची हिस्टरी, इत्यादी.अनेकदा काही स्पाय ॲप कडून माईक आणि कॅमेरा ची परवानगी घेतली जाते. त्यामुळे समोरच्या व्यक्तीकडून तुमचे कॉल्स ऐकले जातात, तसेच कोणत्याही क्षणी तुमचा माईक चालू करून आजू बाजूला चालू असलेले संभाषण ऐकता येऊ शकते. तसेच कॅमेरा चालू करून त्या द्वारे ही हेरगिरी करता येते.मोबाईल ची सध्याची लोकेशन हि सहज बघता येते.ऑनलाईन पेमेंट, किंवा बँकिंग व्यवहार यात अजून स्पाय ॲप ना प्रवेश करता येऊ शकलेला नाही. तसेच फेसबुक सारख्या सोशल नेटवर्किंग साईट्स मध्ये लॉगिन गरजेचं असल्यामुळे ते प्रवेश करू शकत नाही.

स्पाय ॲप आपल्या मोबाईल मध्ये आहे हे ओळखायचे कसे?

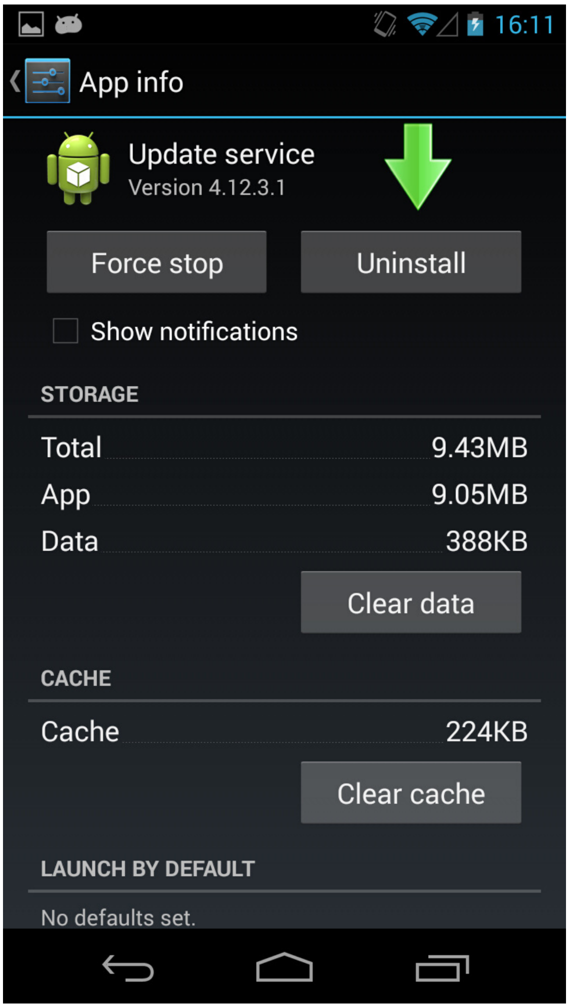
स्पाय ॲप एकदा इन्स्टॉल केले कि ते मोबाईल मध्ये दिसून येत नाहीत. त्यांचे किंचित अस्तित्व तुम्हाला जाणवणार नाही. ॲप्लिकेशन्स मध्ये सर्व ॲप चे नावं असतात, पण या स्पाय ॲप चे नाव दिसत नाही. ज्याने स्पाय ॲप टाकले केवळ त्यालाच हे ॲप मोबाईल मध्ये उघडता येते. आज वर झालेल्या अभ्यासानुसार काही स्पाय ॲप ॲप्लिकेशन्स मध्ये दिसतात, पण वेगळ्या नावाने. जसे - गुगल सर्विस, डेटा सर्विस, डू नॉट रिमूव्ह, ऐवी सर्विस, इत्यादी.
जर एखादे अनोळखी ॲप अचानक जर मोबाईल मध्ये दिसायला लागले तर ते त्वरित 'अन-इन्स्टॉल' करावे.

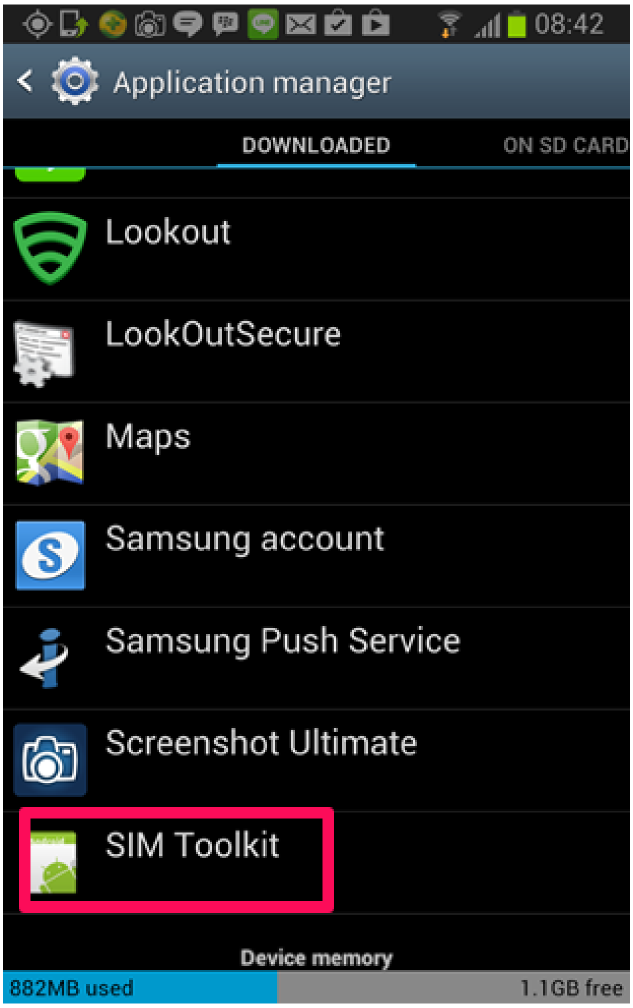
स्पाय ॲप पासून स्वतःला कसे वाचवणार ?

१. मोबाईल मध्ये स्पाय ॲप टाकण्यासाठी केवळ ५ मिनिटांचा वेळ लागतो. आपला मोबाईल इतका कमी वेळ सुद्धा कोणाच्या हातात देऊ नये. दिला तर त्या कडे लक्ष द्यावे. शक्यतो मोबाईल ला पासवर्ड टाकावा ज्यामुळे कोणाला मोबाईल तुमच्या परवानगीशिवाय उघडता येणार नाही.

२. दुसऱ्याचा मोबाईल वापरू नका. सेकंड हॅन्ड मोबाईल घेताना काळजी घ्या. मोबाईल कधीही 'रूट' करू नका, म्हणजेच कंपनीने दिलेल्या सिस्टिम ऐवजी दुसरी सिस्टिम टाकू नका. आयफोन बाबतीत याला 'जेलब्रेकिंग' म्हणतात.

३. मोबाईल मध्ये स्पाय ॲप आहे अशी शंका आल्यास त्वरित तो मोबाईल फॉरमॅट करा. फॉरमॅट करण्यासाठी मोबाईल दुकानात नेण्याची गरज नसते, आपल्याच मोबाईल मध्ये सेटिंग मध्ये फॅक्टरी रीसेट चा ऑप्शन असतो. एकदा फॉरमॅट केला कि त्यातील स्पाय ॲप आपोआप नाहीसे डिलीट होतात.





कोण कोणते स्पाय ॲप आहेत ?

अँड्रॉइड, आयओएस, तसेच विंडोजसाठीही स्पाय ॲप उपलब्ध आहेत. यातील काही सुविधा मोफत आहेत, तर काही ॲप साठी शुल्क भरावे लागते. हे शुल्क एक हजार रुपये महिना पासून अधिक साठी उपलब्ध आहेत. मोफत असलेले ॲप अजिबात वापरू नयेत, कारण त्यातील विश्वासार्हता संशयास्पद असते. एम स्पाय, फ्लॅक्सिस्पाय, स्पॅयेरा, स्पाय फोन, हायस्टर मोबाईल, इत्यादी प्रसिद्ध स्पाय ॲप आहेत.

स्पाय ॲप चा वापर कोण करतो? स्पाय ॲपचा वापर गुन्हा आहे का?

स्पाय ॲप चा वापर संशय असलेल्या जोडीदारावर मोठ्या प्रमाणात केला जातो. बॉयफ्रेंड गर्लफ्रेंड धोका देत आहेत असा संशय आल्यास याचा वापर केला जातो. तसेच नवरा बायको आपापल्या जोडीदाराच्या हालचालींकडे या द्वारे लपून लक्ष ठेवतात. न सांगता केलेली गुप्तहेरी - स्पाय ॲपचा वापर गुन्हा समजला जाऊ शकतो.

१. पालकांकडून आपल्या अल्पवयीन मुलांवर लक्ष ठेवण्यासाठी त्यांच्या मोबाईल मध्ये स्पाय ॲप चा वापर करायला हवा.
२. अनेकदा कंपन्यांकडून कर्मचाऱ्यांना मोबाईल मिळतात, त्यात स्पाय ॲप असतात, आणि त्या द्वारे कर्मचारी केवळ आपल्या कंपनीचाच काम करतोय कि नाही, तसेच काही गैरव्यवहार करत नाही ना याकडे कंपनी लक्ष ठेऊन असते. याबाबत कर्मचाऱ्यांना अनेकदा सांगितलं जात नाही. स्पाय ॲपचा वापर केवळ या दोनच गोष्टींसाठी गुन्हा नाही.
स्पाय ॲप चा वापर कोण आणि कोणत्या उद्देशाने करत आहे हे जास्त महत्वाचे आहे.

ओंकार गंधे

cybersakshar@gmail.com

सावधान, तुम्हाला कुणीतरी पाहतंय, सावधान तुम्हाला कुणीतरी ऐकतय.....

तेजस्विता खिडके

अश्मायुतील माणूस दगडाचा वापर करून स्वत:ची "अन्न" ही गरज भागवायचा,हळु हळु तो शेती करायला शिकला, चाका सोबत नवनवीन अवजारांचा शोध लावत गेला, अन् सोबतच तंत्रज्ञान विकसित होत गेले, अन् आजच्या युगात अन्न वस्त्र निवारा , सेक्स आणि इंटरनेट या माणसाच्या अत्यावश्यक गरजा झाल्या आहेत अस म्हंटले तर काहीच वावग ठरणार नाही; कारण अन्न, वस्त्र अन् निवारा या प्राथमिक गरजा भागल्या की मनुष्य धावतो नवनवीन तत्रज्ञानाने विकसित झालेल्या गोष्टीमागे, आणि आपल सध्या तेच झालं आहे.कुतूहल म्हणून वापरायला सुरुवात केलेली गोष्ट आज गरज बनली आहे हे तितकंच खर..

आजच्या तंत्रज्ञानाच्या युगात स्मार्ट फोन आणि त्याला असलेली इंटरनेट ची जोड ही माणसाच्या रोजच्या जीवनातली एकदम कॉमन अशी गोष्ट, एखादी गोष्ट माहीत नसली तर आपण सहज बोलुन जातो जरा गुगल करून बघ.. पूर्वी असायची वर्तमान पत्र, टिवी, रेडीओ इत्यादी आता मात्र या सर्वांची जागा हळु हळु स्मार्ट फोन अन् त्यातल्या खिडकीतून डोकावणारे वेग वेगळे ॲप्लिकेशन घेत आहेत... सोशल मीडिया नावाचा प्रकार आज खुप वाढला, त्यामुळे माहिती सामान्यांपर्यंत पोहोचणं फार च सोपं झालंय..

आज व्हॉटसअप, फेसबुक, इंस्टाग्राम, यूट्यूब कोणाला नाही माहित?
हे ॲप्लिकेशनस म्हणजे तर अगदीच काहींचे करमणुकीचे साधन, संवाद साधणे यामुळे फारच सोपं झालंय, आजकाल घर साधं असेल तरी चालेल पण स्मार्ट फोन हा हवाच, काळाची गरज च नाही का? आता थोड विचार करू, पूर्वी कसं व्हायचं, टीव्ही विकत घायचा मग त्यावर करमणुकिसोबत जाहिराती ही पहायच्या, सारख्या सारख्या जाहिराती पाहून आपण ही प्रभावित होतोच उदाहरणार्थ, "वॉशिंग पावडर निरमा, दुधसी सफेदी निरमा से आयी, रंगिन कपडा भी खील खिल जाये, सबकी पसंद निरमा, निरमा".. आता खर खर सांगा, हे वाचताना तुमच्या डोक्यात चालि सकट ही जाहिरात वाजली की नाही? मला शंभर टक्के खात्री आहे याचं उत्तर "हो" असच आहे.., अश्या तर्हेने ही निरमा आपल्या डोक्यात शिरली. अन् मग आपल्या घरात , अन् अश्याच बऱ्याच काही गोष्टी जाहिरातींच्या माध्यमातून आपल्या घरात, तसेच आयुष्यात एंटर झाल्या ; ही झाली टीव्ही ची पॉवर...

