**COMPUTER SECURITY – CASE STUDY REPORT**

**CASE STUDY TOPIC: LA COUNTY HEALTH SERVICES: PATIENT’S DATA EXPOSED IN PHISHING ATTACK**

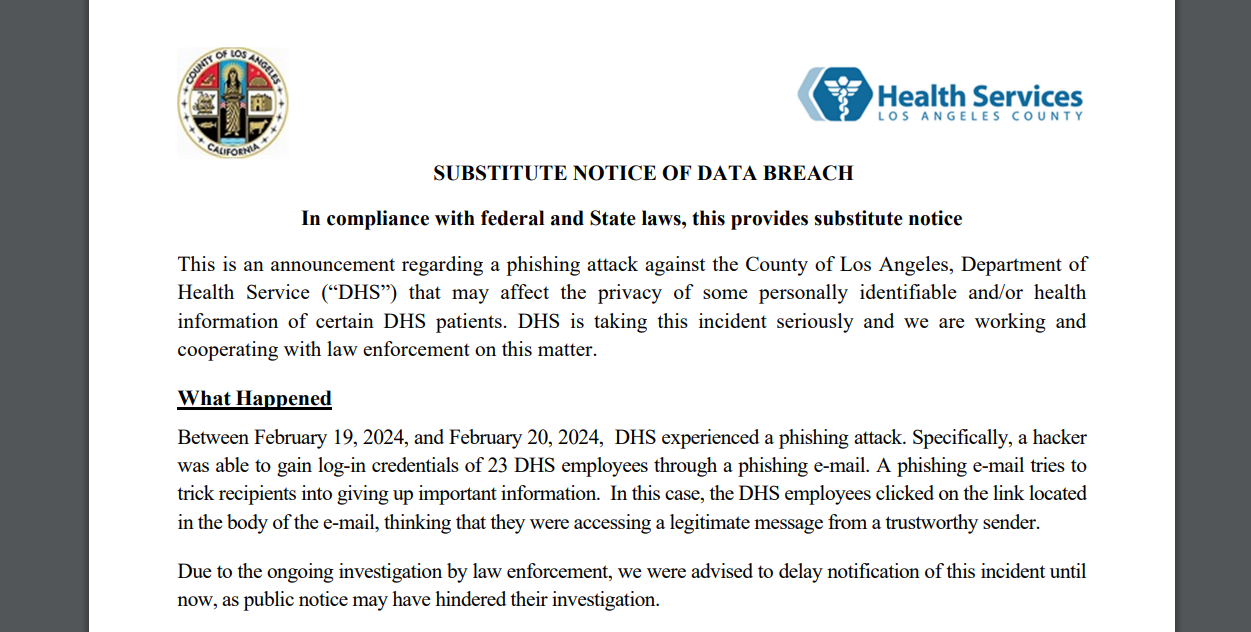
**ELABORATE ON THE CASE STUDY**

 **Image source: EIRE SYSTEMS**

The strength and impact of phishing attacks on industries are experiencing a significant and perilous rise. According to the 2024 worldwide phishing statistics, 94% of organizations fell victim to these attacks, with 96% suffering negative consequences. In 74% of these organizations, the implicated employees faced disciplinary action, dismissal, or chose to leave voluntarily. Additionally, 58% endured account takeover attacks.

In California's LA County, between February 19 and 20, 2024, a phishing attack targeted the LA County Department of Health Services (DHS), the second-largest public health system following NYC Health + Hospitals. This incident resulted in a data breach wherein approximately 23 employees' email accounts were compromised.

This **outsider attacker** is particularly insidious due to his adeptness in crafting phishing emails using legitimate resources. Such precision can only be achieved through the application of social engineering principles.

  
**official notice of data breach by DHS**

The compromised emails contained extensive information including

* First name and Last name, date of birth, home address, phone number(s), e-mail address, medical record number, client identification number, dates of service
* Medical information (e.g., diagnosis/condition, treatment, test results, medications),
* And/or health plan information.

Fortunately, the breached information did not include Social Security numbers (SSNs), as confirmed by the Social Security Office of Retirement and Disability Policy.

