International Journal for Innovation Education and Research
scholarsjournal.net/index.php/ijier ISSN: 2411-2933

DOI: doi.org/10.31686/ijier.vol10.iss8.3822

Consequence of Phishing during the pandemic in Manaus

Rilmar Pereira Gomes (Advisor)
rilmargomes@hotmail.com
Academic coordination of the Metropolitan University of Manaus – FAMETRO - BRAZIL

Caio César Augusto do Carmo Barroncas
barroncasadc@gmail.com
Academic coordination of the Metropolitan University of Manaus – FAMETRO - BRAZIL

Caio Vinícius Pontes Araújo
caioviniciuspontes@gmail.com
Academic coordination of the Metropolitan University of Manaus – FAMETRO - BRAZIL

Luis Gustavo Bastos Moura
gustavobastosmoura123@gmail.com
Academic coordination of the Metropolitan University of Manaus – FAMETRO - BRAZIL

Maik Antônio Costa de Lima
maikantoniolima@gmail.com
Academic coordination of the Metropolitan University of Manaus – FAMETRO - BRAZIL

Jaqueline Silva de Souza Pinheiro
Jaqueline.pinheiro@fametro.edu.br
Academic coordination of the Metropolitan University of Manaus – FAMETRO - BRAZIL

David Barbosa de Alencar
David002870@hotmail.com
Institute of Technology and Education Galileo of Amazon - ITEGAM, BRAZIL

Abstract

In results, we sought to identify the ways in which phishing is used during the pandemic. The discussion sought to report the ways in which the phishing attack works and discussed ways to prevent phishing attacks and make people aware of the risks and precautions when browsing the Internet

Consequence of Phishing during the pandemic in Manaus

Keywords: Information security; Phishing; Social Engineering; Pandemic; Covid19;

1. Introduction

Due to the pandemic resulting from the covid-19, which forced people into total isolation, causing them to migrate to the digital world, many workers switched to the home office model, working from home. In this scenario with increasing dependence on the internet, cyber crimes increased dramatically in 2020 and 2021, and one of the most used virtual attacks was via phishing, with a 100% increase according to a company specializing in monitoring digital risks Axur.

That said, social distancing is the main prevention measure, the increased use of social networks was the most used means of communication, with that the attackers used the "Fake News" related to social assistance programs to apply Phishing and consequently the Frauds with Brazilian data have increased exponentially.

With this, from reading this article, it will be possible to understand the cyber risks of the internet for lay users, the increase in cyber crime and its social impacts, raise awareness of the impact of incorrect use of digital media, consequences of fraud by data theft, demonstrate ways to of prevention for the most affected people and the main means used to capture data.

However, the methodology is based on recent bibliographic review, mainly of scientific articles, analyzes of consulting firms and international institutions to combat cybercrime, analyzes in government agencies to combat cybercrime.

The technology market has provided civilians with easy access to drones of different categories that imply their ability to use. Drones ranging from small flights and minutes in duration to hours of flight and cargo transport. Control and programming systems have been improving over time in terms of safety and integrity, for example. However, there is still a deficiency regarding drone attacks by hackers, which aim to affect, mainly, the integrity of the data that is transmitted between the operator and the drone, causing the drone to deviate from its programmed path. With this scenario, a study was carried out where each tool presented in this article has the ability to help together in the fight against attacks that seek to send false GPS signals to divert drones from their original route.

2. Theorical Reference

The methodology applied in this article is field research that proposes an integration of data collection, relative information and objects of study. According to José Filho (2006, p.64) “the act of research brings with it the need for dialogue with the reality that one intends to investigate and with the different, a dialogue endowed with criticism, channeling creative moments”. It is also used for study methodology research in books, articles and legislation related to the topic.

2.1 Pandemic in Manaus

Located in the Amazon, the city of Manaus, capital of the state of Amazonas, occupies seventh place in the ranking of Brazilian metropolises, with 2,182,763 inhabitants (representing 52% of the state population)

(IBGE, 2020). Access to the city and the State is made, primarily, by air and river, considering that there is no road that connects them to other regions of Brazil.