आता थोड पुढे येऊ, आपल्या हातात आहे हा स्मार्ट फोन ज्यावरून आपण बरेच ऍप्लिकेशन डाऊनलोड करतो आणि वापरतो, तस पाहिलं तर ही सर्व ऍप्लिकेशन फ्री असतात, पण हे वापरण्यासाठी काही टर्म अँड कंडीशन असतात, त्याला परवानगी दिल्या शिवाय आपल्याला हे ॲप वापरताच येत नाहीत, आणि आपण या टर्म अँड कंडीशन न वाचताच येस येस अस करत अक्सेप्ट करतो. थोडक्यात आपण आपल्या आपण पैसे देऊन विकत घेतलेल्या स्मार्ट फोन मध्ये असलेला सर्व डाटा म्हणजे माहिती वापरण्याची सर्व च्या सर्व परवानगी या एप्लिकेशन्सला स्वतः च देतो, जसं की व्हॉटसअपला किंवा इंस्टाग्रामला किंवा फेसबुकला कॅमेरा, मायक्रोफोन, स्टोरेज वापरण्याची परवानगी आपणच कळत नकळत दिलेली असते.. आपण कधी साधा विचार केलाय का, या जगात खरच काही फुकट असते का, अन् जर नसते तर हे ॲप आपल्याला फुकट कसकाय बरे वापरायला मिळत असतील? याच उत्तर अस आहे की जेंव्हा आपणच या अॅप्स ला वरील सर्व गोष्टींची परवानगी दिलेली असते तर ही अॅप्स आपला डाटा गोळा करत असतात, आपण काय बोलतो हे ही ॲप्स मायक्रोफोन द्वारे ऐकत असतात, अन् मग आपल्याला तशाच जाहिराती दाखवल्या जातात, आणि या जाहिरातींच्या माध्यमातून ही ॲप्स पैसे कमवतात. या ॲप्स वाल्यांकडे म्हणे असा खुप लोकांचा डाटा असतो, त्याला म्हणतात "बिग डाटा" मग यात आपण काढलेले फोटो असतील, व्हिडिओ असतील, ऑडियो असतील , डॉक्युमेंट्स असतील, मेसेजेस असतील, एवढंच काय बँकेचे डिटेल्स असतील, ओटीपी असतील, सोशल मीडिया अकाउंट्स चे पासवर्ड असतील, असेल नसेल ती सर्व माहिती या "बिग डाटा" मध्ये असते. मला तर असेही कळले आहे की, हा बिग डाटा म्हणे विकला जातो, एका माणसाच्या वर्ष भराच्या डाटा ची किंमत म्हणे सहा रुपये असते. आता विचार करा हा डाटा जर एखाद्याच्या हातात पडला तर तो एखाद्याचे आयुष्य ही उध्वस्त करू शकतो, एखाद्याच्या काही खाजगी गोष्टी या बिग डाटा मध्ये असल्या अन् त्या कुणाच्या ताब्यात आल्या तर त्या खासगी गोष्टी सार्वजनिक झाल्या तर काय होईल, खासगी गोष्ट सार्वजनिक होणे म्हणजे नागडं होणेच की, मग उरतो एकच पर्याय एकतर आत्महत्या किंवा काही घडलच नाही असा गैरसमज करून जगणे. एखाद्याच्या बँक खात्यातील पैसे चोरणे ही तितकेच सोपे, कैक लोकांच्या बँक खात्यातील रक्कम गायब झाल्याच उदाहरण आहेत. प्रत्येक नाण्याला दोन बाजू असतात, ही झाली नाण्याची निगेटिव्ह बाजु.

आता या गोष्टी जर चुकवायच्या असतील तर आपणही तितकीच काळजी घेणं गरजेचं नाही का? मग आता काळजी घ्यायची म्हणजे नेमक काय करायचं? थोड जागरूक व्हायचं एवढंच, जस आपल्या स्मार्ट फोन क्या सेटिंग मध्ये जाऊन आपण कोणत्या कोणत्या अॅप्स ला कोण कोणत्या गोष्टीच्या अक्सेस ची परवानगी दिली आहे हे तपासणे, मग ज्या अॅप्स ला कॅमेरा वा मायक्रोफोन व इतर गोष्टींच्या अक्सेस ची गरज नाही त्या अॅप्स ला दिलेली परवानगी काढून टाकणे. नेहमी आपल्या सोशल मीडिया अकाउंट्स चा पासवर्ड बदलत राहणे, आपल्या जी मेल चा पासवर्ड वेळोवेळी बदलणे, काम झाले की इंटरनेट बंद करणे, अश्या छोट्या छोट्या गोष्टी आपणास सायबर क्राईम चा व्हिक्टीम होण्यापासून वाचवू शकतात.

आता बोलू थोड सोशल मीडिया विषयी, आजकाल लोकं एकमेकांपासून दुरावली अन् सोशल मीडियाच्या खिडकी तुन मात्र दुसऱ्या च्या आयुष्यात डोकावण्या चा प्रकार मात्र फार वाढला, तस पाहिलं तर आयुष्यात जाम काळोख पण लोकांची सोशल मीडिया अकाउंट्स पाहिली तर एखाद्याला हेवा वाटेल एवढी हिरवळ दिसत असते अन् त्यात काही अती हुशार लोक स्वतःची पुर्ण च्या पुर्ण माहिती फेसबुक वर टाकत असतात, मग लग्नाच्या फोटोंपासून, बाळ जन्माला आले किंवा कुणी दगावले याची एकूण एक माहीती अगदी सहज उपलब्ध होते, म्हणजे गुन्हेगारांना आपल्या अपडेट्स आपणच देत असतो, अन् मग मौका पाहून चोरटे भुरटे बरोबर चौका मारतात. अन् या अश्या फालतू सवयीना आपणच कुठे तरी आवर घालायला नको का? असो शेवटी हा ज्याचा त्याचा खासगी प्रश्न पण कुठली गोष्ट किती ताणायची हेही आपणच ठरवलेलं बर नाही का? कारण याबाबतीत आपण आता सावध झालो नाही तर त्याचे होणारे दुष्परिणाम ही आपल्यालाच भोगावे लागणार आहेत. असे म्हणतात की, "वेळीच घातलेला एक टाका पुढचे दहा टाके वाचवतो" म्हणुन मी एवढंच म्हणेल,

सावधान, तुम्हाला कुणीतरी पाहतंय, सावधान तुम्हाला कुणीतरी ऐकतय....

तेजस्विता खिडके (पुणे)

व्यवसाय रणनीतीकार, सल्लागार आणि वक्त्या

teju.khidke@gmail.com

शुभ दीपावली
Shruti Kothawade

तुमची शाळा, तुमचे कॉलेज सायबर साक्षर आहे का?

सायबरसाक्षर

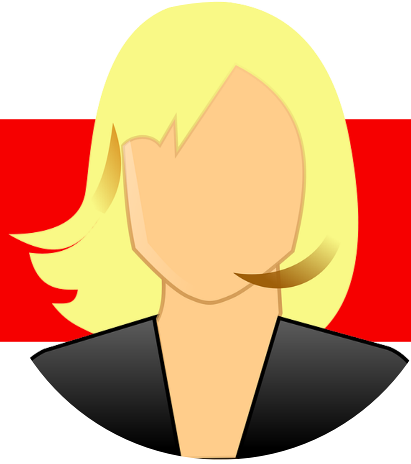
Cyber Literate India

सायबर क्राईम आणि सायबर असुरक्षितता प्रचंड वाढत चालली आहे. शाळा आणि महाविद्यालयीन मुले-मुली यात सर्वाधिक बाली पडतात. त्यामुळे शाळा आणि महाविद्यालये सायबर साक्षर करण्याचा आमचा मानस आहे.

सायबर साक्षर तुमच्या शाळेत, महाविद्यालयात आणि संस्थेमध्ये येऊन विविध सेमिनार घेईल. गरजेनुसार विद्यार्थ्यांसाठी वर्कशॉप घेण्यात येतील. विद्यार्थ्यांसाठी छोटी परीक्षा घेऊन त्यांना सायबर साक्षर प्रमाणपत्रही देण्यात येईल.

सायबर साक्षरतेच्या या उपक्रमात भाग घेण्यासाठी नक्की कळवा:
cybersakshar@gmail.com
किंवा भेट द्या cybersakshar.com ला.

सिम स्वॅप आणि
२० लाख गायब



कविता गांगुर्डे

आजकालच्या या धावपळीच्या जीवनात सायबर सिक्युरिटी चे ज्ञान असणे किती गरजेचे आहे आणि ते ज्ञान कशा पद्धतीने मुंबईतल्या एका गृहस्थाला कसे उपयोगी पडले ते बघूया. हैपतराव नावाचे एक गृहस्थ मुंबईमध्ये आपल्या कुटुंबासोबत सुखाने संसार करत होते. गाडी, बंगला,नोकर-चाकर,चांगल्या कंपनीमध्ये चांगली नोकरी होती. त्यांचा मुलगा विनय, मुलगी प्रिया आणि पत्नी सूशिला हे राहात होते अणि देवाच्या आर्शिवादाने त्यांच्या मुलीचे लग्नही जमले होते. त्यामुळे जरा कामाची धावपळच होत होती आणि आज ते बाहेर काही खरेदी करण्यासाठी जाणार होते. बरीच खरेदी करून आणि विविध दुकानांमध्ये फिरून आले. सकाळी हैपतरावांना लवकर ऑफिसला जायचे होते म्हणून ते ऑफीसला जायला गडबडीतच निघाले. पण ऑफिसला गेल्यावर त्यांना कळतं की ते त्यांचा मोबाईल घरीच विसरलेत. हे कळवण्यासाठी ते घरी फोन करतात पण त्यांचा फोन लागत नाही, म्हणून ते घरच्या फोनवर फोन करून कळवतात. तेवढ्यात त्यांचे मॅनेजर जोशी येतात. ते खूप चिंतेत दिसतात. हैपतराव त्यांना विचारतात की काय झाले मॅनेजर साहेब? मग जोशी त्यांना त्यांची अडचण सांगतात की त्यांच्याही मुलीचे लग्न आहे आणि मुलीच्या लग्नासाठी आठ लाख रूपये हवे होते. ते कसे मागू तुमच्याकडे, या मोठ्या चिंतेत मी होतो, कारण तुमच्या घरीही लग्नकार्य आहे.

हैपतराव - बस एवढचं ना.. हा घ्या आठ लाखाचा चेक. ते बघून जोशींचे डोळे पाणावतात, चेक घेऊन आभार मानून आपल्या टेबलकडे जातात. हैपतरावही त्यांच्या मिटीग साठी निघून जातात. सायंकाळी हैपतराव घरी येतात. रात्रीचे जेवण झाल्यावर सुशीला आणि हैपतराव गॅलरीत गप्पा मारत बसलेले असतात, तेव्हा सुशीला त्यांना सांगते की धर्माजीचा म्हणजेच त्यांच्या होणाऱ्या व्याह्यांचा फोन येऊन गेला. हैपतराव त्यांना लगेच फोन करतात. फोनवर त्यांचे बोलणे ऐकून ते चकित होतात कारण त्यांनी जो ज्वेलरी साठी १0 लाखांचा चेक दिला होता तो बाउन्स झाला होता. हैपतराव विचारात पडले की अकाउंटमध्ये तर २० लाख रूपये होते, मग चेक कसा बाउंस होऊ शकतो. ते हा विचार करतात आणि तसेच विचारात झोपी जातात.

सिम स्वॅप आणि २० लाख गायब

सकाळी त्यांना बँकेत जायचं असतं त्यामुळे ते बँकेत जायला निघतात, पण त्यांचा फोन आऊट-ऑफ-सर्व्हिस असतो. त्यामुळे ते त्यांचा फोन घेऊन आधी त्या सिमकार्ड कंपनीच्या ऑफिसकडे घेऊन गेले. पण त्यांना तिथे गेल्यावर कळले की त्यांचे सिम ब्लॉक केलं गेलं आहे आणि तेही त्यांच्याच सांगण्यावरून. थोडे अजून काळजीत ते बँकेत जातात. बँकेत त्यांना जोशी भेटतात, ते सांगतात कि त्यांना दिलेला ८ लाखाचा चेक बाउंस झाला आहे. अकाउंट मध्ये पुरेसे पैसे असतानाही , धर्माजी आणि जोशी दोघांनाही दिलेले चेक बाउंस झाले होते. त्वरित बँक मॅनेजर ला हा प्रकार सांगितल्यावर त्यांच्या लक्षात आले कि अकाउंट मध्ये तर एक रुपयाही शिल्लक नाही. हैपतरावांना काय चालले आहे त्यांनाही काही समजत नव्हते. त्यांचा सगळं पैसा कुठे गेलाय हेही पत्ता लागेना. बँक मॅनेजर ने सांगितल्या नुसार हैपतराव पोलीस स्टेशनला तक्रार करतात. पोलीसांनी त्यांना हमी दिली की आम्ही तपस करतो. पैसे गेले, सिम बंद, व्याह्यांसमोर नाक कापले गेलेले, या सर्व टेन्शन मध्ये हैपतराव कामावर न जाता घरी येतात. संध्याकाळी अचानक त्यांच्या घरातला फोन वाजला, त्यांना लगेच पोलीस स्टेशनला बोलावले होते. संपूर्ण परिवारासह पोलीस स्टेशन ला गेल्यावर त्यांना कळते की चोर सापडला. पोलीसांनी त्याला खूप चोप दिला होता, त्यामुळे तो सत्य काय आहे हे सांगू लागला. तो चोर एका कापड दुकानात काम करणारा तरुण असतो.

