Paakat
Revista de tecnología y sociedad

Recension. Black internet. The dark side of the web

Recensión. Internet negro. El lado oscuro de la red

http://dx.doi.org/10.32870/Pk.a10n18.465

Patricia Vargas Portillo*
http://orcid.org/0000-0002-0226-3053
ESIC Business & Marketing School

Received: October 8, 2019
Accepted: January 29, 2020

Reviewed work: Peré Cervantes & Oliver Tauste. (2016). *Internet negro. El lado oscuro de la red*. Madrid, Spain: Martínez Roca Editions.

When we type the usual *www* acronym in an electronic device (computer, smartphone, tablet, among others) and then, the address of a webpage, in a matter of seconds we have access to all the information which, without the revolution of technology, would take us days, weeks or months to find. There is no question that Internet has made our life more comfortable and accessible by abruptly changing the way we interact with daily existence but, simultaneously, we have also been exposed to risks which only a few decades ago were fully unimaginable. Again, in the field we are discussing, as we are witnesses and players, reality outdoes fiction.

As is known by everyone, the network of networks was a communications system designed by the North American industry of defense. The most significant reason for the origin of the network lies in political factors, as this was in the 1960s, during the Cold War, when rivalry between the two great powers, Russia and the United States, fostered the arms race without losing sight of the value which the technological development had in the attainment of objectives. In this sense, the persons responsible for Defense Advanced Research Projects Agency (DARPA, an agency in charge of North American research and development projects) tried to find a communications system that could not be blocked by a nuclear threat.

The interconnection system among all the computers took place in view of the appropriation of connection language and by means of protocols. The first network control protocol, the Network Control Protocol (NCP), began its operation in 1970 and

* PhD. in Economic and Business Sciences, University of Huelva, Spain. She has a diploma in Advanced Studies (equivalent to a master's degree) with a distinction grade by the University of Huelva, Spain. Master's in Business Management, International University of Andalucía (Spain) and master's in Touristic Business Management, University Francisco de Vitoria, in collaboration with CESAE Business & Tourism School (Spain).

after 1983 the Transfer Control Protocol/Internet Protocol (TCP/IP) was set up, which currently works in the World Wide Web, and has turned into a system that may cause damage to some extent.

The most feared subjects in the digital format, until a relatively short time, are included in the term of hackers. This word is linked to people who used to repair telephone boxes of the United States in the 1950s, whose main repair tool was a sharp blow to the failing device, which was termed a hack. In advance, it may be said that this is a software resorting to non-programmed penetration techniques to access a computer system with diverse purposes. Within the latter, we can quote, without an exhausting spirit: to satisfy its curiosity, to overcome pre-established filters, to verify the vulnerability of the system to correct its security; to deprive, change, damage or delete information.

The motivations for these actions, presented as an example, also respond to the most varied interests: for profit, anarchist ideology positions, ambition for knowledge, vanity and political dissemination. The activities taking place today, in the deep web or deep Internet field, enjoy a notoriously more significant extension than those seen at the beginning, as a result of malicious actions of hackers. It is necessary to point out that, along with malicious hackers, they made way to those qualified as ethical hackers with more amicable intentions.

The book which is the object of this review has a total of nine chapters that will be discussed below, in a general manner, and highlighting the most outstanding aspects. The first chapter, with the title of “What Google sees”, deals with the most common network frauds. In this sense, among other aspects, it refers to phishing, pharming, ransomware, the Nigerian letters, and fake apps. The range of scams becomes wider, and the methods are most sophisticated. Criminals sharpen their inventiveness to unbelievable limits. Unfortunately, the crisis has caused the most vulnerable or naïve to fall in the trap. The purpose of phishing and pharming is to steal the funds users have in banks. The risk is very high and dangers are more and more extensive. This type of frauds as a whole arrives in the spam format (unsolicited electronic mail) or malicious applications. The latter, as is known, is the big defect of marketing by email and the reason why more companies renounce to this action as they believe it is invasive, with scarce validity and because it is confused as a well-structured campaign with an indiscriminate delivery without any kind of filter.

