International Research Journal of Human Resource and Social Sciences
ISSN(O): (2349-4085) ISSN(P): (2394-4218)
Impact Factor 6.924 Volume 9, Issue 09, September 2022
Website- www.aarf.asia, **Email** : editoraarf@gmail.com

STUDY OF CURRENT SCENARIO OF CYBER CRIMES RELATED BANKING SECTOR IN INDIA

Rakesh Kumar Jha[1], Dr. Parveen Kukkar[2]

[1]Research Scholar, Sunrise University, Alwar, Rajasthan
[2]Research Supervisor, Sunrise University, Alwar, Rajasthan

ABSTRACT

Today, in our globalized world, Online banking, or Internet banking, has transformed a fundamental aspect of contemporary life. Because of his social nature, it is crucial for man to be able to share and learn from the experiences of others. In this article, we explored the latest hacking tactics and trends as they pertain to online banking-related cybercrime. This article also includes data on cybercrime in India. This report also identifies the most recent cybercrime news pertaining to internet banking. The research used only previously collected information. The Global Information Security Survey 2014–15, Press Information Bureau English Releases, and Reserve Bank of India publications were consulted along with annual reports from the National Crime Record Bureau (NCRB), the Indian Computer Emergency Response Team (CERT), and the Internet Crime Complaint Center (IC3). This study's results highlight the increasing prevalence of both online banking-related criminality and the use of information technology in India. Young adults between the ages of 18 and 30 (especially young men) perpetrate the vast majority of cybercrimes. In order to combat and prevent cybercrime, our law enforcement authorities need more resources. Finally, the study's author provides recommendations for the safe and secure usage of online banking services.

KEYWORDS: Information Technology, cybercrimes, cyber-attacks, mobile banking, online banking, National Crime Record Bureau, hacking

INTRODUCTION

Cybersecurity refers to the measures taken to prevent both external and internal parties from gaining illegal access to computer systems, networks, and software applications. When doing business in a digital setting, it is crucial to take measures to protect the privacy and security of sensitive data. Institutions face cybersecurity risk because they don't always have the resources to guarantee that their networks, devices, programs, and data are secure from intrusion. Due to the potential for severe disruption of banking processes and the imposition of considerable direct and indirect losses, cybersecurity risk has altered the paradigm of banking operations over many decades. As a result, financial institutions are more vulnerable to hacking as they move more of their business and customer interactions online.

Overall, market data suggests that compromised cybersecurity has serious repercussions for the financial sector. Experts in the field have been investigating the root reasons of the recent surge in cyber-attacks on the banking and financial industries, as well as potential solutions to the problems that have arisen as a result. Conceptual papers, survey studies, technical reports, policy documents, and media pieces have all contributed to the growing body of literature on cybersecurity and banking operations during the last several years. The global financial sector is particularly susceptible to cyberattacks because of the lack of a robust risk protection and management framework. However, it is still challenging to obtain testable data, therefore additional in-depth empirical study is restricted. The literature on cybersecurity and financial system risk has grown over the last several years, but there has been no comprehensive evaluation to assist us gauge our progress and identify gaps in our understanding. As a result, we work to provide a comprehensive literature assessment covering a wide range of topics relevant to the financial sector, and we provide suggestions for further study.

LITERATURE REVIEW

Al-Alawi, (2020)research "The Role of Cyber Security Systems in Financial Institution Risk Management" This research aims to demonstrate the significant effects and advantages of incorporating cyber security into an organization's systems, with a particular focus on the financial services industry. Cybersecurity is a priority in this study since it helps with data protection and risk management. However, many banks and other financial organizations are still wary of fully embracing cyber security in all their operations. The benefits of cyber security may even be lost on many financial institutions. In addition, the greater costs associated with the application can work against it. Therefore, several questions were asked to assess the banks' cyber security knowledge and preparedness.

Alghazo, Kazmi, &Latif, (2018)I looked at "Cyber Security Analysis of Internet Banking in Emerging Countries: User and Bank Perspectives" The research shows that internet banking, also known as electronic banking (E-banking), online banking (sometimes known as virtual banking), and banking. Internet banking has proven to be the most efficient and fruitful technique of banking for financial institutions. Most financial institutions have jumped on this opportunity to save costs and improve service to customers. Users' decisions on whether or not to embrace new technologies are informed by their efforts to learn about such technologies and establish their own opinions about them. According to the TAM, two factors—ease of use and utility—determine whether or not a user will adopt a new piece of technology.