"सर तुम्ही काही दिवसांपूर्वी कपड्याची खरेदी करायला आमच्या दुकानात आले होते. तुम्ही त्या कपड्यांचे बिल कार्डाने केले होते. तिथे तुम्ही टाकलेला पिन नम्बर मी बघू ठेवला होता. तसेच माझ्या शर्टाला एक छोटा कॅमेरा लावलेला आहे, त्यामुळे तुमचा कार्ड नम्बर आणि सिविवि सुद्धा माझ्याकडे होता. तुमचे नाव, पत्ता आणि इतर सर्व माहिती माझ्याकडे होती."

हैपतराव - "कशी काय ?"

चोर - "पेमेंट केल्यानंतर आम्ही एक फीडबॅक फॉर्म भरून घेतला होता त्यात सर्व माहिती तुम्ही भरली होती. मला गरज होती ती केवळ तुमच्या आईच्या नावाची आणि जन्मतारखेची. या दोन्ही गोष्टी मला तुमच्या फेसबुक अकाउंटवर मिळाल्या. सर्व माहिती माझ्याकडेहोती, आता मला केवळ ऑनलाईन पैसे ट्रान्सफर करायचे होते. तुमच्या अकॉउंट मधून माझ्या अकाउंट मध्ये पैसे टाकण्यासाठी एक ओटीपी तुमच्या मोबाईलवर येणार होता, त्यामुळे मी सिम कंपनीच्या आउटलेटमध्ये जाऊन तुमच्या नावाने ब्लॉक रिक्वेस्ट टाकली. तसेच त्या नम्बर चे नवीन सिम कार्डही मिळवले. ओटीपी मिळाला आणि पैसे पूर्ण माझ्याकडे आले. मी सर्व रक्कम परत करतो, मला कृपा करून सोडा. "

हैपतराव पोलिसांना धन्यवाद देतात, पोलीस अधिकारी हैपतरावांना सांगतात, धन्यवाद आमच्या सायबर तज्ज्ञांचे मन, त्यांनी केवळ २ तासात हा तपास केला.

तात्पर्य : ग्राहकांनी आजकालच्या संगणक युगात काळजी घ्यायला हवी, व्यवहार करताना अनेक धोके आहेत.

कविता संजय गांगुर्डे (चांदवड)

विद्यार्थिनी, आयटी इंजिनीयरिंग

वेडे प्रेम

प्रारब्ध ढवळे

प्रेम या जगातील सर्वात सुंदर गोष्ट.थांबा.. थांबा .. थांबा ... आपण असा विचार करू शकता की "मी योग्य मासिक वाचतो आहे की नाही?" "मला वाटले की हे सायबर संबंधित मासिक आहे".. 'लडकी को पटाया 7 दिन मे' असं काहीतर नाही. तुमचं बरोबर आहे मित्रांनो, हे एक
सायबर मासिकच आहे. पण आजकाल प्रेम देखील ऑनलाइन होत आहे. हि एक कथा आहे किंवा त्याऐवजी एक प्रेम कथा म्हणा जी आपल्याला कदाचित आवडेल.

साक्षी 16 वर्षांची बुद्धिमान, स्मार्ट व थोडी लाजाळू मुलगी होती. तिच्या वयाच्या इतर मुलींप्रमाणेच तीही "लाइफ पार्टनर" शोधत होती. जो तिला समजून घेईल, तिचे ऐकून घेईल अशी तिची इच्छा होती. पण ती खूपच लाजाळू असल्याने तिच्यात एखाद्या मुलाकडे जाण्याचा आत्मविश्वास कमी होता. साक्षी जरा निराश राहत होती. तिच्या वर्गातील प्रत्येक जण रिलेशनशिप मध्ये असल्याने ती निराश असायची. एकदा ती कॅन्टीनमध्ये एकटीच जेवताना तिच्या एका जुन्या मैत्रिणीने तिला पाहिले आणि तिला मिठी मारण्यासाठी हसून तिच्या जवळ गेली. तिने "साक्षी.!!!" म्हणताच साक्षीने त्या आवाजाकडे वळून पाहिले, जेव्हा तिने तिच्या जुन्या मैत्रिणीला पाहिले तेव्हा जवळजवळ एका महिन्यापासून दुखी असलेला चेहरा अचानक आनंदाने हसला आणि तिने देखील आनंदाने आवाज दिला श्रुती !! पूर्वी पासून साक्षी आणि श्रुती उत्तम मैत्रिणी होत्या पण श्रुतीच्या वडिलांची काही व्यवसायिक कारणास्तव मुंबईला बदली करण्यात आली होती. श्रुतीला त्यांच्या सोबत मुंबईला जावे लागले.
मुंबईत काम संपल्यामुळे श्रुतीच्या वडिलांनी नाशिकला परत जाण्याचा निर्णय घेतला म्हणून श्रुती 7 वर्षांच्या अंतरानंतर नाशिकला परतली होती. साक्षीने तिला तिच्या परिस्थितीविषयी सांगितले. श्रुती तिच्याकडे पाहून हसली आणि म्हणाली, "ही तुझी समस्या आहे, खरंच ?"
साक्षी रागात म्हणाली, "माझी मजा नको घेऊस !!"
"अगं साक्षी, आपण एकविसाव्या शतकात राहतो. सर्व काही डिजिटल आहे मग का म्हणून तू एवढी टेन्शन घेते आहेस ?"

ते बोलत असताना श्रुतीने साक्षीला “लव्ह मॅचर” नावाच्या ॲपशी ओळख करून दिली. लव्ह मॅचर किशोरांमधील लोकप्रिय ऑनलाइन डेटिंग साइट होती.
साक्षीला त्यात गोडी निर्माण झाली, तिने "हे सुरक्षित आहे की नाही?" या ॲपशी संबंधित विविध प्रश्न विचारले. श्रुति आत्मविश्वासाने म्हणाली "येस !!" तिने घरी पोहोचताच आपला फोन वायफायशी कनेक्ट केला आणि कोणताही विचार न करता तिने "लव्ह मॅचर" डाउनलोड केले. ॲप डाऊनलोड केल्यानंतर तिने आवश्यक असलेले सर्व साइन-अप केले पण सुरक्षेच्या कारणास्तव डीपी न ठेवण्याचा निर्णय घेतला. ॲप स्थापित करण्याच्या तिच्या पहिल्याच दिवशी तिला 100 मॅचेस मिळाले. पण त्या सर्व मॅचेस मधून विशेषतः 1 जण असा होता की तिला तो आवडला. कुरळे केस आणि गडद तपकिरी डोळे असलेला तिच्या वयाचा तरुण, ज्याचे युसरनेम अँडी ठेवले होते. त्याच्याकडे फॅशनची एक अनोखी शैली होती जी तिला आकर्षित करत होती. त्याने आपला अर्धा चेहरा झाकण्यासाठी मुखवटा वापरला होता आणि सैल कपडे घातले होते. तिने विचार न करताच त्याचा प्रोफाईलवर स्वाइप केली, तिने तिच्या उत्तरासाठी 2 दिवस वाट पाहिली. 3 तारखेला तिने तिच्या फोनवर एक रिंग ऐकली. "ॲप मॅच". अँडीने तिच्या प्रोफाइलवर होकाराने स्वाईप केले होते. अँडीने तिला "हाय" पाठविले. तो मेसेज वाचल्यानंतर ती उत्साहित झाली आणि भयभीत देखील झाली. पण तिने स्वतःला शांत केले आणि हॅलो टाकले. एक आठवडा गेला आणि ते चांगले मित्र बनले. साक्षी सर्वकाही त्याला सांगत असे. हिवाळ्याचे दिवस होते, तिच्या परिवारात कोणाचा मृत्यू झाला होता त्यामुळे साक्षीचे आई वडील बाहेर गावी निघाले होते. साक्षीने त्यांच्याबरोबर येण्याचा आग्रह धरला. पण त्यांनी "आम्ही ५-६ तासात परत येऊ, तू आता एक मोठी मुलगी आहेस. स्वत: ची काळजी घेऊ शकतेस." असे सांगत समजावले.
निघताना ते म्हणाले "बाय, घराची काळजी घे."

साक्षी घरात एकटीच होती, रातकिड्याच्या आवाजाने ती थोडी घाबरलेली होती. तिच्या फोनवर मेसेज आला, तिने पाहिले, मेसेज अँडीचा होता. "हाय, आता भेटू?" साक्षी: "सॉरी मी थोडी कामात आहे."

अँडी : नाही तू कामात नाहीयेस , मी तुला पाहू शकतो.

साक्षी: गम्मत करू नकोस, मी एकटीच घरी आहे.
हे तिने म्हणायला नको होते. तेव्हा साक्षीने विचारले की, मी कोठे राहते हे तुला कसे कळले. अँडीने "मी ॲपवर तुझी लोकेशन बघितली आहे." असे म्हणत रिप्लाय दिला. अचानक साक्षीने दरवाजावर ठोका ऐकला "नॉक-नॉक". ती घाबरुन गेली, दार सतत ठोठावले जात होते. ती भीतीपोटी हलली देखील नाही, दरवाजावरील ठोके थांबले आणि एक आवाज आला, "साक्षी, कृपया दरवाजा उघड!" तो आवाज खूपच आकर्षक होता ज्यामुळे ती दार उघडायला गेली. तो अँडी होता. तिने दरवाजा बंद करण्यापूर्वीच अँडी आत घुसला. आता अँडी भूतासारखे घर फिरत होता. साक्षी त्याला बाहेर जाण्यास विनंती करत होती. पण तिचे तो ऐकत नव्हता. अँडी अचानक थांबला आणि साक्षीला "तुला माझा पूर्ण चेहरा बघायचा आहे का?" अशी पुन्हा पुन्हा वारंवार विचारणा करु लागला. त्यामुळे साक्षीला भीती वाटायला लागली होती.
अँडीने साक्षीकडे वळून आपला मुखवटा काढून घेतला. त्याचा अर्धा चेहरा जाळला होता. अँडीने ज्याप्रकारे तिच्याकडे पाहिले त्या चेहऱ्यामुळे ती प्रचंड घाबरली. त्याने आपल्या शर्टमधून चाकू काढून तिच्याकडे धाव घेतली. ती तिच्या बेडरूममध्ये पळाली. तिने बेडरूममध्ये स्वतःला लॉक केले आणि फोनवरून "100" नंबर डायल केला. अनिकेतबाहेरून दार वाजवत होता. पोलिसांचा नंबर लागला, तिने तक्रार दाखल केली, 15 मिनिटांतच पोलिसांनी येऊन अँडीला अटक केली. घराबाहेर पडताना अँडीने पुन्हा एकदा साक्षीकडे टक लावून बघितले आणि म्हणाला, "जमेल तितकी काळजी घे."

पोलिसांनी साक्षीला अँडी मनोरुग्ण सीरियल किलर असल्याचे सांगितले. त्याने आजवर अनेक तरूण मुलींना आपल्या जाळ्यात फसवून मारून टाकले होते. साक्षीच्या अंगावर काटा आला, त्या घटनेनंतर तिने ॲप काढून टाकले. पुन्हा तशा प्रकारच्या ॲपचे नावही काढले नाही.

प्रारब्ध ढवळे (नाशिक)

विद्यार्थी, ॲनिमेशन डिपार्टमेंट, केटीएचएम कॉलेज, नाशिक

dhavale.prarabdha@gmail.com

व्यवसाय आणि तंत्रज्ञान

प्रदीप मोकळ

आधुनिक काळातील तंत्रज्ञानाचा उपयोग करून आपला व्यवसाय कसा समृद्ध करता येईल याबद्दलचा हा एक विशेष लेख.

