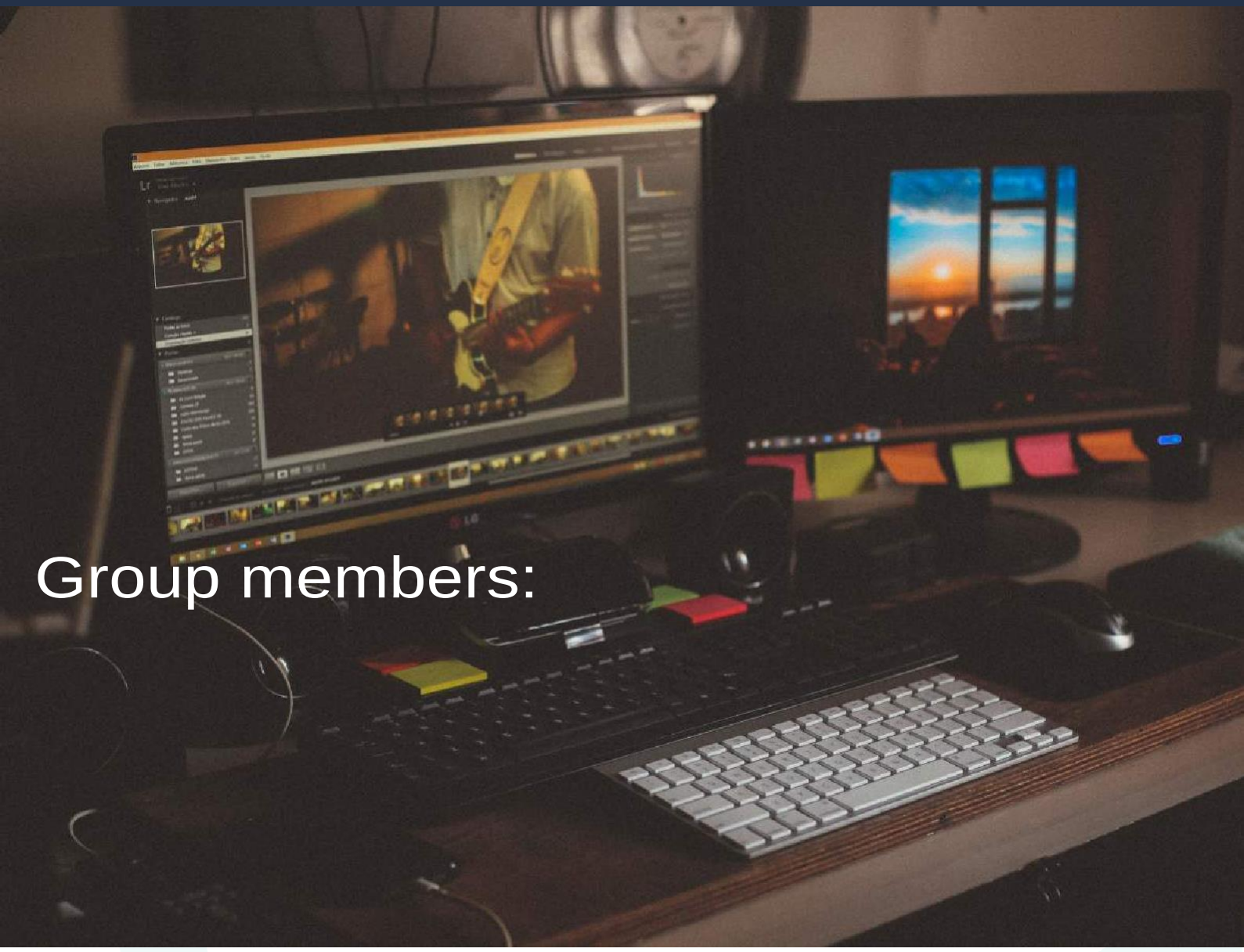
MIT ADT University
MIT School of Engineering
S.Y.(CSE-3)
Mini Project - I