*Assigned at birth, the SSN enables government agencies to identify individuals in their records and businesses to track an individual's financial information.*

**How they went about restoring security after the breach?**

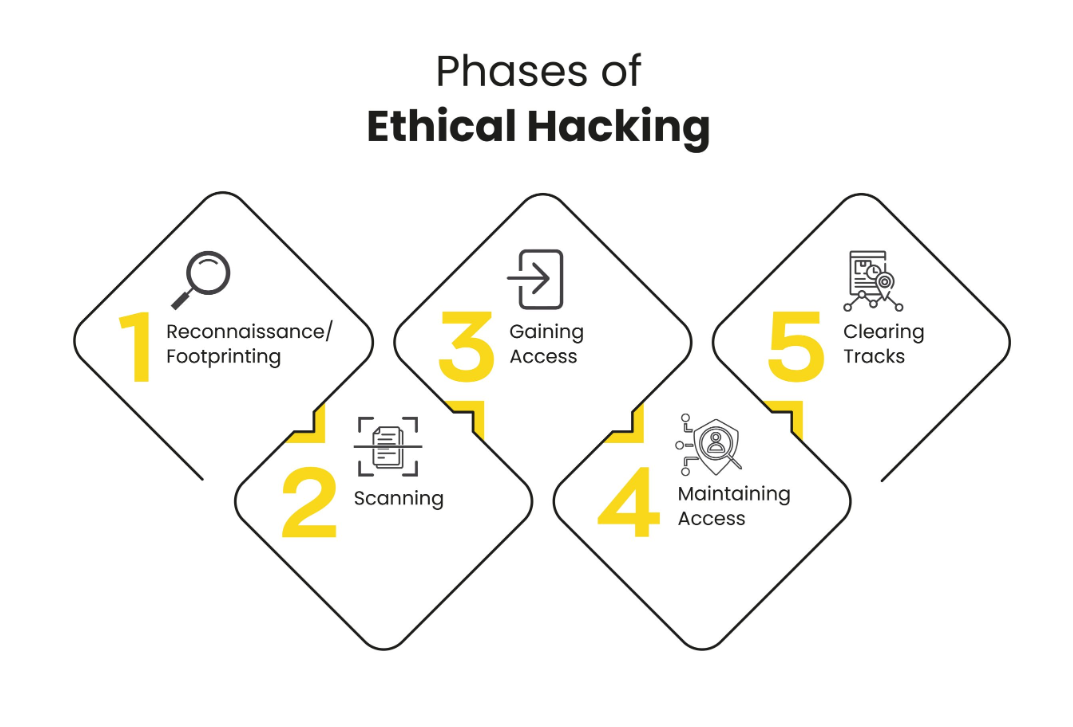
* **Disabling the compromised** email accounts.
* **Re-set and Re-image** (In every system, an initial snapshot of its configurations is taken. When a malicious application affects the system, it experiences a surge in traffic, downloads malicious content, encounters buffer overflows, and various other issues leading to system compromise. Upon detecting the compromise, the system relies on the initial configuration snapshot to restore its original state.) of all victim employee devices.
* After analyzing the situation within the company, they opt to **quarantine all incoming emails** that appear suspicious.
* warned employees to be cautious when analyzing emails, especially **attachments or links**.
* Patients are advised to **review both their personal and health records diligently**. There is a possibility of **data manipulation**, which could alter patients' health status and potentially result in severe problems down the line.

Here are a few examples of how phishing can be made more effective:

* Utilizing public information such as a **company's annual celebration** to create an email inviting the target employee.
* Tailoring the phishing attempt to the target's interests; for instance, sending offers for **the latest tech gear to a tech-savvy individual, or fake announcements of a salary hike, music concerts**, and more.
* Employing **TYPO-SQUATTING**, a technique that involves making slight alterations to legitimate **domain names or email addresses associated with a company, which can confuse the victim** and lead them to click on malicious links. Another tactic is embedding malicious code into images using **steganography**, which can further deceive the target.