आत्तापर्यंत तुम्ही व्यवसायाबद्दल अनेक गोष्टी, टिप्स, सूचना आणि सल्ले घेतले असतील, अभ्यासले असतील आणि बहुतंशी त्यांचा उपयोग देखील करून घेतला असेलच. मुळातच "व्यवसाय किंवा उद्योग" हे एक अजब रसायन आहे आणि म्हणूनच उद्योजकाने सतत प्रयोगशील असणे गरजेचे आहे. गम्मत बघा डॉक्टर, इंजिनीअर किंवा अकौंटंट होण्यासाठी काही विशिष्ठ शिक्षणाची आवश्यकता असते, उदा. डॉक्टर म्हटल कि सायन्स आणि त्यातल्या त्यात जीवशास्त्र शिकणे आवश्यक, इंजिनीअर म्हटले कि गणित कसे पक्के हवे आणि काही क्षेत्रात तर हिशेब जमलाच पाहिजे. पण व्यवसायच कसं आहे बघा ना, इथे सायन्स, कॉमर्स किंवा आर्ट्स काहीही येत असेल किंवा येत नसेल तरी प्रवेश मिळतो. हीच तर गम्मत आहे, महत्वाचे हे नाही कि तुम्हाला काय येते किंवा काय येत नाही, महत्वाचे हे आहे कि तुमची शिकण्याची इच्छा आहे का? आणि फक्त ह्या एका नियमावर तुम्ही तुमचा व्यवसाय वा उद्योग सुरु करू शकतात, वाढवू शकतात आणि मोठा करू शकतात. तर आज मी इथे दिवाळीच्या ह्या शुभमुहूर्तावर आपणा सर्वांना काही अत्यावश्यक अशा गोष्टी सांगणार आहे, ह्या गोष्टींचा तुम्ही व्यवस्थित अभ्यास केला, तुमच्या उद्योग व्यवसायात अवलंब केला तर मला खात्री आहे कि तुमच्या व्यवसाय वा उद्योगाची नक्कीच भरभराट होईल. गेल्या कित्येक वर्षात देशभरातील अनेक व्यवसायिक आणि उद्योजकांना भेटण्याचा, त्यांच्यासोबत बोलण्याचा, काम करण्याची मला संधी मिळत गेली आणि त्या प्रत्येकाकडून नेहमी मला नवीन काही शिकायला मिळाले. त्याच अनुभवातून मी इथे तुमच्यापुढे व्यवसायाची पंचसुत्री मांडत आहे, आशा आहे तुम्ही याचा उपयोग कराल. माझी स्वत:ची व्यवसायाबद्दल एक व्याख्या आहे, मी नेहमी म्हणतो कि

"व्यवसाय म्हणजे फक्त नफा मिळविणे नव्हे तर व्यवसाय म्हणजे वाढत जाणारा नफा."

आणि त्यासाठी अत्यावश्यक अशी हि पाच सुत्र -

१) ग्राहक मिळविणे (CUSTOMER ACQUISITION):

व्यवसायाचे स्वरूप कितीही लहान किंवा मोठे असले तरी हि एक गोष्ट -
"ग्राहक" - म्हणजेच प्रत्येक व्यवसायाचा श्वास आहे. अगदी रस्त्याच्या बाजूचा चहाचे दुकान असो, किंवा मग जगातील सर्वात मोठी चहाची कंपनी, जितकी गरज त्या रस्त्यालगतच्या चहा दुकानदाराची तीच गरज जगातील सर्वात मोठ्या चहा कंपनीची, आणि ती म्हणजे "ग्राहक" तुम्ही कोणत्याही व्यवसायात असले तरी "एक नवीन ग्राहक जोडणे" याला तुमच्या कामात प्राधान्य देणे अनिवार्य आहे.
ग्राहक जोडताना त्याच्या गरजा समजून घेणे, त्याचे समाधान पुरविणे, त्याला त्याच्या गुंतवणुकीचा अधिकाधिक परतावा मिळेल याची काळजी घेणे, मूल्यवर्धित सेवांवर भर देणे, जाहिरात, विपणन, प्रचार, प्रसार, वस्तू वा सेवेचा उत्तम दर्जा या आणि अशा अनेक गोष्टीच्या मदतीने आपण आपले सद्य ग्राहक टिकवून, नवीन ग्राहक जोडू शकतो.
लक्षात असुद्या 'ग्राहक' हा व्यवसायाचा श्वास आहे

आधुनिक काळात वरील सूत्राचा उपयोग करण्यासाठीचे तंत्र:
नवीन ग्राहक मिळविण्यासाठी आधुनिक काळात फेसबुक, इंस्टाग्राम व तत्सम सोशल मिडीयाचा मार्केटिंग करण्यासाठी उपयोग करू शकतात, यात प्रामुख्याने आपल्या व्यवसाय उद्योगाच्या दुष्टीने अनुकूल ग्राहक वर्गापर्यंत कमी वेळेत आणि वाजवी खर्चात पोहचता येते. यासाठी आपल्याला व्यापाराच्या दृष्टीने योग्य अशा सेल्स फनेल चा उपयोग करावा लागेल.

२) ओळख निर्माण करणे (BRAND RECOGNITION):

व्यवसायात ग्राहकांची भुमिका व गरज आपण समजून घेतली आता महत्वाचा विषय आहे की हे ग्राहक आपल्या वस्तू वा सेवा का निवडतील किंबहुना आपल्या वस्तू वा सेवांचा ग्राहक त्यांच्या जीवनाचा अविभाज्य अंग बनवतील का? यासाठी गरज आहे ती म्हणजे आपल्या व्यवसायाची एक विशिष्ठ ओळख निर्माण करणे. एक उदाहरण बघूया, आपल्या ऑफिस किंवा दुकानजवळच एक चहाचे दुकान असते, पण बऱ्याचदा आपण थोडे पुढे जाऊन दुसऱ्या चहाच्या दुकानात जातो आणि तिथे चहा पितो. म्हणजेच एक ग्राहक म्हणून आपण थोडे अधिक कष्ट घेतो आणि एका विशिष्ठ ठिकाणी जाऊन वस्तू खरेदी करतो, थोड्याफार फरकाने

आपल्या सर्वांच्या बाबतीत असे घडते. वरील उदाहरणात विचार करण्याची गोष्ट ही आहे की आपण एक ग्राहक म्हणून तोच चहावाला का निवडतो, याची बरीचशी कारणे असू शकतात, कदाचित चव, स्वच्छता, किंमत, सेवा किंवा त्या दुकानदाराचे त्याच्या ग्राहकांना सेवा देण्याची पद्धत यापैकी काहीही. पण एकमात्र नक्की की त्यात काहीतरी विशेष असते जे आपल्या जवळच्या दुकानात आपल्याला मिळतनाही. आणि बऱ्याचदा किंमत जास्त असली तरीदेखील आपण ते लांबचेच दुकान निवडतो, कारण किमतीपेक्षा मुल्य अधिक असते. हेच आपल्याला आपल्या व्यवसायात करणे गरजेचे आहे. आपली वस्तु किंवा सेवेचा दर्जा, त्याची किंमत, ग्राहकासोबत असलेले आपले नाते या अशा प्रकारच्या गोष्टींमध्ये आपल्याला एक विशिष्ठ ओळख निर्माण करणे गरजेचे आहे यालाच Branding असेही म्हणतात, आणि आपल्या ग्राहकांचा आपल्यासोबतचा Brand Experience यामध्ये अत्यंत महत्वाचा आहे. याचाच उपयोग आपल्या व्यवसायाचे Word of Mouth (मार्केटिंगमधले सर्वात प्रभावशाली तंत्र) निर्माण करण्यासाठी देखील होतो.

आधुनिक काळात वरील सूत्राचा उपयोग करण्यासाठीचे तंत्र:
आपली एक स्वतंत्र ओळख निर्माण व्हावी म्हणून आपल्या व्यवसायाचे Online Presence कसे आहे याकडे काळजीपूर्वक लक्ष द्यायला हवे. जसे कि आपल्या व्यवसायानुरूप सोशल मिडीयाचा उपयोग, त्यावरील बिजिनेस पेज तयार करणे, गुगल सर्च इंजीन च्या तंत्रज्ञानावर बनवलेली वेबसाईट, गुगल च्या लोकल बिजिनेस लिस्टिंग, त्यावरील आपल्या ग्राहकांच्या प्रतिक्रिया (Reviews), त्याचप्रमाणे इतर बिजिनेस लिस्टिंग साईट वरील लिस्टिंग याकडे देखील लक्ष देणे गरजेचे आहे. या सर्व माध्यमांमधून आपल्या व्यवसायाची वैशिष्ठे ग्राहकासमोर वारंवार Text, Image, Video अशा वेगवेगळ्या पद्धतीने जाणे महत्वाचे आहे.

३) महसूल मिळविणे (Revenue Generation):

व्यवसायात फक्त ग्राहक असून किंवा ओळख निर्माण करून होत नाही, सोबत महसुल तयार करणे आवश्यक आहे. याबद्दल थोडे सविस्तर बोलूया, आपल्याकडे किती ग्राहक आहेत, ते वर्षातुन कितीवेळा आपल्याकडून खरेदी करतात, त्यांच्या खरेदीचे मुल्य किती असते हे तपासणे गरजेचे आहे समजा एक ग्राहक महिन्याला एकदा दहा हजारांची रुपयांची खरेदी आपल्याकडून करीत असेल, तर तोच ग्राहक महिन्यातुन एकापेक्षा जास्तवेळा आपल्याकडे कसा येईल यासाठी काम होणे अपेक्षित आहे.

जेंव्हा जेंव्हा ग्राहक येईल त्यावेळी पूर्वीपेक्षा अधिक किमतीची खरेदी करेन यासाठी प्रयत्न केला पाहिजे हे सर्व Cross Selling, Up Selling, Various Offerings, Loyalty Schemes च्या माध्यमातून साध्य होऊ शकते, लवकरात लवकर ही तंत्र आत्मसात करून त्यांचा अवलंब करा.

आधुनिक काळात वरील सूत्राचा उपयोग करण्यासाठीचे तंत्र:
महसूल मिळविण्यासाठी सर्वात प्रथम महसूल जमा करण्याच्या पद्धतीमध्ये आधुनिक तंत्रज्ञानाचा उपयोग करणे क्रमप्राप्त आहे, त्यासाठी फोनपे, पेटीएम, गुगल पे किंवा तत्सम UPI Based प्रणाली आणि विविध Payment Gateways चा उपयोग करता येयील. त्याचबरोबर विविध प्रकारच्या cashback, promo code, reference code, loyalty program, club membership program, revisit coupons, add on offer हि देखील काही पर्याय उपयोगात आणू शकतात.

४) मूल्यवर्धन करणे (Value Proposition):

Value Proposition म्हणजेच मूल्यवर्धन करणे ही खरं म्हणजे एक कला आहे. हे कसब एकदा अंगी भिनले की व्यवसायाची मजा काही औरच. त्यासाठी आपण 'मूल्यवर्धन करणे' म्हणजे नेमके काय हे समजुन घेऊया. वस्तूला एक किंमत असते आणि एक असते 'मुल्य' एकाच नाण्याच्या दोन बाजु समजा, खरेदी-विक्रीत जी काही देवाण घेवाण होते ती किंमत आणि मूल्याची असते. किंमत ही बऱ्याचदा रुपयांमध्ये (Unit) मोजली जाते तर मुल्य हे प्रमाणात (Ratio) मोजले जात असते. किमतीच्या बदल्यात मुल्य जितके अधिक तितकिच व्यवसायातील शाश्वतता आणि विश्वास यांत वाढ होत असते. वरील उदाहरणांचाच संदर्भ घेऊया, एका विशिष्ट किंमतीत आपण जेव्हा तो चहा विकत घेतो त्यावेळी त्याचे उत्पादन मुल्य, सेवा मुल्य याहूनही अधिक त्याचे ग्राहकाच्या लेखी समाधान मुल्य किती यावर त्या व्यवसायाचे यश अवलंबुन आहे, यासाठी कदाचित किमतीपेक्षा वेगळ्या काही गोष्टींची गरज असते आणि त्या म्हणजे त्या चहाची चव, तो चहा देण्याची पद्धत, त्या दुकानातील स्वच्छता आणि तो चहा ग्राहकांना देतांना तेथील कर्मचाऱ्यांचा ग्राहकांसोबतचा व्यवहार ह्या सर्वच गोष्टी ग्राहकाचे समाधान मुल्य ठरविण्यास भाग पाडते. ग्राहकाने मोजलेल्या किंमतीच्या प्रमाणात जितके समाधान मुल्य जास्त तितका तो व्यवसाय समृद्ध होत जाणार. तुम्हीदेखील तुमच्या वस्तु व सेवा प्रदान करतांना त्यांच्या विक्री किमतीसोबतच त्याचे मुल्यवर्धन कसे करता येईल याकडे लक्ष द्यायला हवे.

आधुनिक काळात वरील सूत्राचा उपयोग करण्यासाठीचे तंत्र:
आपल्या वस्तू किंवा सेवा यांत मूल्यवर्धन करण्यासाठी आजचे आधुनिक तंत्रज्ञान एक जादूचा दिव्यातील जीन प्रमाणे काम करते. आपल्या वस्तू किंवा सेवा यांना जागा, स्थळ, काळयांच्या कक्षेतून बाहेर काढून योग्य ग्राहकांपर्यंत पोहचविण्याची किमया याजिनीमध्ये आहे. घरपोच सुविधा, नो कोस्ट EMI, ईझी रिटर्न, मुबलक ऑप्शन, वस्तूंची सर्व माहिती एकाच ठिकाणी, तुलनात्मक तक्ते, इतर वस्तुन्सोबतची तुलना व फरक या सर्व गोष्टी एकाच ठिकाणी उपलब्ध करून देता येतात. Shopify, Amazon, Instamojo, Weebly यासारखे बरेचशे platform उपलब्ध आहेत ज्यातून आपण आपल्या वस्तू आणि सेवांचे मूल्यवर्धन करू शकतात.