ARK

TEAM MEMBERS:

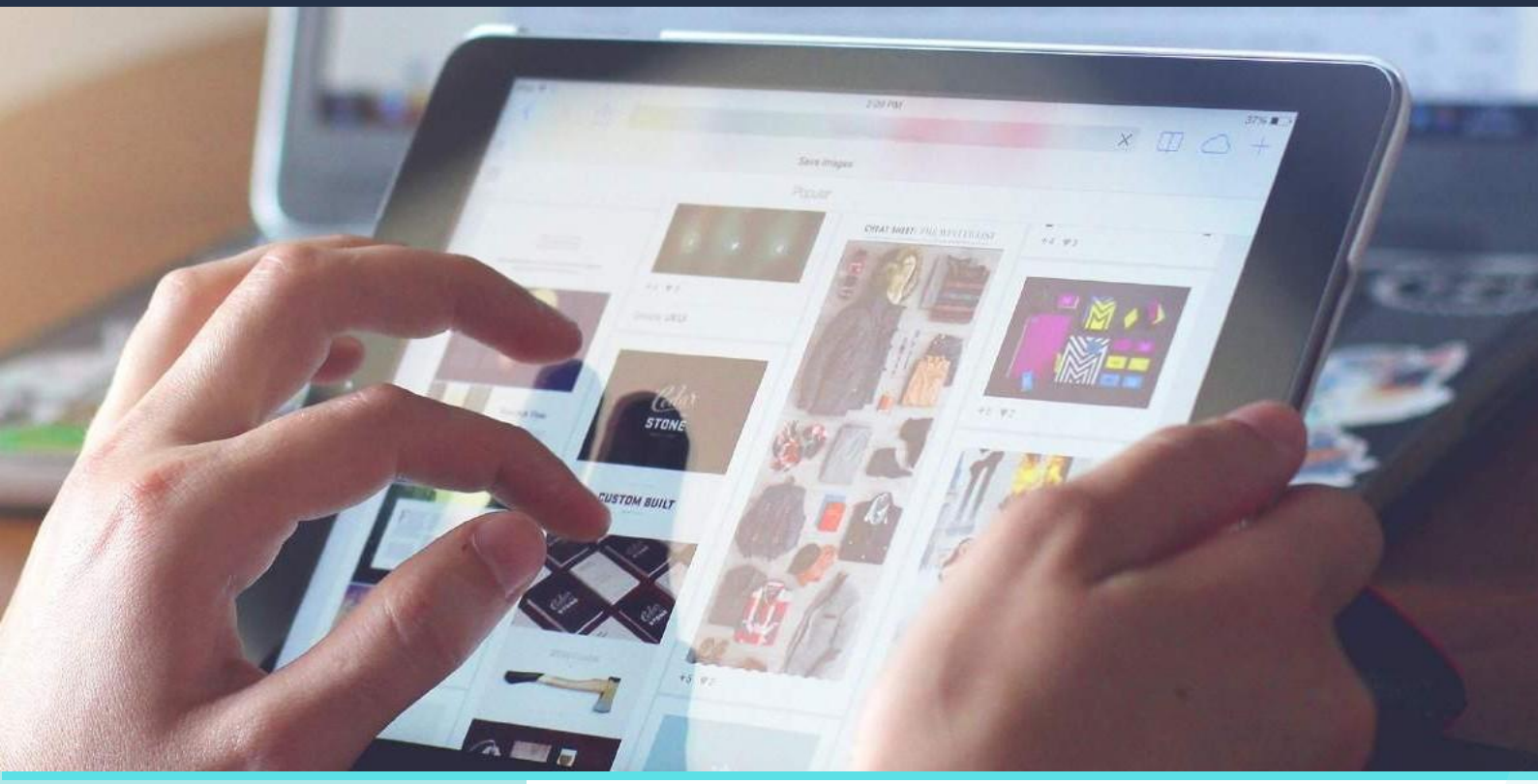
- S. UTKARSH RAO
- MANAN KUKREJA
- MOHAMMAD MUSAIB AKHTER

