Security Council

Topic B: Addressing Phishing in Social Media

President: Mia Peña
Moderator: Ana Daniela Cortazar Rojas
Official Assistant: Karla Alejandra Santiago Pliego

Introduction to the Committee

The Security Council is one of the six main organs that form the United Nations. It has 15 members whose main objective is to preserve peace and security worldwide without using violence. Its responsibility is to determine when and where the United Nations peace operation can be deployed. To achieve peace, the Security Council members can dispute and recommend agreements or actions that prevent or eradicate threats to international peace. The council is formed by 15 States: the G5 permanent members, China, France, the Russian Federation, the United Kingdom and the United States of America, which all have veto power; and 10 nonpermanent members (United Nations Security Council, n.d.). This year's nonpermanent members are: Estonia, India, Ireland, Kenya, Mexico, Niger, Norway, Saint Vincent and the Grenadines, Tunisia, and Viet Nam.

Introduction to the Topic

Cybercriminals use cyberattacks to steal data or to damage other computer networks, a technique consisting of using different computers or systems against one or others. A derivative of the last is cyberterrorism, which, as its name states, is a type of terrorism that has the objective to provoke fear, incite armed groups' acts, and intimidate others through the use of data processing machines and information technology. These acts can be considered as propaganda, funding, and in some cases planning of radical attacks (UNODC, 2012, pg. 3). At the same time, this can be related to phishing, a type of social engineering attack that scams people by making them believe they are contacting someone else and then stealing their information. Likewise, social engineering attacks are those that use psychological manipulation tricks to engage a target and make them give away sensitive information; they rely on human mistakes rather than in detecting the vulnerabilities in a system. Besides phishing, other types of social engineering attacks are the following:

- Baiting: Similarly as phishing, baiting benefits from human curiosity or greed. The hacker promises an item, good, or service to the victim in exchange for some information or download of a malware-infected application (Nadeem, 2020).
- Scareware: This tactic uses fear to manipulate the user through a series of false alarms and fictitious threats, claiming that the files on their computer are infected and offering them a fake antivirus that is actually malicious software designed to steal personal data (Kaspersky, 2021).
- Pretexting: Here, hackers research their victims before contacting them, then use the information to start a conversation and blackmail them by divulging sensitive information regarding the victim’s personal and professional life (Gendre, 2020).

It is this way, cyberterrorism and phishing are both types of cyberattacks since their main objective is to steal or damage others through social media or the internet, mostly to steal funds and data. In some cases, these can be used, as said above, to promote armed groups’ propaganda or to make outsiders do things against their will. Terrorism financing is the act of funding an armed group’s acts. In most cases, the resources that pay for these acts come from money laundering or similar illicit acts. These illicit acts can affect people through frauds or by attacking real foundations by hacking their data through phishing. The following list explains some types of phishing:

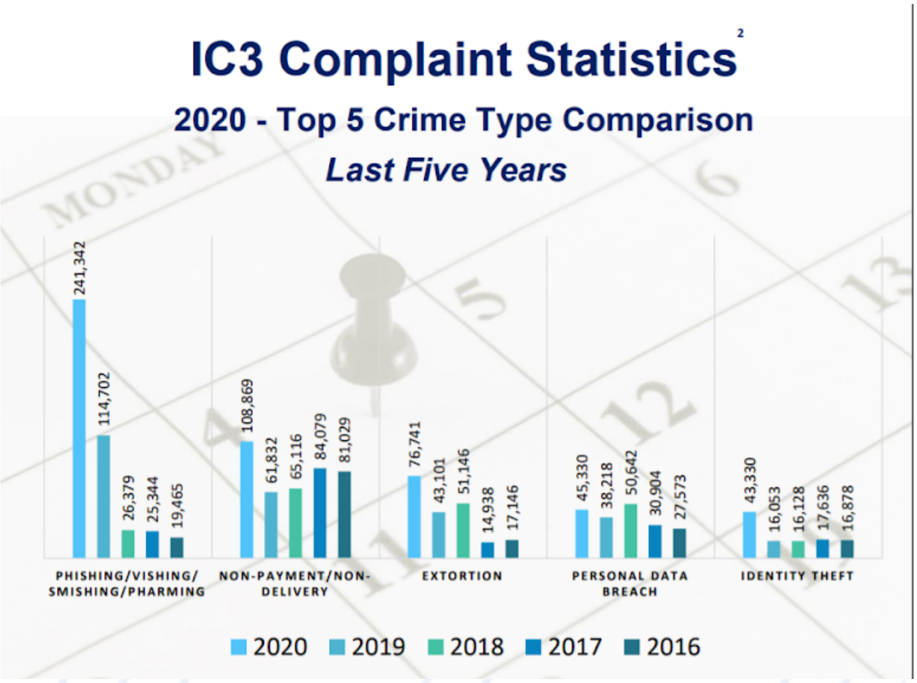
Business Email Compromise (BEC): Also known as email account compromise (EAC), BEC scams consist of sending an email message from a supposedly known source. Most of the time they are designed to pretend to be senior executives or employees and trick other workers, customers, or vendors into transferring payment for items or services to alternate bank accounts. They are one of the most financially damaging cybercrimes.

- Spear phishing: This is the tactic that some people use to involve others through social media, emails, or any other thing that makes the other person give personal information. It can cause financial and data loss (Joque, 2018).
- Whaling: This is a technique used through social media, email, or any other media to make the victim do a secondary action, like transfer funds (National Cyber Security Center, 2020).
- Smishing (SMS-phishing): Messages are the main tool used for smishing; their main point is to spread malware through texts.
- Vishing: This is the combination between voice and phishing; it consists of pretending to be someone else in order to steal financial data.
- Email phishing/spam: This is used to steal sensitive information through emails, sending advertisements.
- Ransomware: It is a type of malware. A malware is a software designed to harm or attack devices, programs, etc. These attack phones or computers, making them fail and freeze. Their objective is to make the other person pay a ransom to free the device.
- Malvertising: This tactic involves malware through online advertisements, usually sent by email, that take advantage of different online patterns (Forcepoint, 2021).

These types of phishing attacks are possible attempts to steal data, funds, devices, or to hack any software to launch another attack (Tunggai, 2021). Any cyber incident can disrupt individually owned devices, transportation, power, and other critical services for the correct function of society's infrastructure. Besides, phishing attacks are easier to carry out successfully because hackers do not precisely break into a system; they just need to send an email and wait for the person to open it. As Joe Ferrara (2018), general manager of Security Awareness Training for Proofpoint, said "email is the top cyberattack vector, and today's cybercriminals are persistently targeting high-value individuals who have privileged access or handle sensitive data within an organization".