५) व्यवसाय विस्तार करणे (Business Expansion):

व्यवसायात वरील चतु:सूत्रीचा उपयोग करुन यश मिळवता येईलच, परंतु व्यवसायाचा प्रवास इथेच संपत नाही, व्यवसायाचा मुख्य उद्देश हा "स्वातंत्र्य" आहे. निर्णयाचे स्वातंत्र्य, आर्थिक स्वातंत्र्य, निवडीचे स्वातंत्र्य. आणि अशा स्वातंत्र्यप्राप्तीसाठी गरज असते व्यावसायिक साम्राज्य निर्माण करण्याची, व्यवसाय सुरळीतपणे पुढे जाऊ लागला की वेळ असते ती व्यवसायाचा विस्तार करण्याची. बऱ्याचदा व्यवसायाचा विस्तार करणे खुप सोपे वाटते परंतु ते तितकेच क्लिष्ट आहे, व्यवसाय वाढवताना ज्या तंत्र मंत्रांचा आपण उपयोग करतो त्याहून थोडे वेगळ्या कार्यपद्धतीचा अवलंब करणे इथे क्रमप्राप्त आहे. आपल्या व्यवसायात नेतृत्वाची दुसरी फळी निर्माण करणे, मागणी आणि पुरवठ्यावर नियंत्रण ठेवणे, व्यवसाय मुल्य वाढवणे, नवीन तंत्रज्ञानाचा अवलंब करणे, वेळोवेळी विशिष्ट तज्ज्ञांकडून मार्गदर्शन घेणे, एकाचवेळी वेगवेगळ्या विभागांमध्ये संयुक्तिकरित्या काम करवून घेणे आणि सर्वात महत्वाचे म्हणजे व्यवसायाचा विस्तार करताना आपल्या व्यवसायात इतर व्यवसायांना सामील करून घेणे जमायला हवे.

आधुनिक काळात वरील सूत्राचा उपयोग करण्यासाठीचे तंत्र:

एकदा व्यवसाय गती धरायला लागला कि आधुनिक तंत्रज्ञानाची मदत घेवून तुम्ही त्याचा विस्तार करू शकतात, यासाठी CRM, ERP या सारख्या उद्योग व्यवस्थापनास लागणाऱ्या सोफ्टवेअर पासून ते वेगवेगळ्या ठिकाणी लक्ष ठेवणाऱ्या CCTV पर्यंतचा उपयोग करू शकतात. यातच बिलिंग, स्टोअर किंवा मार्केटिंग साठी देखील काही विशिष्ठ सोफ्टवेअर उपलब्ध आहेत.

अपेक्षा आहे, व्यवसायातील ह्या आधुनिक पंचसूत्रांचा आपण पुरेपूर उपयोग कराल आणिआपल्या व्यवसायाला समृद्ध कराल.

सर्व वाचकांना दिवाळीच्या आणि नववर्षाच्या खुप खुप शुभेच्छा.

Stay Inspired, Believe in Karma!!!

प्रदीप मोकळ

व्यवसाय मार्गदर्शक
About.me/Mokal.Pradeep

सुरक्षित आर्थिक व्यवहारांसाठी....

विहंग घाटे

डेबिट कार्डचा वापर जितक्या सहजतेने विविध प्रकारच्या व्यवहारांसाठी केला जाऊ शकतो, तितक्याच सहजतेने फसवणुकीचे प्रकारही सहज घडवून आणले जाऊ शकतात. कोणताही सायबर गुन्हेगार तुमची कष्टाची पूंजी क्षणात नाहीशी करण्यासाठी तुमचा पिन क्रमांक, सीव्हीव्ही क्रमांक आदी संवेदनशील माहिती मिळवू शकतो. हे टाळण्यासाठी डेबिट कार्डचा वापर करताना नेहमी काळजी घेणे आवश्यक आहे.

डेबिट कार्ड सुरक्षित आहे का?

डेबिट कार्ड थेट तुमच्या बँकेच्या खात्याशी जोडलेले असून, त्यामध्ये तुमची बचत ठेवलेली असते. डेबिट कार्डचा बहुतांश वापर क्रेडिट कार्डप्रमाणेच केला जातो. याचा अर्थ असा की तुमच्या खात्यामध्ये पुरेशी रक्कम असेल तरच डेबिट कार्डच्या माध्यमातून ऑनलाइन पेमेंट आणि खरेदी करता येऊ शकते, तसेच रक्कमही काढता येते. मात्र, डेबिट कार्डाच्या माध्यमातून वापर वाढल्याच्या पार्श्वभूमीवर ऑनलाइन घोटाळेही वाढण्याची शक्यता नाकारता येत नाही.

घोटाळे टाळण्यासाठी काय कराल?

१. महत्त्वाचे क्रमांक लक्षात ठेवा

डेबिट कार्डाच्या मागे असणारा सीव्हीव्ही क्रमांक लक्षात ठेवण्याचा प्रयत्न करा. हा क्रमांक कृपया मोबाइलवर सेव्ह करून ठेवू नका.

२. कोणावरही विश्वास नको

आपल्या कुटुंबातील सदस्य सोडून अन्य कोणत्याही व्यक्तीला आपल्या डेबिट कार्डची माहिती देऊ नका. डेबिट कार्डचा पिन क्रमांक कोठेही अथवा मोबाइलवर लिहून ठेवण्याची चूक करू नका.

३. पिन क्रमांक बदलण्याची गरज

वेळोवेळी ग्राहकांनी डेबिट कार्डचे पिन क्रमांक बदलण्याची गरज आहे. कोणत्याही संकटात अडकायचे नसेल तर पिन क्रमांक असा ठेवा की सहज लक्षात येईल. ऑनलाइन खरेदी करताना विश्वासार्ह वेबसाइटचीच निवड करा. जे ऑनलाइन पेज ओपन करणार असाल, त्याच्या ॲड्रेस बारमध्ये HTTP ही अक्षरे असणे आवश्यक आहे.

४. संशयास्पद ई-मेलना उत्तरे देऊ नका

हल्ली सायबर चोरट्यांकडून कॉल, ई-मेल आणि मेसेजच्या माध्यमातून ग्राहकांना लुबाडण्याचे गोरखधंदे वाढले आहेत. हे चोरटे आपण बँकेतून, कंपनीतून फोन करीत असून, ग्राहकांचा विश्वास संपादन करून बँकेच्या खात्याचा क्रमांक, पिन आणि अन्य वित्तीय माहिती मिळवतात. अशा प्रकारचे फोन आल्यास लगेच बँकेशी संपर्क साधावा.

५. मोबाइल सुरक्षित ठेवा

विविध प्रकारच्या बँकिंग व्यवहारांसाठी मोठ्या प्रमाणावर मोबाइलचा वापर केला जातो. त्यामुळे कोणत्याही तिऱ्हाइत व्यक्तीच्या हाती मोबाइल सोपवू नका. डिजिटल व्यवहारांचे प्रमाण वाढल्याने सर्व प्रकारचे ओटीपी आणि पासवर्ड हल्ली मोबाइलवरच येतात. सर्वांत महत्त्वाचे म्हणजे मोबाइलला शक्यतो पासवर्डचे संरक्षण द्या.

विहंग घाटे (पुणे)

गेल्या दहा वर्षांपासून महाराष्ट्र टाइम्स, पुण्यामध्ये कार्यरत...
टेक्नॉलॉजी, पर्सनल फायनान्स आणि व्यापार हे आवडीचे विषय...
तत्पूर्वी मुंबई प्रहार, सकाळ आणि लोकसत्तामध्ये कार्यरत..

gvihang@gmail.com

थोडक्यात

आर जे शोनाली

आज आपल्या आयुष्यातील जवळपास ८० % गोष्टी या इंटरनेट चा वापर करून होतात. पण हे करत असताना सतर्क राहणे आवश्यक आहे. आपली खासगी माहिती ही सोशल मीडियावर पोस्ट न करणे. ज्याचा गैरफायदा घेऊन कुणी तुम्हाला अडचणीत आणू शकते. कोणत्याही अनोळखी लिंक वर क्लिक करण्यापूर्वी विचार करा, त्यामुळे तुमचे अकाऊंट हॅक होऊ शकते.

जर एखाद्या व्यक्तीचे अकाऊंट संशयीत वाटल्यास त्याचा स्क्रीनशॉट काढावा, आणि ती लिंक सायबर पोलिसांच्या कडे तक्रार करावी. दर तीन महिन्यांनी आपला पासवर्ड बदलावा. आणि कितीही चांगली मैत्री झाली असेल तरी आपले आर्थिक व्यवहार हे सोशल मीडिया वर भेटलेल्या लोकांपासून दूर ठेवावे.

जागरूक राहून सायबर विश्व एन्जॉय करा.

आर जे शो शो शोनाली

रेडिओ सिटी ९१.१ पुणे

मनांत

पराग आचलिया, सायबर तज्ज्ञ

इंटरनेटच्या वाढत्या वापरामुळे सायबर फसवणुकीचे प्रकारही वाढत चालले आहे. या सर्वप्रकारांपासून स्वत:ला वाचण्याचा एकमेव उपाय म्हणजे सतर्कता आणि जागरूकता. मोबाईलवर येणारा ओटीपी कुणासोबतही शेअर न करणे आणि इंटरनेट बँकिंगचा पासवर्ड वारंवार बदलणे हे आपणास सायबर फसवणुकीपासून वाचवू शकतात. तरी सुद्धा फसवणूक झाली असल्यास ताबडतोब सायबर पोलिसांना संपर्क करून झालेल्या सर्व प्रकारची माहिती देऊन पोलिसांची मदत घेणे महत्वाचे आहे.

महिला सुरक्षा ॲप्स

तेजा दुर्वे, कोल्हापूर

महिला सुरक्षा ॲप्स अस्सल आहेत की नाही ते कसे कळणार.? खासगी कंपन्या सुद्धा असे ॲप्स विकसित करतात. उदा. महिला सुरक्षा ॲप्स वगैरे.. यामध्ये महिलेची वैयक्तिक माहिती द्यावी लागते आणि आपले लोकेशन शेयर करावे लागते. मग यावर विश्वास कसा ठेवावा.? याचा गैरफायदा घेतला गेला तर काय.?

महिला सुरक्षेचे सरकारचे जरी ॲप्स असो तरीही त्याबद्दल काही खात्री असते.? आणि महिलांनी कसं तपासून पाहायचं कि ते ॲप्स सरकारी आणि सुरक्षितच आहेत? प्रत्यक्ष काही गंभीर परिस्तिथी निर्माण झाल्यावर ते कसे वापरावे? त्वरित प्रतिसाद मिळावा म्हणून काही वेगळी उपाययोजना करण्याची गरज आहे.

सायबर दोस्त

मनीषा रतिलाल बागुल

आधुनिक तंत्रज्ञान वाढत असतानाच देशात सायबर गुन्हेही वाढत आहेत. लोकांमध्ये याविषयी माहिती नसल्यामुळे अशा प्रकारचे गुन्हे होत आहेत. या गुन्ह्यांना आळा घालण्यासाठी लोकांमध्ये जागृती होणेही महत्त्वाचे आहे. बँकेचा यूजर आयडी, एटीएम/डेबिट कार्डचा क्रमांक व पिन, पासवर्ड, ओटीपी कोणाही व्यक्तीला देऊ नये, तसेच सायबर गुन्हे कसे घडतात, त्यांची कार्यपद्धती कशी आहे, त्यापासून वाचण्यासाठी काय करावे, याबद्दलची माहिती असणे आवश्यक आहे, इंटरनेट आणि मोबाइलने आपल्या सामान्य जीवनावर आक्रमण केले आहे.इंटरनेटचा जेवढा सकारात्मक वापर केला जातो, तेवढाच किंवा जरा त्यापेक्षा जास्तच नकारात्मक वापर केल्या जातो. हा वापर देशाची अर्थव्यवस्था व जनजीवन डळमळीत करू शकतात. अशा ऑनलाईन गुन्हेगारीपासन सावध रहायला पाहिजे. ह्यालाच माझ्या दृष्टीने सायबर क्राईम म्हणतात. सुक्ष्म विचार जर केला तर आपल्याला रोजच या सायबर क्राइमचा सामना करावा लागतो. आपल्या ई-मेल वर स्पॅम मेल येतात, मोबाईलवर येणारे अनोळखी कॉल्स, मेसेजेस, नेट बँकींग असेल तर त्याचा पासवर्ड, आयडी हॅक होणे हे सर्व प्रकार सायबर क्राइम मध्ये मोडतात. मेलद्वारे फसवणूक, धमकी देणे, खंडणी मागणे अशा कारवायांना सुध्दा सायबर क्राइम म्हणता येईल. हे तंत्र रोजच्या रोज बदलत असत.

दुसरा प्रकार हा सायबर स्टॉकींग..ई-मेल अथवा फेसबुक, सोशल साईट्सद्वारा चॅटींग,वा सरफींगच्या माध्यमातून गुन्हेगार आपली संगणकीय ओळख (आय.डी.),पासवर्ड हॅक करतात...बँक अकाऊंट न पासवर्ड चोरून नागरिकांना मोठ्या प्रमाणात आर्थिक भुर्दंड सोसावा लागतो..
तिसरा प्रकार हॅकींग..संगणकामधे हायकर व हॅकींग ह्या दोन संकल्पना समोर येतात...ई-कॉमर्स साईटवर हॅकींगचे प्रमाण अधिक आहे...ई-मेल,चॅटींग याद्वारे व्हायरस पाठवून संगणक प्रणाली हॅकर च्या नियंत्रणाखाली आणली जाते...व्हायरसचेही विविध प्रकार आहेत...ट्रेजन सारख्या व्हायरसद्वारे कुठल्याही कोपऱ्यात बसून जगभरातील कुठल्याही संगणकावर नियंत्रण ठेवल्या जावू शकते....इतके ह्याचे स्वरूप गंभीर आहे...