Project Guide - Dr. Rajani Sajjan



Group members:

Name	Roll no.	e-mail id	Contact no.
S. Utkarsh Rao	2203153	utkarshrao1177@gmail.com	6204644100
Manan Kukreja	2203180	manan241202@gmail.com	9511169915
Mohammad Musaib Akhter	2203280	musaabmallick163@gmail.com	7256013404

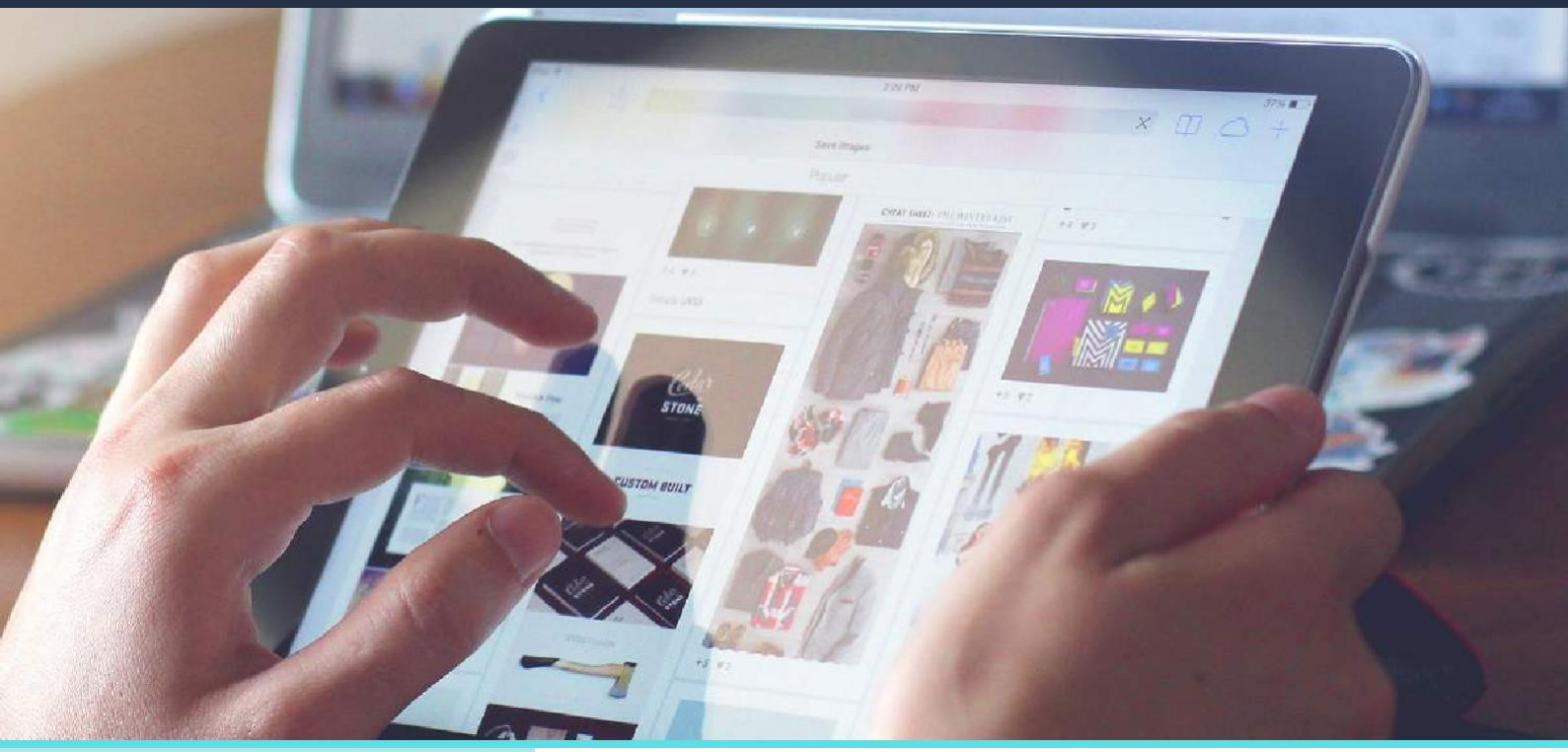


Problem statement: -

To prepare a utility software to prevent phishing through e-mails and URLs.

