REVIEW OF LITERATURE

Kim, D., Y. Song, S. Braynov, & H. Rao (2001)

In this paper Cyber Law is the law governing cyber space. Cyber space is a very wide term and includes computers, networks, software, data storage devices (such as hard disks, USB disks etc), the Internet, websites, emails and even electronic devices such as cell phones, ATM machines etc.

Cyberspace is an intangible dimension that is impossible to govern and regulate using conventional law. Cyberspace has complete disrespect for jurisdictional boundaries. Cyberspace handles gigantic traffic volumes every second. Billions of emails are crisscrossing the globe even as we read this, millions of websites are being accessed every minute and billions of dollars are electronically transferred around the world by banks every day. Cyberspace is absolutely open to participation by all.

Ferguson, A. J. (2001)

In this paper Cyberspace offers enormous potential for anonymity to its members. Readily available encryption software and steganographic tools that seamlessly hide information within image and sound files ensure the confidentiality of information exchanged between cyber-citizens. Cyberspace offers never-seen-before economic efficiency. Billions of dollars worth of software can be traded over the Internet without the need for any government licenses, shipping and handling charges and without paying any customs duty.

R. Dhamija and J. D. Tygar (2001)
According to this paper electronic information has become the main object of cyber crime. It is characterized by extreme mobility, which exceeds by far the mobility of persons, goods or other services. International computer networks can transfer huge amounts of data around the globe in a matter of seconds. A software source code worth crores of rupees or a movie can be pirated across the globe within hours of their release. Theft of corporeal information (e.g. books, papers, CD ROMs, floppy disks) is easily covered by traditional penal provisions. However, the problem begins when electronic records are copied quickly, inconspicuously and often via telecommunication facilities. Here the “original” information, so to say, remains in the “possession” of the “owner” and yet information gets stolen.


This paper describes cyber crimes may be defined as unlawful acts wherein the computer is either a tool or a target or both. Under the Information Technology offences committed within the encompass in which the investigation agency requires access to information being processed or transmitted in a computer system is a cyber crime. Computer crime can involve criminal activities that are traditional in nature known as conventional crimes such as theft, fraud, forgery, defamation and mischief etc.


In this paper 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.

**Kumaraguru (2003)**

In this paper 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.


According to this paper the simplified flow of information in a phishing attack is:

1. A deceptive message is sent from the phisher to the user.
2. A user provides confidential information to a phishing server (normally after some interaction with the server).
3. The phisher obtains the confidential information from the server.
4. The confidential information is used to impersonate the user.
5. The phisher obtains illicit monetary gain.

Steps 3 and 5 are of interest primarily to law enforcement personnel to identify and prosecute phishers. The discussion of technology countermeasures will center on ways to disrupt steps 1, 2 and 4, as well as related technologies outside the information flow proper.
Before steps 1-5 above, a phisher must set up a domain to receive phishing data. Pre-emptive domain registration may reduce the availability of deceptively named domains. Additionally, proposals have been made to institute a “holding period” for new domain registrations during which trademark holders could object to a new registration before it was granted. This might help with the problem of deceptively named domains, but would not address the ability of phishers to impersonate sites. As email authentication technologies become more widespread, email authentication could become a valuable preventive measure by preventing forged or misleading email return addresses. Some services attempt to search the web and identify new phishing sites before they go “live,” but phishing sites may not be accessible to search spiders, and do not need to be up for long, as most of the revenues are gained in the earliest period of operation. The average phishing site stays active no more than 54 hours.

Dhamija, R. & J. D. Tygar (2005)

This paper describes that phishers are targeting the customers of banks and online payment services. E-mails, supposedly from the Internal Revenue Service, have been used to glean sensitive data from U.S. taxpayers. While the first such examples were sent indiscriminately in the expectation that some would be received by customers of a given bank or service, recent research has shown that phishers may in principle be able to determine which banks potential victims use, and target bogus e-mails accordingly. Targeted versions of phishing have been termed spear phishing. Several recent phishing attacks have been directed specifically at senior executives and other high profile targets within businesses, and the term whaling has been coined for these kinds of attacks.

In this paper most methods of phishing use some form of technical deception designed to make a link in an e-mail (and the spoofed website it leads to) appear to belong to the spoofed organization. Misspelled URLs or the use of subdomains are common tricks used by phishers. In the following example it appears as though the URL will take you to the example section of the yourbank website. Phishers have used images instead of text to make it harder for anti-phishing filters to detect text commonly used in phishing e-mails.

**T. Dierks and C. Allen (2005)**

In this paper once a victim visits the phishing website the deception is not over. Some phishing scams use JavaScript commands in order to alter the address bar. This is done either by placing a picture of a legitimate URL over the address bar, or by closing the original address bar and opening a new one with the legitimate URL.

**A. Freier, P. Kariton, and P. Kocher (2006)**

According to this paper an attacker can even use flaws in a trusted website's own scripts against the victim. These types of attacks (known as cross-site scripting) are particularly problematic, because they direct the user to sign in at their bank or service's own web page, where everything from the web address to the security certificates appears correct. In reality, the link to the website is crafted to carry out the attack, making it very difficult to spot without specialist knowledge. Just such a flaw was used in 2006 against PayPal.