पोनोग्राफी हा पाचवा प्रकार... ह्या प्रकारात अश्लील चित्रफीत, छायाचित्रे, मजकूर इंटरनेटद्वारे डाऊनलोड करून प्रसारित करणे, पहाणे,असे प्रकार पोनोग्राफीत सापडतात..... पोनोग्राफीत आपल्या देशात जरी बंदी असली तरी इंटरनेटच्या महाजालातअजून तरी त्यावर बंधने नाहीत... विविध वेबसाईटनी जर पोनोग्राफीच्या लिंक अजिबातबंद केल्या तर अनेक लोक नेटसर्फींग किंवा इंटरनेटचा वापर बंद करतील....संगणक, इंटरनेटवापरतांना आपली कुठलीही गोपनीय माहिती कोणतीही अनोळखी व्यक्ती अथवा वेबसाईटवर अपलोड करू नका....आपला पासवर्ड वेळोवेळी बदलत रहा...इंटरनेटचावापर सुरक्षीत करण्यासाठी एन्टिव्हायरस, एन्टिस्पँनवेअर व फायरवॉँल इंस्टॉल करूनवेळोवेळी ते अद्ययावत करावे... पासवर्ड, पिनकोड सुरक्षित राहण्यासाठी आँनलाईन व्यवहार पुर्ण होताच लाँग आऊट करा..ई-मेल द्वारा आलेल्या कोणत्याही लिंक्स काँपीकरू नका...

Tips

१. संगणक वापरकर्त्यांनी हॅकर्सपासून त्यांचे संगणक सुरक्षित करण्यासाठी फायरवॉल वापरावा.

२. वापरकर्त्यांनी त्यांच्या खात्यावर मजबूत संकेतशब्द विकसित केले पाहिजेत, म्हणजे संकेतशब्दामध्ये अक्षरे आणि संख्या समाविष्ट करा आणि संकेतशब्द आणि लॉगिन तपशील सतत अद्यतनित करा.

३. संगणक वापरकर्त्यांनी मॅकॅफी किंवा नॉर्टन अँटी-व्हायरस सारखे अँटी-व्हायरस सॉफ्टवेअर स्थापित केले पाहिजे.

४. मुलांवर लक्ष ठेवा आणि त्यांचा इंटरनेट वापर मर्यादित करा.

५. फेसबुक, ट्विटर, यूट्यूब च्या सुरक्षा सेटिंग्ज तपासा आणि काळजी घ्या.

मनीषा रतिलाल बाग़ुल

प्रिंट मॉडेल आणि 4-5 ब्रँडची राजदूत
अनेक राष्ट्रीय व आंतरराष्ट्रीय पुरस्कार, तरुणांसाठी प्रेरणा म्हणून पुरस्कार प्राप्त

जबाबदारी

ज्योती वाकचौरे

ज्या प्रमाणे शाळेत ज्ञानात्मक विषय शिकविले जातात त्या प्रमाणे शालेय अभ्यासक्रमामध्ये सायबर सुरक्षा हा विषय शिकविण्याची वेळ आलेली आहे. कारण आज अगदी ५-६ वी पासुन च पालक मुलांकडे मोबाइल द्यायला लागले आहे. याचाच विपर्यास होताना दिसतो आहे.

तासतास मोबाइल वर गाणे, गेम, व्हाट्सअॅप, फेसबुक, इंटरनेट वर नको ते मुले बघायला लागली आहे. तसेच शिक्षित, अशिक्षित लोक देखिल सायबर च्या जाळयात अडकताना दिसतात. बँकमधील पैसे, किंवा स्वतःच ओटीपी शेयर करणे या चुकामूळे फसवणूक झालेली आपण बघतो.

यासाठी
१. मुलाना मोबाइल देऊ नये.
२. ओटीपी कोणालाही देऊ नये. कोणतीही बँक कोणताच ओटीपी ग्राहकाकडून घेत नाही.
३. ऑनलाइन व्यवहार करताना सावधानता बाळगावी.
४. ऑनलाइन खरेदी करताना विशेषतः महिलांनी खबदारी घ्यावी.
५. पासवर्ड कोणालाही देऊ नये.

ज्योती वाकचौरे

सामाजिक कार्यकर्त्या

सुरेल

आनंद ओक

आजकाल प्रत्येकाच्या हातात स्मार्टफोन आहे. फेसबुक, इंस्टाग्राम, ट्विटरच्या ह्या सोशल माध्यमातून प्रत्येक छोट्याछोट्या गोष्टीचं स्टेटस पोस्ट केले जातात. कित्येक पर्सनल गोष्टीही सोशल मिडियावर शेअर केल्या जातात.

अनेकदा ह्याचीच माहिती काढून ब्लॅकमेल किंवा मुलींना मेसेज करून वा अन्य प्रकारे त्रास दिला जातो आणि ह्यातूनच पुढे वाईट गोष्टीही घडू शकतात. आपलं सोशल लाईफ आणि पर्सनल लाईफ हे वेगळं ठेवता आलं पाहिजे.

आपल्याबद्दलच्या सगळ्या गोष्टी उघडपणे सोशल मिडियावर पोस्ट करताना त्याने आपल्याला त्रास होणार नाही ह्याची दक्षता प्रत्येकाने घेतली पाहिजे.

आनंद ओक

संगीतकार,
संगीत देवबाभळी ह्या नाटकाच्या संगीतासाठी झी नाट्यगौरव, मटा सन्मान
महाराष्ट्र शासनाचा पुरस्कार
स्पंदन मिडिया स्टुडिओ नावाने रेकॉर्डिंग, पोस्ट प्रॉडक्शन स्टुडिओ
सध्या चित्रपट आणि मालिकांचे काम सुरू

धक्कादायक अनुभव

शलाका भेंडे

माझा व्यवसाय ग्लॅमरस, आव्हानात्मक, बोल्ड आणि सर्जनशील आहे. अँकरिंग म्हणजे दररोज नवीन लोकांना भेटणे, त्यांच्याशी संवाद साधणे, नवीन गोष्टी शिकणे. प्रत्येक फंक्शन मला वेगवेगळ्या प्रकारच्या प्रेक्षकांना सामोरे जाण्याचे नवीन आव्हान देते. आजकाल डिजिटल मीडिया एक लाट आहे. आपण आपला ब्रँड आणि आपला व्यवसाय मोठ्या प्रमाणात बाजारात आणायचा असल्यास, डिजिटल मीडिया उत्तर आहे. परंतु जसे आपण म्हणतो की प्रत्येक नवीन विकासाच्या मागे काही कमी जास्त गोष्टी असतात, तसेच डिजिटल मीडियाचेही आहे. डिजिटल मीडियाच्या सामर्थ्याविषयी आणि त्याच्या फायद्यांविषयी सर्वांना माहिती आहे, परंतु आज मी डिजिटल मीडियाचे माझे काही विकृत अनुभव सांगणार आहे.

मी एक विख्यात सूत्रसंचालक आहे आणि मी कोणत्या प्रकारचे कार्य करते हे लोकांपर्यंत पोहोचवण्यासाठी मी माझी अनेक छायाचित्रे, शोचे व्हिडिओ व्हॉट्सअॅप, फेसबुक, इन्स्टाग्राम इत्यादी सोशल प्लॅटफॉर्मवर पोस्ट करते.! आता जेव्हा मी फोटो खाजगीपणे पोस्ट करते तेव्हा ते केवळ माझ्या फ्रेंडलिस्ट मधील लोकांनाच दिसतात, परंतु त्याचकाही उपयोग नाही. म्हणून मी माझे सर्व फोटो सार्वजनिकरित्या पोस्ट करते. एके दिवशी मला अज्ञात व्यक्तीकडून ईमेल मिळू लागले, त्याने माझ्यासाठी काही वेगळेच नाव वापरले आणि मीच ती व्यक्ती असल्याचा दावा केला! जेव्हा मी त्याच्याशी अक्षरशः भांडण केले , तेव्हा त्याने मला चॅट चा स्क्रिनशॉट पाठवला, ज्यात प्रोफाइल फोटोला चेहरा माझा होता. तेव्हा मला धक्का बसला. हा तर माझ्या फोटोंचा सरळसरळ गैरवापर होत होता. मी त्वरित सायबर सेलकडे तक्रार नोंदविली.

सायबर विभागाने आयपी ॲड्रेस शोधून त्या द्वारे व्यक्तीचा शोध लावला. आणि त्याच्यावर आवश्यक ती कारवाई केली. सर्वात आधी केवळ स्क्रिनशॉट वरून माहिती काढणे, संबंधित वेबसाइटशी संपर्क करणे, त्यांच्याकडून आयपी ॲड्रेस मिळवणे, मोबाईल कंपनीकडून त्या आयपी ॲड्रेस ची लोकेशन मिळवणे, आणि ते सर्व ट्रेस करणे या मोठ्या आणि किचकट प्रक्रियेमधून गेल्यावर खरा गुन्हेगार सापडला.

पुढील धक्का तर मोठा होता जेव्हा माझ्या मित्रांनी विचित्र मजकूर आणि चुकीच्या वयासह वेगवेगळ्या डेटिंग ॲप्सवर वापरल्या गेलेल्या माझ्या फोटोंचे स्क्रीनशॉट्स पाठविणे सुरू केले.

हे खूप त्रासदायक होते आणि आपली व्यावसायिक तसेच वैयक्तिक प्रतिमा धोक्यात आल्याचेही लक्षात आले. परंतु अशावेळी कणखर बनणे, सतर्क आणि सक्रिय असणे महत्वाचे असते.

तर मित्रांनो, सोशल मीडियाचा योग्य प्रकारे वापर कसा करावा हे शिका. वेळप्रसंगी आवश्यक कारवाई करण्यास कधीही अजिबात संकोच करू नका. प्रत्येक समस्येसाठी उपायही आहेत. मजबूत व्हा आणि त्यासाठी संघर्ष करा.

कारण ज्या गोष्टीला मी सामोरे गेले, त्या गोष्टीला इतर कोणी सामोरे जाऊ नये अशी माझी इच्छा आहे. म्हणून जर तुम्ही खबरदारी घेतली तर तुम्हाला कधीही या तणावाचा सामना करावा लागणार नाही.

शलाका भेंडे

सुप्रसिद्ध सूत्रसंचालिका, मॉडेल

आम आदमीवाली सायबर सुरक्षा

आर जे शुभी

सायबर सिक्युरिटी हा खूप मोठा विषय आहे. बऱ्यापैकी माहिती असूनही नसल्यासारखं आपण दर्शवतो, आपल्यासारखी साधी लोक, आम आदमी.. ! बँकेकडून किंवा इतर अनेक स्रोतांकडून नेहमी सांगितलं जात की 'ओटीपी' सारख्या गोष्टी कधीच कोणासोबतही शेयर करायच्या नसतात, हे म्हणजे अगदी दागिन्यांसारखं आहे, कोणी मागितला आणि तुम्ही लगेच काढून दिला. इतका महत्वाचा तो 'ओटीपी' असतो, आणि अनेक लोक सर्रास कसलाही विचार न करता शेयर करत असतात.

आपण एवढी छोटीशी जरी गोष्ट पाळली ना की आपला 'ओटीपी' कोणालाही शेयर करायचा नाही, तरी खूप मोठे नुकसान होण्यापासून आपण स्वतःला वाचवून शकतो. स्वतःची सायबर सुरक्षा पाळली जाऊ शकते. सध्या काही दिवसांपूर्वीच नाशिक मध्ये पेटीएम सारख्या दिसणाऱ्या पण खोट्या ॲप आणि वेबसाईट वरून पैसे उकळण्यात आले. ऑनलाईन व्यवहार करताना वेबसाईटचा युआरएल (URL) व्यवस्थित बघायला हवा, HTTPS म्हणजेच सुरक्षित आहेत कि नाही हे तपासायला हवं. एवढं जरी केलं तरी मला असं वाटतं की आर्थिक फसवणुकीपासून आपण वाचू शकतो. खूप छोट्या छोट्या गोष्टी शेयर करतानाही आपण लक्ष ठेवलं पाहिजे. आपण अनेक गोष्टी सोशल मीडियावर केवळ आपल्या फ्रेंड लिस्टमधल्या लोकांसाठी शेयर करत असतो, पण जे फ्रेंड नाहीयेत त्यांनाही हा ताबा मिळू शकतो. त्यामुळे जर छोट्या छोट्या गोष्टींकडे आपण बारकाईने लक्ष दिलं तर अडचण येणार नाही. एखादं ॲप डाउनलोड केल्यावर किंवा एखाद्या गेम मध्ये कॅमेरा चालू करण्याची परवानगी देण्याची काहीच गरज नाहीये. काही गोष्टी आपण व्यवस्थित पाळल्या तर आपण 'सायबर संकटात' सापडण्यापासून वाचू शकतो.

