Cybersecurity Attacks on Smart Home During Covid-19 Pandemic.

1st Roberto O. Andrade
Faculty of Informatics
Escuela Politécnica Nacional
Quito, Ecuador
roberto.andrade@epn.edu.ec

2nd Iván Ortiz-Garcés
Universidad de las Américas
Quito, Ecuador
iva.ortiz@udla.edu.ec

3rd María Cazares
IDEIAGEOCA
Universidad Politécnica Salesiana
Quito, Ecuador
mcazares@ups.edu.ec

***Abstract*—COVID-19 has generated that dynamics in the context of cybersecurity change significantly, due to the displacing of activities of organizations in the city to home in telework mode. The cybersecurity architecture at home does not have the same levels of security as in organizations, even more if the house has been developed under a smart infrastructure (smart home) scheme, the cybersecurity attack surface expands. This context could be one of the reasons why the number of attacks has increased significantly to more than 35%. VPN solutions are uses to protect telecommuting communications but security attacks exploit vulnerabilities of home-equipment and people, so VPN solutions could reduce their efficiency. Attackers have focused on social engineering attacks that use the concerns generated by the covid-19 pandemic to be more effective in their attacks. This study presents an analysis of cybersecurity attacks that have appeared during this pandemic and how it forces to change defense strategies in cybersecurity.**

Keywords—smart city, social engineering, cybersecurity, phishing

I. INTRODUCTION

The Internet of Things (IoT) has allowed the development of smart infrastructures to build sustainability and resilience cities. Today some buildings and homes are becoming smarter and more connected. These massive interconnections unlock enormous data-value for consumers, organizations and cities. However, the security risks in smart homes and smart buildings are more relevant due to the changes that the covid-19 pandemic. Smart home's attack surface has grown with the changes on human behavior related with covid-19, loss of sensitive information is not only related with people whom live in the home, also organizational information due to telework. Many of the activities of the city are now support on telework model, so the affectation to technological devices on smart home not only affect the citizen, also can impact the daily activities of the city, reducing their ability to operate normally.

In the context of cybersecurity, attackers seek new ways to affect organizations and people; cybersecurity strategies need to be adapted to the situational context. Globally, the pandemic generated by covid-19 has made changes in daily aspects such as study, work and shopping, and trough technology these activities continue operating from home. However, telecommuting, tele-education and e-commerce has been affected by security attacks. A hospital in the Czech Republic's was forced to deactivate all IT systems and cancel all planned operations for ransomware attack [1]. In other hand, a high school in Boston- Massachusetts report intrusions on on-line class using the teleconferencing software Zoom, the attacker shouted the teacher's home address in the middle of instruction [2].

Cybercriminals try compromise enterprise equipment, but due to the covid-19 pandemic and the remote digitalization of the work force, remote software and digital services have come under target. According Trendmicro, since February to March of year 2020, spam increase in 220 percent and malicious URL in 260 percent. Trendmicro, also shows covid-19-related threats in the first quarter of year 2020 [3]:

- 907K spams messages,
- 737 new malwares,
- 48K malicious URL.

Attackers taken advantage of the pandemic situation to generate attacks based on the curiosity generated in people to understand aspects related to COVID-19. BBC has tracked five of the campaigns [4]:

1. Click here for a cure,
2. Covid-19 tax refund,
3. Little measure that saves,
4. The virus is now airborne,
5. Donate here to help the fight.

Related to the first scope of the campaign, the attackers send messages indicating that they have information related to the development of the vaccine. The second campaign is focused on indicating that there is a tax refund. The third campaign attackers use names of organizations known as the World Health Organization, stating that it contains useful information related to managing the pandemic. The fourth campaign focuses on indicating that data is required to manage the pandemic. Finally, the latest campaign focuses on indicating that donations are needed to fight the pandemic.

In this work is our interest analyze cybersecurity aspects related to vector attacks mainly those that are focused on smart home and social engineering that have been taken more relevance during the time of the covid-19 pandemic. For this purpose, this paper seeks to identify cybersecurity attacks that have arisen during the covid-19 pandemic or the modification that existing attacks have had. Understand the vulnerabilities and aspects that are considered by cybercriminals during the pandemic that have allowed the increase in security attacks. Finally, analyze the possible lines of action that could be used to reduce the impact of the attacks.