Introduction: -

Phishing is an act attempting to acquire information such as user name password and credit card details as a trustworthy entity in an electronic communication. Communications purporting to be from popular social websites, auction sites, online payment process or IT administrators are commonly used to lure the unsuspecting public. Phishing emails may contain links to website that are infected with malware.



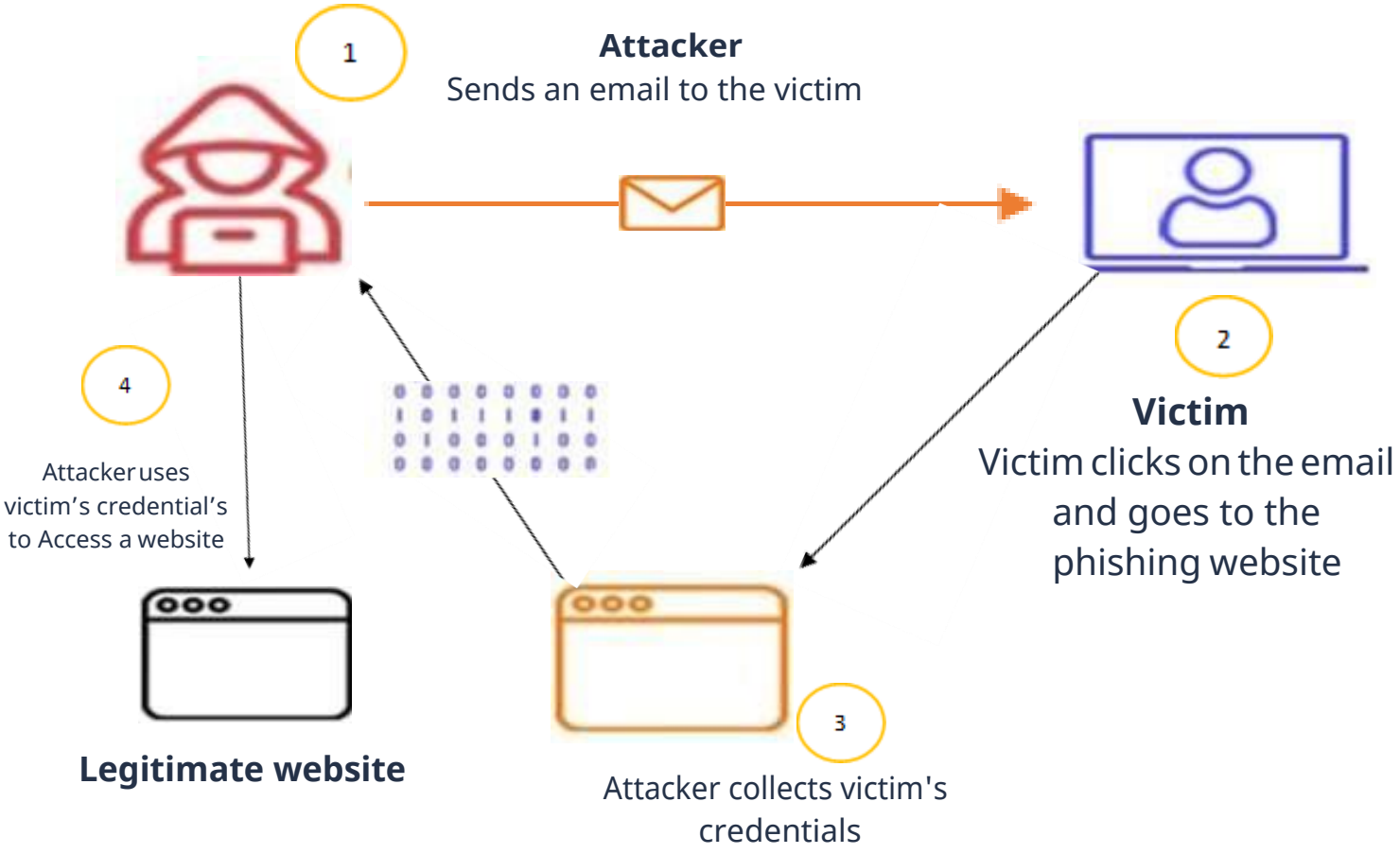
Working: -

If the user receives a mail (say in the name of their bank) asking to submit details for regular updates or something as such through ane-mail then as the user will click on the URL it will direct them to a website. Here our software comes into play, it will detect that the website is really an authentic one or not. If it is authentic then the software will let you proceed and if it is fake then it will send a warning message that this website might be fake.