However, according to (Costa Silva, R. G. Finisterra, LV(115), 2020, pp. 69-74), the condition of near geographic isolation did not become an obstacle to the expansion of Covid-19 in the city of Manaus, which quickly passed to be the metropolis in which the pandemic reached the greatest public calamity. The first records of Covid-19 occurred in early March, when some citizens had returned from Europe, rising to a chaotic situation in the month of May, when it reached 15,020 cases (FVS, 2020). Currently (10/26/2020), the city of Manaus has 61,422 confirmed cases (39% of the state rate – 157,688 total), 2,834 deaths (63.5% of the state – 4,460 total), a case fatality rate of 4, 6% (the state is 2.8%, the national is 2.9%), and the mortality rate is 132.1 (109.3 in the state and 75.2 in the country). (Magazine. Finis earth, 5 Aug 2021).

2.2 Phising During the Pandemic

In the current scenario, with the escalation of the covid 19 pandemic, companies and people have been forced into a new reality, with the isolation imposed on the population and companies, work has moved from the office to a physical environment to a digital one, many companies have adopted work from home. office, where people started to work from home in front of the computer, with schools the situation is similar, where students also migrated to the digital world. With people at home vying for internet resources with work, study and leisure making people easy prey for internet criminals who use phishing to carry out scams, many companies have suffered from phishing attacks during the pandemic, many of these attacks were carried out through the worker who was using the internet at home, these workers had no or little training on how to use the internet safely, what facilitated the phishing attacks was that the workers did not use the corporate internet of the company that provides the appropriate security.

Gordon and Ford (2006), digital crime is separated into two factors, the technological and the human, the technological factor and focused on technology the software, to prevent this crime from happening it is necessary to invest in software and hardware and an investment in information security tools. As for crime with the human factor, an investment in digital training is necessary as a way to prepare the professional to protect themselves on the internet, and in the current case, the pandemic helps the professional to adapt to the remote environment.

According to Ariane G. (2022) "Phishing is a cyber crime in which ordinary people are contacted via email, telephone or text messages (SMS) by another person or company. The contact is made in a genuine way, to attract and induce the contactee to provide confidential information, bank details, credit card details, passwords and other confidential information."

According to Kaspersky in 2020, many of the phishing attacks abused the Covid-19 theme to steal information such as: personal data, online account credentials and, mainly, bank passwords. The ploys used by cybercriminals ranged from offers of masks and alcohol gel, to false registrations for social aid programs, the PIX registration and, more recently, fraudulent registration pages for the vaccine.

Despite the high rate, it is worth noting an important drop compared to 2019. That year, more than 30% of Brazilians had tried, at least once, to open a link that led to a phishing page, ten percentage points more than in 2020.

The survey also shows that the rate of Brazilian phishing targets (20%) is above the world average (13%). For our specialist, this difference can be explained by the difficulty of Internet users in recognizing a fake mail. “A survey showed that about 30% of Brazilians do not know how to recognize a fake e-mail message”, he points out. (Kaspersky, March 2, 2021).

2.2.1 Phising

According to Martins (2017), Phishing is defined as techniques that combine social engineering and Hacking. It is a form of cyber fraud in which an individual tries to obtain personal information from the victim, usually to misuse it, using anonymity, the subject impersonates a company or entity, through emails, instant messages, among others, such as: Facebook, WhatsApp, Instagram and other social media.

2.2.2 Phising Attacks

According to Conteh and Schmick (2016), when it comes to phishing, it is a scam that works only if the victim believes the content of the email or message, clicks on the link, provides data or downloads the infected file.

During the 2020 pandemic, the various forms of phishing gained prominence with attacks involving fake pages with topics related to Covid-19According to the Checkpoint Research report (2020), email phishing was the most common type of branded phishing attacks, accounting for 44% of attacks, and web phishing ranked second among the types are:

- Email Phishing: Most phishing attacks are sent via email. Attackers often register fake domain names that mimic real organizations and send thousands of common requests to victims.
- Spear Phishing: It is a type of phishing that is commonly directed at a specific target, usually an individual, company or institution, so criminals collect information about the target and execute the attack using this obtained data, the intention is to appear the as legitimate as possible what is being sent, increasing the chances that the scam will succeed.
- Vishing: In a typical voice phishing scam, an attacker pretends to be a scam investigator for a credit card company or bank, informing victims that their account has been breached. The criminals then ask the victim to provide payment card information, supposedly to verify their identity or transfer money to a secure account (which is actually the attacker's).

