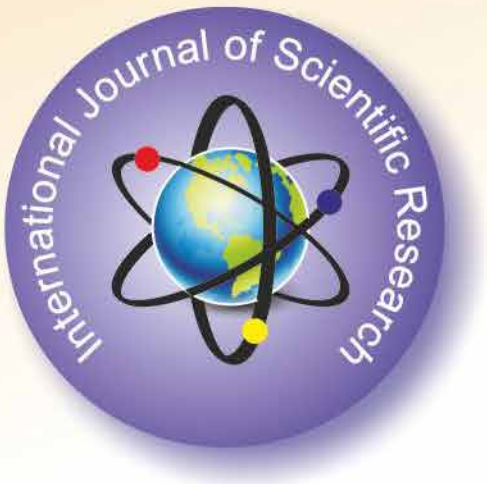
International Journal of Scientific Research

Indexed with International ISSN Directory, Paris

Volume 1 | Issue 2 | July 2012



ISSN No. 2277 – 8179

A Multi-Subject Journal

ISSN No. 2277 – 8179

International Journal of Scientific Research

Journal for All Subjects

Advertisement Details

Position	B/W (Single Color)	Fore Color
Full Inside Cover	₹ 6250	₹ 12500
Full Page (Inside)	₹ 5000	-

Subscription Details

Period	Amount Payable
One Year (12 Issues)	₹ 3000
Two Year (24 issues)	₹ 5800
Three Year (36 issues)	₹ 8700
Five Year (60 issues)	₹ 14400

You can download the Advertisement / Subscription Form from website www.gra.in. You will require to print the form. Please fill the form completely and send it to the **Editor, International Journal of Scientific Research** along with the payment in the form of Demand Draft/Cheque at Par drawn in favour of **International Journal of Scientific Research** payable at Ahmedabad.

Editor-In-Chief

Khansa Memon
Editor, Sarah Publishing Academy

Editorial Advisory Board

Dr. Ashok S. Pawar
Associate Professor, Dept. of Economic
Dr. Babaasaheb Ambedkar
Marathwada.University, Aurngabad

Dr.(Prof) Vijay Kumar Soni
Principal,
Jai Meenesh College, Phagi,
Jaipur, Rajasthan

Dr. A.R. Saravankumar
Assistant Professor in Education
DDE, Alagappa University,
Tamilnadu

Dr.R.Ramachandran
Commerce Dde
Annamalai University
Tamilnadu India

Dr. R Ganpathy
Assistant Professor in Commerce
Directorate of Distance Education
Alagappa University Karaikudi.

Dr. Amit Bandyopadhyay
Assistant Professor
Department of Physiology
University of Calcutta

Dr. V. Kumaravel,
Professor and Head
Vivekanandha Buss. School for Women
Tiruchengode, Namakkal Dist

Dr. K. Prabhakar,
Professor,
Department of Manag. Studies,
Velammal Engg College, Chennai

Dr. Sunita J. Rathod
Maharashtra Education
Service Group-B
DIET Dist. Jalna

1. Thoughts, language vision and example in published research paper are entirely of author of research paper. It is not necessary that both editor and editorial board are satisfied by the research paper. The responsibility of the matter of research paper/article is entirely of author.
2. Editing of the **International Journal of Scientific Research** is processed without any remittance. The selection and publication is done after recommendations of atleast two subject expert referees.
3. In any condition if any National/International University denies accepting the research paper published in IJSR then it is not the responsibility of Editor, Publisher and Management.
4. Only the first author is entitle to receive the copies of all co-authors
5. Before re-use of published research paper in any manner, it is compulsory to take written permission from the Editor-IJSR, unless it will be assumed as disobedience of copyright rules.
5. All the legal undertaking related to **International Journal of Scientific Research** is subject to Ahmedabad Jurisdiction.
7. The research journal will be send by normal post. If the journal is not received by the author of research papers then it will not be the responsibility of the Editor and publisher. The amount for registered post should be borne by author of the research paper in case of second copy of the journal.