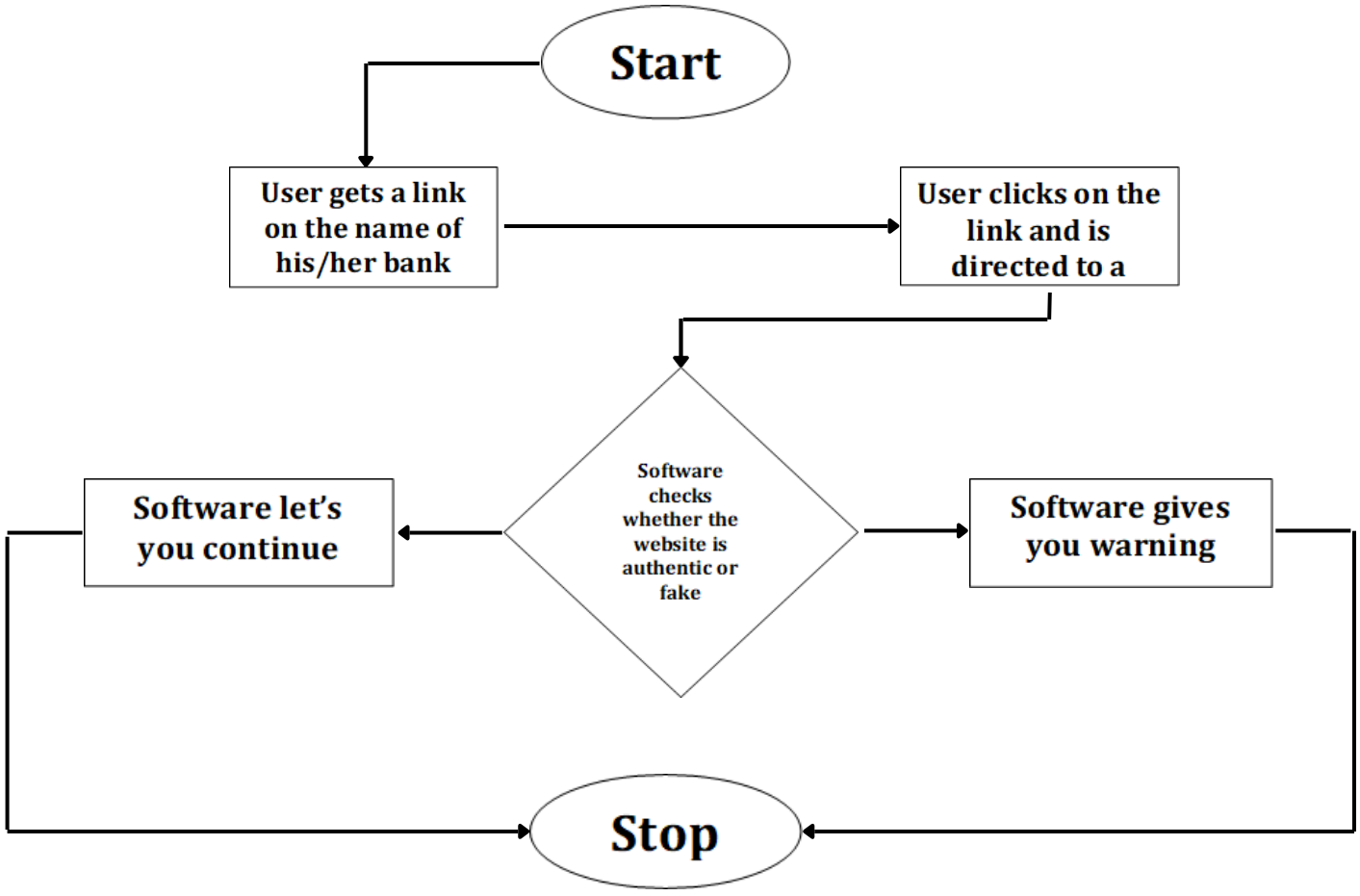
Features: -

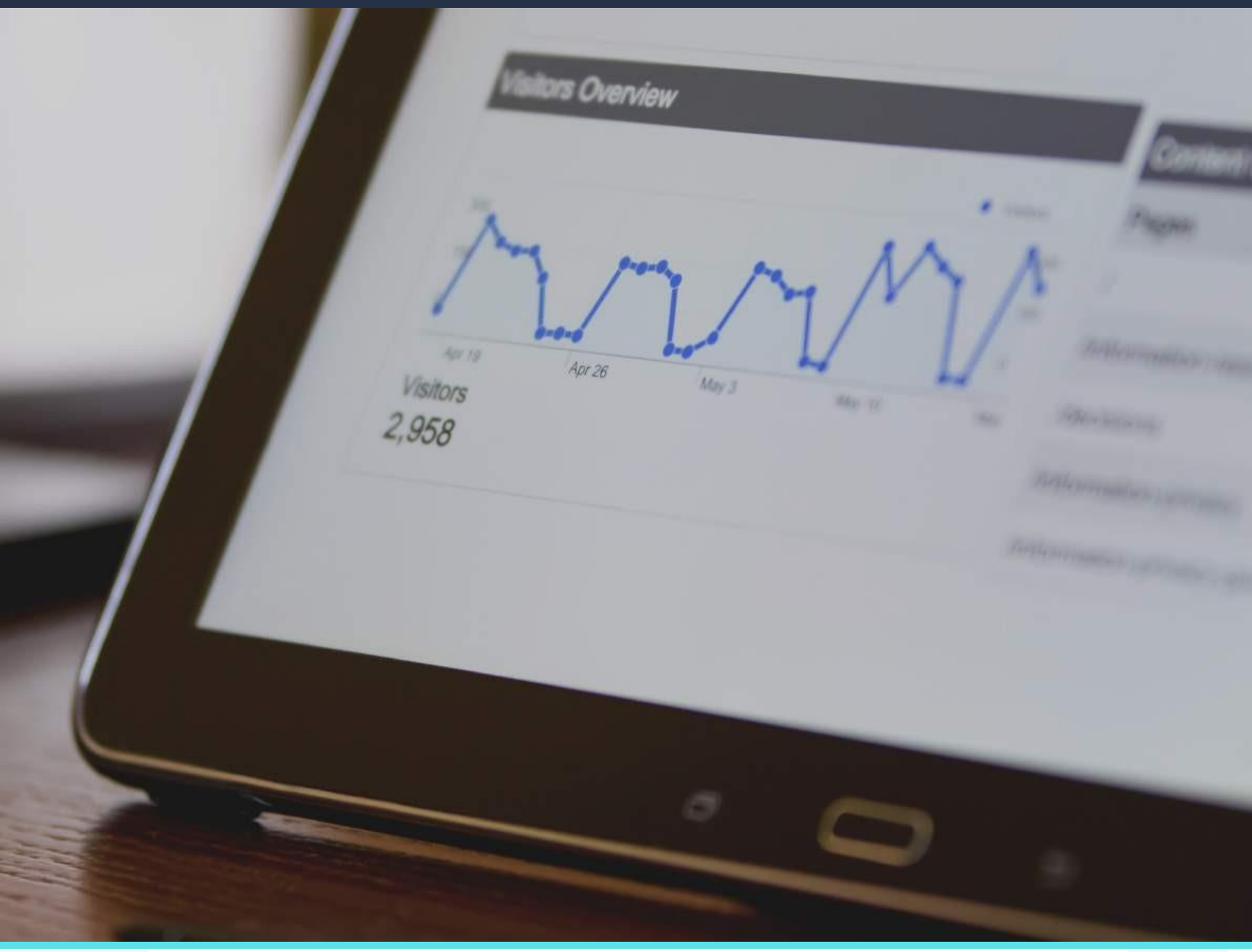
- Preventing a phishing attack through e-mails and URLs before it begins.
- Detecting a phishing attack.
- Preventing the delivery of phishing mails.
- Interfering with the use of compromised information.
- Counter measures.