With this, the criminal induces the victim to give him their passwords and banking information, this method is called social phishing, which consists of collecting relevant social information from the victim so that he can more effectively carry out his approach, pretending to be a friend. , relative or an acquaintance of the victim, one of the most used communication tools according to CheckPoint Research (2020) WhatsApp has moved from 6th to 3rd position, now accounting for 11% of all phishing attempts.

2.2.3 Phising Campaigns

According to a survey by Kaspersky, a company specializing in information security, Phishing campaigns are commonly disseminated via email, with fraudulent links and adopting the appearance of communications from large companies, trying to appear as legitimate as possible, often having a short period of dissemination. But now, research has shown just how big these operations are, with a third of them lasting less than a day and sometimes disappearing even after their first few hours of activity. (Woburn, MA – December 9, 2021).

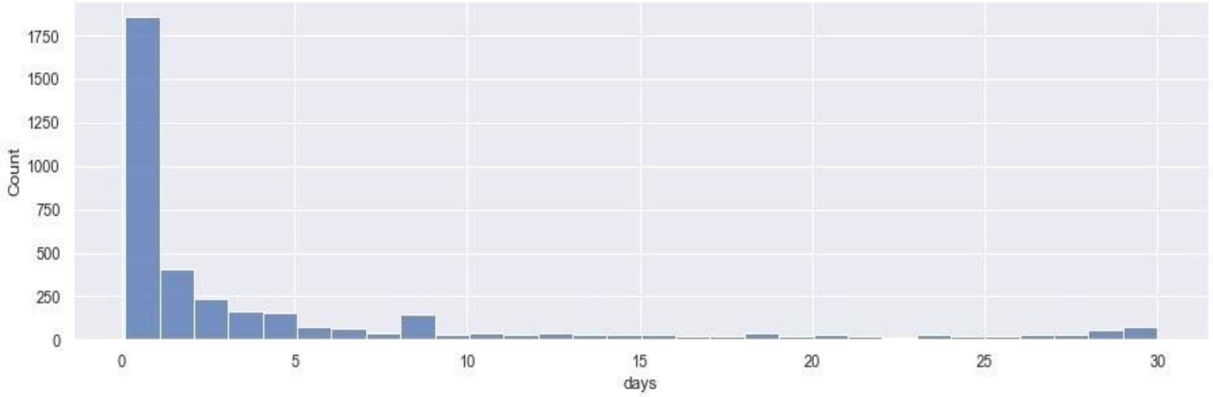

Figure 1: Kaspersky study shows lifetime of Phishing campaigns over time, with a third of them lasting no more than 24 hours; most cease to exist within three days.
Source: kaspersky - classification of phishing (2021).

2.3 Cyber Crimes in Manaus

According to Law 12,737, of April 2, 2013, entitled the Carolina Dieckman Law, cyber crimes are all or the act of invading someone else's computer device, connected or not to the computer network, through improper violation of a security mechanism and with the purpose of obtaining, tampering with or destroying data or information without the express or tacit authorization of the device owner or installing vulnerabilities to obtain unlawful advantage.

In 2020, Bill nº 4.554/2020 was sanctioned, which extends penalties for crimes of theft or embezzlement committed with the use of electronic devices, such as cell phones, computers and tablets. The amendment of the Law aggravates the crime, which previously had a detention of 3 (Three months) to 1 (one) year and a fine, to a penalty with imprisonment of 4 (Four) to 8 (Eight) years, whether the form of action such as breaches of passwords, security mechanisms or the use of rogue programs.

In addition, if the crime is committed against the elderly or vulnerable people, the penalty increases from one third to double, considering the consequences on the victim's life. And, if it is practiced with computer resources outside the country, the penalty increase can go from one third to two thirds.

Knowing these Laws, the internet has been used for numerous purposes, whether to carry out commercial negotiations, seek knowledge, meet people, maintain relationships, produce personal marketing activities, seek entertainment and, in some cases, promote inconvenience to other people, including damages. victims' financials.

Due to this growing expansion of the use of the internet, the exposure of users is increasing, generating interest and enabling the practice of crimes. These crimes can happen in different ways and places, being a criminal action involving computers and networks. Intended to typify these crimes.