The rest of the paper is organized as follows. Section II identify the most relevant threats that have been identified by

security firms during the covid-19 pandemic. Section III analyze the vulnerabilities from the context of the people that have allowed the increase in cyber-attacks. Section IV analyzes characteristics of cybersecurity mechanisms in homes to support tele-work. Section V shows cyber-security incident response to phishing attacks during covid-19 pandemic. Finally, section V shows conclusions related to the cybersecurity aspects that must be considered to face the changes due to covid-19 pandemic.

II. COVID-19 RELATED SECURITY THREATS

According to several cybersecurity firms worldwide have determined attacks that have existed during the covid-19 pandemic, they agree that the number of attacks has increased considerably, and the movement of work activities to home has increased attacks by 35%. Smart homes designs could increase the attack surface, which allow that the number of attacks increase more.

Attackers have used as a strategy offer applications that provide real-time coronavirus outbreak such as coronavirus-map, but really they try to gain administrative access to install malicious code on people's computers.

Using phishing techniques attackers stealing valuable data, such as usernames and passwords, credit card information, and other personal information. In the context of the covid19 pandemic attackers looks for impression of authenticity to appear to come from a trustworthy source such as the World Health Organization (WHO). Phishing technique uses three vectors of attacks web-pages, email and SMS.

Attackers in web-phishing use URL-personalization through of include words related with covid or coronavirus, such as the following URLs:

- covid19mobile.app
- covid19-stats.co.za
- coronavirusnotalone.com
- sars-cov2numbers.com
- limpiezascovid.com
- coronademic.net
- coronavirusalerts.com
- coronavirus.technology
- coronavirusmedicine.com
- covidrule.com

The domain-tools [5] portal has a record of 162,364 malicious URLs with word related to the covid-19 pandemic since January to May of year 2020, while security enterprise firm PaloAlto says the increase of malicious URL are 1,300 domains every day [6]. Figures 1 and 2 show websites with fake news and antivirus to cheat people when found covid-19 information.

Fig. 1. Websites with fake news.

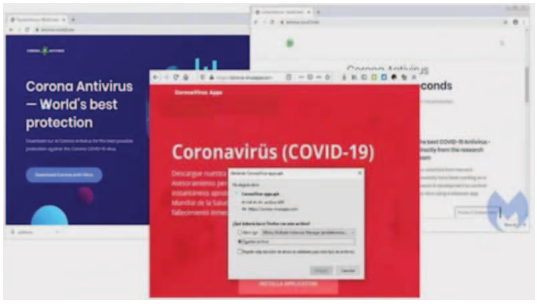

Fig. 2. Websites with fake antivirus.

In this paper, we carried out a qualitative analysis of 146,000 records associated with malicious URLs using a text mining tool (see, Figure 3), although the predominant word is covid19 or coronavirus, attackers also use words associated with events that occur during the covid-19 pandemic such as people searching for return flights to home or those looking for a relationship. From the analysis we found words in the malicious URLs such as:

- Flight,
- Love,
- Support,
- Stories,
- Guru, and
- Passports.

This can be challenging for security analysts if they want to implement the use of machine learning tools to detect malicious sites if they only consider covid or cornonavirus as training data. Is necessary to understand, like the attackers do, the personal needs that this covid-19 pandemic is generating.

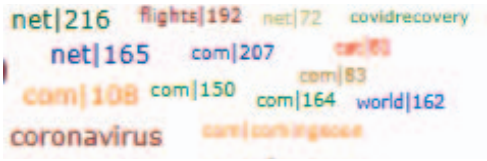

Fig. 3. Extract of text data mining of malicious URLs.

Attackers try to get that victims open emails and download malicious code clicking on them. Attackers in email-phishing use words relate with covid19-pandemic such as: vaccine-trials or free tests for covid19. To be more effective, attackers use in the email-subject names of recognized organizations in the field of health such as WHO or government agencies such as us.gov [7]. Figure 3 shows an extract of phishing email that pretend indicate how protect friends from covid-19.

Spam attacks use delivery notification email indicate that the package cannot be delivered due to the pandemic (see, figure 4 and 5), so the recipient must go to the warehouse and pick it up in person; the attacker requests personal information stating it is necessary for delivery. Attackers, sometimes insert images of documents in a message to add credibility

Fig. 4. Extract from phishing email.

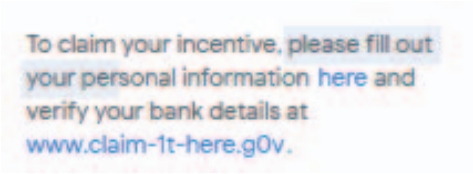

Fig. 5. Extract of email spam related with pick-up delivery.