आर जे शुभी

रेडिओ मिरची ९८.३ नाशिक

PRO TIPS

संतोष खडसरे

सायबर सेक्युरिटी ही महत्वाकांक्षी लोकांसाठी आकर्षक कारकीर्द आणि जगाला एक चांगले स्थान बनवण्याचा एक चांगला मार्ग आहे. आपणास सायबर सेक्युरिटीमध्ये करियर हवे असल्यास प्रतीक्षा करू नका. आपणास विशिष्ट वय किंवा लिंग असणे आवश्यक नाही. आपल्याला पुढे जाण्यासाठी कोणत्याही विशिष्ट मान्यता किंवा प्रमाणपत्र किंवा अभ्यासाचे स्थान आवश्यक नाही. सायबर सिक्युरिटीमधील बऱ्याच नोकऱ्या अत्यंत तांत्रिक असतात, परंतु काही तांत्रिक नसतात. सायबर सिक्युरिटीच्या क्षेत्रामध्ये लोक कौशल्ये, नेतृत्व कौशल्य आणि व्यवसाय समजून घेणे आवश्यक आहे.

अशी अनेक क्षेत्रे आहेत ज्यात आपण आपले करियर बनवू शकता:

फॉरेन्सिक संगणक विश्लेषक
माहिती सुरक्षा विश्लेषक
पेमेंटेशन टेस्टर
सुरक्षा आर्किटेक्ट
आयटी सुरक्षा अभियंता
सुरक्षा प्रणाल्या प्रशासक
आयटी सुरक्षा सल्लागार
नेटवर्क प्रशासक
नेटवर्क अभियंता
वेब प्रशासक
मुख्य माहिती सुरक्षा अधिकारी (सीआयएसओ)

मी तुम्हाला काही टिपा आणि सूचना देऊ इच्छित आहे -

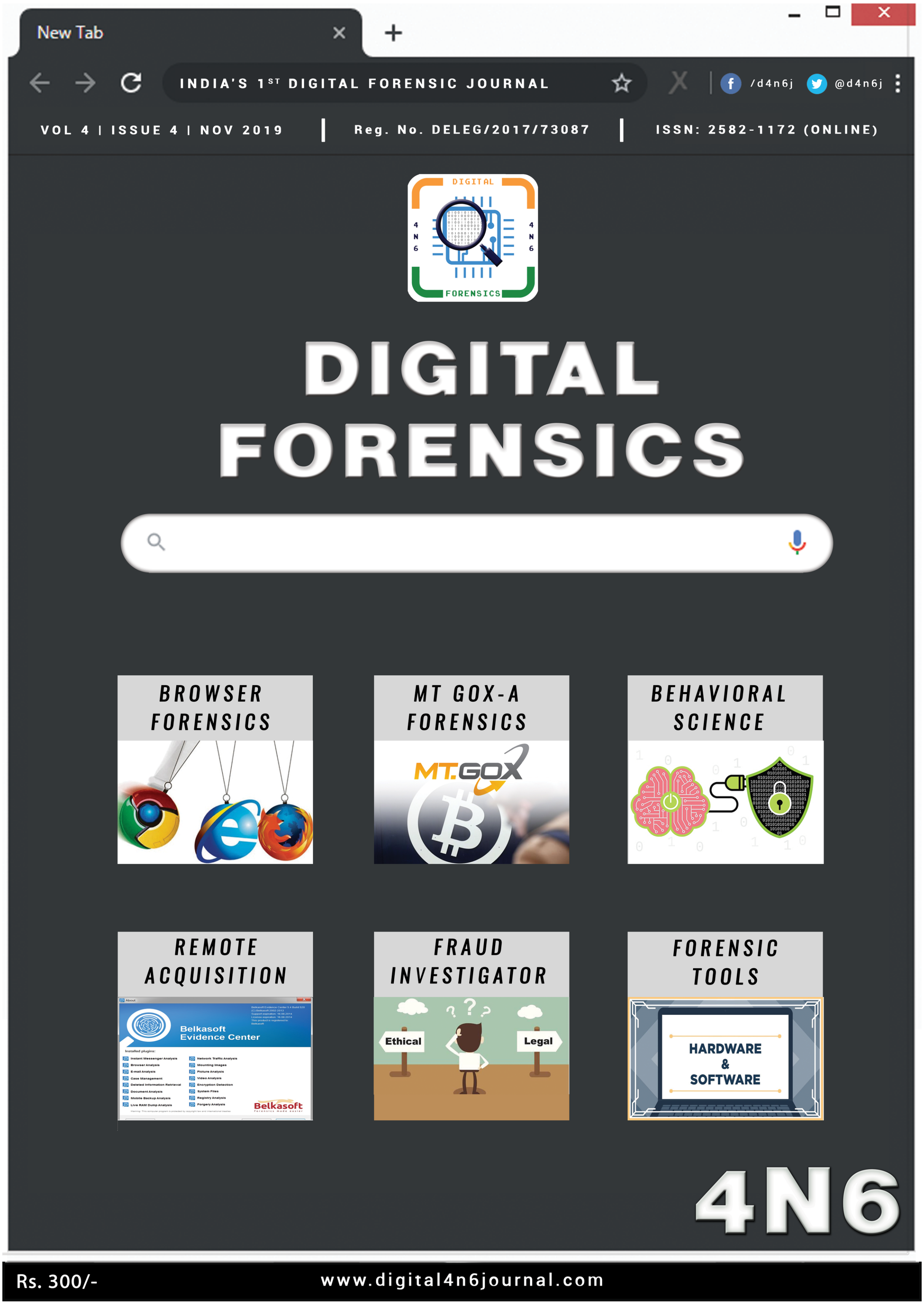
- या क्षेत्रात प्रवेश करण्यासाठी आपल्याला अभियंता किंवा संगणक विझार्ड असणे आवश्यक नाही.
- आपल्याकडे संगणक, नेटवर्किंग, प्रोग्रामिंग इ. बद्दल ज्ञान असले पाहिजे.
- नामांकित संस्थांकडून व्यावसायिक सायबर कोर्स करा.
- मार्गदर्शन करणार्या मार्गदर्शकाचे मार्गदर्शन घ्या.
- इंटर्नशिप प्रोग्राममध्ये भाग घ्या.
- ब्लॉकचेन, आयओटी, मशीन लर्निंग, कृत्रिम बुद्धिमत्ता इ. सारखी नवीन तंत्रज्ञान जाणून घ्या सायबर सुरक्षेसंदर्भात परिषद, कार्यशाळा आणि चर्चासत्रांमध्ये भाग घ्या.
- नामांकित राष्ट्रीय आणि आंतरराष्ट्रीय जर्नल्समधील आपल्या कौशल्य क्षेत्रात आपले लेख प्रकाशित करा.

नॅसकॉमने नुकताच असा अंदाज लावला आहे की वेगाने वाढणाऱ्या अर्थव्यवस्थेच्या मागण्या पूर्ण करण्यासाठी फक्त 2020 पर्यंत एकट्या दशलक्ष सायबरसुरक्षा व्यावसायिकांची आवश्यकता असेल. 2021 पर्यंत 3.5 दशलक्ष सायबर सुरक्षाची पदे रिक्त होतील असा अंदाजही वर्तविला जात आहे.

मी फक्त इतकेच म्हणू शकतो की जर आपण सायबर सिक्युरिटीमध्ये करिअरसाठी आहात तर तुम्ही योग्यमार्गावर आहात. धीर धरा, कष्ट करा.

संतोष खडसरे

सायबर फॉरेन्सिक लॅबोरेटरी सीईआरटी- इंडिया,
(इलेक्ट्रॉनिक्स आणि माहिती तंत्रज्ञान मंत्रालय) प्रमुख



DIGITAL FORENSICS (4N6)

Discount code for subscribing for November issue of Digital Forensics (For both online and print version). Print version postage only in India

Apply code 'D1WALI'- for 10% discount

Subscribe at www.digital4n6journal.com

फेसबुक व धार्मिक भावना

आवेज काझी

हल्ली सोशल मिडीया हा आपल्या वैयक्तीक जीवनाचा अविभाज्य अंग बनला आहे.त्यातल्या त्यात फेसबुक,व्हाटसअ‍ॅप,ट्वीटर या सारखे अ‍ॅपलीकेशन जास्तीत जास्त बहुतांश लोकांकडुन वापरले जात असल्याने आपल्या सर्वांना "ऑनलाईन" राहण्याचे जणु व्यसनच जडलेल आहे.सोशल मिडीयाच्या जादुई जाळ्यात आपण नकळतपणे गुंतत चाललेलो आहे आणी सोशल मिडीयाच्या जाळ्यात गुरफटल्यामुळे प्रत्यक्ष गाठीभेटी घेऊन वैयक्तीक संवाद साधण्याची पद्धत जणु विरळ होत चालल्याने मानवी संवेदना,नात्यातली घट्टपणा विरळ होत चाललेला दिसतोय.त्यामुळे एखादी बातमी,पोस्ट व्हायरल करताना आपण त्यामागचा खरेखुरपणा,सत्यता पडताळणी ह्या गोष्टीकडे गांभिर्याने न घेता,एखादी पोस्ट व्हायरल करण्याची घाई आततायीपणा आपल्याला एखाद्या वेळेस गंभीर गुन्हयात नकळतपणे ओढु शकतो,या गोष्टीचा विसर आपल्याला पडतो.एखाद्या धर्माविषयी धार्मिक भावना दुखावणारा, महापुरुषाविषयी बदनामीकारक मजकुर पोस्ट करण्यापुर्वी त्याचा उद्देश व परिणाम जाणुन न घेतल्याने त्यामुळे सामाजीक जीवनात माजणारी अशांतता,दोन जातीधर्मात दुफळी माजविण्यासाठी,सार्वजनिक सलोखा,शांतता भंग करण्यासाठी यासाठी आहे का?आपले माथे भडकवुन देशांतील तरुणांमध्ये एखाद्या विषयी रोष,विष पेरण्याचा,अनर्थ घडविण्याचा हेतु तर नाही ना याबाबत आपण सर्वांनी गांभिर्याने , सदसदविवेकबुद्धीने विचार करण्याची गरज आजच्या दैनंदीन जीवनात करण्याची खुप आवश्यकता आज भासत आहे.एखादी पोस्ट लाईक,पोस्ट करण्याच्या विळख्यात अडकण्यापुर्वी त्याची सत्यता,गरज,उद्देश तपासुन पाहणे आवश्यक आहे.मानवी जीवनात दहशत,गैरसमज पसरविणे याकरिता रचलेले बनावट आय टी सेल्स चे विषारी,दुषित उद्देश ओळखण्याचे कौशल्य आत्मसात करणे काळाची गरज बनली आहे. सायबरक्राईम, फिशींग, क्रेडीटकार्ड फ्रॉड, सायबर स्टॉकिंग, सायबर बुलिंग, रॅन्समवेअर, सायबर दहशतवाद ,बीटकॉइन फ्रॉड, मालवेअर ,सिम स्वॅप फ्रॉड,ओएलएक्स चे धोके,ऑनलाईन फ्रॉड याविषयी आपल्या सर्व भारतीय लोकांनी सजग राहुन ऑनलाईन जगात वावरण ही काळाची गरज बनली आहे अन्यथा ऑनलाईन व्यव्हार करताना क्रेडीट कार्डची माहितीविषयी गोपनियता पाळणे,सेफ लॉग इन सेफ लॉग आऊट स्टॅट्रजी,नियमितपणे

पासवर्डमध्ये बदल करण्याची सवय,अनोळखी लिंक, इनसिक्युअर लिंकवर क्लीक करण्यापुर्वी त्याचे संभाव्य धोके ओळखण्याचे कौशल्य, फेसबुक वरील खोटे बनावट अकांऊट काढण्यापुर्वी त्याचा माहीती तंत्रज्ञान कायद्या 2000 अन्वये गुन्हे करत असण्या बाबतचा दृष्टीकोन वृद्धीगंत न झाल्याने, हॅकिंग तसेच व्हाटसअॅपवर एखाद्या व्देष पसरण्याच्या संदेश, माहीती व्हायरल करण्याची धडपड प्रत्यक्ष अप्रत्यक्षपणे आपण सुद्धा "सायबर क्राईमचा" बळी बनु शकतो याची दक्षता घेणे अनिवार्य बनले आहे.

सायबर क्राईम केल्यास पोलीस तपास करुन आपल्या पर्यंत पोहचु शकतात याचा विसर पडता कामा नये. डिजीटल, ऑनलाईन गुन्हेगारी कमी करण्यासाठी आपण सर्वांनी सजग राहुन, सक्रिय योगदान दिल्यास आपण 'सायबरसेफ' सोयायटी निर्माण करु शकतो
अशी प्रार्थना जागतीक सायबर सेक्युरिटी महिन्याच्या निमीत्ताने मी करु इच्छितो.