3. Methodology

In Brazil, despite all the legislation, virtual crime has been growing more and more, especially during the pandemic, according to Safernet, in 2020, 156,692 complaints were registered, a number much higher than the number presented in 2019, when 75,428 cases were recorded.

On the other hand, cyber crimes of a financial nature, such as computer hacking, theft of passwords and bank data, in addition to general extortion scams, have increased, and a large part of the actions take advantage of the pandemic. In 2020, there were records of a 41,000% increase in websites with terms related to "coronavirus" and "Covid" in their domain. Of this portion, the Amazonas Public Security Department (SSP-AM) warns of the increase in cyber crimes. In the first half of 2021, the State of Amazonas recorded 4,750 cases of crimes committed online, an increase of 198.7% compared to the same period in 2020. From January to June of last year, 1,590 cases were reported through the Bulletin of Occurrence (BO).

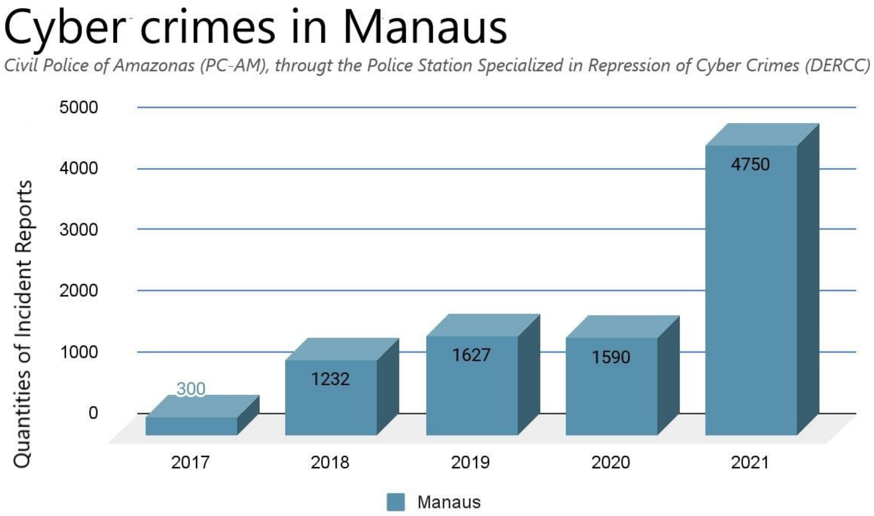

Figure 2: Increase in cyber crime in the city of Manaus.
Source: Department of Public Safety (SSP-AM) – 2021.

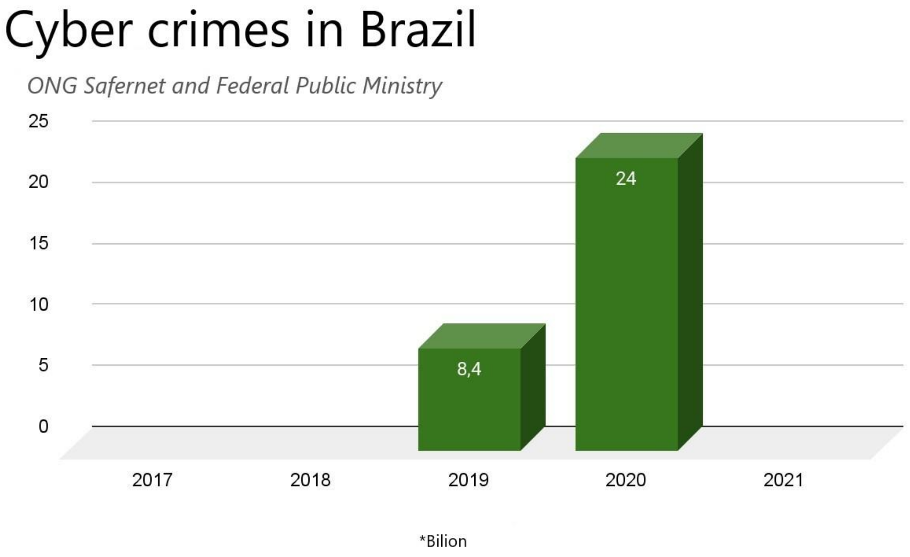

Figure 3: Increase in cyber crime in Brazil.
Source: Portal G1 – 2021.

