**6(a). CYBERSQUATTING**

The word ‘squatting’ means occupying an abandoned place illegally over which the occupier had no rights. Cybersquatting is almost a same type of offence. It means registering, selling, trafficking-in or anyway using a domain name by someone over which he has no right over, to make profit from the good-will of the another person or entity, who actually has the right over such domain name, by using such domain name in bad faith.

Cybersquatting is nothing but a trademark infringement. The trademark which has been used by one entity, is used by another. But, in the cyberspace, such trademark is actually nothing but Domain Name. Entities’ domain names are qualified to be their trademarks. If such or confusingly identical to such domain name is used by another entity over cyberspace, such amounts to cybersquatting. So, it is a type of Domain Name dispute in fact. Domain Names, in easy language are nothing but the identity of an website. For example, ‘google’ is the domain name for Google; similarly ‘facebook’ is also a domain name; and ‘.com’, ‘.in’ - these are also considered as domain names.

In perhaps the most famous cybersquatting case, Marks Spencer public limited company and others Vs One in a Million LTD, the English Court of Appeals held that by registration of distinctive household names like Marks & Spencer public limited company, J. Sainsburry public limited company, etc., a false representation was made to the person who consulted the register, that the registrant was connected with the name registered and constituted passing off.

In Rediff Communications LTD, v Cyberbooth (AIR 2000 Bom 27), plaintiff, the owner of the well-known portal and domain name rediff.com filled for injunction against the defendant, registrant of the domain name "rediff .com". There was a common field of activity and the judge was satisfied that there was a 'clear intention to deceive' and granted interim relief to the plaintiff. The judge stated, "A domain name is more than an Internet address and is entitled to the equal protection of trademark."

**6(b). CYBERSTALKING**

Cyber stalking may be defined as the use of the Internet or other electronic means to stalk or harass an individual, a group, or an organization. It may include false accusations, defamation, slander and libel. It may also include monitoring, identity theft, threats, vandalism, and solicitation for sex, or gathering information that may be used to threaten or harass an individual.

Cyber stalking is often accompanied by real time or offline stalking. Both are criminal offences. They are motivated by a desire to control, intimidate or influence a victim. A stalker may be an online stranger or a person whom the target knows. He may be anonymous and solicit involvement of other people online who do not even know the target.

Cyber stalking is a criminal offence under various nations’ anti-stalking, slander and harassment laws. A conviction can result in a restraining order, probation, or criminal penalties against the assailant, including jail time.

Under the Nigerian Cyber Crime Prohibition Act, 2015, Section 24 states that:

“Any person who knowingly or intentionally sends a message or other matter by means of computer systems or network that:

1. Is grossly offensive, pornographic or of an indecent, obscene or mincing character or causes any such message or matter to be so sent; or
2. He knows to be false, for the purpose of causing annoyance, inconvenience, danger, obstruction, insult, injury, criminal intimidation, enmity, hatred, ill will or needless anxiety to another or causes such a message to be sent, commits an offence under this Act and shall be liable on conviction to a fine of not more than N7,000,000.00 or imprisonment for a term of not more than 3 years or to both such fine and imprisonment.

Some form of cyber stalking activities which is usually carried out by assailants on social media as it relates to cybercrime includes:

* Sexual Harassment – This is the most common type of harassment and stalking online.  Online sexual harassment makes it very easy for the stalker to be anonymous. This action may or may not be carried out by someone who knows the victim. Often the online harasser has no fear of physical retaliation (slap in the face) and does not have to leave the comfort of his home to find, pursue and harass targets. The stalker usually has soft targets such as teenagers and other vulnerable people (lonely female teenagers or heartbroken adults).
* Love Obsession – Love obsession stalkers often believe that the target of their desires is really in love with them, which means they cannot understand the word ‘NO’.  A love obsession can start from an online romance, where one person then halts the romance, and the rejected lover cannot accept the end of the relationship. These stalkers usually do not have the ability to physically confront the victims. (In this case, detailed personal information is often shared between the persons involved).
* Hate/Revenge Vendettas – Hate vendettas may have nothing to do with sexual harassment at all.  There are more male targets in this category.  Hate vendettas may begin with an argument or disagreement that escalates out of control.  A vendetta may also be waged against someone because of their beliefs.
* Power Trips/Ego Trips – The victim is usually selected as a random target by someone they do not know. The motivation of the harassers is to show off their skills to themselves and their friends.  They do not have a personal grudge against the victim – they are using the victim to demonstrate their power among their own group.

**6(c). SPAM/PHISHING.**

Spam also known as electronic junk mail are unsolicited messages sent by email, text message or instant message without the recipient’s consent. Spam messages often contain offers of free goods or ‘prizes’, cheap products, promises of wealth or other similar offers. You might be asked to pay a joining fee, to buy something to ‘win’ a prize.

It is generally used by advertisers because there are no operating costs beyond that of managing their mailing lists. It could also take place in chat rooms, in blogs and more recently within voice over internet conversation (such as Skype). Beyond being a simple nuisance, spam can also be used to collect sensitive information from users and has also been used to spread viruses and other malware.