Some of the most frequent frauds were “muleteers”. These are intermediaries between actual criminals and users who have been the victim of phishing. The manner to recruit muleteers, apparently legitimate, is by means of fake job offers in domestic portals, but also in instant messaging channels or, even, spam. Another of the mostly used frauds of later years is the phishing car, which consists of automobile advertisings,

generally of high range, advertised at a very sales price. Once the price has been paid, the seller will never appear.

In spite of technological advances in the subject of bank cards, carding, or card cloning continues. The cloning method is so vertiginous that any person could be an actual victim who may have not felt anything wrong about the usual payment methods. Criminals manage to have access to our information to transfer them to a blank card or to make online transactions, where physical cloning is not necessary. In addition, the authors say, in a general manner, that we ought to be cautious with the so-called malware, malicious programs used by criminals with different purposes, mainly to extract personal information (like card numbers or bank passwords). Therefore, you have to be selective and careful with regards the contents you have access to.

We should also note other more sophisticated frauds currently taking place. We refer to the practice called vishing, or telephone fraud. Impersonation of telephone calls from fake bank institutions is another way of *cybercriminals* to operate. By means of deceit and by repeating the audio image of the financial entity, they contact customers and mention of a possible non-recognized charge; as the full name and some numbers linked to cards are given, cybercriminals disturb and worry the victims and, therefore, thanks to the surprise factor on their side, they perform an apparent process and cancel the transaction.

Chapter two is devoted to scams which minors may be the subject to. We are referring, among other actions, to cyberbullying. According to data of the World Health Organization (WHO), Spain is one of the countries with the greatest *cyberbullying* index. The Save the Children Foundation, as a result from a survey done to more than 21,000 Spanish children, has confirmed that half of them said they had cyberbullied and a very significant number admitted they did not know the reasons why they had done it. Now then, we ought to consider that this type of practices has been extrapolated, as stated by the authors of the work, to professors who are the target of humiliation by students who record these actions. This behavior is dubbed as *cyberbaiting*, the lack of education and values on this type of actions is a constant. Although minors do not take this as mockery or a challenge to see who humiliates the professor more, *cyberbaiting* leads to serious and punishable violations against the honor, offenses, threats and battery. All of these actions represent felonies typified in the criminal code.

Minors may undergo other type of actions from which they ought to be fully protected, such as grooming, sexting and, to a lesser extent, hacking or personal password theft. To prevent this type of actions, parents or guardians ought to use extreme surveillance measures. As a complementary character, parental control filters ought to be installed, such as *Safesearch*. The lack of moral bases in the future adult causes serious problems connected to the practices and new ways for its development. Victimization of women in the electronic stage has become especially preeminent

induced by two added features in the network itself; first off, it is about the facility to cause damage, aided by a high level of lawlessness and by problems to protect privacy; in the second place, insoluble contact with the victim of the offender, specifically, by means of intelligent telephones, social networks and applications of a different scope.

Another chapter deals with old age in the network. As disclosed by its item, the most analogous, in the same mode, are the most vulnerable. Internet, without the necessary precautions, may be an inhospitable place for older adults. Among the most usual risks to older internet users, we can mention: interacting with websites or malicious emails with illegal ends; sharing photos or videos with criminals without being aware; violation of privacy without their knowledge; and the most usual: being victims of scams of a diverse nature. There are leading companies in the matter of computer security performing instruction activities in this subject. McAfee, which is integrated in Intel Security, launched its Online Safety for Silver Surfers program (online security for older surfers). This is a free initiative where McAfee and Intel employees make for older people and teach them how they can surf the web in a safe way, to safeguard their information and the devices they have access from.