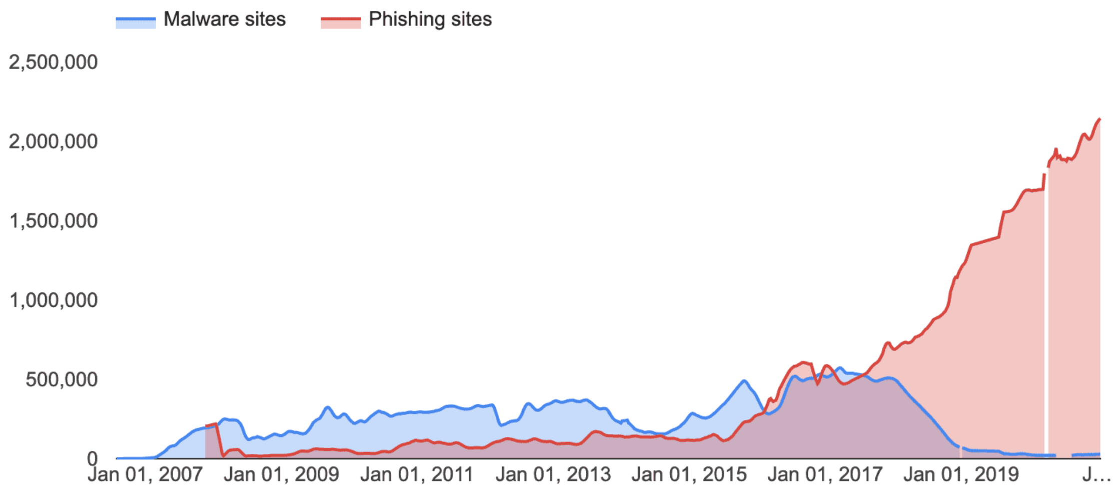
Cyberattacks have been a problem since technology started to become a part of daily life. Over time, there were many other technological advances and with this, more attacks were presented, such as the case of Hilary Clinton and her campaign. Everyday people are more prone to be victims of these crimes. This can be seen in the 2020 Internet Crime Report released by the FBI's Internet Crime Complaint Center (IC3), which established that in 2018 only 26,379 incidents of that type were counted; the next year, there were 114,702; and in 2020, over 240,000 phishing scams were reported, which produced adjusted losses of more than $54 million dollars. Phishing scams were the type of cybercrime with more victims in all the year, mostly because cybercriminals have taken advantage of the new dependence on technology that developed over the COVID-19 pandemic.

The IC3 received more than 28,500 complaints regarding COVID-19 topics, such as scams asking people to pay for the vaccine, be put on a waiting list, or obtain early access. These scams appeared on social media platforms, email, calls, and unknown websites (Internet Crime Complaint Center, 2021).



Number of victims per top 5 cybercrimes from 2016 to 2020
(Internet Crime Complaint Center, 2020)

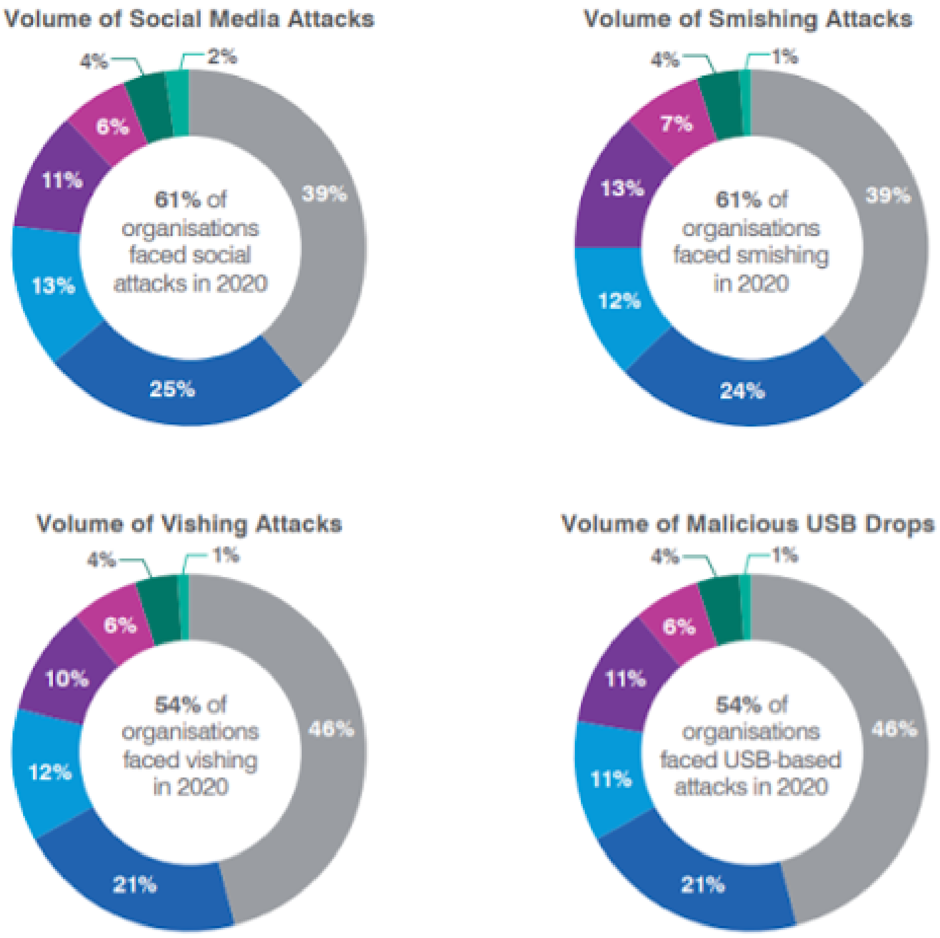
Similarly, phishing sites are increasing. For instance, on January 17, 2021, Google registered 2,145,013 phishing sites around the world wide web, while on January 19, 2020, the number of websites was about 1,690,000.



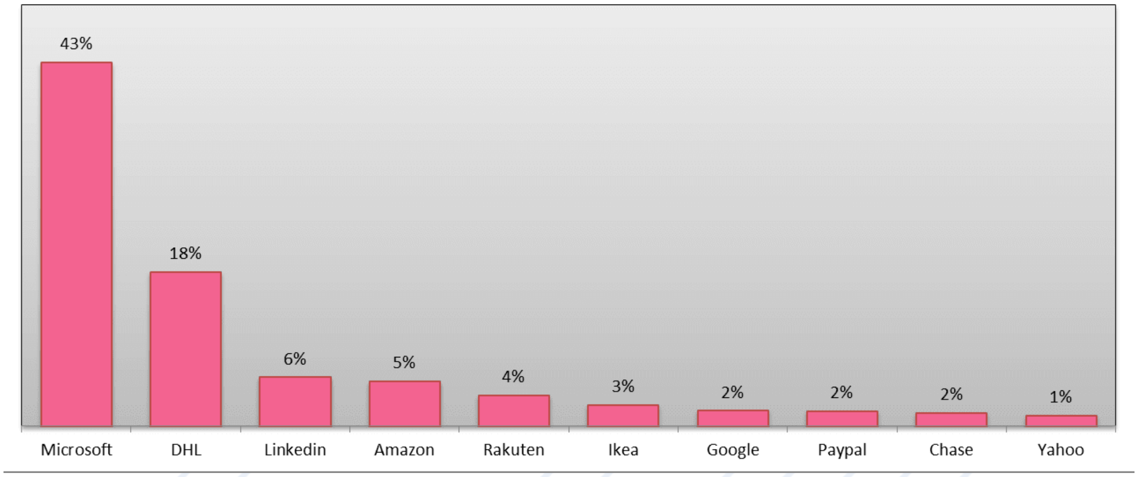
Number of websites deemed unsafe between January 2016 and January 2021 (Google Safe Browsing, n.d.)

Phishing attacks are becoming more frequent, sophisticated, and harder to detect; in 2020 more than 75% of organizations around the world suffered phishing attacks, and just in the United States, 74% of the companies faced a successful phishing attack. Mostly, all those incidents occurred through emails, especially due to the use of popular platforms, such as Twitter, Amazon, Zoom, Google, or Apple in the subject line to attract the victim and make employees open the links, unwittingly giving up personal and corporate information (Bay, 2021).

Sometimes scammers can create fake login pages to persuade users to insert their legitimate identifications. As a result, the scams can compromise personal data (name, address, email), credentials (passwords, usernames, PINs), and medical information (insurance claims, treatment information). Besides, they can have serious consequences for corporations; for example, they can cause the loss of data and compromise the enterprise's accounts, experience financial losses, and even infect their digital infrastructure with ransomware or malware (Rosenthal, 2021).