**STATEGY OF THE ATTACKER**

Upon going by the methodology of attacking



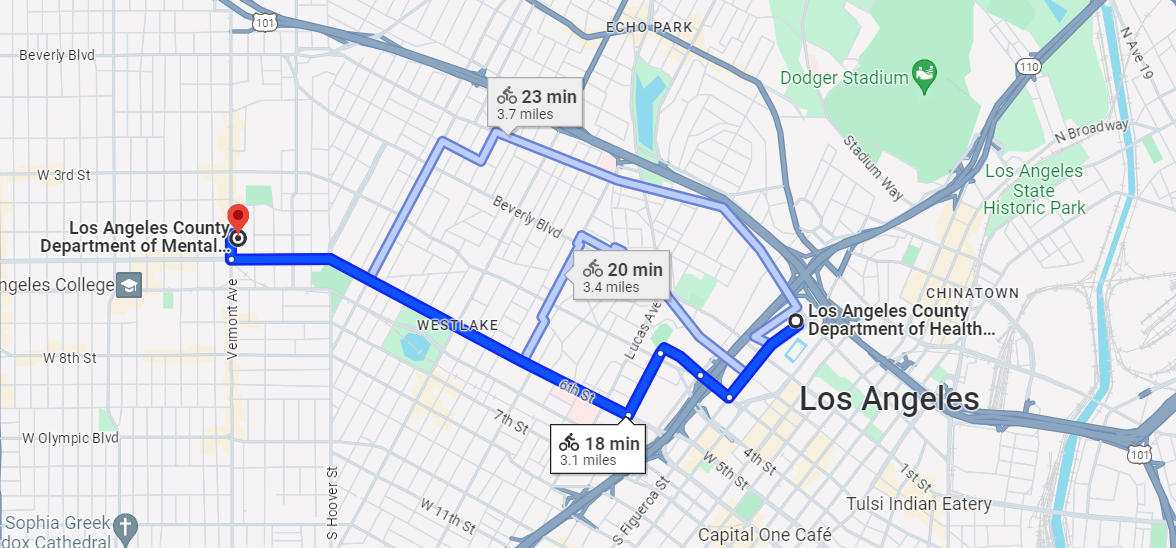
* During phase 1, the attacker meticulously conducts foot-printing on the employees, employing various techniques. They officially mark all the social media accounts such as **Facebook, Instagram, LinkedIn, Discord, Telegram, among others**. Additionally, the attacker attempts to acquire further data through methods like **Google Dorking, vishing calls**, and more, all aimed at obtaining the **victim’s emails or other ways to get the emails**
* During phase 2, Scanning reveals crucial information such as the type of operating system, open port activity (like SMTP when targeting emails), company architecture, least privileged roots and their servers, and firewall data. This allows the attacker to potentially infiltrate the system and manipulate defender settings or firewall configurations, facilitating the execution of "**click and allow**" phishing tactics.
* During phase 3, Gaining access can be achieved through various means:

