

Anusandhanvallari
Vol 2024, No.1
December 2024
ISSN 2229-3388

Challenges for Cyber Citizens in the 21st Century

Advocate Hemant Chavan, Dr. Kirti Gupta

¹Research Scholar, IMED,
Bharati Vidyapeeth (Deemed to Be University), Pune
²Professor, Bharati Vidyapeeth (Deemed to Be University),
Institute Of Management And Entrepreneurship Development, Pune
Kirti gupta2004@yahoo.co.in

Abstract

The era of Industry 4.0 has brought about the revolution in the cyberspace – a space that connects millions of individuals and organizations across the world. Along with the opportunities for expansion and progress, cyberspace presence brings with it the serious and deeper challenges of cyber security in the form of cyber-crimes, cyber-warfare, privacy issues, intellectual property and so on.

This paper explores the challenges of cyber presence and the imminent potential threats alongwith mitigation techniques that need to be adopted for addressing the threats from cyber crimes. Results of a perception survey on the awareness about cyber crimes are also discussed.

Keywords: Cyber space, cyber crimes, Cyber presence, mitigation.

Introduction

The 21st century has been marked as the century of information and knowledge, and the drivers for these are the advancements in the information technology and globalization. These changes have a positive as well as a negative impact on individuals, organizations and society.

Information technology and latest techniques like Big Data, Business Analytics tools, Informatics and data mining etc. are being deployed to meet the challenges of designing efficient decision support systems. Hence the present environment is a combination of VUCA – (Volatile, Uncertain, Complex and Ambiguous) and Industry 4.0.



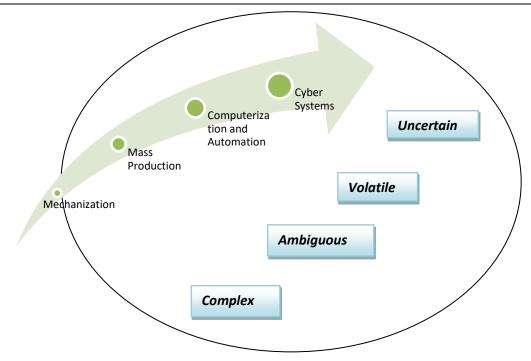


Figure 1: Industry 4.0 and the VUCA world

In VUCA world of 21st century, some of the challenges that organizations are likely to face are:

- Management of technology
- > Managing workforce diversity gender, generation, professionals etc
- > Cyber security awareness, safety and mitigation.
- Health and lifestyle management
- Leadership
- > Change management
- > Skills up-gradation for individuals
- Leadership
- ➤ Youth Employment

This paper addresses the issues related to cyber security as every individual and organization is having a presence today in the cyber space and is under the constant threat of being a victim of cyber crimes in some way or the other. This paper discusses the facets of cyber security like – awareness, safety and mitigation regarding the cyber crimes and cyber security and aims to explore the issues related to the security in the cyber space or cyber world.

Cyber Revolution: Advances in technology have moved the world from real to virtual and now cyber world cyber space. As the operations in the cyber space are growing in volumes, there is an imminent need to ensure that there is enough security in this space.

Objectives:

a) To assess the level of awareness of individuals regarding cyber security and cyber crimes



Anusandhanvallari
Vol 2024, No.1
December 2024
ISSN 2229-3388

- b) To identify the different threats faced by individuals and organizations in the cyber space of the 21st century
- c) To suggest suitable policy measures for government and organizations and suggestions for individuals for ensuring cyber safety.

A pilot survey on awareness of individuals regarding cyber crimes was conducted and the results are discussed in the discussion section.