Block diagram: -



Flow chart: -





How our idea isunique: -

1)Less interfaces will be provided.

2)We will provide it as a chrome extension.

3)It is not only restricted to official works and is available to every individual.

Application area of the project: -

Phishing protection software can help to prevent an attack by shielding employees from suspicious emails, blocking malicious links, stopping weaponized attachments and identifying signs of fraud and impersonation. It is often integrated with web browsers and email clients as a toolbar that displays the real domain name for the website the viewer is visiting, in an attempt to prevent fraudulent websites from masquerading as other legitimate websites.

Conclusion: -

No single technology will completely stop phishing. However, a combination of good organization and practice, proper application of current technologies, and improvements in security technology has the potential to drastically reduce the prevalence of phishing and the losses suffered from it.

References

1) “Phishing Knowledge based User Modelling in Software Design” - Linfeng Li, Timo Nummenmaa, Eleni Berki, Marko Helenius. Beijing Institute of Petrochemical Technology, Beijing, China, University of Tampere, Tampere, Finland, Tampere University of Technology, Tampere, Finland.

http://ceur-ws.org/Vol-1525/paper-16.pdf

2) “Types of anti-phishing solutions for phishing attack” - Siti Hawa Apandi, Jamaludin Sallim and Roslina Mohd Sidek Faculty of Computing, College of Computing and Applied Sciences, University Malaysia Pahang, Gambang, Kuantan, Pahang, Malaysia.

https://iopscience.iop.org/article/10.1088/1757-899X/769/1/012072/meta

3) “Machine learning based phishing detection from URLs”- Ozgur Koray Sahingoz, Ebubekir Buber, Onder Demir, Banu Diri. Istanbul Kultur University, Computer Engineering Department, 34158 Istanbul, Turkey b Marmara University, Technology Faculty, Computer Engineering Department, Istanbul, Turkey c Yildiz Technical University, Computer Engineering Department, Istanbul, Turkey.

https://www.researchgate.net/profile/Ebubekir-Buber/publication/344952543_Machine_learning_based_phishing_detection_from_URLs/links/5f9acba0299bf1b53e4f22e1/Machine-learning-based-phishing-detection-from-URLs.pdf

4) “Phishing E-mail detection based on Structural Properties” - Madhusudhana Chandrasekaran, Krishnan Narayan and Shambhu Upadhyaya Department of computer science engineering, state university of New York at Buffalo.

https://www.albany.edu/wwwres/conf/iasymposium/proceedings/2006/chandrasekaran.pdf

5) “An Efficient Approach to Detecting Phishing A Web Using K-Means and Naïve-Bayes Algorithms” - Ms. Kranti Wanawe, Ms. Supriya Awasare, Mrs. N. V. Puri. Computer
Department Universal College Of Engineering and Research, Pune

https://citeseerx.ist.psu.edu/viewdoc/downloaddoi=10.1.1.428.4810&rep=rep1&type=pdf