The experiment, carried out by ETH Zurich (December, 2021) with more than 14,000 participants over a period of 15 months, sent fake messages to their work emails, and their inboxes also had a button to report. fraudulent communication.

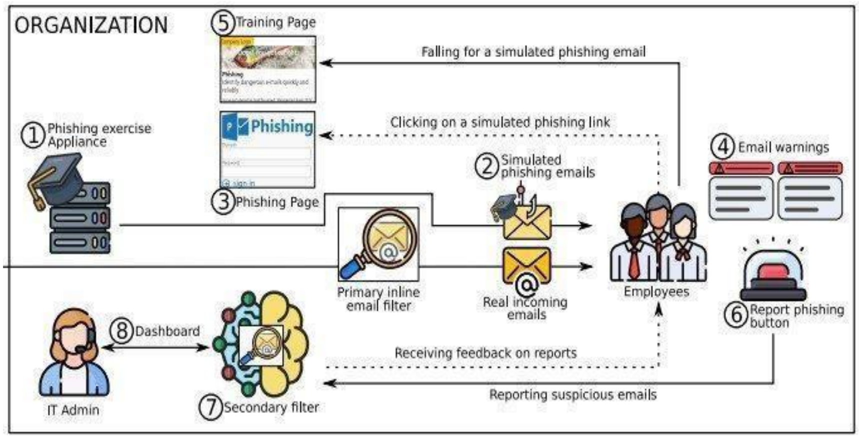
ORGANIZATION
5 Training Page
Falling for a simulated phishing email
Phishing
Clicking on a simulated phishing link
1 Phishing exercise Appliance
2 Simulated phishing emails
4 Email warnings
3 Phishing Page
Primary inline email filter
Real incoming emails
Employees
6 Report phishing button
8 Dashboard
Receiving feedback on reports
IT Admin
7 Secondary filter
Reporting suspicious emails

Figure 4: Flow of a Phishing Attack.
Source: Arxiv.org.

From a diverse demographic, researchers found that people's gender is related to the incidence of opening untrue phishing emails. Instead, the person's age is an important factor, with the elderly, children and teenagers among the most open to the fake messages.

4. Results.

According to the result presented in figures 2 and 3, it has been proven that the increase in cyber crimes has been growing more and more during the pandemic, figure 2 represents a significant increase in the city of Manaus between 2017 and 2021 and double when compared to Brazil with that we have a constant increase until today.

To avoid being a victim of phishing, there are numerous measures that you can take, including:

* Caution when opening attachments or clicking on links without emails: Be careful if you receive emails from friends with links, as they may have been one of the victims and contribute to criminals to spread new malicious emails, the same valid for financial institutions, online stores, airlines, travel agencies, among others (KASPERSKY, 2015).

* Always do your own typing: If a company or organization you know sends you a link or phone number, don't click. Use search engines to find the website or phone number provided. Even if a link or phone number looks like the real thing, criminals manage to hide the true destination (FTC, 2017).

* Call if unsure: Do not respond to emails asking for personal information or financial details. Criminals use pressure tactics and prey on fear. If you believe that a business, a friend, or someone close to you really needs your personal information, pick up the phone and call back using the number found on the real website or address book, not the one in the email (FTC, 2017).

* Avoid accessing bank accounts on public Wi-Fi networks, as well as accessing financial websites on public networks, cafes or on the street. It can happen that these connections are created by criminals, with the aim of spoofing website addresses during the connection, and redirecting data traffic to fake websites. It is recommended to use your mobile data from the telephone company or wait until you have a known and reliable internet connection (KASPERSKY, 2015).

* Always check the link before accessing: If you are careful to detect any spelling problems, be sure, criminals are trying to trick you with a fake page (KASPERSKY, 2015).

5. Acknowledgement

To the Metropolitan University of Manaus - FAMETRO, the Academic Coordination for the support and assistance in the development of teaching and research.

6. References

ALLEN, Malcolm. (2007). Social engineering: a means to violate a computer system.

Disponível em: https://www.sans.org/reading-room/whitepapers/engineering/social-engineering-means-viol ate-computer-system-529. Acesso em: 16 mar. 2019.