Background of the study:

Singh(2012), paper explores some key issues/aspects related to development of e-Skills, while attempting to provide some benchmarking tools by which European countries may be able to access their current and future challenges regarding e-Skills. Today's thief can steal more with a computer than gun and today's terrorist can harm more with a keyboard than a bomb. Chinese see cyber warfare as a tool to reduce the technological gap with the United States

Common terminology of cyber space related cyber crimes

A look at some of activities and their impact

Cyber crimes types:

Individuals face the constant threat of succumbing to cyber crimes like harassment through emails, cyber stalking and transmission of child pornography (Salem 2002)

Weapons used in cyber crimes:

Fraud, gambling, destroying work, stealing data, privacy issues, hacking are the means of committing cyber crimes Cyber terrorism:

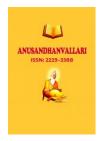
activities against the government, religious associations, non-profit organizations etc

Cyber warfare

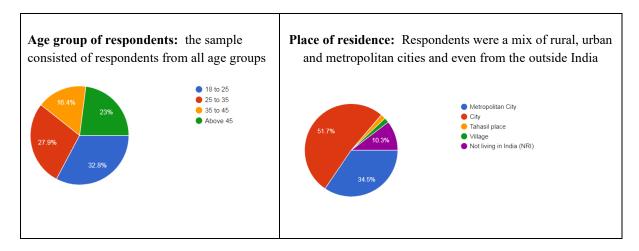
Resorted to using computers to attack other computers or networks through electronic means, to conduct sabotage and espionage, steal Intellectual property

Methodology

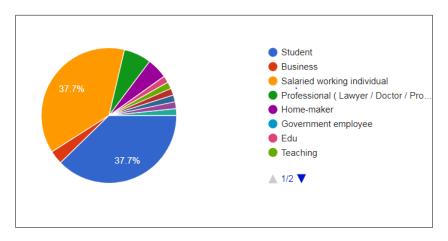
A pilot survey of 61 individuals was conducted to find out the awareness levels regarding cyber crimes and mitigation techniques suggested to combat cyber crimes. The respondents were contacted through questionnaire circulated through Google forms.



Discussions:



Occupation: Students, salaried individual, business men, government employees and even housewives, constituted the sample.

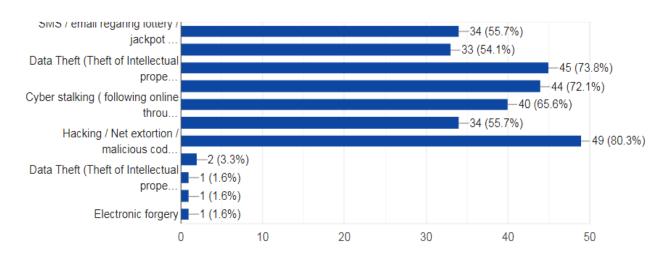


Nature origin of cyber crime:

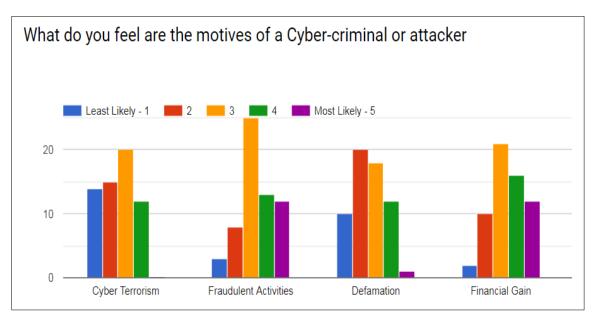


From Below options which of these you feel is a part of cyber crime?

61 responses

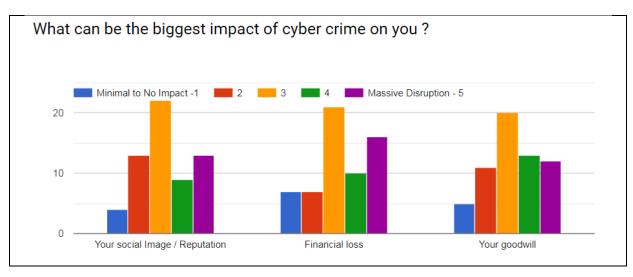


Motives of cyber crimes



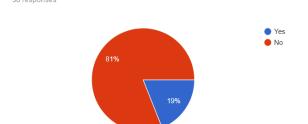


Impact



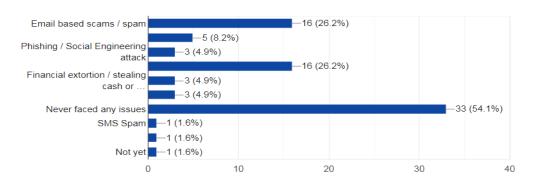
Victim?