Marshall, (2010)read the research paper "Online Banking: Information Security vs. Hackers" Financial organizations, such as banks and savings and loans, are entrusted with their customers' funds, but they also have a special duty to protect their customers' private information and historical records. Financial institutions are the custodian of records for their commercial and individual banking customers, which includes information such as day-to-day transactions such as deposits, withdrawals, balance amounts, social security numbers, birth dates, loan information, partnership agreements related to a loan, year-to-date statements, and a host of other extremely sensitive financial information. More than half of the aforementioned paperwork, business, and private data takes place online.

Ojeka, Ben-Caleb, &Ekpe, (2017) research into "Cyber Security in the Nigerian Banking Sector: An Appraisal of Audit Committee Effectiveness" found that online fraudsters are constantly developing more sophisticated schemes, costing banks in the country billions of dollars annually. Since the criminal has greater power and better technology facilities to conduct the crime, the audit committee will need to acquire technological abilities to keep up. The best interest of banks requires the audit committee to keep up with the technological advances of the global community. For an audit committee to effectively oversee a company's financial management and reporting, it has to possess a high degree of financial competence in cyber security. The audit committee is charged with monitoring the full risk management procedure as part of its oversight of managerial accountability. For the audit committee to fully grasp the monetary effects of cybercrime, they will need accounting expertise.

Rajendran, (2018)research "BANK CYBER SECURITY" I was reading an article titled "BANK CYBER SECURITY" when I learned that cybercrime may be outsourced. Customers nowadays are usually as tech-savvy as, if not more so than, the average bank employee because of the pervasiveness of technology in modern banking. Banks can no longer utilize the same old cliches "it's a computer problem," "it's a software issue," or "it's a technological failure" when a client reports an issue with their remittance, statement, or Account View, for example. Without a shadow of a doubt, the customer is aware of the predicament.

METHODOLOGY USED

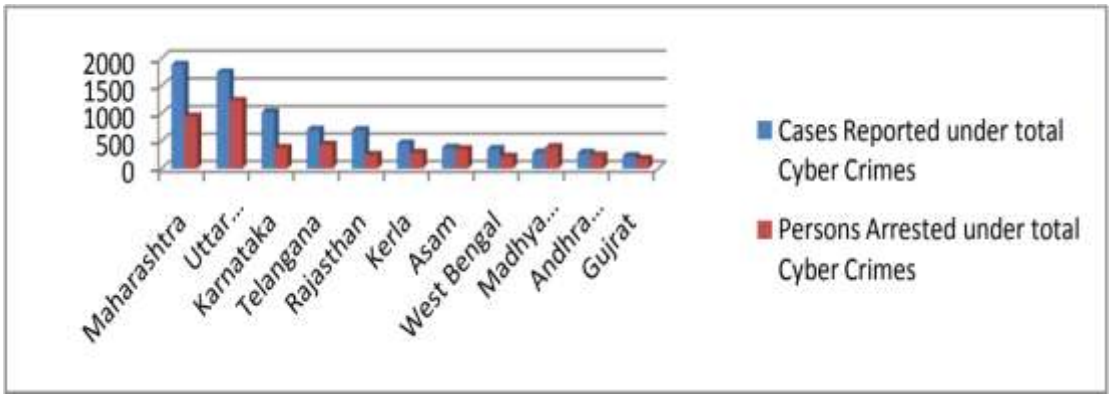
The information used in this analysis is secondary. In order to achieve the first goal of the research, a literature analysis, the Information Technology Act of 2000, and the cybercrime investigation unit in Mumbai's website are all investigated. Case studies from a variety of media outlets are referenced to in order to examine the methods used by cybercriminals to get into financial systems and commit cybercrud. The yearly reports of the National Crime Record Bureau (NCRB) are mined for information on the state of cybercrime in India and the state of Maharashtra.

DATA ANALYSIS

CURRENT SCENARIO OF CYBER CRIMES RELATED BANKING SECTOR IN INDIA.