CASOS DE CRIMES CIBERNÉTICOS, (2019). Delegacia Interativa registrou mais de 1,2 mil casos de crimes cibernéticos. Disponível em: http://www.ssp.am.gov.br/delegacia-interativa-registrou-mais-de-12-mil-casos-de-crimes-cib erneticos/. Acesso em: 11 abr. 2022

CERT.BR. Cartilha de Segurança para Internet. Versão 4.0. São Paulo: Comitê Gestor da Internet no Brasil, 2012. Disponível em: https://cartilha.cert.br/livro/cartilha-seguranca-internet.pdf. Acesso em: 25 fev. 2019.

CRIMES CIBERNÉTICOS O QUE SÃO. (2021). Crimes cibernéticos: o que são, tipos, como detectar e se proteger. Disponível em: https://fia.com.br/blog/crimes-ciberneticos/. Acesso em: 11 abr. 2022

DEMARTINI, Felipe. (2022). 1/3 das campanhas de phishing duram menos tempo do que as pessoas imaginam. Disponível em: https://canaltech.com.br/seguranca/13-das-campanhas-de-phishing-duram-menos-tempo-do -que-as-pessoas-imaginam-213268/. Acesso em: 11 abr. 2022

GILSON, Costa Silva, R. G. (2021). Pandemia e desigualdades socioespaciais no Brasil.: O caso de Manaus, Amazônia. Finisterra, 55(115), 61–68. https://doi.org/10.18055/Finis20341 . Acesso em: 11 abr. 2022

GUSMÃO, Lane. (2021). Crimes pela internet aumentam 198,7% em Manaus, diz polícia.

Disponível em: https://g1.globo.com/am/amazonas/noticia/2021/10/12/crimes-pela-internet-aumentam-1987percent-em-manaus-diz-policia.ghtml. Acesso em: 11 abr. 2022

MORGENSTERN, Grasiele Giusti. (2015). CRIMES CIBERNÉTICOS: PHISHING - PRIVACIDADE AMEAÇADA. Disponível em: https://www.publicacoeseventos.unijui.edu.br/index.php/salaoconhecimento/article/view/5 174. Acesso em: 11 abr. 2022

PREVENIR GOLPES DE PHISHING. (2020). Confira dicas para se prevenir de golpes de phishing, o famoso crime virtual. Disponível em: https://fdr.com.br/2020/11/03/confira-dicas-para-se-prevenir-de-golpes-de-phishing-o-famos o-crime-virtual/. Acesso em: 11 abr. 2022

ROCHA,Carol. (2020). Crimes cometidos na internet levam 4 por dia à delegacia no AM. Disponível em: https://www.acritica.com/manaus/crimes-cometidos-na-internet-levam-4-por-dia-a-delegaci a-no-am-1.49956. Acesso em: 11 abr. 2022

RODRIGUES, Renato, (2021). Brasileiros são principais alvos de ataques de phishing no mundo. Disponível em: https://www.kaspersky.com.br/blog/brasileiros-maiores-alvos-phishing-mundo/17045/. Acesso em: 11 abr. 2022

SAN CARLOS, CA, (2020). Microsoft is Most Imitated Brand for Phishing Attempts in Q3 2020.

Disponível em: https://www.checkpoint.com/press/2020/microsoft-is-most-imitated-brand-for-phishing-atte mpts-in-q3-2020/. Acesso em: 11 abr. 2022

SAN CARLOS, CA, (2021). DHL Replaces Microsoft as Most Imitated Brand in Phishing Attempts in Q4 2021. Disponível em: https://www.checkpoint.com/press/2022/dhl-replaces-microsoft-as-most-imitated-brand-inphishing-attempts-in-q4-2021/. Acesso em: 11 abr. 2022

VILELA, Pedro Rafael. Lei com penas mais duras contra crimes cibernéticos é sancionada.

Disponível em: https://agenciabrasil.ebc.com.br/politica/noticia/2021-05/lei-com-penas-mais-duras-contra-c rimes-ciberneticos-e-sancionada. Acesso em: 11 abr. 2022

WOBURN, MA. (2021). Powerful but short-lived: One third of phishing pages cease to be active after a single day. Disponível em: https://usa.kaspersky.com/about/press-releases/2021_powerful-but-short-lived-one-third-ofphishing-pages-cease-to-be-active-after-a-single-day. Acesso em: 11 abr. 2022