Percentage of different cyberattacks (successful and unsuccessful) in 2020 (Proofpoint.com, 2021)



Top brands used in brand phishing attempts in the Q4 2020
(Check Point, 2021)

The pandemic completely changed the way cybercriminals execute their attacks. Phishing and business email compromise are one of the greatest cyber threats since they are difficult to identify with a traditional security solution, meaning new methods must be employed. However, not even the most sophisticated technologies can completely block all cyberattacks. Phishing awareness training can reduce the probability of social engineering attacks; all citizens need to understand the characteristics and tactics commonly used by cybercriminals and learn when it is safe to share or receive data.

Historical Background

On October 29, 1969, the first computer message was delivered from a device located in a research lab at UCLA to a second computer at Stanford, each the size of a small house, through “node to node” communication. It wasn’t until 1983, however, that researchers began to assemble the “network of networks” that is what nowadays is now known as the modern internet. Later on, in 1990 computer scientist, Tim Berners-Lee, invented the World Wide Web, which is the most common means of accessing data online and became the tool that helped popularize the internet. On the other hand, the personal computer industry truly began in 1974, making it more accessible for people to have their computers at home.

After the popularization of the internet, little by little, people's personal information started being exposed. In 1996, the term phishing was first used after hackers stole America Online accounts and passwords. According to Kay (2004), this term was used referring to an analogy between Internet Scammers using e-mail lures and setting out hooks to "fish" for passwords and financial data from the "sea" of Internet users.

America Online (AOL), first named Quantum, was a company created on May 24, 1985. By 1993, AOL introduced its own email addresses, a Windows version, and access to the rest of the Internet for its users. The number of customers the company had drastically increased. becoming the number one provider of internet access in America. Consequently, due to the millions of users AOL had, phishing attackers found their main target. AOHell, invented in 1994, a credit card number generator for AOL users, was the first hacking program used for phishing, which allowed "phishers" to occasionally hit a correct credit card number they could steal from. America Online received multiple complaints and in 1995, the company applied security measures to stop the random generation of credit card numbers. After these measures were taken, phishers found new ways to steal people's information; using messenger and email systems, they pretended to be AOL employees asking users to confirm their billing information. Since phishing was a relatively new problem, people usually just gave them their information without questioning.

Phishers continued attacking through different means. In May 2000, a worldwide phishing attack generated chaos among web users. It was caused by a virus nicknamed “The Love Bug”, which was sent to people by email. Users received an email titled: “ILOVEYOU” with the text body “Kindly check the attached love letter from me!”. After the user clicked the link, the computer became infected with the virus. “It’s a very effective virus. It’s one of the most aggressive and nastiest I’ve ever seen”, said Kieran Fitzsimmons (2000) of MessageLabs, which screens millions of company emails for viruses. “It manifests itself almost everywhere in the computer”. To that day, “The Love Bug” was the most dangerous and fastest virus ever created; after the user’s computer became infected, the email forwarded itself to every contact in the computer.

However, in 2001, scammers saw a new opportunity for phishing attacks in the recently created online payment systems. The first incident registered to target a financial institution took place in June 2001, to E-Gold. E-Gold was one of the first successful digital gold currency systems that allowed customers to open an account with gold or other precious materials and to make transactions with other E-Gold accounts. Because of their early success, the cryptocurrency store was a target of financial malware and phishing attacks performed by criminal syndicates in Eastern Europe (Dixon, 2013). Although most of the attempts were unsuccessful, with each of them hackers refined the technique to use it against other financial institutions.

In 2003, the first fake banking sites appeared: dozens of domains that looked like legitimate sites such as eBay and PayPal. On November 17, 2003, eBay clients received email worm programs that sent them to pages that looked just like eBay’s home page and made them register to provide their credit card data, ATM personal identification numbers, Social Security number, and date of birth. Months later, the Federal Trade Commission informed that 9.9 million

US residents had been victims of identity theft, and financial institutions reported losses of $48 billion and consumers $5 billion in non-remunerated business expenses (Kay, 2004).

By the beginning of 2004, the outbreaks were very successful, including the ones targeting banking sites. As a result, organizations were losing nearly $2 billion per year. On September 14, 2007, the online broker for online stock trading, TD Ameritrade, was a victim of a data breach using investment-themed phishing emails. Although the attackers had access to 6.3 million customer account records, they were not able to steal sensitive data like security numbers. Because of that, no identity theft was reported; users just received spam emails. The FBI and US financial regulators investigated the case but they never found the perpetrator (Carnegie Endowment for International Peace and BAE Systems, n.d.).

On the other hand, one of the largest phishing investigations carried out by the United States was Operation Phish Phry. It began in 2007 when the Federal Bureau of Investigation (FBI) allied with financial institutions to identify and take down criminal networks and enterprises targeting financial infrastructure in the US. Eventually, Egyptian authorities joined the operation after investigators from both nations discovered an international conspiracy allegedly operating a phishing scheme that targeted American-based institutions and victimized hundreds of account holders by stealing their financial data to transfer about $1.5 million to bogus accounts they controlled. The process lasted two years, until, in 2009, more than 50 US citizens and around 50 Egyptian inhabitants were accused of computer fraud, aggravated identity theft, conspiracy to commit bank fraud, and money laundering (Federal Bureau of Investigation, 2009; McGlasson, 2009).

Current Relevance

Throughout the years, social media has become more and more popular, making it an ideal target for phishers. Phishing in social networks is a fraud that happens when a user receives an interesting invitation that leads to a link with a virus or in which they must provide personal information. People use Instagram, Twitter, WhatsApp, and many other platforms to keep up with friends and family, stay informed of the latest news, and even buy different products. At the same time, businesses and online stores also use social media to keep their customers updated about their latest products and event offerings, marketing, and attract new business. As a result, diverse actors use social media as a platform to launch their phishing networks. Modern phishing tools, like Hidden Eye or Shell Phish, make these phishing attacks as easy as pressing a couple of buttons in an app. Information collected by hackers includes social media account login credentials, credit card information, and personal data.

While initially, human beings used the internet as a formal communication tool, it has turned into an international platform where people develop and cultivate their relationships. While most of the initial research in this field concluded with the internet mostly having negative impacts on social life and well-being, the recent study of Catellacci "Internet use and well-being: A survey and theoretical framework" focused on social networking sites, like Facebook and Instagram, and found out that users have increased social capital, social support, sense of community, and improved well-being.

Cases. Marketing teams monitor social media to protect their brand and communicate; they are not equipped to handle the increasingly frequent advances in social networks since more discoveries in the technological field every day. It is a burdensome and complex task to keep track of each one of them. Email security faces problems due to the absence of social engineering-based attacks and so do the tools commonly used to monitor social media. That is why many companies could not stop attacks that were made in the past 12 years.

Cryptolocker ransomware. In 2013, the Cryptolocker ransomware event occurred, which had a significant impact on people since the way they attacked was innovative. The perpetrator used a virus that attacked Microsoft Windows computers. According to the SecureWorks CTU security intelligence research team, the new ransomware malware named Cryptolocker was first published on the internet on September 5, 2013. This virus was spread through files by emails containing viruses; when activated, the malware encrypted on local network drives with certain types of files and mounted using RSA public-key cryptography.

Google and Facebook payment scam. Between 2013 and 2015, one of the biggest electronic scams happened when some people managed to trick Google and Facebook into paying tens of millions of dollars in fraudulent invoices. They managed to steal over $100 million from Facebook and Google by sending phishing emails to employees through fake email accounts from a ghost business. The Justice Department alleged that Evaldas Rimasauskas and other anonymous conspirators posed as Taiwan-based hardware maker, Quanta Computer, and created Latvia.