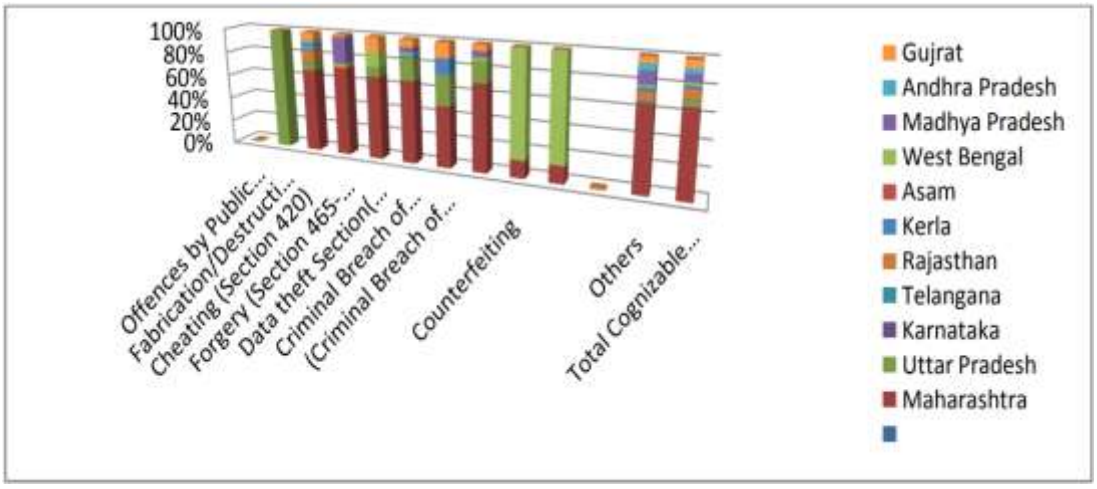
incidence of Cognizable Crimes under IT Act

1. Cases Reported and Persons Arrested under Cyber Crime



The data shown in the above graph relates to cybercrime cases reported and arrests made.The top number of reported cybercrime incidents occurred in the state of Maharashtra (1879), as seen in the above graph. While more incidents of cybercrime are reported, fewer people are arrested (942). In terms of both the number of cybercrimes committed there (1,737) and the number of people arrested for them (1,222), Uttar Pradesh ranks second. The state of Gujarat ranks dead last in the nation for cybercrime.

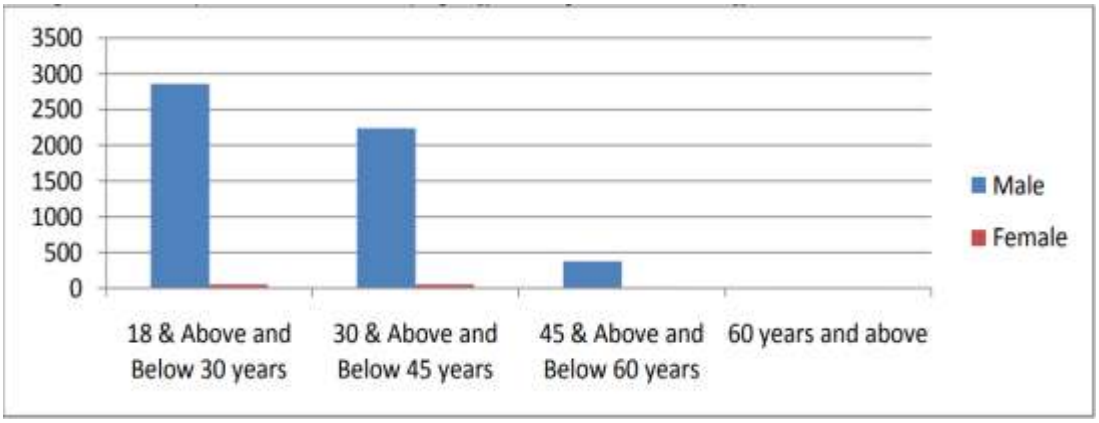
Incidence of Cognizable Crimes under IPC (involving Computer As Medium/Target)



The state of Maharashtra had the highest rate of offences classified as "cognizable" under the Indian Penal Code (involving Computer as Medium/Target). Theft of information under sections 379 and 381 (17), criminal breach of trust/fraud involving debit cards and others under sections