**Jagatic, T., N. Johnson, M. Jakobsson and F. Menczer (2006)**

In this paper many different technologies may be employed to detect a phishing attack, including: Providing a spoof-reporting email address that customers may send spoof emails to. This may both provide feedback to customers on whether communications are legitimate, and
provide warning that an attack is underway. Monitoring “bounced” email messages. Many phishers email bulk lists that include nonexistent email addresses, using return addresses belonging to the targeted institution. Monitoring call volumes and the nature of questions to customer service. Monitoring account activity for anomalous activity such as unusual volumes of logins, password modification, transfers, withdrawals, etc.

A. Herzberg and A. Gbara (2007)

In this paper monitoring the use of images containing an institution’s corporate logos and artwork. Phishers will often use the target corporation to host artwork that is used to deceive customers. This may be detected by a web server via a blank or anomalous “referrer” for the image. Establishing “honeypots” and monitoring for email purporting to be from the institution. Email filters intended to combat spam are often effective in combating phishing as well. Signature-based anti-spam filters may be configured to identify specific known phishing messages and prevent them from reaching a user.

R. Clayton (2008)

According to this paper message authentication techniques such as Sender-ID have considerable promise for anti-phishing applications. Sender-ID prevents return address forgery by checking DNS records to determine whether the IP address of a transmitting mail transfer agent is authorized to send a message from the sender’s domain. Yahoo! Domain Keys provides similar authentication, using a domain-level cryptographic signature that can be verified through DNS records. Some form of lightweight message authentication may be very valuable in the future in combating phishing.

M. Jakobsson (2009)
In this paper before entering any information on the page, make sure that URL on the top of the browser is correct even if you find the look and feel of the page is quite similar to the real login page but make sure to verify that the URL on the top of the browser belongs to the right domain name. Make sure to verify the SSL Certificate over the domain is there and do belongs to the right Certifying Authority. For example login page of orkut have a ssl certificate of thawte. You can also check the "Lock" icon There is a de facto standard among web browsers to display a "lock" icon somewhere in the window of the browser.

**G. Goth (2009)**

This paper describes many anti-viruses today have phishing protection and works in the similar way as explained above. For example, in case of Norton, Norton Internet Security 2010 Blocks phishing websites and authenticates trusted sitesYou can further use various password managers that are available as password manager will only work on the real websites and not on the phishing websites. For example, in case of passpet, Passpet have Convenient Password Management and Phishing Protection

**Fette, I., N. Sadeh and A. Tomasic (2009)**

In this paper a case that is you are suspicious about a page but the URL seems to be correct then you should verify the IP address of that domain , you may be a victim of DNS poisoning. These were the few security measures , by which you can protect yourself from becoming a victim of phishing.

**Lininger, R. and R. Dean (2010)**
According to this paper one strategy for combating phishing is to train people to recognize phishing attempts, and to deal with them. Education can be effective, especially where training provides direct feedback.

The Anti-Phishing Working Group, an industry and law enforcement association, has suggested that conventional phishing techniques could become obsolete in the future as people are increasingly aware of the social engineering techniques used by phishers. They predict that pharming and other uses of malware will become more common tools for stealing information. Everyone can help educate the public by encouraging safe practices, and by avoiding dangerous ones. Unfortunately, even well-known players are known to incite users to hazardous behaviour, e.g. by requesting their users to reveal their passwords for third party services, such as email.

**Kim, D., Y. Song, S. Braynov, & H. Rao (2010)**

In this paper anti-phishing measures have been implemented as features embedded in browsers, as extensions or toolbars for browsers, and as part of website login procedures. The following are some of the main approaches to the problem.

**N. Haller (2010)**

This paper describes the standard display for secure browsing from the mid-1990s to mid-2000s was the padlock. In 2005, Mozilla fielded a yellow URL bar 2005 as a better indication of the secure connection. This innovation was later reversed due to the EV certificates, which replaced certain certificates providing a high level of organization identity verification with a green display, and other certificates with an extended blue favicon box to the left of the URL bar (in addition to the switch from "http" to "https" in the url itself).
The user is expected to confirm that the domain name in the browser's URL bar was in fact where they intended to go. URLs can be too complex to be easily parsed. Users often do not know or recognise the URL of the legitimate sites they intend to connect to, so that the authentication becomes meaningless. A condition for meaningful server authentication is to have a server identifier that is meaningful to the user; many ecommerce sites will change the domain names within their overall set of websites, adding to the opportunity for confusion. Simply displaying the domain name for the visited website as some anti-phishing toolbars do is not sufficient.

A. Genkina, A. Friedman, and J. Camp (2011)

In this paper the browser needs to state who the authority is that makes the claim of who the user is connected to. At the simplest level, no authority is stated, and therefore the browser is the authority, as far as the user is concerned. The browser vendors take on this responsibility by controlling a root list of acceptable CAs. This is the current standard practice.

The solution to this is that the browser should show, and the user should be familiar with, the name of the authority. This presents the CA as a brand, and allows the user to learn the handful of CAs that she is likely to come into contact within her country and her sector. The use of brand is also critical to providing the CA with an incentive to improve their checking, as the user will learn the brand and demand good checking for high-value sites.

Lee, M. & E. Turban (2011)

In this paper specialized spam filters can reduce the number of phishing e-mails that reach their addressees' inboxes. These approaches rely on machine learning and natural language processing approaches to classify phishing e-mails. Several companies offer banks and other organizations
likely to suffer from phishing scams round-the-clock services to monitor, analyze and assist in shutting down phishing websites. Individuals can contribute by reporting phishing to both volunteer and industry groups, such as PhishTank. Individuals can also contribute by reporting phone phishing attempts to Phone Phishing, Federal Trade Commission.