Hacking is the main problem of the following chapter. Although generally, hacking, as pointed out, is related with a pejorative movement as it drags illegal connotations, there is a figure that needs to be considered. We refer to the ethical hacker, who is devoted to access a system to determine its potential vulnerabilities, which, in turn, prevents infiltration of hackers with illegal ends. They are experts in accessing computer systems and software to assess, invigorate and optimize security.

Another chapter is titled “Protecting the company in the network”, and it refers to attacks that may be sustained by small and medium size companies currently. Although there are no statistics on the number of crimes suffered by these companies, researchers say that computer attacks to SMEs are increasing at the same pace as web crime: approximately 30% annually without including the black figure (which refers to non-denounced crime, whose specific data are hardly quantifiable). Most of the small and medium size enterprises cannot assume the economic effort a large company makes to safeguard its server infrastructure. Cybercriminals elect to commit minor felonies instead of a single big hit. Likewise, it must be said that the biggest threat to SMEs are cyberattacks like ransomware.

With a good judgment, the book also studies techno-addictions or addictions to specific electronic devices, that are each time more frequent and intense. The phenomenon we are referring to includes all the manners of abusing information and communication technologies (ICT), that are commonly linked to an extreme addiction to the network or to intelligent telephones (which includes videogames on the network). As reality shows, each time we are more dependent on these devices. The need to be

interconnected in a permanent manner is one of the signals of dependency linked to the anxiety of not having Wi-Fi, navigational data or battery in electronic terminals.

Another chapter is devoted, in the broad sense, to the dark side of the network and it is titled "What Google does not see". Deep web is accessible through the TOR network. Almost always, the media speaks of deep web to relate it to criminal activities performed in insurmountable bottoms of the network and hardly ever explain what it is. Approximately 90% of the Internet content is not accessible through search engines. If a simile is allowed, it is like an iceberg: a minimum section is visible. This is a section of the deep web, which encompasses all the information the public cannot have access to. They may simply be conventional websites preserved by a paywall, but also saved files in Dropbox, emails deposited in the servers of a provider and all the pages that are created during small time tags, for example, when you have access to a travels search engine and the content is presented.

If the deep web is as we have pointed out, 90% of the network, the dark web, would use, to mentione a figure, only 0.1% of it. This is a fraction of Internet concealed from search engines, with undercover IP addresses and only accessible with a specific web browser for that purpose. The dark web, therefore, is an inseparable part of the deep web. The dark web represents the content that may be found in different *darknets*, which comprise each of the networks to which access may be possible with specific programs. The best known is TOR, but there are others like Freenet, I2P and ZeroNet.

It must also be stated that the dark web is not illegal *per se*, as there are abundant websites with a constructive content. In addition, the dark web is used as a shelter for hunted revolutionaries in their respective countries where there is no freedom of speech. The book refers to one of the most popular cases in this sense: The Silk Road portal, a black market to which people could only have access through a TOR browser and that only admitted payments with bitcoins (an electronic currency based on anonymity). The products on sale were drugs, weaponry and another type of illegal activities. The success of this portal (with transactions for a value higher than 9.5 million bitcoins, which in turn, is equivalent to 1.4 billion dollars) caused the North American authorities to become aware of their illegal activities.

Its founder, who used the nickname of Dread Pirate Roberts, was recognized as Ross Ulbricht, who grew in a middle-class family and as a child he had been a boy scout. Paradoxically, Ross was not the perverse genius which the media and the authorities had predicted. It was not proven that Dread Pirate Roberts was a single person, because the anonymity system left a number of aspects blank. Dread Pirate Roberts stated in an interview with Forbes that he was not the creator of Silk Road. In this sense, it was said that this username was a title that would pass from one person to another in the advance of the website. He was trialed and sentenced with life sentence. There are many particularities in this case that could make us reflect on

whether the sentence was clearly disproportionate. Engaging in this subject, undoubtedly, would overcome the objectives of this review.

This is an exciting book. As emphasized by its afterword, we are undergoing an authentic revolution thanks to Internet. Could anyone imagine life without Internet? No question about it, it has come to stay and evolve with us with its lights and shadows.