Google, says that blocks more than 100 million emails with phishing every day, Gmail has detected 18 million emails a day related to the Covid-19 pandemic [8]. Another spam attack uses the strategy of offering free Netflix accounts during the pandemic. Figure 6 shows an example of spam using Netflix context.

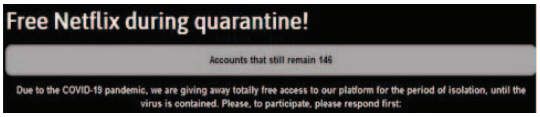

Fig. 6. Extract of spam related witd free Netflix.

SMS phishing including government payments and tax rebate as part of the lure. WhatsApp has been used to carry out phishing campaigns focused on aids from supermarkets related to the delivery of products. The characteristics of this type of message is that they are short and use a hidden link to redirect to another site (see, figure 7).

Fig. 7. Extract of spam using WhatsApp related with products services.

Phishing attacks are in different languages: English, Spanish, French, Italian, among others. Some relevant information about phishing during covid19- pandemic are the following [9]:

- $17,700 is lost every minute due to phishing attacks
- Data breaches cost enterprises an average of $3.92 million
- Phishing attacks account for more than 80% of reported security incidents
- 94% of malware is delivered by email

Scammers, use phone or email phishing techniques to try and obtain personal data [10], Table I shows a summarizes of spam attacks.

TABLE I. SUMMARIZES THE TARGET OF SPAM ATTACKS RELATED TO COVID-19.

Vector attack	Domain Target
SPAM	• Covid-19 treatment, • Delivery products, • Teleconferencing logins. • Products offer.

.

The covid-19 pandemic generates a confinement in people's homes. Cities together with companies, have chosen to maintain their operations through telework. Access to corporate services from home in secure way requires VPN, several organizations have robust business solutions to implement this VPN mechanism at home. However, this option is not generalized in all companies and sometimes people should look for VPN solutions and downloaded without validation. “VPN Proton” for example is a solution used by several people, but again this need in the period of the covid-19 pandemic is used by attackers, who generated a fake “VPN Proton” and included a malware called AzorUlt. AzorUlt malware is a variant of “corona.exe”, an Trojan focus on steals information.

Video-teleconferencing platforms allow to stay connected in the COVID-19 pandemic. However, attackers try use these platforms to do cybersecurity attacks. Zoom-bombing is a worldwide attack that occurs when a conference call is hi-jacked to share offensive images, post hate speech or otherwise behave offensively in the conference call [11]. Zoom-bombing has the potential of compromise systems and generate lack of privacy. Zoom-bombing not only affected educational institutions, US government entities mentioned that they were victims of attacks during meetings. Attackers have taken advantage of the increased in the use of video conferencing tools for teleworking or tele-education, to send malicious emails using references of video conferencing tools such as “zoom-us-zoom_##########.exe” and “microsoft-teams_V#mu#D_##########.exe”.

Table II, summarize the types of attacks that have arisen or have modified their attack strategy during the context of the covid-19 pandemic.

TABLE II. ATTACKS DURING COVID-19 PANDEMIC

Attacks	Description of attacks
Phishing	• 2020 Coronavirus Updates, • Coronavirus Updates, • 2019-nCov: New confirmed cases in your, • 2019-nCov: Coronavirus outbreak in your city (Emergency).
Malware	• BabyShark • Mirai • Rammit • Matsnu • Necurs • Pizd • Simda • DirCrypt • Suppobox • Banjori
Ramsom ware	• CovidLock • Netwalker
Online meeting hijacking	Zoom-bombing
Fake apps	Fake coronavirus maps

III. PSYCHOLOGICAL IMPACT AND BEHAVIORS IN TIMES OF PANDEMIC

The responses or coping that the population has been adopting during the covid-19 pandemic are linked to cultural scripts, which determine the behaviors that will be accepted or rejected by society. They impulse the degree of social control, based on social rules that manage our feelings of fear, uncertainty and anxiety, as well as the scope, direction and duration of these feelings. People try found information related with guidelines for drive their emotions and behaviors to face the pandemic.

Results of one investigation archived in Spain show that people during covid-19 quarantine, look for topics related to health, labor or business regulations [13]. We can contrast with google search reports during the quarantine period (See figure 8 and 9). The most query search was the term "coronavirus".

Fig. 8. Google search during quarantine.

Fig. 9. Google post quarantine search.