Spam is the use of electronic messaging systems to send unsolicited bulk messages indiscriminately.

While the most widely recognized form of spam is e-mail spam, the term is applied to similar abuses in other media: instant messaging spam, Usenet newsgroup spam, Web search engine spam, spam in blogs, wiki spam, online classified adds spam, mobile phone messaging spam, Internet forum spam, junk fax transmissions, social networking spam, television advertising and file sharing network spam. Perpetrators of such evil use e-mail extractor to extract all user of a particular domain and this is mostly common with yahoo mails. Some of these address harvesting approaches rely on users not reading the fine print of agreements, resulting in them agreeing to send messages indiscriminately to their contacts. This is a common approach in social networking spam such as that generated by the social networking site.

Under the definition section of Nigeria’s Cybercrime (Prohibition, Prevention, etc.) Act 2015, phishing means “the criminal and 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 through emails or instant messaging either in form of an email from what appears from your bank asking a user to change his or her password or reveal his or her identity so that such information can later be used to defraud the user.”

The statutory definition above is quite similar to Ramzan’s definition of phishing as “the attempt to acquire sensitive information such as usernames, passwords, and credit card details (and sometimes, indirectly, money), often for malicious reasons, by masquerading as a trustworthy entity in an electronic communication.”

So phishing is a social-engineering technique that fraudsters use to deceive people into giving out personal sensitive information that compromise their security.

Phishing is a prevalent cybercrime in Nigeria, aided by an alarming youth-unemployment rate and unhealthy value system. Before the Cybercrime (Prohibition, Prevention, etc.) Act became the governing law from May 2015, the offence of phishinghad not been created in any criminal laws in Nigeria. For too long, thousands of fraudsters took advantage of this legislative gap.

Law-enforcement agencies in the country generally prosecuted persons they suspected were involved in phishing and electronic-fraud related offences based on the provisions of some preexisting criminal laws in the country.  These laws include the Criminal Code (in the South), and the Advance Fee Fraud and other Fraud-Related Offences Act 2006.

Section 1, 6, and 8(a) of the Advance Fee Fraud and other Fraud Related Offences Act 2006 have spread nets wide enough to catch persons who phish or scam online. The State can charge an accused person with obtaining money by false pretenceunder sections 1, 6, and 8(a) of the Act.

Section 1 provides that any person who by any false pretence and with intent to defraud obtains from or induces any other person in or outside Nigeria is guilty of an offence. Section 1(3) uses the phrase ‘obtains any property”. If the person is found liable, the punishment is imprisonment for a minimum of 7 years and maximum of 20 years. There is no option of fine.

So section 1(1) and (2) above requires the State to prove defendant’s false pretence and intent to defraud, two elements that are also present in phishing. In State v Ajuluchukwu, a case of fraud, the Court of Appeal has stated what the prosecutor must prove to get conviction:

1) There was a pretence

2) The pretence emanated from the accused person

3) That it was false

4) That the accused person knew of its falsity

5) That there was an intention to defraud

6) That the thing was capable of being stolen and that the accused person induced the owner to transfer the whole interest in the property.

While section 1 of the Advance Fee Fraud and other Fraud Related Offences Act 2006 is appreciably useful, prosecutions find it inadequate in certain cases where for instance no propertyin the sense it is used in the Act has been stolen. Though induce and obtain are quite apt for phishing activities.

**6(d) LOGIC BOMBS**

Logic bombs are a malicious programming code that is inserted into a network system or a single computer for the purpose of deleting data or creating other malicious acts on a specified date. A logic bomb works similar to a time bomb because it can be set to go off at a specific date. A logic bomb does not distribute malicious codes until the specified date is reached.

Logic bombs are created by criminals who are well-versed in computer programming and are generally use to performing acts with malicious intent that threaten network security. The criminal acts include setting a virus to be released into a network system or PC at a specified date or other actions such as deleting or corrupting data and completely reformatting a computer hard drive.

A logic bomb works through a code that is inserted into existing software on a network or in a computer where it will lie dormant until a specific event occurs such as a date or time or other command from the computer programmer. When the bomb finally releases the code it can delete files, send confidential information to unauthorized parties, wipe out databases, and disable a network for a period of days.

A logic bomb can be used by a disgruntled employee or other IT personnel that has the knowledge of how to program a logic bomb to threaten network security. Other than targeting a specific computer or network system, a logic bomb can also be used to demand money for software by creating a code that makes the software application into a trial version. After a specific period of time the user must pay a specified sum of money to continue to use the software.

Logic bombs can also be used for blackmail and if the demand is not met, the logic bomb will detonate into a computer system or network to destroy data and perform other malicious acts that are included in the command codes.

Logic bombs are fairly easy to create if you have a lot of knowledge in computer programming and they do not replicate like other malicious programs. For this reason, logic bombs are usually targeted to specific victims and will not spread to unintended victims.

A logic bomb can be rather difficult to detect, however you can take security measures such as constantly monitoring the network system for any suspicious activity, using antivirus applications and other scanning programs that can detect any new activity in the data on a network system. The scanning systems should also monitor the entire network and the individual computers connected to the network.