Have you ever been a victim of Cyber crime in last 5 year?

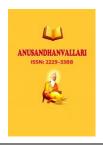


If you have been victim of cyber crime what was the nature of crime

61 responses

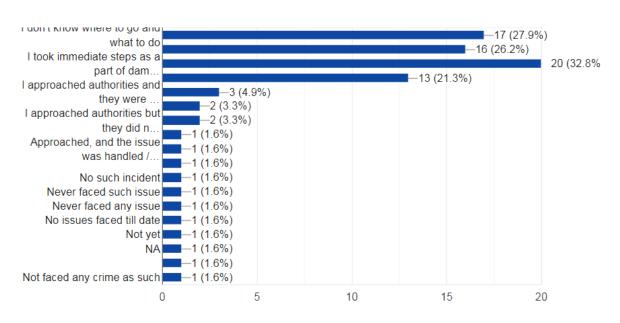


Actions taken by you



On identifying a cyber attack on you, what would you do first

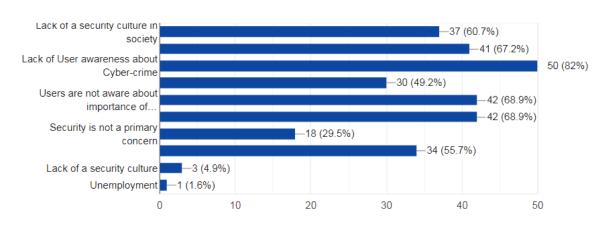
61 responses



Reasons

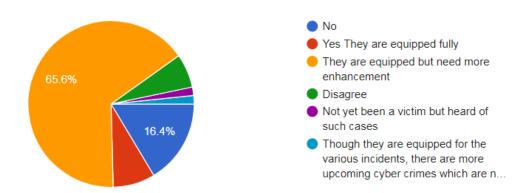
What do you think are the reasons for the increased incidents of cybercrimes in recent years?

61 responses





In your opinion are Law Enforcement Agencies (LEA) well equipped?



Majority feel they are not equipped

Findings:

- (i) Inadequate awareness levels: 80 percent of the respondents agreed that the awareness levels were very poor. The awareness levels are up to 4 on a scale of 1-10 which is not satisfactory.
- (ii) Frauds and scams constitute majority of cyber crimes: A look at the statistics reveals that frauds constitute (% of cyber crimes)
- (iii) Majority of respondents agree that there is minimal awareness and that measures should be taken for creating awareness, procedure of handling cyber crimes and consequences of cyber crimes.
- (iv) Respondents agree that the Law Enforcement Agencies are not adequately equipped to handle the cyber crimes.
- (v) Reputation and financial losses are perceived to be on stake due to cyber crimes

Suggestions

A. Suggestions for Govt. / Organizations

- i. There should be a separate department of cyber security and more skilled people should be hired. Also various awareness campaign should be organized to make the people aware about the importance of personal data
- ii. Cyber security subject has to be added to the curriculum of school students
- iii.Strict actions against cyber criminals to be taken
- iv.Repeated Advertisements on popular TV shows will help in creating awareness and warnings about cyber threats
- v. Trainings on Awareness and precautions to be actively conducted
- vi. Compulsory for Schools to conduct trainings on the aspect of social networking etiquettes
- vii.Helpline for addressing the cyber crime
- viii. Need mass level awareness messages to be given through TV, Radio, in theatres etc

Anusandhanvallari
Vol 2024, No.1
December 2024
ISSN 2229-3388

ix. Awareness drives for common people, especially senior citizens, who quickly panic upon receiving messages related to their bank accounts.