People face the consequences of covid-19 pandemic building networks that connected to each other. Although in quarantine or confinement several measures were adopted around the world causing breakdown of daily life, and changing the way we make social connections. People seek means to connect emotionally with others, specialy who are significant in their lives, to share experiences, or create solutions to face negative problems and feelings caused by the covid-19 pandemic. People try in the networks they built change the moods, and develop a vision of hope for the future.

At the individual level, social isolation allows moments of introspective reflection, and the evaluation about oneself and the society. On the other hand, at the cognitive level it promotes predictive thinking to anticipate problems, and planning strategies to achieve a new balance due to limitations or uncertainty products of covid-19 pandemic. This process of adaptation to the new normality generates an interest of learning about habits that were part of the daily routine and that people does automatically. So, people now seek every day for information related to new habits, and new behaviors.

Additionally, sometime the communication failures and little credibility of the information that is transmitted in official media, awaken the innate curiosity of our thinking, leading to people a need to access more information from all possible sources without checking its veracity. In this way, people try satisfied their desire to know the health situation of the country and the world related with covid-19 pandemic.

IV. SMART HOME ARCHITECTURE FOR TELEWORK

The smart home architecture is built with sensors, actuators and controllers that allow the generation of intelligence based on data. However, generally the security architecture maintains the elements of traditional houses, in which the router by service provider (ISP) distributes the network services in the house, is not common to have a perimeter security firewall, intrusion prevention system (IPS) or web filter-spam (see, figure 10).

Fig. 10. Extract of spam using WhatsApp related with products services.

Teleworker uses VPN to connect remotely to enterprises-services, however this mechanism protects the confidentiality of the information that is transmitted between the home and the enterprise; in case the attacker accesses to home-computer resources, sensitive information of the people at home could be exposed, but also the sensitive information of the

enterprise. Employers and colleagues clicking on malicious URLs increases the cyber-security risks. Attackers spreading misinformation online through spoofed emails and social media. People is concerned about covid-19, so they are less likely to follow security procedures of security training and will be more likely click a link on web-page or phishing email to learn more about the virus.

V. CYBER KILL CHAIN OF SPEAR-PHISHING

We propose in this study, to understand the effective of cyber-attacks during covid-19 pandemic analyzed cyber kill chain (See, figure 11).

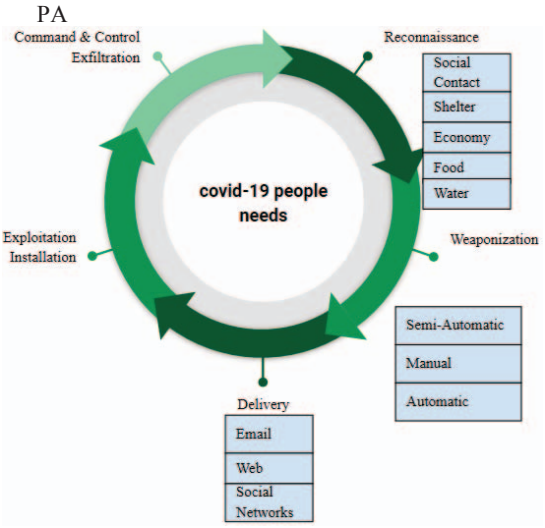

Fig. 11. Cyber kill chain for covid-19 spear-phishing

Reconnaissance: attacker seeks relevant information from the target to get their attention. During Scovid-19 attackers know the interests of most people due to changes in daily habits such as tele-work or the buy of food using online methods. There are needs required by people. Maslow's pyramid has proposed a classification of needs and we show in Figure 9 those that have taken greater relevance during the covid-19 pandemic. This needs can be exploited by attackers in the reconnaissance phase.

Weaponization; attacker determines the attack surface in the smart home / home domain. The best known cyber weapons are: Botnet, DoS and Malware. The architecture of the home design network varies is basic and does not have the security layers that are established in enterprises; in houses is not common to find perimeter security devices such as firewalls, intrusion prevention sensors (IPS) or anti-spam. This scenario allows attackers to develop weapons that do not have great complexity or it requires a long deployment time (See, figure 12).