Editor,
INTERNATIONAL JOURNAL OF SCIENTIFIC RESEARCH
3, SUHANA, Nr. Rubi Apartment, B/H NID, Rajnagar Road,
Paldi – 380007. Ahmedabad-Gujarat. (INDIA)
Contact: +91 98247 02127, +91 88660 03636
Www.theglobaljournals.com | ijsr@theglobaljournals.com

INDEX

Sr. No.	Title	Author	Subject	Page No.
1	Ionic composition of a freshwater lake and its implications on aquaculture	Dr. Shankar P. Hosmani	Biotechnology	1-2
2	Growth and Performance of Mutual Fund Industry in India	Dr. M. K. Maru	Commerce	3-4
3	Waste Management: A New Paradigm of Contemporary Business	Dr. Vipul Chalotra	Commerce	5-6
4	Rural Financial Services in J&K (A study in the field of financial services sector development)	Tarsem lal	Commerce	7-8
5	Banyan, the National Tree of India	Dr. J.K. Sehgal	Commerce	9-10
6	Impact of Online Marketing on Customers with Special Reference to Coimbatore City	Dr. R. Ganapathi	Commerce	11-15
7	Customers' Attitude towards Housing Loan With Reference to Commercial and Rural Banks	Dr. R. Ganapathi, Mrs. B. VIDYA	Commerce	16-23
8	Consumer Behaviour towards Broiler Chicken Retail Stores With Reference to Madurai City	P. Easwaran, J. Gnanadevan, Dr. R. Ganapathi	Commerce	24-30
9	Data Security and Protection in Cloud Computing	Shameena Begum, V. Ratna Vasuki, K.V.V.Srinivas	Computer Science	31-34
10	Foreign Direct Investment in India – An Explanatory Study	Dr. K.Madhu Babu	Economics	35-38
11	Growth - Saving Causality in India: A Cointegration Analysis	Dr. Shradha H. Budhedeo	Economics	39-42
12	Constitutional perspectives on Labour Wages in India	Dr. Shankar Ambhore, Dr. Dilip Arjune, Manish Parshuram Pawar, Dr. Ashok Shankarrao Pawar	Economics	43-45
13	A Critical Study of Special Economic Zones in India	Dr. Shankar Ambhore, Dr. Dilip Arjune, Manish Parshuram Pawar, Dr. Ashok Shankarrao Pawar	Economics	46-48
14	Industrial Relations - Settlement of Disputes in India	Dr. Shankar Ambhore, Dr. Dilip Arjune, Manish Parshuram Pawar, Dr. Ashok Shankarrao Pawar	Economics	49-50
15	AMLA - ITS MEDICINAL USES	Manisha Gaur	Economics	51-52
16	The Role Of Total Quality Management In Higher Education	Ramesh B. Sakhiya	Education	53-55
17	Perceived Competencies Of Graduate Teacher Trainees In The Intensive Teaching Practice [I T P] Session	Dr M. Parimala Fathima, N.Sasikumar, M. Panimalar Roja	Education	56-58
18	Uchch Siksha Ki Rah Men Dushvariyan	Dr. Anup Chaturvedi	Education	59-60
19	Fault Diagnoses of Rotating Machinery with Advance Signal Processing Methods	Prof. Divyang H. Pandya, Prof. Ankit A. Darji	Engineering	61-63
20	A Hybrid Neural Network Approach for Wind Speed Prediction	S.N Deepa, K.gnana Sheela	Engineering	64-67
21	A Study on Phishing: Preventions and Anti-Phishing Solutions	V.Karamchand Gandhi, Prof R.Senthil Kumar	Engineering	68-69
22	The Killari 1993 Intracratonic Earthquake- a Comparative Study	S.S. Patil, K.L. Karkare, I.B. Ghorade	Environment	70-72
23	Cosmic Plants as Alternative Medicine	Dr. Sneh Harshendra Sharma	Environment	73-77