x.SOME GUIDELINES

- 1. How and what we need to share on social media guidelines need to be made aware to masses,
- 2. Govt. should constantly take efforts to make awareness about Cyber Crimes and how to safeguard citizens.
- 3. Govt. Agencies should have controls on Social media sites and impose strict controls to minimize Cyber Crimes,
- 4. Peoples involvement is prime mover in this movement with guided controls and awareness will help to reduce and control the Cyber Crime in near future.
- 5. As any crime may not be fully monitored and controlled but can be managed in such a way that it will give some symptoms before it exploits to masses.
- xi. Periodic checks and up-gradation of systems and software. Open source hackathon
- xii. Tighten internet security and avoid data theft. Create overall awareness
- xiii. Organisations likes banks should be held responsible for lac of security in the systems.
- xiv. ATMs and any Point of Sales should be under surveillance for anybody to tamper with them and should be caught. If frauds happens from POS they should be held responsible for the financial loss.
- xv. All apps should be mandated not to collect personal data.
- xvi. General awareness of the consequences of cyber crime.
- xvii. there has to be be softwares screening the content being uploaded and what damaging effect it could have on society but that should not lead to suppressing the voice of people on any account

In particular - Suggestions For Organizations

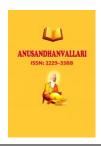
- Company rules on use of technology by employees
- Written copy of rules
- Training on use and safety of technology
- Better technology and training of personnel required to tackle high tech crimes
- Organizations should educate people on security practices, handling of sensitive data, transactions,
- Invest in security technology like, anti-virus software, technology, authentication services and intrusion detection technology
- Blocking telephone connections and internet connections
- Productivity measures: Cyber loafing should be controlled through devices
- Code of ethics and code of conduct
- Employees should be made aware about the policies regarding the use and abuse of the social media at workplaces.

B. Suggestions for Individuals

• should ensure there is least possibility of data leakage and keep our passwords strong and required to set several settings like incognito modes etc.

Conclusion:

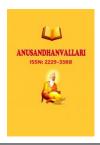
What has been discussed is just a tip of the iceberg. It is in the interest of all to be aware about the threats posed by the cyber crimes. Organizations need to adopt the latest tools and techniques and also ensure that there are



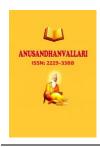
enough safety measures in place while using them. The The role of government is a major one so as to ensure that the Law Enforcement Agencies are empowered to tackle the issue efficiently.

References

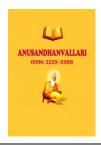
- 1. "Technology and the Law on the Use of Force: New Security Challenges in the Twenty-First Century", 2015, *The George Washington International Law Review*, vol. 48, no. 1, pp. 261-264.
- 2. Adewoye, A. (2013). *Unique competencies required for female leadership success in the 21st century* (Order No. 3603342). Available from ABI/INFORM Global. (1469609727). Retrieved from https://search.proquest.com/docview/1469609727?accountid=150530
- 3. Ajith, P. (2012). B-academic scene: India to lead? *SCMS Journal of Indian Management*, 9(2), 5-12. Retrieved from https://search.proquest.com/docview/1536045154?accountid=150530
- 4. Alexander, D. (2012). Cyber threats in the 21st century. *Security*, 49(9), 70-70,72,74,76. Retrieved from https://search.proquest.com/docview/1223497697?accountid=150530
- 5. Ali, L. 2019, "CYBER CRIMES-A CONSTANT THREAT FOR THE BUSINESS SECTORS AND ITS GROWTH (A STUDY OF THE ONLINE BANKING SECTORS IN GCC)", *The Journal of Developing Areas*, vol. 53, no. 1, pp. 267-279.
- 6. Augustine, N. R. (1996). The 20th century company meets the 21st century board. *Directors and Boards*, 21(1), 14-24. Retrieved from https://search.proquest.com/docview/215826976?accountid=150530
- 7. Boateng, R., Heeks, R., Molla, A., & Hinson, R. (2008). E-commerce and socio-economic development: Conceptualizing the link. *Internet Research*, 18(5), 562-594. doi:http://dx.doi.org/10.1108/10662240810912783
- 8. BROWN, B.R., 2016. *Measuring the level of security in the K-12 IT environment in Southern California*, Capella University.
- 9. Buchanan, W. L. (2013). Exploring sustainability: The key to corporate profitability in the 21st century (Order No. 3604426). Available from ABI/INFORM Global. (1476397048). Retrieved from https://search.proquest.com/docview/1476397048?accountid=150530
- 10. Cash management in the 21st century. (2001). *Asiamoney*, *12*(2), 84-90. Retrieved from https://search.proquest.com/docview/206607963?accountid=150530
- 11. CURRAN, J., 2016. NSA CHIEF URGES 'BROADER DIALOGUE' ON PRIVACY, ENCRYPTION, CYBER WAR. *Cybersecurity Policy Report*, , pp. 1.
- 12. Das, G. (2018, May 20). E-commerce goes rural. *Business Today*, Retrieved from https://search.proquest.com/docview/2033608234?accountid=150530
- 13. Davis, A. (2016). Preparation for a global economy: 21st century career-readiness and academic-citizenship skills for african-american workforce entrants (Order No. 10160166). Available from ABI/INFORM Global. (1841910171). Retrieved from https://search.proquest.com/docview/1841910171?accountid=150530
- 14. Fayol, H. (2000). Managing in the 21st century. *Manager*, (18), 8-10. Retrieved from https://search.proquest.com/docview/224622057?accountid=150530
- 15. Gandhi, M. M. (2014). Emerging profile of ICT-enabled commerce and management education in india. Paper presented at the, 5(2) 172-188. Retrieved from https://search.proquest.com/docview/1559079467?accountid=150530
- Gupta, K. M., & Gunasekaran, A. (2005). Costing in new enterprise environment: A challenge for managerial accounting researchers and practitioners. *Managerial Auditing Journal*, 20(4), 337-353. Retrieved from https://search.proquest.com/docview/274630223?accountid=150530
- 17. Gupta K, (2011), Research Methodlogy, Nirali Publications, Pune. ISBN: 978-93-5164-123-0 1, 162