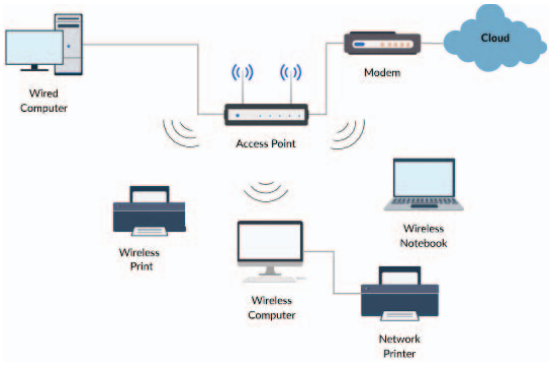

Fig. 12. Common network architecture in home.

Delivery: attacker deliver the attack. In the case spear-phishing the goal is send attachments with an access link that impersonate a legitimate url.

Exploitation: In this phase the attacker gains access and starts executing arbitrary source code where the attacker can access the operating system.

Installation: in this phase the attacker generates remote access or leaves a backdoor on the victim's computer, generating persistence at the system level (root kit, remote access trojan -RAT), at network level (through the acquisition of credentials).

Command & Control: in this phase the attackers have already generated the mechanism to have direct communication with the victim by sending commands, the main objective by attacker is not be detected.

Exfiltration: may be focused on exfiltration of sensitive information, denial of services or destruction.

VI. CASE STUDY OF CYBER-INCIDENT RESPONSE IN COVID-19 PANDEMIC

A spear-phishing attack came to the organization with the following URL: https://mail-xxxxx.000webhostapp.com/. This URL generates a web phishing where it indicates the organization's email as can be seen in the Figure 13.

Fig. 13. Fake Login Email Screen

Next step is validate the url domain and all ips addresses that were related to this attack to obtain network segments that are causing this type of attack: 145.14.X.X -173.255.X.X - 173.255.X.X, and then blocked for new attacks. Figure 14 shows detection of ip addresss from attacks sources.

Fig. 14. Geographic location of attacks source.

This solution is optimal if the staff only works within the organization, as we are experiencing this pandemic with the covid-19, the cyber-attacks increased and the coverage is no longer within the organization. This context increases the complexity and time to resolve the cyber-incident. Next, we need the support for National CERT to block attacker´s address for all national territory because is no possible configure a rule in perimeter security equipment, and then notify to specialized portals (See, Figure 11 y 12).

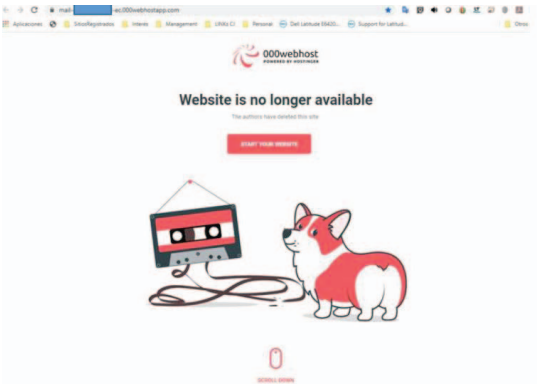

Fig. 15. Fake web page after blocking process.

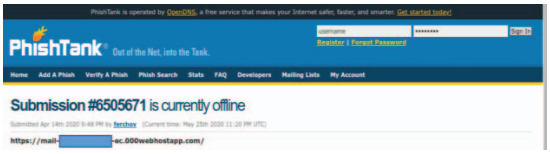

Fig. 16. Subission for blocking process of fake web page.

VII. CONCLUSIONS

Cyber-attackers are taking advantage of the move to telework exploiting a variety of publicly known vulnerabilities in VPNs and other remote working tools. Additionally, attackers exploit psychological aspects of people related with covid-19 pandemic.

The curiosity and concern of people to learn about the covid-19, has been used by cyber attackers to generate attacks that use aspects related to the covid-19 pandemic such as treatment, vaccines, methods of protection, among others. By displacing access to business services to the home and the high exploitation of social engineering techniques based on the generation of false news or misinformation related to the covid-19, opening a gap that can be exploited by attackers to steal sensitive information of people and organizations.

Cybersecurity culture is essential to minimize the potential impact of cyber-attacks, but is important to understand that attackers approach for human factors such as fear, curiosity, or anxiety. From the psychological context, there is a relationship between emotions and logical thinking controlled by the prefrontal cortex and the amygdala; in situations of uncertainty with levels of anxiety, people could not choose the most logical or safe decision (for instance, open an email with malicious content). Another relevant human aspect is risk perception, if the person considers that they will don't receive a malicious email that uses the identity of an organization or authority, their sense of protection will be minimal, even they know about the existence of cyber-threats. There are cognitive procedural processes that are automatically trigger based on risk stimuli that are controlled by the amygdala; if the perception of risk is low, the decision is more likely to be made from a more emotional perspective (amygdala) than logic perspective (pre-frontal cortex). In this context, cybersecurity strategy enhanced the digital culture of people, but also consider aspects of decision-making in environments of uncertainty.