24	Green Initiatives for Reducing Carbon Footprint	Dr Mahalaxmi Krishnan	Environment Science	78-79
25	Prediction of Urban Sprawl in Hyderabad City using Spatial Model, Remote Sensing and GIS Techniques	S. Indhira Gandhi, Dr. V. Madha Suresh	Geography	80-81
26	Tectono-Provenance and Reservoir Rock Characteristics of the Tipam Sandstones in Parts of Upper Assam Basin	Dr. Pradip Borgohain	Geology	82-84
27	(Jansanchar Aur Bharatiya Samaj)	Dr Subodh Kumar	Journalism	85-86
28	An Overview of Industrial Disputes Settlement Authorities in India	Manish Parshuram Pawar, Dr. Ashok Shankarrao Pawar	Law	87-88
29	Innovative Method of Role Play for Developing English Language Teaching and Learning	K Rajkumar	Literature	89-91
30	Impact of Workers Participation in Management on Industrial Relations	Anuradha Averineni	Management	92-93
31	Consumers Preferences , Behaviour and Satisfaction with respect to banking services quality in Ghaziabad(NCR Region)	Prof(Dr.)H. P. Pandey, Mr. Ashish kumar Singh	Management	94-96
32	Factors Influencing Employee Branding in Higher Educational Institutions: A Special Reference to Management Institutions in Virudhunagar District in Tamilnadu	Jegadeeswari. Mani, Dr. S. Franklin John S.	Management	97-98
33	Evaluation of Service Quality in Internet Banking: An Empirical Study in Coimbatore	Ms. R. Gokilavani, Dr. R. Ganapathi	Management	99-101
34	To Study the Relationship Between Gender & Banking Preferences of Management Graduates at Ibmrd, Ahmednagar	Rajendrasingh Pardeshi, Gadekar Vithal Laxman	Management	102-103
35	FCB model of Advertising Strategy	Prof. Arvind Rathod	Management	104-107
36	Assessing Beneficiary Satisfaction with Service Delivery of Non Governmental Organizations (NGOs)	Dr Papori Baruah, Bhaskar Jyoti Barthakur	Management	108-111
37	Current Trends in Human Resource Management	Dr. Kalyani Kenneth, Mrs.R.Aruna jayamani	Management	112-113
38	“Indian Banking – A Future Ahead”	Haresh B. Barot	Management	114-116
39	Financial Inclusion-Banking Services to the Common Man	Dr. M. Venkata Subba Reddy, Mr. M.s.udaya Banu	Management	117-118
40	A study of Service Marketing Mix w.r.to b-schools in Mumbai	Dr. Balaji S. Mudholkar	Management	119-120
41	A Study on the Customers Opinion on the Benefits of the Credit Cards Around Combatore District	Mrs. G. Murali Manokari	Management	121-123
42	A Study on the Job Satisfaction of the Employees at Sri Kannan Departmental Stores, Coimbatore	Mrs. G. Murali Manokari, Mrs.r.kanaka Rathinam, Mr. G. Lenin Kumar	Management	124-126
43	Foreign Direct Investment In Indian Retail Sector: A Critical Evaluation	Dr. Raghavendra Dwivedi, Ram Kumar	Management	127-128
44	Emerging Challenges to Cyber Security-Internet Monitoring with Specific reference to National Security	Triveni Singh	Management	129-131
45	An Empirical Study of Consumer Impulse Buying Behavior in domestic Markets (special reference to Ahmednagar, (M.S) India.)	Gadekar Vithal Laxman	Marketing	132-135
46	Insomnia and the performance of general population: Results from the Insomnia Survey	Miss Ketaki Sathe, Dr G S Shekhawat	Medical Science	136-137
47	Transition in Human Resource for Health: Challenges Ahead	Dr. Pawan Kumar, Dr. Abdul Majeed Khan	Medical Science	138-139

48	Kartageners Syndrome- A Case Report	Dr. Ramakrishna Ghubde, Dr. Archana Shekokar	Medical Science	140-141
49	Perceptual challenges in auditory neural processing in neurodegenerative conditions like Fredereich Ataxia	Mr. Ayas Muhammed, Ms. Archana, Dr. Rajashekhar	Medical Science	142-143
50	Transient Auditory Dysynchrony Due to Non-Maturational Causes Evidenced by ABR – A Case Report	HariPrakash. P, Sangeetha. G, Bhargavi P.G	Medical Science	144-146
51	Study on Sphenoid Sinsuses Variants in Magnetic Resonance Imaging of South Indian Population	Suresh Sukumar, Sushil Yadav	Medical Science	147-148
52	A Study to Find out the Prevalence and Effectiveness of Occupational Therapy Intervention for Pain and Activity Performance in Mobile Users with Risk of Repetitive Strain Injury	KR.Banumathe, V.Guruprasad, Leena Ann Lukose	Medical Science	149-151
53	Modified Falls Behavioral Scale for Indian Community Dwelling Older Adults	V.Guruprasad, Sebestina A D'Souza, KR.Banumathe	Medical Science	152-154
54	The Essence of Employees Training and its Impact on the Work Force in an Industry	Dr. Mohan Singhe	Organization Behavior	155-156
55	Scientific Behaviourism of Watson and Hull : A Philosophical Perspective	Dr. Jatinder Kumar Sharma	Philosophy	157-158
56	The growth of manganese oxide thin films by spray pyrolysis technique	M.Sudha, P.Duraisamy	Physics	159-161
57	Terrorism and Competitive Terrorism in India	S. Sreejith, P. Sakthivel	Political Science	162-164
58	Kuposhan Se Karahta Bachpan	Dr. Anup Chaturvedi	Social Science	165