Both fake technology companies did business, which used many forged invoices, contracts, letters, corporate stamps, and the general confusion created by the corporate to open and control various bank accounts. The scam involved the employees who “regularly conducted multimillion-dollar transactions” and tricked them into carrying out payments that were transferred to bank accounts controlled by Rimasauskas, which subsequently divided the economic resources into other bank accounts in Latvia, Cyprus, Slovakia, Lithuania, Hungary, and Hong Kong. Investigators found one person that led the scam, Evaldas Rimašauskas, a 50-year-old man who was extradited to New York in 2017 who pleaded guilty to one count of wire fraud and agreed to pay $ 49.7 million (Huddleston, 2019).

This type of scam, which has become more prevalent in recent years, can affect companies large and small worldwide. Experts suggest that any employee who makes a payment to an external company first calls the company directly to confirm the validity of the invoice sent by email and confirm the bank details. Once the funds have been dispatched, they should also contact them by phone one more time to ensure they were received.

Crelan Bank CEO fraud attack. In 2016, the Belgian bank Crelan became a victim of scammers. According to a statement published by the Dutch bank on January 16 of the same year, the bank lost more than 70 million euros after foreigners perpetrated the theft; this was discovered in an internal audit. In order to prevent this from happening again, the bank established additional security measures. At the same time, the Belgian authorities were immediately informed of the matter, including the bank’s risk and audit committees. “Thanks to the reserves accumulated in the past, Crelan can bear this loss without consequences for the bank’s customers and partners”, said Luc Versele (2016), the bank’s chief executive. According to the Belgian newspaper Het Nieuwsblad, the bank was the victim of the so-called CEO fraud or BEC-Business Email Compromise scam.

In these attacks, scammers generally manage to compromise the CEO or other senior manager’s email account. They tend to impersonate them by creating a convincingly similar email account and sending an email to someone in the finance department, ordering a payment to be made to a bank account owned by the scammers.

Hillary Clinton's campaign attack. Through the use of phishing emails, Russian hackers were able to infiltrate into the personal gmail account of Clinton's campaign chairman, John Podesta, in March 2016. The scammers sent spear-phishing emails to the people who worked with her and to some senior Democratic staffers to steal the login credentials for their email accounts; whoever opened the files was directed to a website operated by a Russian Intelligence organization. Podesta was one of the victims who accidentally handed over the information. Because of that, hackers had access to the data stored there and stole over 50,000 emails, which were later exposed on the website WikiLeaks (Gilbert, 2016).

Cryptocurrency phishing sites. Phishing attacks and ransom demands have long plagued the bitcoin and cryptocurrency world. From June 2017 to 2020, two Russian hackers, Danil Potekhin and Dmitrii Karasavidi, coordinated a phishing operation that consisted of creating fake websites for the Poloniex, Gemini, and Binance cryptocurrency exchanges to steal their account credentials and the Bitcoin (BTC) and Ether (ETH) crypto assets. They managed to hack 313 Poloniex users, 142 Binance customers, and 42 Gemini users; the scheme resulted in losses of $16,876,000. Despite all that, the US Secret Service was able to trace their digital movements and seized them in September 2020 (Cimpanu, 2020).

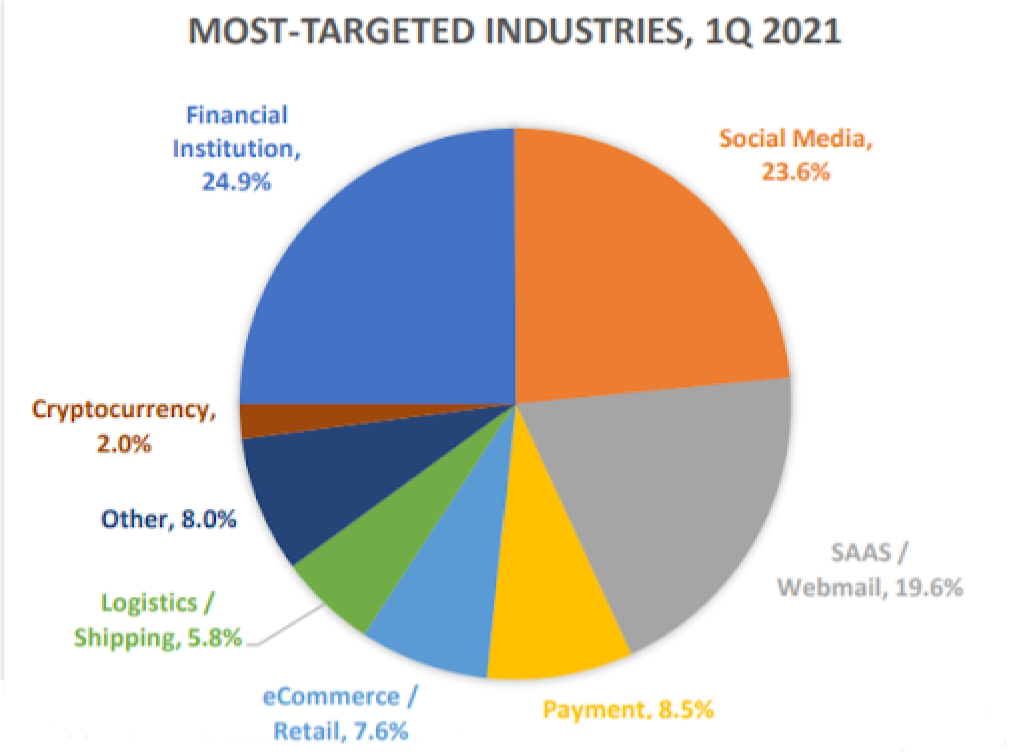
Bitcoin blackmail scams. In the same year, Bitcoin users started to receive phishing emails from scammers that claimed to have hacked the victim's computer and used spyware, which is unwanted software that infiltrates computing devices, to steal internet usage data and sensitive information to film the blackmail victim watching adult videos. Reflecting the current trends in online video conferencing and with the help of zoom, email campaigns claimed to have spied on people. Blackmailers demanded that the affected people transfer economic resources to a particular account and threatened to leak information were their demands not met. All that led to a data breach of about 250,000 people from more than 20 countries. The nations most compromised were Australia, South Africa, United Kingdom, and the United States (Helms, 2020). The media component was supposed to be a strong argument in the victim's eyes to pay the ransom without delay. As such, cybercriminals cited the example of media personalities whose reputations suffered due to the posting of an explicit video.

Blackmailers that year began to take advantage of news and trending topics to devise new techniques, such as "Nigerian" scammers, posing as actual political figures or their relatives, offering a large number of economic resources, or linking their messages to concurrent global events.
Nigerian scams involve someone abroad offering users a portion of a large sum of money or a payment on the condition that they transfer money out of their country. While these scams originated in Nigeria, they now come from all over the world. The scammer would contact the user out of the blue by email, letter, text message, or social media. They would tell them an elaborate story about large sums of their money trapped in banks during events such as civil armed conflicts or coups often in countries currently in the news, like Nigeria, Sierra Leone, and Iraq, or a large inheritance that is hard to reach due to government restrictions or taxes in their country.