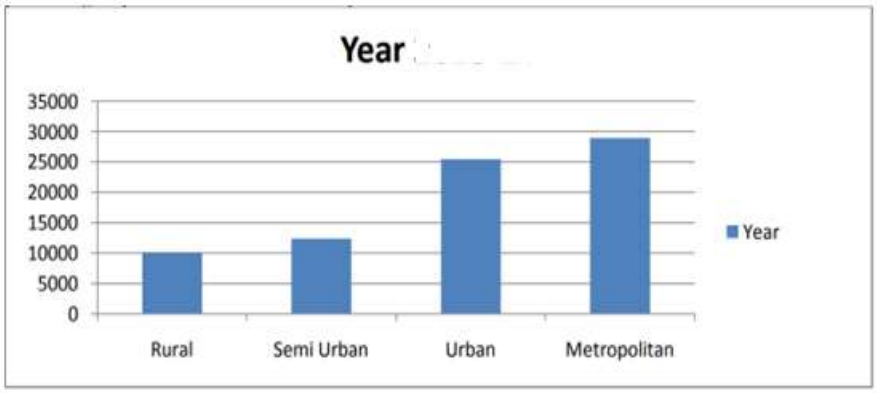
406, 408, and 409 (33), and cheating under section 420 (671). The state of Rajasthan comes in at number two (145). Karnataka, with just two offenses that qualify as "cognizable," ranks worst.

3. Total Cyber Crimes (IT Act + IPC +SLL) by Age Groups & Sex



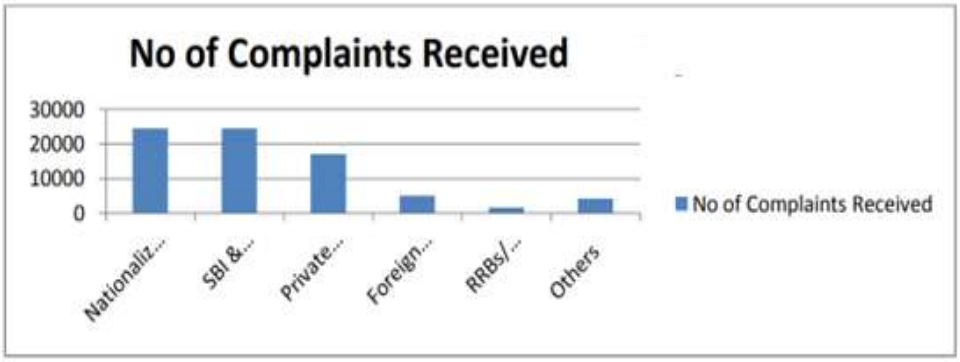
Total cybercrime committed under IT Act, IPC, and SLL, broken down by age and gender, is shown above. The majority of those involved in cybercrime are males (2859), especially those between the ages of 18 and 29 but younger than 30. And there are just 54 women in the same age range. Maximum participation for perpetrating the cybercrimes is discovered in the under 18 & above and below 30 age group, in comparison to other age groups (30 & above, 45 & above, and 60 years and above). People aged 60 and older are also heavily represented in this study's participant pool. The percentage of females who conduct cybercrime is much lower than the percentage of males across all age categories.

4. Population group-wise distribution of complaints received to RBI



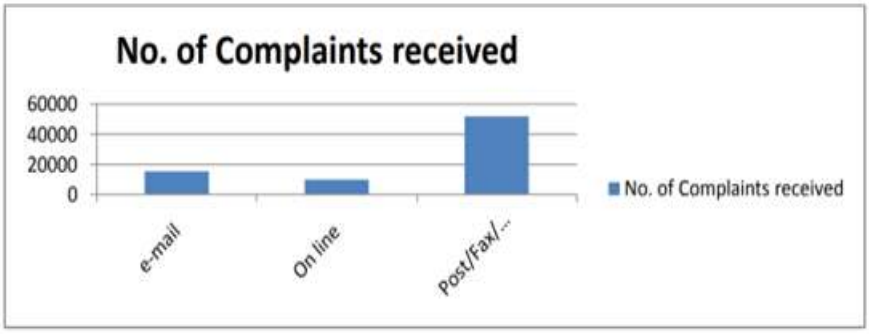
The RBI found that, when comparing urban, semi-urban, and rural areas, the number of complaints received from metropolitan areas (28884) was much higher. RBI receives hardly any complaints from rural areas (9,927).