Volume : 1 | Issue : 2 | July 2012 • ISSN No 2277 - 8179

Research Paper

A Study on Phishing: Preventions and Anti-Phishing Solutions

Engineering

KEYWORDS : phishing, fraudulent email, personal firewall

V.Karamchand Gandhi Assistant Professor, Bharath College of Science and Management, Tamil Nadu

Prof R.Senthil Kumar Assistant Professor, Bharath College of Science and Management, Tamil Nadu

ABSTRACT

Phishing is a form of online identity theft that aims to steal sensitive information such as online banking passwords and credit card information from users. Phishing scams have been receiving extensive press coverage because such attacks have been escalating in number and sophistication. According to a study by Gartner, 57 million US Internet users have identified the receipt of e-mail linked to phishing scams and about 2 million of them are estimated to have been tricked into giving away sensitive information. Phishing scams are now a part of everyday life. It's important that you know how to spot one and avoid becoming a victim. Phishing scams are just another attempt to get valuable information. Scammers send a mass email to every address they can find. Typically the message will appear to come from a bank or financial institution. The email states that you should update your information for one reason or another, and they usually provide a link that we can click to do so. This all sounds reasonable and it may look legitimate, but phishing scams are anything but legitimate. The link provided does not take we to the financial institution's website. Instead, we will be submitting our information to a website run by the scammers. This paper deals with the importance of phishing preventions and its solutions.

1. INTRODUCTION

The word "phishing" has its origins in the underground language used by hackers. It first entered the Internet lexicon in 1996 when hackers were stealing America Online accounts and passwords. Always clever, these early hackers defined their crime as "sport," instituting angling metaphors to describe their work. They would send email "lures" (i.e. hooks or bait) to "fish" for passwords and financial data from the Internet "sea" of millions of users. The "ph" instead of the "f", used in hacker language, is an acknowledgment to the original form of hacking known as phone phreaking, invented in the 1970s. A blue box emitting audible sounds let the phreakers hijack phones, placing thousands of dollars in long distance calls. The legitimate phone line owner would not know of the fraud until a bill for the unauthorized phone calls arrived in their mailbox. From the earliest days of hacking to today's phishing schemes and other forms of fraud, success is achieved because consumers or companies are oblivious to the fraud for some period of time minutes, hours, days or weeks. Hackers and phishers work in the anonymous world of the Internet, which makes tracing these criminals extremely difficult. In addition, fraudulent websites are up for an average of only two days, disappearing before anyone is even aware of their existence.

2. FORMS OF PHISHING

Phishing is an online scam where fraudsters impersonate a trusted person or organization in an attempt to obtain personal information that may be used for identity theft. Scammers send emails pretending to be from a legitimate retailer, bank, organization or government agency [1]. The emails generally ask you to confirm your personal information by clicking on a link to a phoney website where you are asked for personal information such as identifiers or passwords. The websites may look very similar to a real company or organization you deal with on a regular basis. Sometimes you can tell that a website or email is a false one if there are spelling and grammatical errors. Websites or emails from legitimate companies should not contain spelling and grammatical errors.

3. SIGNS OF PHISHING

Phishing can take many forms and recognizing the signs can help protect you from identity theft. A fraudulent email can often seem innocent or even helpful. For example, the email sender could be contacting you for the following reasons:

- your account or credit card is about to be closed
- an order for something has been placed in your name
- your personal information has been lost because of a computer error or breakdown
- there is suspicion that your account or credit card has been subject to fraud

The giveaway is that the email will ask you to supply personal information that could be used to create a false identity or to impersonate us [2] (such as asking for our account numbers, passwords or other sensitive personal information).

4. PRECAUSIONARY ACTIONS

4. 1. NEVER RESPOND TO AN EMAIL ASKING FOR YOUR PERSONAL INFORMATION

Phishers often send authentic looking messages that appear to come from legitimate companies requesting personal information or asking you to confirm personal information which is then used for fraudulent purposes. Do not respond to email claiming to be from, for example, your financial institution or other legitimate organizations, asking you to provide your passwords, financial information or other personal information. Your bank should never send you an email asking you to provide this information. Even though your bank may call you if they suspect fraudulent activity on your bank account or credit card, they should never ask you to provide your passwords or account numbers verbally or via the telephone keypad.