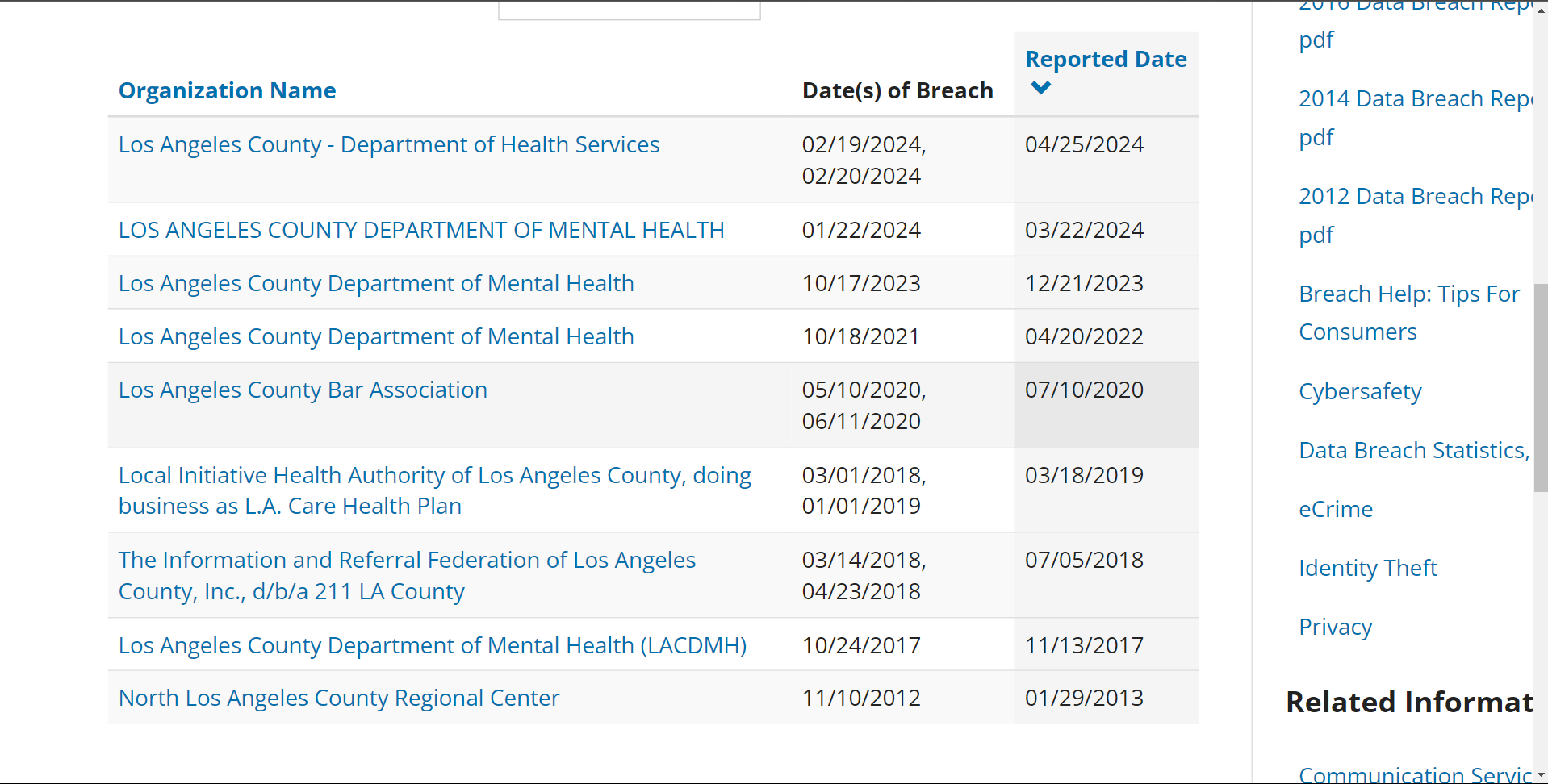
1. Phishing emails may contain links embedded with **backdoors, remote access Trojans (RATs), keyloggers, or another malicious spyware.**

2. Once a malicious file **infiltrates the system, a reverse shell** is established between the victim and the attacker, enabling the attacker to enter the system and extract email data from the compromised system.

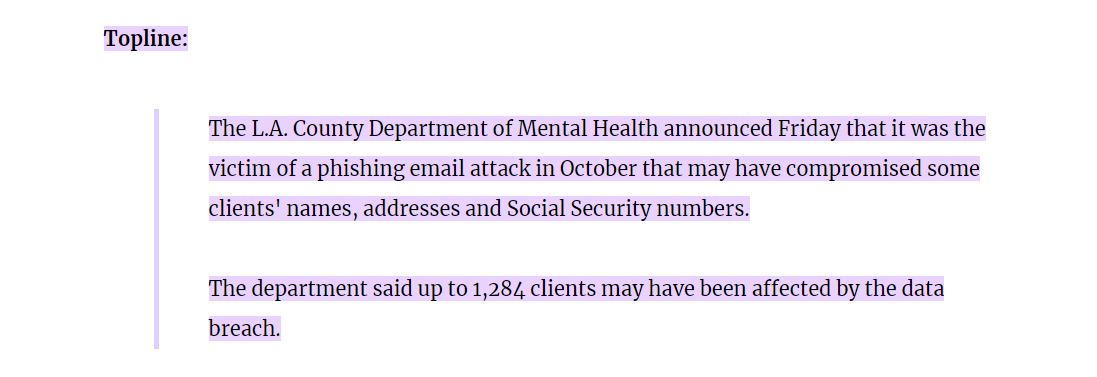
* During phase 4, Malware or backdoors often persist within the system even after the defender removes the initial file by **obfuscating themselves**, thus enabling the attacker to regain system access. (depends on the need of attacker)
* During phase 5, **Clearing tracks makes attacker invisible.**