Twitter phishing attack. On July 15, 2020, the social media platform, Twitter, reported a phone spear-phishing attack orchestrated by 17-year-old Graham Clark with the help of two other individuals named Nima Fazeli and Mason Sheppard. They tricked some employees by calling them and pretending to be from Twitter's Information Technology department to direct them to a clone phishing twitter website they created. There, the employee needed to enter their credentials, simultaneously giving the hackers access to the real Twitter website. When they broke into the site, they seized the accounts of celebrities, politicians, and other high profile people. Some of the victims were Barack Obama, Joe Biden, Bill Gates, Kim Kardashian, Jeff Bezos, and Elon Musk. The outbreak lasted several hours and during that time the scammers stole over $118,000 worth of bitcoin (Berman et al., 2020).

Statistics and other data. In 2018, social media abuse increased by nearly 200%, a number that only continues to rise. Besides, just in 2020, there was a 45% increase in the social penetration rate. In total, more than 5% of phishing attacks are associated with social media; additionally, it was the second-largest industry with phishing attacks in 1Q 2021. However, these platforms still offer minimal controls to prevent the further spread of account acquisitions (Ellis, 2019). Because social media accounts must generally be approved before connecting with people, they offer a greater sense of trust.

According to 2020 statistics from Interpol, there are 3.5 billion social media users, of which a significant number of profiles are created with fake names and documents. These accounts threaten other users with hacking, social media identity theft, and other cybersecurity issues. Spammers have thousands of fake profiles that become an obstacle for legitimate users to interact and expand networks. Furthermore, counterfeit posts and junk advertisements do nothing more than divert attention and manipulate the thoughts of users.



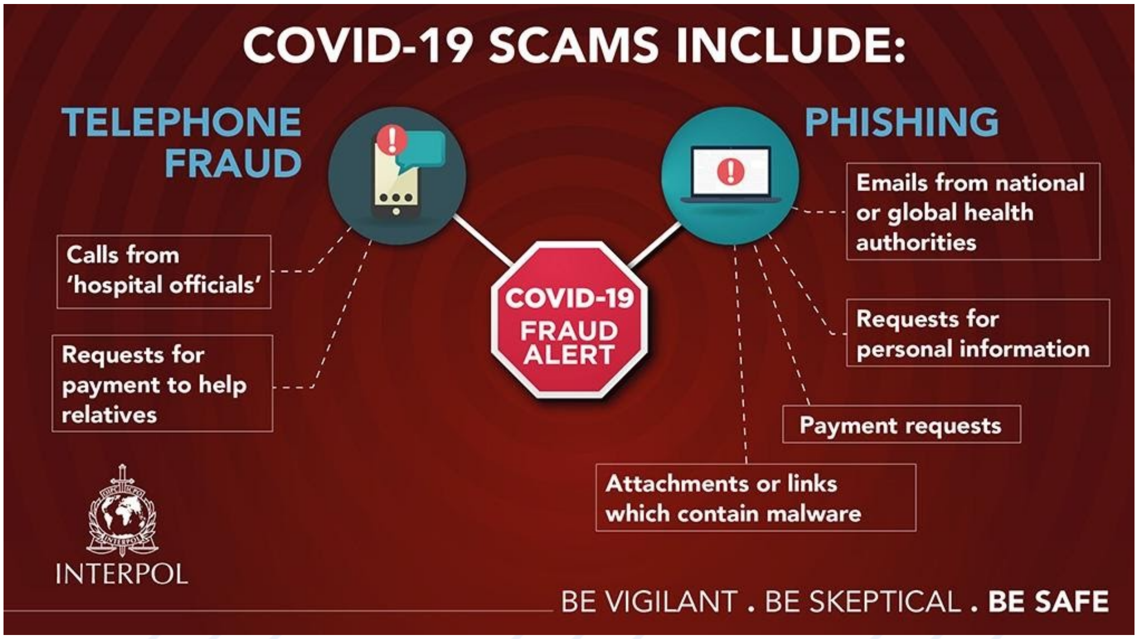
Distribution of organizations affected by phishing attacks by category in 1Q 2021
(Anti-phishing Working Group, 2021)

Social networks have penetrated all corners of the world and are now a fundamental source of communication. Some of the top scams in the social media world that every user should beware of are:

- Sale of fake accounts: The profiles sold can be cloned accounts.
- Romance scam: Through fake relationships, scammers trick other users into sending them money.
-

- Scam vouchers: Also known as gift card scam, it is when fraudsters persuade the victim to pay their bills, fees, or debts using a voucher. Sometimes scammers offer vouchers to steal someone's identity.
- Friend scam: The defrauder entices people to trust the phisher and in a short time they promise money or ask for it.
- Loan scam: Illegitimate businesses offer loan facilities to solve financial problems at a low rate or with the promise of "free" money, but take economic resources from users.
- Pyramid schemes: This is an illegal investment scam where social media users make income by linking items on social media against some membership fee (Smith, 2020).

Nowadays, scammers tend to offer things like a "COVID-19 kit," a "coronavirus pack," or virus-related Medicare benefits and ask to verify personal information like bank accounts and Social Security or Medicare numbers. The crisis derived from the Coronavirus has forced many companies to implement teleworking and to develop digitalization measures in record time. This has created many new security loopholes and breaches well known to cybercriminals, so much so that 70% of companies want to increase their cybersecurity in the future, according to a survey by LearnBonds. In this sense, the need for qualified workers in cybersecurity and data protection is correspondingly high.



COVID-19 SCAMS INCLUDE:

TELEPHONE FRAUD

- Calls from 'hospital officials'
- Requests for payment to help relatives

COVID-19 FRAUD ALERT

PHISHING

- Emails from national or global health authorities
- Requests for personal information
- Payment requests
- Attachments or links which contain malware

INTERPOL

BE VIGILANT . BE SKEPTICAL . BE SAFE

COVID-19 most common cyberattacks
(Interpol, 2020)

The FTC (Federal Trade Commission) receives many reports of fraudulent calls, texts, and emails from individuals claiming to be from the Social Security Administration, Internal Revenue Service (IRS), Census, US Citizenship and Immigration Services (USCIS), and Federal Deposit Insurance Corporation (FDIC). These bogus government messages can say that a person has been approved to receive economic resources, get aid payments quickly, or get cash grants due to the Coronavirus. Scammers can also promise small business loans or send a phishing alert that a check is ready to be cashed. These are all scams and none of those messages come from a government agency.

Besides the mentioned COVID-related scams, the widespread vaccination and relaxed travel restrictions redirected scammers' attention to the tourism industry. Travel apps, such as Airbnb and Expedia Group, are frequently targeted by phishing attacks. Cloned fake pages of the official websites are stealing credit cards, credentials, and accounts, sometimes for money laundering. Another strategy used by hackers is to trick victims into renting apartments in rental offer pages they created, where hackers ask for an advance payment and as soon as the client deposits, they disappear (Kulikova, 2021b).

In research from Barracuda Networks (2021), along with investigators from Colombia University, the five countries with the highest proportion of sent email phishing attacks were all from Eastern Europe. In descending order, they were Lithuania, Latvia, Serbia, Ukraine, and Russia. The next countries on the list were from America and Asia: Bahamas, Puerto Rico, Colombia, Iran, Palestine, and Kazakhstan. While large volumes of phishing emails were recorded in some countries, the overall large number of emails originating from them meant that the proportion of phishing messages was deficient.

For example, 129,369 phishing emails were sent from the US in the dataset, representing 0.02% of the total number of emails. Most countries had a 10% or less probability of phishing, according to the report. Barracuda Networks also noted that phishing emails are more likely to be sent across multiple countries than benign emails. While 60% of phishing emails crossed two or fewer countries, this was 80% for non-phishing emails. After the United States and Germany, Spain has been the country most threatened by cybercriminals in 2020, a finding that corresponds to the risk assessments of proven experts. To exemplify, according to the DsiN-Praxis Report published in Germany in October 2020, almost half of companies (46%) reported cyberattacks in recent months. This trend also occurs among individuals, since 20.2% of private computers in Spain have reported malware threats, although 9 out of 10 (90.4%) have security software installed. Most countries except Belgium have also implemented extensive cyber protection laws to protect businesses and individuals against data theft on the Internet at the national level.

