INTRODUCTION

The aim of our research is to explore phishing attacks and their solutions as the implementation of Cyber Laws to deal with Phishing.

**Cyber Law is the law governing computers and the internet.** In today’s highly digitalized world, almost everyone is affected by cyber law. Almost all transaction in Shares are in demat form. Almost all Companies extensively depend upon their computer networks and keep their valuable data in electronic form. Government forms including income tax returns, law forms etc are, now filled in electronic form. Consumers are increasingly using credit cards for shopping. Most people are using email, cell phones and SMS messages for communication. Even in “non-cyber crime cases” important evidence is found in computers/ cell phones e.g. in cases of divorce, Murder, kidnapping, tax evasion, organized crime, terrorist operations, counterfeit currency etc.

Phishing is a huge problem in today's world. Every year, the number of cases and amount worth of damage is caused, throughout the world. In the field of computer network security, phishing is the criminally fraudulent process of attempting to acquire sensitive information such as usernames, passwords and credit card details by masquerading as a trustworthy entity in an electronic communication. Today, 10 times more Indians use the internet for their banking needs than five years ago. And not surprisingly, the number of fraudsters eyeing our accounts has also multiplied. Globally, a large amount is stolen from consumer accounts by attacks such as phishing and the scale of such fraud in India is fast catching up.
Phishing is a way of attempting to acquire sensitive information such as usernames, passwords and credit card details by masquerading as a trustworthy entity in an electronic communication. Communications purporting to be from popular social web sites, auction sites, online payment processors or IT administrators are commonly used to lure the unsuspecting public. Phishing is typically carried out by e-mail or instant messaging, and it often directs users to enter details at a fake website whose look and feel are almost identical to the legitimate one. Phishing is an example of social engineering techniques used to fool users and exploits the poor usability of current web security technologies. Attempts to deal with the growing number of reported phishing incidents include legislation, user training, public awareness, and technical security measures.

Phishing is a form of identity theft in which deception is used to trick a user into revealing confidential information with economic value. Similar forms of identity theft, in which worms or viruses install key loggers, are sometimes also referred to as phishing. This synopsis focuses on phishing involving deceptive electronic messages. Phishing presents direct risks through the use of stolen credentials and indirect risk to institutions that conduct business on line through erosion of customer confidence.

The term phishing is a general term for the creation and use by criminals of e-mails and websites – designed to look like they come from well-known, legitimate and trusted businesses, financial institutions and government agencies – in an attempt to gather personal, financial and sensitive information. These criminals deceive Internet users into disclosing their bank and financial information or other personal data such as usernames and passwords, or into unwittingly downloading malicious computer code onto their computers that can allow the criminals
subsequent access to those computers or the users’ financial accounts. Although phishing, identity theft and identity fraud are terms that are sometimes used interchangeably, some distinctions are in order. Phishing is best understood as one of a number of distinct methods that identity thieves use to “steal” information through deception that is, by enticing unwitting consumers to give out their identifying or financial information either unknowingly or under false pretenses, or by deceiving them into allowing criminals unauthorized access to their computers and personal data.

Cyber crime cases such as online banking frauds, online share trading fraud, source code theft, Credit card fraud, tax evasion, virus attacks, cyber sabotage, phishing attacks, email hijacking, denial of service, hacking, pornography etc are becoming common. Digital signatures and e-contracts are fast replacing conventional methods of transacting business.

Cyber crimes are unlawful acts where the computer is used either as a tool or a target or both. The enormous growth in electronic commerce (e-commerce) and online share trading has led to a phenomenal spurt in incidents of cyber crime.

Cyber law is important because it touches almost all aspects of transactions and activities on and concerning the Internet, the World Wide Web and Cyberspace. Initially it may seem that Cyber laws is a very technical field and that it does not have any bearing to most activities in Cyberspace. But the actual truth is that nothing could be further than the truth. Whether we realize it or not, every action and every reaction in Cyberspace has some legal and Cyber legal perspective