- 18. Harper, R. L., Jr. (2001). *The professionalization of logistics: A management specialty to meet 21st century challenges* (Order No. 3015882). Available from ABI/INFORM Global. (252131380). Retrieved from https://search.proquest.com/docview/252131380?accountid=150530
- 19. HULTQUIST, K.E., 2011. An analysis of the impact of cyber threats upon 21st century business, The College of St. Scholastica.
- Ionita (Moldoveanu, I. M. (2016). Challenges of marketing in today's management of shopping centers.
 Paper presented at the 283-290. Retrieved from https://search.proquest.com/docview/1860271546?accountid=150530
- 21. Kuthiala, S. K. (2003). E-COMMERCE IN INDIA: CHALLENGES AND CHOICES. *Journal of Services Research*, 2(2), 139-155. Retrieved from https://search.proquest.com/docview/195550303?accountid=150530
- 22. Malik, R. (2012). Management education and corporate expectations: Bridging the gap. *Drishtikon : A Management Journal, 3*(1), 191-219. Retrieved from https://search.proquest.com/docview/1477997502?accountid=150530
- 23. Maliti, B., & Matembo, D. (2015). Implementation challenges in the management and placement of skilled staff in a civil service institution. *Journal of Strategic Human Resource Management*, 4(3) Retrieved from https://search.proquest.com/docview/1839194124?accountid=150530
- 24. MUJTABA, B.G., GRIFFIN, C. and OSKAL, C., 2004. Emerging Ethical Issues in Technology and Countermeasures for Management and Leadership Consideration in the Twenty First Century's Competitive Environment of Global Interdependence. *Journal of Applied Management and Entrepreneurship*, 9(3), pp. 34-55.
- 25. Munkeby, S. H. (2007). *Middle manager competencies required for success in the 21st century* (Order No. 3272243). Available from ABI/INFORM Global. (304731119). Retrieved from https://search.proquest.com/docview/304731119?accountid=150530
- 26. Neureuther, B. D., & O'Neill, K. (2011). Sustainable supply chain management programs in the 21st century. *American Journal of Business Education*, 4(2), 11-18. Retrieved from https://search.proquest.com/docview/856124082?accountid=150530
- 27. O'Lawrence, H. (2017). Eliminating poverty in the 21st century: Using entrepreneurship, innovation, and technology to help the poor help themselves. *Monthly Labor Review*, , 1-3. Retrieved from https://search.proquest.com/docview/1917915603?accountid=150530
- 28. Pandiyan, A. V. R. (2011). Effectiveness of MBA curriculum and its implementation in the business schools and colleges in chennai: An empirical study. *ASBM Journal of Management*, 4(1), 35-51. Retrieved from https://search.proquest.com/docview/1870952371?accountid=150530
- 29. Patra, S. K., Mahapatra, D. M., & Patnaik, R. (2016). Diffusion of technological innovation in business: A study on new generation business in india in E-business environment. *Parikalpana: K11T Journal of Management, 12*(2), 121-134. Retrieved from https://search.proquest.com/docview/2130696656?accountid=150530
- 30. Popescu, F., PhD. 2015, "EARLY WARNING MECHANISM IN CYBER SPACE", Niculescu Publishing House, Bucharest, 10, pp. 196.
- 31. Quayle, M. (2002). E-commerce: The challenge for UK SMEs in the twenty-first century. *International Journal of Operations & Production Management*, 22(9), 1148-1161. Retrieved from https://search.proquest.com/docview/232347922?accountid=150530
- 32. Racolta-Paina, N., & Luca, T. A. (2010). SEVERAL CONSIDERATIONS REGARDING THE ONLINE CONSUMER IN THE 21st CENTURY A THEORETICAL APPROACH. *Management & Marketing*, 5(2), 85-100. Retrieved from https://search.proquest.com/docview/749213392?accountid=150530