International actions

National Cyber Security Center. All people can be victims of phishing; however, to prevent this, countries have different websites to teach people how they can prevent this fraud.

The National Cyber Security Center (NCSC), located in the United Kingdom, provides cybersecurity advice and effective incident response to reduce the consequences that cyberattacks can cause to UK organizations. It secures both public and private sectors to make online work safe. In 2018, they developed the guide “Phishing attacks: Defending Your Organisation”, which recommended a multi-layer security approach to fight phishing since this type of defense makes phishing more difficult and helps detect emails that might be considered “spam”. The NCSC has been working against phishing since 2017 and now has around 102 different items in order to inform and guide businesses and people to stop and detect phishing (National Cyber Security Center [NCSC], 2019).

Anti-phishing Working Group (APWG). The Anti-phishing Working Group (APWG) is an international coalition that recollects and helps companies that were victims of phishing, crimeware, and email spoofing to help them to reestablish and to give information to prevent and defend themselves from it. It was founded in 2003 and since then has gathered more than 2,000 enterprises to be part of the group. Between 2009 and 2010, in conjunction with the National Cyber Security Alliance (NCSA), they created the STOP. THINK. CONNECT. Messaging Convention to provide a global unified cybersecurity awareness message (Anti-Phishing Working Group, n.d.).

National Cyber Security Alliance (NCSA). It is a non-profit public-private partnership that works with the Federal US government, leading private-sector companies, trade associations, and educational companies to promote education and cybersecurity awareness for home users, businesses, and schools. Since its establishment in 2001, the NCSA has worked with the Department of Homeland Security (DHS) and volunteer leaders from technological organizations, such as Microsoft, Symantec, CISCO, McAfee, American Online, among others. Ever since 2004, each October, as a result of its collaboration and under the leadership of the DHS, the NCSA launches the Cybersecurity Awareness Month to ensure the divulgation of cybersecurity information through traditional and social media channels (National Cyber Security Alliance, 2021).

Federal Trade Commission (FTC). Another great ally of the APWG is the Federal Trade Commission (FTC). It is a bipartisan federal agency dedicated to stop fraudulent practices and promote safe competition in the marketplace. It was established in May 2019 as a guide that provides some tips and solutions for when someone is a victim of any type of phishing. Its main purpose is to work with the APWG to report and detect different cyber attacking techniques and groups (Federal Trade Commission, 2019).

Econsumer.gov. The econsumer.gov is an international forum to report scams, learn how to fight fraud, and protect personal participation from cyberattacks. More than 40 countries are part of this network and their governments have complete access to the website’s database. Nowadays, this forum works within the International Consumer Protection and Enforcement Network (ICPEN) in a no governmental campaign that reports international frauds and checks if the corresponding laws are used correctly. This alliance has worked since 2001 and they have done reports all around the world. Their website shares all the advances that were achieved and is available in English, French, German, Korean, Japanese, Polish, Spanish and Turkish (International Consumer Protection and Enforcement Network, n.d.).

Phishing.org. Phishing.org is a project made by KnowBe4, the world's largest security awareness training platform that works with 37,000 organizations around the globe. Its mission is to help educate others about cybersecurity and to provide reliable data and updates to maintain its program secure and trustworthy. The website has all types of phishing and all the possible solutions for them. They also teach how to be safe with users' passwords and how to avoid becoming a victim of phishing (KnowBe4, n.d.).

European Union Agency for Cybersecurity (ENISA). ENISA Europe centers are institutions that work with the EU cyber policy to treat and prevent different cyber incidents. It has been working since 2009 and provides events and conferences to inform the consequences of cybercrimes and how to protect information; it also provides news and advances in cybersecurity. Nowadays, as a consequence of the pandemic, its main project against phishing is "phishing in COVID times". The official website gives useful information about how to recognize the different techniques and how they can affect people by stealing economic and personal data. It also gives information to take action against perpetrators (European Union Agency for Cybersecurity, n.d.).

Google Safe Browsing. Established in 2007, it is a Google blacklist service that verifies the sites the user visits against URLs Google has determined as unsafe web sources. It can detect social engineering sites and web sources infected with malware. The product has evolved and is compatible with other Google products like Gmail, Android, Google Analytics, etc. Moreover, it has a website that provides tips and tools to help users to stay safe while surfing the internet (Google, 2021).

Council of Anti-Phishing Japan (APC). The Council of Anti-Phishing Japan was founded in 2005 in an attempt to counter the new cyberattack that had just appeared in AOL. Members focus on collecting and analyzing information to emit alarm alerts about phishing attacks and promote anti-phishing measures. It is composed of 80 potential target companies that can provide means of protection against phishing attacks, mostly trying to close phishing sites and collect information regarding identity theft frauds. This council is also a supporter of the APWG campaign STOP. THINK. CONNECT (Council of Anti-Phishing Japan, n.d.).

UN Actions

World Health Organization. The World Health Organization (WHO) shares information on how to know if a website could be a possible hacker. At the same time, it indicates that on the official WHO website will never ask for any username or password, send emails users did not ask for, or encourage people to win a prize and/or apply for a job. Furthermore, from May to June 2020, they enabled a partnership with the Government of the United Kingdom to carry out a campaign named Stop the Spread to raise awareness of misinformation around COVID-19 with the purpose of teaching people to identify phishing emails and WhatsApp messages that try to steal sensitive information (World Health Organization, n.d.).

International Organization for Migration (IOM). The International Organization for Migration (IOM) warns against the stealing of personal information by a fake organization using its official name, promoting communication and giving information to prevent more fraud. They also warn immigrants to be careful with the offers they find on the internet or in their inbox, mainly because those messages trick people by promising easy visa obtention, transportation assistance, resettlement opportunities, job recruitment, and opportunities abroad (International Organization for Migration, 2015, 2019).

Document A/65/201. In 2010, the Group of Governmental Experts (GGE) on Development in the Field of Information and Telecommunications in the Context of International Security, a gathering of legislative specialists, was able to agree upon a vital set of suggestions on standards, rules, and principles of responsible behavior by States in cyberspace. Legislative specialists from the five permanent members of the UN Security Council and 10 leading cyber powers from all regions of the world have recognized that international law, counting the standards of the law of state responsibility, completely applies to state behavior on the internet. This recognition speaks to a step toward all-inclusive acknowledgment of the lawful framework. The past need for clarity as to what rules apply on the internet was one of the components contributing to precariousness and the hazard of acceleration. The unequivocal certification that worldwide law, especially the standards of the UN Constitution, is pertinent to state exercises on the internet, counting to exercises of nonstate on-screen characters inferable to states, will permit the universal community and influenced state.

In the framework, the experts recommended further dialogue between States to discuss the norms of use regarding the information and communications technologies (ICT) products to ensure the safety of international infrastructure. ICT goods are defined by the Organization for Economic Co-operation and Development (OECD, n.d.) as those products that "are either intended to fulfill the function of information processing and communication by electronic means, including transmission and display, OR which use electronic processing to detect, measure and/or record physical phenomena, or to control a physical process". That type of product can provoke disruptions, so

States need to exchange information on national legislation and communication technologies security tactics to reduce the risk ICTs represent.