6) “URL based Email Phishing Detection Application” - Roshan Ravi, Abhishek Arvind Shillare, Prathamesh Prakash Bhoir, K.S. Charumathi, B.E. Student, Department of Information Technology, Pillai College of Engineering, New Panvel, Navi Mumbai, Maharashtra – 410206, India 4Assistant Professor, Department of Computer Engineering, Pillai College of Engineering, New Panvel, Navi Mumbai, Maharashtra – 410206, India

https://irjet.com/archives/V8/i4/IRJET-V8I466.pdf

7) “A Transformer-based Model to Detect Phishing URLs” - Pingfan Xu School of Computer Science University of Guelph Guelph, Canada.

https://arxiv.org/pdf/2109.02138.pdf

8) “URL Phishing Analysis using Random Forest” - S. Jagadeesan (Asst. Professor) (jagadeesan.s@ktr.srmuniv.ac.in), Anchit Chaturvedi (anchitmudit@gmail.com), Shashank Kumar(shashank.kumar14@gmail.com), Department of Computer Science and Engineering SRM Institute of Science and Technology Chennai.

http://www.acadpubl.eu/hub/2018-118-21/articles/21e/49.pdf

Annexure II: FORM B- Market and financial feasibility

Sr. No.	Parameters	Description about project	Marks
1	Business ideas and implementation from project.	This software is specially designed to prevent people from getting phished and would be initially used mainly to detect fake websites and URLs received through e-mails or text messages.	
2	Market Survey (competitors, substitute products, potential market, etc.)	Avanan, IRONSCALES, Proofpoint, trustifi etc.	
3	Market Acceptability of Product	Product will help the user to let them identify whether the website is authentic or not. If it is a fake website, it will give an alert to the user.	
4	Emerging trends about project and product.	Our product will give the user a user-friendly environment, easy to use, highly secured software & cost friendly.	
5	Income generation ideas through project.	For income generation, first we will provide our product for a nominal fee to expand our market and in future we are thinking of tying-up with companies to sell our product on higher level.	
6	Project Profitability	In the beginning, we will sell our product at very low price and will expand our market and cover all our expenditures and after that we will introduce new features which are not available in the other products available in the market but we will make sure that our product is still at low price.	
7	Cost Benefit analysis	As such we have not decided any price for it but as we go on with the project, we will set the price according to our expenditure but we will make sure it will be cheaper than the products available in the market.	
8	Any other point	Full time assistance will be provided to the users.	
Remark:			

Commercial Feasibility of project is evaluated based on the above parameters.
Project Approval Status: Approved / Not Approved

(Name & Designation of Market Expert)

Signature with Date.

Annexure III: Literature surveypapers

Linfeng Li et. al. proposed the usage of metamodelling frameworks and software tools for implementing software systems where phishing prevention is already designed as a part of the system itself. An expressive computational, verifiable and validatable metamodel is created that captures user behaviour. Next it is shown through examples that the metamodel follows and describes reported phishing scams accurately. The model is then used to create specification in an executable formal specification tool. The formal specification, which can be executed to observe user behaviour, can be used as a building block in the specification of a larger software system, resulting in an inherently phishing-resilient software system design in the form of a formal specification.

Madhusudhana Chandrasekaran et. al. proposed a novel technique to discriminate phishing e-mails from the legitimate e-mails using the distinct structural features present in them. The derived features, together with one-class Support Vector Machine (SVM), can be used to efficiently classify e- mails before it reaches the user's inbox.

Aside from discussing the prevalence of phishing attempts and the consequences of these attacks, current literature also explores techniques that may protect against them. Friedman and Hoffman (2008) provide a taxonomy that divides threats to mobile devices into seven categories, with phishing and social engineering being one of them. They describe phishing and social engineering attacks as attempts to dupe computer users into either sending confidential information to third parties or downloading malware. They suggest that educating computer users and filtering for malicious content or spam are the two major defence mechanisms against phishing and social engineering.