- 33. Sadri, S., Tara, S., & Patil, D. Y. (2012). India as a future super power: Conjectures and refutations. *Indian Journal of Economics and Business*, 11(2) Retrieved from https://search.proquest.com/docview/1629920925?accountid=150530
- 34. SAIER, M.H., J. and TREVORS, J.T., 2010. Global Security in the 21st Century. *Water, Air and Soil Pollution*, **205**, pp. 45-46.
- 35. Shacklett, M. (2011). 21st century automation and what it means. *Network Computing Online*, Retrieved from https://search.proquest.com/docview/881681828?accountid=150530
- 36. Singh, S. (2012). Developing e-skills for competitiveness, growth and employment in the 21st century. *International Journal of Development Issues*, 11(1), 37-59. doi:http://dx.doi.org/10.1108/14468951211213859
- 37. Sirisetti, S. (2011). Quality leadership in the public sector: Strategies and challenges. *The Journal of Commerce*, 3(4), 45. Retrieved from https://search.proquest.com/docview/898705369?accountid=150530
- 38. The impact of digital commerce advertising supplement]. (1998, Dec). *Canadian Business*, 70, Insert 1-15. Retrieved from https://search.proquest.com/docview/221361690?accountid=150530
- 39. Warikoo, A. 2013, "CYBER WARFARE CHINA'S ROLE AND CHALLENGE TO THE UNITED STATES", *Himalayan and Central Asian Studies*, vol. 17, no. 3, pp. 61-0 4.
- 40. Warren, J. S. (2016). The case for trust as a soft or behavioral control for organizational effectiveness (OB). *Academy of Business Research Journal*, 2, 59-73. Retrieved from https://search.proquest.com/docview/1863560945?accountid=150530
- 41. Xu, Q., Chen, J., Xie, Z., Liu, J., Zheng, G., & Wang, Y. (2007). Total innovation management: A novel paradigm of innovation management in the 21st century. *Journal of Technology Transfer*, 32(1-2), 9-25. doi:http://dx.doi.org/10.1007/s10961-006-9007-x
- 42. Yadav, S. (2016). E-commerce: The rise and rise of E-commerce in india. *Splint International Journal of Professionals, 3*(10), 23-29. Retrieved from https://search.proguest.com/docview/1906048933?accountid=150530
- 43. Yorke, C. 2015, "21ST CENTURY BURGLARY", Manager, , pp. 22.
- Anand, R., Medhavi, S., Soni, V., Malhotra, C., & Banwet, D. K. (2018). Transforming information security governance in india (A SAP-LAP based case study of security, IT policy and egovernance). *Information and Computer Security*, 26(1), 58-90. doi:http://dx.doi.org/10.1108/ICS-12-2016-0090
- 45. Shaji, R. S., Dev, V. S., & Brindha, T. (2018). A methodological review on attack and defense strategies in cyber warfare. *Wireless Networks*, , 1-12. doi:http://dx.doi.org/10.1007/s11276-018-1724-1
- 46. Sales, N. A. (2013). REGULATING CYBER-SECURITY. *Northwestern University Law Review*, 107(4), 1503-1568. Retrieved from https://search.proquest.com/docview/1499304970?accountid=150530
- 47. Popescul, D., & Radu, L. D. (2016). Data security in smart cities: Challenges and solutions. *Informatica Economica*, 20(1), 29-38. doi:http://dx.doi.org/10.12948/issn14531305/20.1.2016.03
- 48. Gerencser, M. (2009, 02). Preparing for the next game. *Vital Speeches of the Day, 75*, 74. Retrieved from https://search.proquest.com/docview/221483422?accountid=150530
- 49. Shackelford, Scott J,J.D., PhD. (2017). The law of cyber peace. *Chicago Journal of International Law, 18*(1), 1-47. Retrieved from https://search.proquest.com/docview/1991567004?accountid=150530
- 50. Zekos, G. I. (2012). CYBER-TERRITORY AND JURISDICTION OF NATIONS. *Journal of Internet Law, 15*(12), 3-23. Retrieved from https://search.proquest.com/docview/1021058027?accountid=150530