Open-Ended Working Group (OEWG). In 2019, the UN General Assembly established a group to discuss the protection of human rights. Eleven years later, on March 10, 2021, the third and final substantive session of the UN cybersecurity Open-Ended Working Group (OEWG) was held to discuss the implication of development in ICTs and their use for malicious purposes. Since its creation, the OEWG has involved the participation of about 150 countries and observers, producing nearly 200 written submissions and over 110 hours' worth of on-record statements. The whole committee agreed on a report in which they reiterate the previous Group of Governmental Experts (GGE) recommendations on voluntary norms and international law, this time in a process that included all countries, which serves as an indirect yet meaningful reinforcement to the UN. These include references to protecting medical and other specific critical infrastructure, as well as the affirmation that countries will try to ensure the general availability and integrity of the Internet. The report further endorses the need for capacity building in international law and both supports the responsible reporting of vulnerabilities by States and also encourages states to protect the integrity of the supply chain ICTs (General Assembly, 2021).

Cybersecurity and New Technologies programme. Founded by the UN Office of Counter-Terrorism, this program searches to mitigate technological developments made by armed groups and violent extremists. It is supposed to seize the threat cyber-attacks represent to critical infrastructure and develop the use of social media to create a database with open source information and digital evidence to counter online extremist violent groups while respecting Human Rights (Office of Counter Terrorism, n.d.).

Points to Discuss

1. **Context**
    a. Data breaches
        i. Impact on economic and healthcare systems
    b. Lack of IT investment and training
        i. Deficiency of education regarding prevailing cyber-attack tactics and basic preventative measures
    c. Network security vulnerabilities
    d. Why do the tactics used by phishers work?
        i. Social Engineering manipulating emotions
            1. Fear
            2. Curiosity
            3. Empathy
    e. New targets of opportunity
        i. Social Media
        ii. SMS
2. **Development**
    a. Relationship between personal data protection and use of information in order to fight online armed groups propaganda, recruitment, and radicalization
    b. Growing attacks on the corporate sector due to remote work
        i. How and why has the mass transition to remote work and online communication made employees more vulnerable to phishing and cyberattacks?
    c. Implementation of security awareness training to internet users
        i. Emphasis on teenagers
    d. Understanding the factors that influence users to fall for phishing techniques
    e. Reducing the information available to attackers

References

Official Sources

Anti-Phishing Working Group. (n.d.). Unifying The Global Response To Cybercrime. *APWG*. Retrieved from https://apwg.org/

Anti-Phishing Working Group. (n.d.). About us. *APWG.* Retrieved from https://apwg.org/about-us/

Anti-Phishing Working Group. (2021). Most Targeted Industries, 1Q 2021 [image]. Retrieved from https://docs.apwg.org/reports/apwg_trends_report_q1_2021.pdf

Anti-Phishing Working Group. (2021b). *Phishing Activity Trends Report 1st Quarter 2021*. https://docs.apwg.org/reports/apwg_trends_report_q1_2021.pdf

Berman, J., Blattmachr, J., Brookes, D., Emami, S., Francis, R., Henry, M., Herring, J., Homer, M., Lemire, K., Matthew, S., Mulvihill, C., & Weber, R. (2020). Twitter Investigation Report. *Department of Financial Services*. Retrieved from https://www.dfs.ny.gov/Twitter_Report

Carnegie Endowment for International Peace and BAE Systems. (n.d.). Timeline of Cyber Incidents Involving Financial Institutions. *Carnegie Endowment for International Peace.* Retrieved from https://carnegieendowment.org/specialprojects/protectingfinancialstability/timeline#click-hide

CFR Staff. (2020). The UN Security Council. *Council on Foreign Relations*. Retrieved from https://www.cfr.org/backgrounder/un-security-council

Econsumer.gov. (n.d.). Alerta de estafa: Préstamos de día de pago [Scam alert: Payment day loans]. *Econsumer.gov.* Retrieved from https://www.econsumer.gov/es/News/News/6#crnt

European Union Agency for Cybersecurity. (n.d.). About ENISA - The European Union Agency for Cybersecurity*. ENISA*. Retrieved from https://www.enisa.europa.eu/about-enisa

European Union Agency for Cybersecurity. (n.d.). Understanding and dealing with phishing during the COVID-19 pandemic. *ENISA*. Retrieved from https://www.enisa.europa.eu/news/enisa-news/understanding-and-dealing-with-phishing-during-the-covid-19-pandemic

Federal Bureau of Investigation. (2009). Operation "Phish Phry". *FBI.* Retrieved from https://archives.fbi.gov/archives/news/stories/2009/october/phishphry_100709

Federal Trade Commission. (2019). How to recognize and avoid phishing scams. *FTC.* Retrieved from https://www.consumer.ftc.gov/articles/how-recognize-and-avoid-phishing-scams

Federal Trade Commission. (2021). Coronavirus Advice for Consumers. *FTC.* Retrieved from https://www.ftc.gov/coronavirus/scams-consumer-advice

General Assembly. (2021). Open-ended working group on developments in the field of information and telecommunications in the context of international security. *United Nations.* Retrieved from https://front.un-arm.org/wp-content/uploads/2021/03/Final-report-A-AC.290-2021-CRP.2.pdf

General Assembly. (2010). Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security. *United Nations.* Retrieved from https://unidir.org/files/medias/pdfs/final-report-eng-0-189.pdf

International Consumer Protection and Enforcement Network. (n.d.). econsumer.gov: About Us. *Econsumer.Gov*. Retrieved from https://www.econsumer.gov/AboutUs#crnt

International Organization for Migration. (2015). Fraudes en Internet. *Organización Internacional para las Migraciones*. Retrieved from https://www.iom.int/es/fraudes-en-internet

International Organization for Migration. (2019). SCAM ALERT! *IOM.* Retrieved from https://www.iom.int/scam-alert

Internet Crime Complaint Center. (2021). Internet Crime Report. *FBI.* Retrieved from https://www.ic3.gov/Media/PDF/AnnualReport/2020_IC3Report.pdf

KnowBe4. (n.d.). Phishing | About Us. *Phishing.Org*. Retrieved from https://www.phishing.org/about-us

KnowBe4. (n.d.-b). Phishing | History of Phishing. *Phishing.Org*. Retrieved from https://www.phishing.org/history-of-phishing

KnowBe4. (2021). *Q1 2021 KnowBe4 Finds Users Are Becoming More Savvy Regarding COVID-19 Phishing Attacks*. KnowBe4. Retrieved from https://www.knowbe4.com/press/q1-2021-knowbe4-finds-users-are-becoming-more-savvy-regarding-covid-19-phishing-attacks

National Cyber Security Alliance. (2021). About Cybersecurity Awareness Month (October). *Stay Safe Online*. Retrieved from https://staysafeonline.org/cybersecurity-awareness-month/about-the-month/

National Cyber Security Center. (2019). Phishing attacks: defending your organisation. *NCSC*. Retrieved from https://www.ncsc.gov.uk/guidance/phishing

National Cyber Security Center. (2020). Whaling: how it works, and what your organisation can do about it. *NCSC*. Retrieved from https://www.ncsc.gov.uk/guidance/whaling-how-it-works-and-what-your-organisation-can-do-about-it

Office of Counter Terrorism. (n.d.). Cybersecurity. *UN*. Retrieved from https://www.un.org/counterterrorism/cct/programme-projects/cybersecurity

Organisation for Economic Co-operation and Development. (n.d.). INFORMATION, COMMUNICATION TECHNOLOGY (ICT) GOODS. *OECD.* Retrieved from https://stats.oecd.org/glossary/detail.asp?ID=6274