If you are asked for this type of information, phone the organization to verify that the request is valid, but do not use the email address or telephone contact information provided in the email as it could be false as well. Instead, look up the contact information for the organization on their website, in the phone book or on printed correspondence you may have from them.

4. 2. NEVER ENTER YOUR PERSONAL INFORMATION IN A POP-UP SCREEN

Phishers can direct you to a real company's website, but then an unauthorized pop-up screen created by the phisher will appear asking you to provide personal information. Legitimate companies do not ask for personal information via pop-up screens.

4. 3. NEVER OPEN EMAIL ATTACHMENTS FROM SOMEONE YOU DON'T KNOW

Even if the message looks like it came from someone you know, it could be from phishers, trying to steal your information. If you are not expecting an email attachment from someone, verify with that person before opening it.

4. 4. INSTALL ANTI-VIRUS AND FIREWALL SOFTWARE

Phishing emails may contain software and computer viruses that can harm your computer or track your activities on the Internet without your knowledge. Many Internet Service Providers (ISPs) in Canada provide security software to their customers for free.

Anti-virus software can help protect your computer from computer viruses. It can also help remove known viruses from an infected computer system. Make sure you choose anti-virus

software that is up-to-date so that it recognizes current and old viruses.

A personal firewall is a software package that helps you control information that is received and sent from your computer. Make sure to choose a firewall that provides protection for information you receive (incoming) and information you send (outgoing).

4. 5. UPDATE YOUR ANTI-VIRUS PROGRAM AND PERSONAL FIREWALL REGULARLY

New computer viruses are found every day. Many software packages allow you to check for viruses and download updates automatically (auto-update). You may be able to find more details on how to update your software in the information available with each software package.

There are ways to fight phishing and they start with your Internet Service Provider (ISP). Most ISPs have filtering tools that scan emails before they reach your computer and automatically get rid of known phishing emails. Most ISPs offer this service, sometimes for a monthly fee.

It is important to also set up your own filtering service on your email account. Many free email services offer these filtering services. You can also download many phishing filters or anti-phishing programs for free by searching the Web. Ensure that you only download programs from trusted sources.

Some financial institutions and credit card companies offer online examples of what phishing emails look like. Some may also offer specific email addresses where you can send any phishing emails that you have received. Contact your financial institutions and credit card companies by telephone or visit their websites for more information on the resources and services they offer to report phishing.

5. ANTI-PHISHING SOLUTIONS

Banks now face enormous pressure to quickly and effectively shore up their online commerce sites. Many long-range solutions are in the works, but immediate solutions are necessary to ensure the well being and growth of online banking commerce.

A review of anti-phishing solutions reveals a general agreement about where the technology is heading to prevent phishing attacks. Most concentrate on managed anti-phishing services, password management, user and provider authentication through a trusted third party, shared-secret authentication and Internet caller ID.

5.1 Managed Anti-Phishing Services

Anti-Phishing Services work to quickly detect a phish attack after it has been launched and to minimize damage by monitoring accounts that have been compromised. The services try to catch phishers by monitoring suspicious domains or trying a version of entrapment, setting up false accounts to try and bait the phisher at his own game [3]. These services are aimed more at catching phishers, than preventing attacks. Once an attack has been made, the services use varied methods to shut the phisher down.

5.2 Internet Caller ID

Many companies are working on creating an Internet Caller ID, similar to caller ID for the telephone. This solution would correct weaknesses in Internet security and web browsers, but will also involve major Internet infrastructure changes and significant changes in commonly used web browsers. Industry experts agree that although the solution is very promising, Internet Caller ID is more of a hype technology rather than a solution ready for mass deployment.

5.3 Authentication through a Trusted Third Party

Employing smart cards and biometric authentication, online commerce sites can employ a trusted third-party approach to secure their transactions. Users would have to verify their identity through a fingerprint or other biometric method. Practical for static participants, the system may be too complex and economically unfeasible for banks, which have a changing consumer base.

5.4 Shared-Secret Authentication

A consumer would select a secret that is shared only with the bank, such as a photo of the family pet. The picture is then displayed to the consumer when he or she logs on, and the consumer would have to verify the secret to continue [4]. The secret is not entered during the login process, so even if a phisher captures a consumer's account information, he would be unable to access the account because he doesn't know the secret. This type of shared-secret authentication, however, raises numerous questions regarding privacy issues and is impractical for banks with a global customer base with differing laws and cultural sensitivities. Shared-secret authentication schemes must be more sophisticated and be based on modern cryptographic technology.