- 51. Fletcher, N. (2007). Challenges for regulating financial fraud in cyberspace. Journal of Financial Crime, 14(2), 190. doi:http://dx.doi.org/10.1108/13590790710742672
- 52. Modi, N. (2015, 11). DIGITAL INDIA: OPPORTUNITIES FOR US, AND FOR YOU. Vital Speeches Day, 81, Retrieved from https://search.proquest.com/docview/1729751139?accountid=150530
- 53. Mondal, (2016, 22). ducks. Business Today, Retrieved May Sitting from https://search.proquest.com/docview/1786755703?accountid=150530
- 54. Kshetri, N. (2016). Cybercrime and cybersecurity in india: Causes, consequences and implications for the future. Crime, Law and Social Change, 66(3), 313-338. doi:http://dx.doi.org/10.1007/s10611-016-9629-3









Net policing comes to India

SPAMMERS CAN STEAL ENTIRE IDENTITI

SPEAR phishing takes place when a

spammer has a name and email address for a target they know has ties to a particular website or brand.

They will send out phishing emails which look like genuine communication from a retailer or bank the target uses regularly.

The target may be asked to fill in an online form providing a raft of details, including credit card numbers and the answer to their security question.
This information can be enough to allow a criminal to steal their entire

identity and access shopping and bank

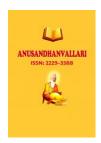
Identity and access shopping and bank accounts.

Often the spam will come with an attachment. Clicking on it will automatically download some malicious software -known as 'malware'.

The target may find they are bombarded with pop-up advertisements.

Alarmingly the criminal may be able to spy on the target's internet activity.

Security experts say the best advice when dealing with a suspect email is simply to delete it and never open the attachments that come with it.



Unsafe in cyberspace

- A bulk of the 225 cybercrime cases reported from Kerala between June, 2016 and February, 2017 relates to online stalking wherein women were abused on social media platforms
- Emakulam tops the chart with 51 cases, closely followed by Thiruvananthapuram with 47 cases. Kottayam comes third with 19 cases
 Poor rate of detection is a cause for concern as serve prominent social media sites are located outside India.
- Officials say several of the accused live abroad and it is difficult to trace them
- Around 1,150 cases had been registered across Kerala in this connection between 2012 and 2016
- 15 police officers facing action for Facebook and WhatsApp posts

Student held for cyber crime

युवक ने इंगलैंड रहती युवती को अश्लील वीडियो क्लिप भेजा