Technology comes

Technology

Technologycomes in with a lot of benefits as it simplifies work and increases integration of various countries and business organizations world wide, but it also brings in new threats to personal and property security, one of the greatest security threats people are now facing in the wake of accelerated technology is phishing, which is a means by which unauthorized people obtain someone’s personal information with the intention of using it to assume the identity of the victim so as to be able to stealmoneyor other benefits that accrue to the victim.

The phishers usually communicate with the victim via e-mail or any other mode ofcommunication. They usually pretend to be legitimate agents of a bank, retailer or the government. The victim is in most cases directed to a web site, where they are required to revise their personal information such as social security, credit card, bank account numbers, and pass words which are already in the possession of the legitimate organization. However, the web site is a sham and it is only intended to steal the personal information of the user (Emigh, Para 3-4) Identifying phishing schemes

It is always very important to identify a phishing scam, since one is likely to loose a lot in the event of falling prey to a phishing trap. The use of e-mails is the most popular method of phishing nowadays; the phishers send an e-mail which is deceptive, in which the user is required to act on by clicking to a link. Such requirements include a statement indicating that there is a problem with the users account at a bank, microfinanceinstitution or any other financial institution. In the e-mail the victim is usually asked to visit a certain web in order to correct the problem.

Whenever one receives such an e-mail it is always good to try as much as possible to communicate with the institution in question so as to verify the whether the information found in the e-mail is true. Whenever, one receives some information that is suspicious especially where they are required to provide their personal details, such information should always be treated with the contempt that it deserves, and more so if the mode of communication is not the normal one usually used (Emigh, Para 5) One can also be in a position to identify a phishing scam through the tone and language used in the e-mail.

In most cases there is an element of urgency. Such messages usually indicate thatfailureto act urgently your account will be closed or suspended. These messages will also in all cases require one to give their personal details, which should be submitted to false links. It is also possible to identify false e-mails as they will not be reflected in the company's websites, since in almost all cases company's websites usually shows all the communications done via e-mails thus if such cannot be verified then most likely that e-mail received is fraudulent.

By receiving an e-mail that requests your personal details and other information that is not likely to be asked ordinarily should act as the first step in identifying a phishing scam (Heim, Para 6) Preventing phishing schemes Once a person becomes victim of a phishing scam a major loss is likely to occur through loss of money or some other valuables. It is therefore, very important for people to protect themselves.

One of the best ways of preventing your self of becoming a victim to a phishing scam is failing to respond to a request that is unsolicited by providing your personal details. Such information should not be provided whether it is over the internet or the phone. Users should know that the internet and e-mail pages that are usually used by the phishers look similar to those used by the legitimate institutions and it might be quite hard to distinguish between the two. So if one believes that the contacts could be valid them they should contact the institution in question themselves.

They can do so by either visiting the company's website and instead of using the provided link one should actually type the address or use a page that you might have book marked earlier. One should initiate the contact using the information that you have verified (Naraine, Para 3) There is no single legitimate financial institution that would require their client to verify their pass words and information about their accounts online thus one should avoid providing such information online.

It is also important to keep reviewing the bank statements regularly so as ensure that all the charges indicated are correct and that none has been transacted by unauthorized persons. One should avoid disclosing of personal information such as the account numbers, passwords, and social security numbers either over the internet or phone especially if you are not the one who had initiated the contact. One should also avoid clicking on links that for any reason they believe that they could be fraudulent as such links could be containing viruses.

One should also be strong so as not to get intimidated quickly by e-mails which give warnings of dire consequences for failure of verifying or providing financial or other personal information online, instead it is always good to report such cases to the relevant authorities. Once you fall victim to such an attack, you should act fast to mitigate any further losses. You should immediately alert the financial organization, ensure that your credit files are placed with fraud alerts and also closely monitor the account statements and credit files (Emigh, Para 8)

Conclusion Phishing is a serious fraudulent activity and once one falls prey to it can end up loosing significantly. It is thus good to increase awareness of such vices so that when people are targeted for such acts they can be able to identify them and subsequently be in a good position to protect them. People should also do all that is possible in order to conceal their vital information and ensure that it is only given to the relevant authorities when needed. Work cited: Emigh, Aaron.

Online Identity Theft: Phishing Technology, Chokepoints and Countermeasures (2005): Retrieved on 21st April from, http://www. antiphishing. org/Phishing-dhs-report. pdf. Heim, Kristi. Hackers extract personal data from eBay, Earthlink, Yahoo in 'phishing' theft. (2004): Retrieved on 21st April from, http://www. highbeam. com/doc/1G1-118630507. html. Naraine, Ryan. Phishing without bait: The in-session password theft attack (2009): Retrieved on 21st April from, http://blogs. zdnet. com/security/? p= 2390.