आवेज मक्सुद काझी (लातुर)

लातुर नियंत्रण कक्ष येथे **PSI** पदावर,
सायबर गुन्हे डिटेक्शन केल्याबद्दल बरेच पुरस्कार प्राप्त
सायबर क्राईमसारख्या ज्वलंत विषयावर वर्तमानपत्रात लेख,
महाविद्यालयात व्याख्याने देऊन जनजागृती

awezkazi@gmail.com

अर्थसाक्षर

सीए अभिजित कोळपकर

तंत्रज्ञान आपल्या आयुष्याचा अविभाज्य भाग बनला आहे. अन्न, वस्त्र, निवारा आणि शिक्षण यांच्या बरोबर माहिती-तंत्रज्ञान आपली मुलभूत गरज झाली आहे. मोबाईल, कॉम्प्यूटर्स, स्मार्ट डिव्हायसेस शिवाय आपण आपल्या दैनंदिन जीवनाची कल्पना करू शकत नाही.

आजकाल अनेकदा तुम्ही बातम्या वाचत असाल की सोशल मीडियाचा गैरवापर करून फसवणूक, फोन कॉल द्वारे आमिष दाखवून फसवणूक, पासवर्ड चोरून बँक खात्यातून पैसे लांबवले वगैरे. तंत्रज्ञानाच्या गैरवापराची अशी अनेक उदाहरणे देता येतील. फसवणूक हा मनुष्यस्वभाव अनादि काला पासून कायम आहे आणि पुढेही कायम असणार आहे.

आपण काय करायला हवे? मोबाईल, इंटरनेट असे तंत्रज्ञान आजिबात वापरायचे नाही ठरवले तर आपण घडाळ्याचे काटे उलटे फिरवल्यासारखे होणार. आपल्या प्रश्नाचे उत्तर एकदम साधे आहे पण सोपे बिलकुल नाही. आपण कायम "चौकस" असायला हवे. आता तुम्ही म्हणाल की त्यात काय एवढे आम्ही कायमच तयारीत असतो. आपण समजून घेण्याची, शिकण्याची इच्छा ठेवली, जिज्ञासू वृत्तीने जगाकडे बघितले तर संभाव्य धोके आणि अडचणींशी सहज दोन हात करता येतात.

यासाठी सायबर साक्षर द्वारे आपल्याला बहुमोल मदत होणार आहे. सोप्या शब्दांत, नेमकी आणि खरी माहिती सायबर साक्षर देईल याची मला खात्री आहे!
या सर्व उपक्रमासाठी टीम सायबर साक्षरला शुभेच्छा!!

सीए अभिजित कोळपकर

चार्टर्ड अकाउंटंट
arthasakshar.com या अर्थसाक्षरतेचा प्रसार करणाऱ्या वेबसाईटसाठी लेखन

माझ्या नजरेतून...

अक्षय भाटकर

सायबर सुरक्षा विषय वाटतो तितका सोप्पा नाहीये. फेक कॉल्स, फेक मेल्स, फेक रिक्वेस्ट या पासून सावध राहायलाच हवे. त्याही पुढे जाऊन एक विषय आहे त्यावर कोणी बोलताना दिसत नाही भारतात. तो म्हणजे गुगल, फेसबुक यासारख्या काही बड्या ॲप्स आणि वेबसाईट्स कडून होणारी हेरगिरी. हेरगिरी हा शब्द मोठा वाटेल पण त्यात तथ्य आहे. युरोपमध्ये याविरोधात लोकांनी आवाज उठवला भारतात मात्र अजून लोकांना याबद्दल खूप कमी जागरूकता आहे. याचे एक उदाहरण सांगतो.

फेसबुकवर तुम्ही कोणत्या पोस्ट टाकता, त्या कोणत्या भाषेत असतात, त्यात कोणत्या लोकेशनचा उल्लेख आहे, त्यात कोणत्या ब्रँड बद्दल किंवा दुकानाबद्दल उल्लेख याचा सर्व डेटा फेसबुक ठेवतो. पुढच्या वेळेपासून पोस्ट टाकायला गेलात की तुमच्या भाषेत फेसबुक तुमच्याशी बोलतो. म्हणजे आपल्या पोस्ट मराठीत असतील तर मराठीत सर्व नोटिफिकेशन येणार, "इथे काहीतरी लिहा" असे लिहून येणार. याप्रकारे तुमच्यावर हेरगिरी केली जाते. अश्याच प्रकारे गुगलवर तुम्ही कोणती गोष्ट सर्च केली तर तुम्ही ज्या ज्या वेबसाईटवर जाल त्या त्या ठिकाणी किंवा फेसबुकवर तुम्हाला त्याच गोष्टींची जाहिरात दिसू लागते. ही पण एकप्रकारे हेरगिरीच आहे नाही का?

आपण एखादी वेबसाईट ओपन करण्यासाठी ज्यावेळी www नंतर त्या वेबसाईटचे पहिले अक्षर टाइप करतो त्यावेळी पुढे ती संपूर्ण वेबसाईट येते म्हणजे ज्यावेळी तुमचा पीसी बंद होता, तुम्ही मोबाईल वापरत नव्हता त्यावेळी देखील गुगल तुमच्या मोबाईल किंवा पीसी मध्ये या वेबसाईट द्वारे लक्ष ठेऊन असतो. यावर युरोप मध्ये नाराजी व्यक्त केल्यानंतर तिथे ही हेरगिरी बंद झाली. आपल्याकडे मात्र अजूनही याबद्दल जागरूकता नाही.

अनेकांना तर या सोयी सुविधा वाटतात ज्या गुगल आणि फेसबुक आपल्याला देतो. पण असे नाहीये. आज ही हेरगिरी कमी प्रमाणात आहे काही वर्ष्यांनी तुम्ही काय विकत घ्यायचे, काय जेवायचे, कुठे जायचे अश्या आपल्या गोष्टी पण थेट या वेबसाईट ऑर्डर देऊन सांगायला लागल्या तर? आताही आपली सर्च हिस्टरी, आपल्या पोस्ट आणि इतर सर्व गोष्टी तत्सम कंपन्यांना विकले जात असल्याचे सांगितले जाते आणि ते खरे देखील आहे.

त्यामुळे सायबर सुरक्षा याबद्दल बोलत असताना या गोष्टी प्रामुख्याने लक्षात घ्यायला हव्यात. यावर मी शोधलेला एक उपाय म्हणजे Incognito मोड वर जाऊन सर्च करणे. त्याची हिस्टरी गुगल सेव्ह करत नाही असे सांगितले जाते. सध्या तरी माझा यावर विश्वास आहे.

मात्र आपल्या पाठीमागे काय होत असेल कोणाला ठाऊक....?

अक्षय भाटकर

गेल्या 8 वर्षांपासून पत्रकारिता
सध्या एबीपी माझा ठाणे जिल्हा चीफ

ई-कॉमर्स धोके

निकिता कोल्हे - डोखे

सध्या ऍमेझॉन सारख्या वेबसाईट्सने सणावारांमुळे खूप नवनवीन स्कीम सुरु केल्या आहेत. मोठ्याप्रमाणात सवलती उपलब्ध असल्यामुळे ऑनलाईन खरेदी करण्यासाठी झुंबड उडते. ऍमेझॉन, फ्लिपकार्ट यासारख्या वेबसाईटवर फ्री डिलिव्हरी असल्यामुळे लोकांचा ऑनलाईन खरेदीकडे कल वाढू लागला आहे. परंतु याचा फायदा घेत काही हॅकर्स ने डुप्लिकेट वेबसाईट बनवल्या आहेत.

या फेक वेबसाईट्स दिसायला अगदी हुबेहूब खऱ्या वेबसाईट सारख्या असतात. या वेबसाईट तांत्रिकदृष्ट्या खऱ्या वेबसाईटच्या कॉपी असतात. सामान्य माणूस त्या फेक वेबसाईट मध्ये आणि खऱ्या वेबसाईट मध्ये पटकन फरक ओळखूही शकणार नाही.

फेक वेबसाईट चे धोके:

फेक वेबसाईट चा अनेक लोकांना आर्थिक फटका बसला आहे. फेक वेबसाईट वर पेमेंट केल्यावर पैसे कापले जातातच तसेच वेबसाईटच खोटी असल्यामुळे वस्तू मिळतच नाही. आपली फसवणूक झाले असल्याच लक्षात येई पर्यंत वेळ गेली असते. तसेच फेक वेबसाइटवरून पेमेंट केल्यामुळे कधी कधी नेटबँकिंग अकॉउंट हि हॅक होते.

निकिता कोल्हे - डोखे

संचालिका, ऑन वेब टेक्नॉलॉजिज, पुणे

सायबर प्रेम

आर जे प्रथम

सायबर प्रेम म्हणजेच ऑनलाईन केलं गेलेलं प्रेम. आता आपण अनेक कथा ऐकल्या असतील जिथे ऑनलाईन प्रेम होतं, लोक एकमेकांना भेटतात, मग त्या नंतर लग्न होत. पण याची एक दुसरी बाजू आहे, ती सांगणार आहे मी आज तुम्हाला.

दुसरी बाजू अशी की आजकाल डेटिंग ॲप्स खूप आलेत. या डेटिंग ॲप्स सोबत माणसाच्या 'भावना' वाढत गेलेल्या आहेत. तुम्ही अगदी बरोबर ओळखलंत 'त्या'च भावना.. या भावना जेंव्हा आणखी वाढत जातात, तेंव्हा 'ऑनलाईन प्रेम' त्यांना कसं उपयोगी पडतं हे मला आज या कथेतून सांगायचं आहे.

या कथेमध्ये एक मुलगा आणि एक मुलगी आहे आणि ते दोघे फक्त 'किंटर' नावाच्या एका ॲपवरून एकमेकांना भेटतात. त्यानंतर हव्या तशा सगळ्या गोष्टी त्यांच्यामध्ये होतात.. सारखेच एकमेकांना भेटणे, 'त्या'च संदर्भात नेहमी बोलणे, म्हणजे एखाद्याचा बोलण्याचा जो दृष्टीकोन असतो तो त्याच विषयावर आहे हे समोरच्या व्यक्तीला कळून येत. पण तरीही समोरच्या व्यक्तीला ते चांगलं वाटत असतं. अशाच या पूर्ण प्रक्रियेमधून ते जातात. त्यानंतर सगळ्यात शेवटी जेंव्हा त्यांची लग्नाची वेळ येते, तेंव्हा मात्र त्यांचं एकच असतं - ते म्हणजे आपल्याला 'हीच' गोष्ट हवीये ना, मग लग्न कशाला करायचं.?

हा प्रश्न सध्याच्या तरुणपिढी समोर आहे आणि मला असं वाटतं दिवाळी अंकातून ही गोष्ट समोर यायला पाहिजे की ऑनलाईन प्रेम शोधा.. त्यातल्या वासना शोधू नका.

आर जे प्रथम (टकाटक प्रथम)

रेडिओ सिटी ९५ FM नाशिक, लेखक

शुभ
दीपावली

तुमची शाळा, तुमचे कॉलेज सायबर साक्षर आहे का?

सायबरसाक्षर
Cyber Literate India

सायबर क्राईम आणि सायबर असुरक्षितता प्रचंड वाढत चालली आहे. शाळा आणि महाविद्यालयीन मुले-मुली यात सर्वाधिक बाली पडतात. त्यामुळे शाळा आणि महाविद्यालये सायबर साक्षर करण्याचा आमचा मानस आहे.

सायबर साक्षर तुमच्या शाळेत, महाविद्यालयात आणि संस्थेमध्ये येऊन विविध सेमिनार घेईल. गरजेनुसार विद्यार्थ्यांसाठी वर्कशॉप घेण्यात येतील. विद्यार्थ्यांसाठी छोटी परीक्षा घेऊन त्यांना सायबर साक्षर प्रमाणपत्रही देण्यात येईल.

सायबर साक्षरतेच्या या उपक्रमात भाग घेण्यासाठी नक्की कळवा:
cybersakshar@gmail.com किंवा भेट द्या **cybersakshar.com** ला.

POSTING ON SOCIAL MEDIA IS NOT PRIVATE
LOOSE CLICKS INVITE HACKER TRICKS
SMS
'THINK BEFORE YOU POST'
'THINK BEFORE YOU CLICK'

Prasad More

हा दिवाळी अंक 'ई-दिवाळी अंक' पीडीएफ स्वरूपात आहे, जास्तीत जास्त लोकांपर्यंत शेयर करा, जास्तीत जास्त लोकांना सायबर साक्षर होण्यास मदत करा.

पुढील अंकामध्ये सहभागी होण्यासाठी आपणही लेख पाठवू शकता.

आपल्या सूचना आणि प्रतिक्रिया नक्की कळवा -

cybersakshar@gmail.com

© सर्व हक्क संपादकांकडे राखीव

या मासिकात लिहिलेले लेख आणि व्यक्त केलेली मते ही संबंधित लेखकांची आहेत, त्या मतांशी सायबर साक्षर मासिक किंवा संपादक, प्रकाशक सहमत असतीलच असे नाही. टंकलेखनात, अक्षर जुळवणीत किंवा भाषांतरात चुका आढळल्यास क्षमस्व.

सायबरसाक्षर
Cyber Literate India

सायबर साक्षर - ई दिवाळी अंक २०१९
पाने - ८४
संपादक - प्रा. ओंकार गंधे

cybersakshar@gmail.com
www.cybersakshar.com

प्रकाशन दिनांक : २५ ऑक्टोबर २०१९