5. Bank group-wise classification



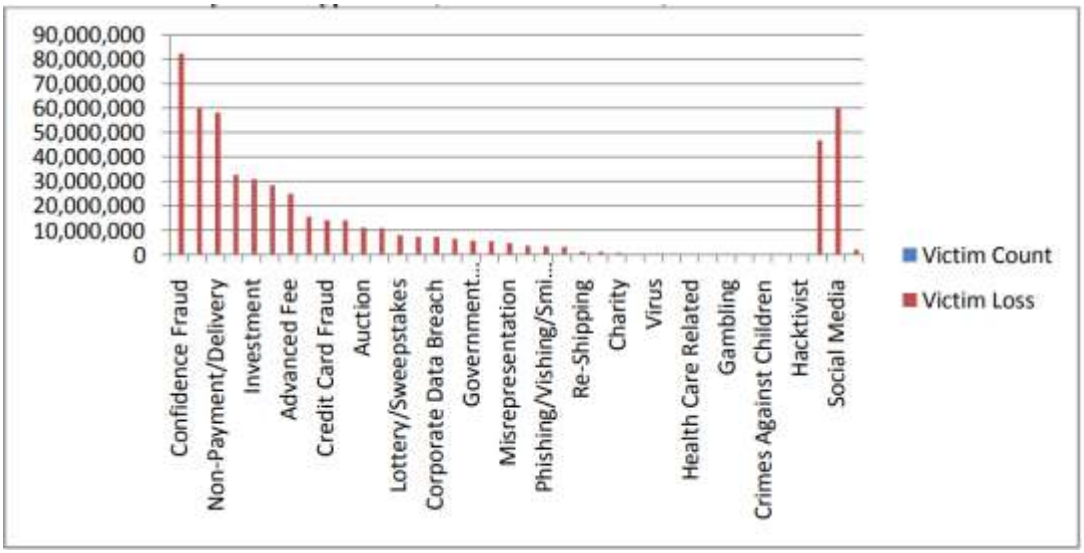
The above chart categorizes complaints received by banking group in 2013–14. The Nationalized Banks category (24391), which includes the largest number of banks, receives the most complaints, followed by SBI & Associates (24367), private sector banks (17030), foreign banks (5016), and others (4179). RRBs/Scheduled Primary Urban Co-op Banks only report receiving 1590 complaints each year.

6. Receipt of complaints Mode-wise



The RBI mostly received complaints via the mail, fax, and courier (51607). Only a small fraction of RBI complaints are being submitted through the website or email.

7. Six Month Statistics by Crime



The following chart provides RBI data for the six months between June 1, 2014 and December 31, 2014, broken down by crime category. It details numerous crimes according to their category, number of victims, and monetary cost. Non-payment and late delivery result in the greatest number of casualties (31760 and $5813,9846, respectively). The victims and types of cybercrime are shown graphically here. There were 9833 victims of social media attacks and a total loss of $604,18243; 7783 victims of credit card fraud; 6495 victims of phishing; 421 victims of viruses; 819 victims of malware; 417 victims of denial-of-service attacks; 1349 victims of gambling; 273761 victims of hacktivism; and 1058 victims of a breach of personal data.

Cyber Security Risk Scenarios

Phishing, the use of stolen Credit Cards / Debit Cards, unauthorized fraudulent Real Time Gross Settlement transactions, fictitious offers to cheap fund (funds transfer, lottery payment, money circulation schemes, etc.) are all examples of the types of cyber fraud, including mobile banking fraud, that have been reported in the country. Third, they seem to be on the rise.

Activities / Items[4]	**2018**	**2019**	**2020**	**2021**
Phishing	887	955	1122	534
Network probing	2866	3239	3317	3673
Virus/malicious code	3149	4160	4307	9830
Website defacements	23014	24216	25037	26244

Website intrusion / malware propagation	4591	5265	7286	961
Others	2417	3484	3610	8213
Cyber security incidents reported / handled by CERT-IN	**36924**	**41319**	**44679**	**49455**
Cyber-crime registered as per NCRB[5A]	**2876**	**5693**	**9622**	**11592**
Cyber financial frauds registered with RBI[5]	**8322**	**9500**	**13083**	**16468**
BOT Infected systems tracked by CERT-IN	6494717	7457024	7728408	9163288

Cybersecurity is the state of being able to prevent or counteract assaults in the cyber realm. When it comes to cyber security, it takes a global effort to get the job done. Credit and debit card fraud has been on the rise for some years. According to NCRB statistics, some of the worst-hit states for cybercrime include Maharashtra, Uttar Pradesh, Karnataka, and Andhra Pradesh. Also, the number of internet users in these states is higher than in the rest of the country.