Tolppa, M. (n.d.). First UN OEWG concludes with a consensus report – what does it mean for future cybersecurity discussions under the auspices of the First Committee? *CCDCOE.* Retrieved from https://ccdcoe.org/library/publications/first-un-oewg-concludes-with-a-consensus-report-what-does-it-mean-for-future-cybersecurity-discussions-under-the-auspices-of-the-first-committee/

United Nations Office on Drugs and Crime. (n.d.). Cybercrime Module 14 Key Issues: Cyberterrorism. *UNODC*. Retrieved from https://www.unodc.org/e4j/es/cybercrime/module-14/key-issues/cyberterrorism.html

United Nations Office on Drugs and Crime. (2012). The use of the Internet for terrorist purposes. *UNODC*. Retrieved from https://www.unodc.org/documents/frontpage/Use_of_Internet_for_Terrorist_Purposes.pdf

World Health Organization. (n.d.). Cybersecurity. *WHO.* Retrieved from https://www.who.int/about/cyber-security

Other Sources

Check Point. (2021). Brand Phishing Report – Q4 2020*. Check Point Software*. Retrieved from https://blog.checkpoint.com/2021/01/14/brand-phishing-report-q4-2020/

Cimpanu, C. (2020). the US charges two Russians for stealing $16.8m via cryptocurrency phishing sites. *ZDNet.* Retrieved from https://www.zdnet.com/article/us-charges-two-russians-for-stealing-16-8m-via-cryptocurrency-phishing-sites/

Council of Anti-Phishing Japan. (n.d.). フィッシング対策協議会について [About the Anti-Phishing Council]. *Council of Anti-Phishing Japan.* Retrieved from https://member.antiphishing.jp/about_ap/

Dixon, J. (2013). The e-gold story. *Digital Gold Currency Blog.* Retrieved from https://dgcmagazine.com/the-e-gold-story/

Ellis, J. (2019). Why Social Media is Increasingly Abused for Phishing Attacks. *PhishLabs.* Retrieved from https://www.phishlabs.com/blog/how-social-media-is-abused-for-phishing-attacks/

En Naranja. (2020). ¿Qué es el vishing y cómo puede evitarlo? [What's vishing and how can you avoid it?]. *En Narajana.* Retrieved from https://www.ennaranja.com/economia-facil/vishing-que-es/

Fruhlinger, J. (2020). What is phishing? How this cyber attack works and how to prevent it. *Csoonline.com.* Retrieved from https://www.csoonline.com/article/2117843/what-is-phishing-how-this-cyber-attack-works-and-how-to-prevent-it.html

Forcepoint. (2021). What is Malvertising? *Forcepoint.* Retrieved from https://www.forcepoint.com/es/cyber-edu/malvertising

Gendre, A. (2020). Pretexting: 5 Examples of Social Engineering Tactics. *Vade*. Retrieved from https://www.vadesecure.com/en/blog/pretexting-5-examples-of-social-engineering-tactics

Gilbert, B. (2016). Hillary Clinton's campaign got hacked by falling for the oldest trick in the book. *Insider.* Retrieved from https://www.businessinsider.com/hillary-clinton-campaign-john-podesta-got-hacked-by-phishing-2016-10?r=MX&IR=T

Google. (2021). Protecting more with Site Isolation. *Google Online Security Blog*. Retrieved from https://security.googleblog.com/

Helms, K. (2020). Personal Data of 250,000 People From 20 Countries Leaked by Bitcoin Scam. *Bitcoin.com.* Retrieved from https://news.bitcoin.com/personal-data-250000-20-countries-leaked-bitcoin-scam

Houcheime, W., Hasson, E., Hasson, E., McKeever, G., Hansen, R., Schoenfeld, S., Prevost, C., & Oh, J. (2019). Social Engineering. *Learning Center*. Retrieved from https://www.imperva.com/learn/application-security/social-engineering-attack/

Huddleston, T. (2019). How this scammer used phishing emails to steal over $100 million from Google and Facebook. *Make it.* Retrieved from https://www.cnbc.com/2019/03/27/phishing-email-scam-stole-100-million-from-facebook-and-google.html

Internet Crime Complaint Center. (2020). 2020- Top 5 Crime Type Comparison [image]. Retrieved from https://securityaffairs.co/wordpress/wp-content/uploads/2021/03/2020-Internet-Crime-Report.png

Joque, J. (2018). *Deconstruction machines: writing in the age of cyberwar* (Vol. 54). U of Minnesota Press.

Kaspersky. (2021). Ransomware: qué es, cómo se lo evita, cómo se elimina. *Kaspersky.com.* Retrieved from https://latam.kaspersky.com/resource-center/threats/ransomware

Kaspersky. (2021). ¿Qué es el smishing y cómo defenderse contra él? *www.kaspersky.es*. Retrieved from https://www.kaspersky.es/resource-center/threats/what-is-smishing-and-how-to-defend-against-it

Kay, R. (2004). How-to Phishing. *Computerworld.* Retrieved from https://www.computerworld.com/article/2575156/phishing.html

Kulikova, T. (2021). Spam and phishing in 2020. *Securelist*. Retrieved from https://securelist.com/spam-and-phishing-in-2020/100512/

Kulikova, T. (2021). Spam and phishing in Q3 2020. *Securelist.* Retrieved from https://securelist.com/spam-and-phishing-in-q3-2020/99325/

Marketing Team. (2021, February 22). *5* Costly phishing attacks in recent history. *Graphus*. Retrieved from https://www.graphus.ai/blog/5-costly-phishing-attacks-in-recent-history/

McGlasson, L. (2009). “Phish Fry” Nets 100 Fraudsters. *BankInfoSecurity*. Retrieved from https://www.bankinfosecurity.com/phish-fry-nets-100-fraudsters-a-1846

Nadeem, S. M. (2020). Social Engineering: What is baiting? *Mailfence Blog*. Retrieved from https://blog.mailfence.com/what-is-baiting-in-social-engineering/

Proofpoint.com. (2021). *2021 State of the Phish*. Retrieved from https://www.intelligentcio.com/wp-content/uploads/sites/20/2021/03/2021-State-of-the-Phish-WP.pdf

Proofpoint.com. (2021b). Percentage of different cyberattacks (successful and unsuccessful) in 2020 [image]. Retrieved from https://www.intelligentcio.com/wp-content/uploads/sites/20/2021/03/2021-State-of-the-Phish-WP.pdf

Race, S. (2016). Cyber Security. In Construction Manager’s BIM Handbook (pp. 107–112). Chichester, UK: John Wiley & Sons, Ltd.

Rosenthal, M. (2021). Must-Know Phishing Statistics: Updated 2021. *Tessian.* Retrieved from https://www.tessian.com/blog/phishing-statistics-2020/#the-most-targeted-industries

Sardanyés, E. (n.d.). Primer ciberataque de la historia y los ciberataques que han perdurado en el tiempo [First cyberattack in history and the cyberattacks that have lasted over time]. *Esed*. Retrieved from https://www.esedsl.com/blog/primer-ciberataque-historia-y-ciberataques-que-han-perdurado-tiempo

Smith, O. (2020). Rising Social Media Scams in 2020 Calling for Digital Identity Verification. *Shufti Pro.* Retrieved from https://shuftipro.com/blog/rising-social-media-scams-in-2020-calling-for-digital-identity-verification/

Suciu, P. (2020). Twitter Spear Phishing Attack Highlights Security Weaknesses Of Social Media. *Forbes.* Retrieved from https://www.forbes.com/sites/petersuciu/2020/08/01/twitter-spear-phishing-attack-highlights-security-weaknesses-of-social-media/?sh=9b9033a7a297