5.5 Time-Based Passwords

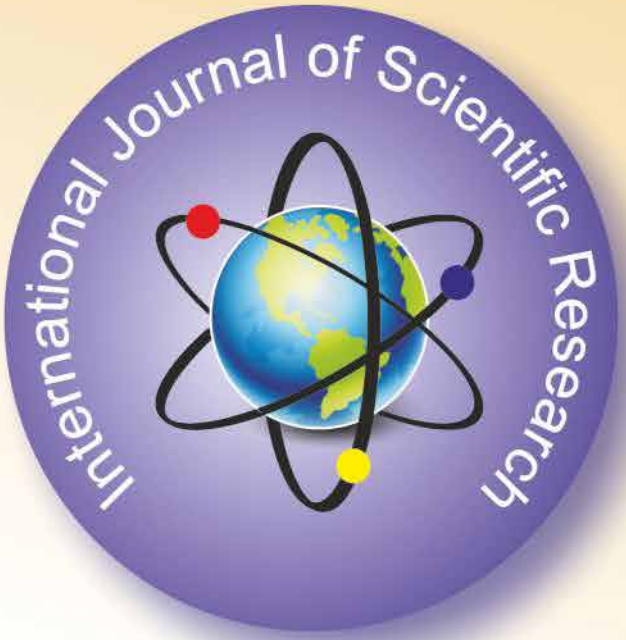
The quickest way to prevent most phishing is the use of token-protected, time-limited passwords. Almost all industry experts believe that static passwords have no place in online banking and e- commerce and that they will soon be obsolete. Requiring little consumer education and cost effective to employ, time-limited passwords may prove to be the first defense against phishing attacks. Proven to be scalable, low total cost of ownership and robust enough, time-based passwords can be rapidly deployed and seamlessly integrated with other bank applications.

6. CONCLUSION

Phishing is a form of online identity theft that aims to steal sensitive information from users such as online banking passwords and credit card information. The last years have brought a dramatic increase in the number and sophistication of such attacks. Although phishing scams have received extensive press coverage, phishing attacks are still successful because of many inexperienced and unsophisticated Internet users. Attackers are employing a large number of technical spoofing tricks such as URL obfuscation and hidden elements to make a phishing web site look authentic to the victims. The most effective solution to phishing is training users not to blindly follow links to web sites where they have to enter sensitive information such as passwords. However, expecting that all users will understand the phishing threat and surf accordingly is unrealistic. There will always be users that are tricked into visiting a phishing web site. Therefore, it is important for researchers and industry to provide solutions for the phishing threat.

REFERENCE

[1] Lance James, "Phishing Exposed", Syngress Publishing Inc., 2006. ISBN: 159-74-9030X. | [2] Markus Jakobsson and Steven Myers, "Phishing and Countermeasures", John Wielly & Sons Inc., 2007. ISBN: 0-471-78245-9. | [3] Adrew Lockhart, "Network Security Hacks – Tips and Tools for Protecting your privacy", O'Reilly Media Inc., 2007. ISBN: 0-596-52763-2. | [4] Jonathan Hassell, "Securing Access to Private Resources – RADIUS", O'Reilly Media Inc., 2003. ISBN: 978-0-596-00322-7. | [5] Peter Stavroulakis and Mark Stamp, "Handbook of Information and Communication", Springer. E-ISBN : 978-3-642-04117-4. ISBN: 978-3-642-04116-7. | [6] Mark Stamp, "Information Security – Principles and Practices", John Wiley & Sons Inc,. ISBN: 978-0-470-62639-9.



Sara Publishing Academy
INTERNATIONAL JOURNAL OF SCIENTIFIC RESEARCH
Journal for All Subjects

The Editor,
INTERNATIONAL JOURNAL OF SCIENTIFIC RESEARCH
8-A, BANAS, Opp. SLU Girls College, NR. Congress Bhavan,
Paldi – 380006. Ahmedabad-Gujarat. (INDIA)
Contact: +91 98247 02127, +91 88660 03636
Website : www.theglobaljournals.com
Email Id: ijsr@theglobaljournals.com

Printed at Unique Offset, Novatsing Rupam Estate, Opp. Abhay Estate, Tavdipura, Shahibaug, Ahmedabad