Covid-19 pandemic generates a rethinking of the approach to security strategies. Organizational infrastructures designed with layers of security are challenged to leave centralized designs and look for distributed cyber-security approaches. The telework and tele-education will be means of operation in cities for a long time and is not always feasible to invest in sophisticated security solutions at home, so is necessary to take advantage of the opportunities of data-based decision-making and predictive projection techniques to be brought home at a low cost.

REFERENCES

[1] Scmagazineuk.com. 2020. Coronavirus Test Results Delayed By Cyber-Attack On Czech Hospital. [online] Available at: <https://www.scmagazineuk.com/coronavirus-test-results-delayed-cyber-attack-czech-hospital/article/1677194> [Accessed 26 May 2020].

[2] Boston.com. 2020. Massachusetts Schools, Churches Have Been Targeted By Hackers On Zoom | Boston.Com. [online] Available at: <https://www.boston.com/news/local-news/2020/04/07/massachusetts-schools-churches-zoom-hackers> [Accessed 26 May 2020].

[3] Trendmicro.com. 2020. Developing Story: COVID-19 Used In Malicious Campaigns - Security News - Trend Micro GB. [online] Available at: <https://www.trendmicro.com/vinfo/gb/security/news/cybercrime-and-digital-threats/coronavirus-used-in-spam-malware-file-names-and-malicious-domains> [Accessed 26 May 2020].

[4] BBC News. 2020. How Hackers Are Preying On Coronavirus Fears. [online] Available at: <https://www.bbc.com/news/technology-51838468> [Accessed 26 May 2020].

[5] Domaintools. 2020. [online] Available at: <https://www.domaintools.com/resources/blog/free-covid-19-threat-list-domain-risk-assessments-for-coronavirus-threats> [Accessed 26 May 2020].

[6] Szurdi, J., Chen, Z., Starov, O., McCabe, A. and Duan, R., 2020. Studying How Cybercriminals Prey On The COVID-19 Pandemic.

[online] Unit42. Available at: <https://unit42.paloaltonetworks.com/how-cybercriminals-prey-on-the-covid-19-pandemic/> [Accessed 26 May 2020].

[7] US-CERT. 2020. [online] Available at: <https://www.us-cert.gov/ncas/alerts/aa20-099a> [Accessed 26 May 2020].

[8] europapress.es. 2020. Gmail Bloquea 18 Millones De Correos Maliciosos Al Día Relacionados Con El Coronavirus En La Última Semana. [online] Available at: <https://www.europapress.es/portaltic/ciberseguridad/noticia-gmail-bloquea-18-millones-correos-maliciosos-dia-relacionados-coronavirus-ultima-semana-20200417110637.html> [Accessed 26 May 2020].

[9] Infosecurity-magazine, 2020. Cybercrime Costs Global Economy $2.9M Per Minute. [online] Infosecurity Magazine. Available at: <https://www.infosecurity-magazine.com/news/cybercrime-costs-global-economy/> [Accessed 26 May 2020].

[10] Terranova Security. 2020. Protect Yourself From COVID-19 Cyber Scams | Terranova Security. [online] Available at: <https://terranovasecurity.com/protect-yourself-from-covid-19-cyber-scams/> [Accessed 26 May 2020].

[11] Fbi.gov. 2020. FBI Warns Of Teleconferencing And Online Classroom Hijacking During COVID-19 Pandemic — FBI. [online] Available at: <https://www.fbi.gov/contact-us/field-offices/boston/news/press-releases/fbi-warns-of-teleconferencing-and-online-classroom-hijacking-during-covid-19-pandemic> [Accessed 26 May 2020].

[12] Bill Durodié. 2020. Handling Uncertainty and Ambiguity in the COVID-19 Pandemic [online] Available at: <https://doi.apa.org/fulltext/2020-37336-001.html> [Accessed 26 May 2020].

[13] Nekane Balluerka Lasa. 2020. Las Consecuencias psicológicas del covid 19 y el confinamiento | [online] Available at: <https://www.ub.edu/web/ub/ca/menu_eines/noticies/docs/Consecuencias_psicologicas_COVID-19.pdf> [Accessed 26 May 2020].