CONCLUSIONS

There has been a sharp increase in the number of cybercrimes in India. Social media crimes, credit card fraud, phishing, viruses, malware, denial of service attacks, gambling, hacktivism, data breaches (both personal and corporate), and virtual currencies are common targets for cybercriminals. Men between the ages of 18 and 30 are disproportionately represented among those who conduct cybercrime. People in their 60s and older are just as likely to commit a cybercrime as anybody else. Involvement in cybercrime by the elderly is a worrying trend. When compared to other states, Maharashtra has the highest rate of cybercrime. Nationalized Bank Group is the target of the vast majority of cyberattacks. The majority of victims experienced financial and personal information loss from all types of institutions. Because of the internet's role as a global hub for information and communication, it's important to exercise care while using it. It is important to exercise care while using a computer or the internet in order to avoid being a victim of cybercrime. The best way to prevent cybercrime is through education and awareness. This includes teaching people how to use and handle mobile and online banking safely, how to secure personal information, how to use different applications, and what precautions to take when conducting financial transactions over the internet. It's crucial for the strict enforcement of cybercrimes laws.

REFERENCE

1. Al-alawi, P. A. I. (2020). The Significance of Cybersecurity System in Helping Managing Risk in Banking and Financial Sector. Journal of Xidian University, 14(7). https://doi.org/10.37896/jxu14.7/174

2. ghazo, J. M., Kazmi, Z., & Latif, G. (2018). Cyber security analysis of internet banking in emerging countries: User and bank perspectives. 4th IEEE International Conference on Engineering Technologies and Applied Sciences, ICETAS 2017, 2018-January (November 2018), 1–6. https://doi.org/10.1109/ICETAS.2017.8277910

3. Baur-Yazbeck, S., Frickenstein, J., &Medine, D. (2019). Cyber Security in Financial Sector Development: Challenges and Potential Solutions for Financial Inclusion, (November). Retrieved from https://www.findevgateway.org/paper/2019/11/cyber-security-financial-sector-development- challenges-and-potential-solutions

4. Karunakar Mohapatra. (2018). effective operational risk management Cybersecurity vulnerability in Indian banks. Cybersecurity Framework in Banks. Retrieved from https://financialit.net/sites/default/files/customerxps_white_paper_cybersecurity_vulnerability_in_indian_banks_1.pdf

5. Marshall, P. J. (2010). Online Banking: Information Security vs. Hackers Research Paper. International Journal of Scientific and Engineering Research, 1(1), 1–5. https://doi.org/10.14299/ijser.2010.01.001

6. Ojeka, S. A., Ben-Caleb, E., & Ekpe, I. (2017). Cyber Security in the Nigerian Banking Sector: An Appraisal of Audit Committee Effectiveness. International Review of Management and Marketing, 7(2), 340–346.

7. Ponemon. (2020). TAILORING CYBERSECURITY, (May).

8. Rajendran, V. (2018). Security in Banks. The Journal of Indian Institute of Banking and Finance, 89(01), 26–32.

9. Manisha M. More and Dr. K. M. Nalawade(2014) :Cyber Crimes and Attacks: The Current Scenario,1st National Conference organized by NESGOI, Pune

10. Susheel Chandra Bhatt and Durgesh Pant (2011): Study of Indian Banks Websites for Cyber Crime Safety Mechanism, (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 2, No.10, Jayshree Chavan(June 2013): Internet Banking- benefits and challenges In An Emerging Economy, International Journal of Research in Business Management (IJRBM) ,Vol. 1, Issue 1, 19-26

11. Rupinder Pal Kaur(Aug.2013)-Statistics of Cyber Crimes in India: An Overview, International Journal of Engineering and Computer Science ,Vol 2,Issue 8.

12. National Crime Record Bureau: Cyber Crime Statistics In India 2014: http://ncrb.gov.in/pdf

13. Computer Emergency Response Team(CERT):http://cert.India.com