**BREACHES HAPPENED TILL DATE AND LOSS OCCURRED**

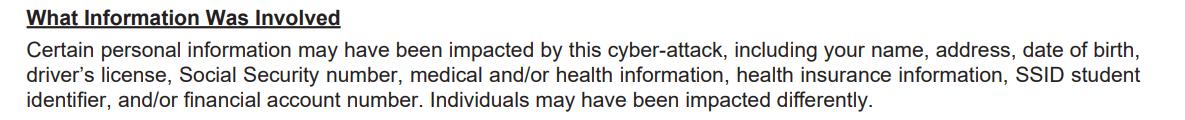
Both the organization are got affected for phishing email attacks

List of attacks happened in LA COUNTY

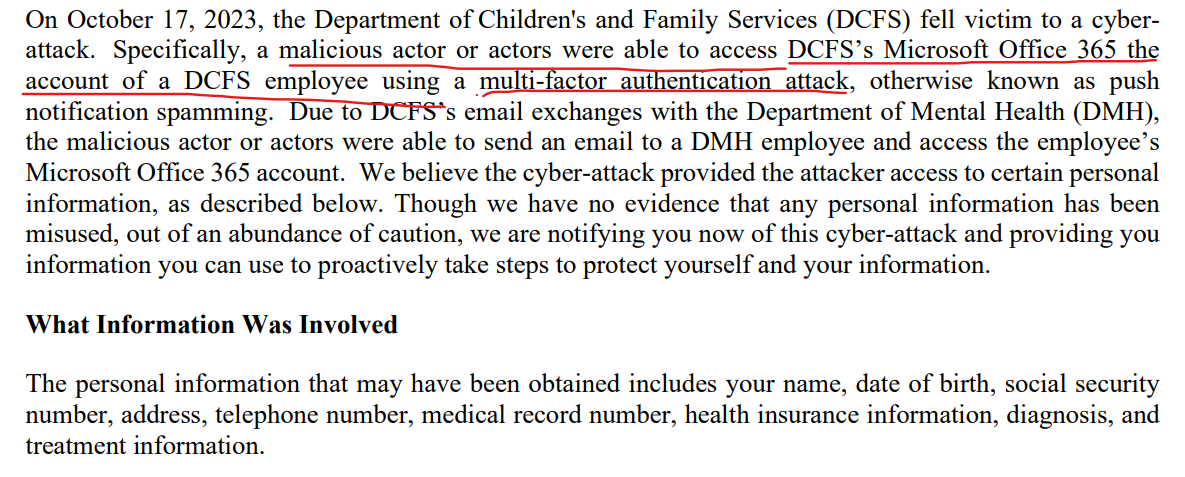
* From 2012 till 2024, there are huge scale of attacks on LA county has reported and also many attacks on health departments, The attack happened in 2024 nearly same as the attack happened in 2017 phishing email attack where SSN are compromised.

  
**2017 phishing email attack on LA COUNTY MENTAL HEALTH SERVICES**

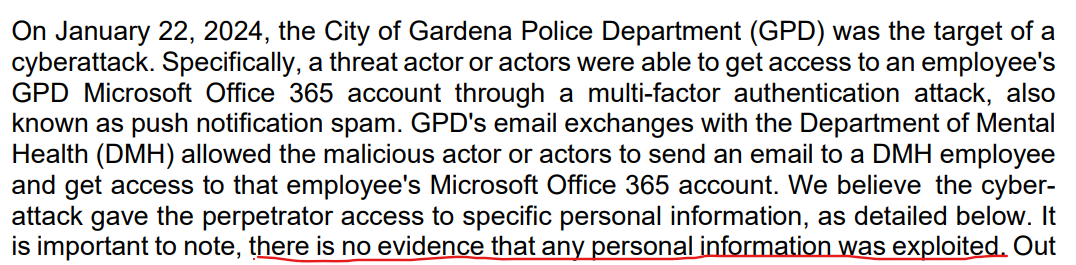
* No strategy changes and simultaneously no attack pattern change, in 2021 again phishing emails affected three DMH employee email accounts, but there is no evidence that the breached personal data is accused or misused.

  
**2021 phishing email attack on LA COUNTY MENTAL HEALTH SERVICES**

* In 2023, the Department of Children's and Family Services (DCFS) experienced a cyberattack. This attack involved a combination of techniques, including **MFA attack/Push notification attack/MFA phishing attack**. In this scenario, the attacker gained access to login credentials and exploited them in real-time. When a user attempted to log in, the attacker simultaneously used the stolen credentials and flooded the user's mobile device with fake or phishing messages, exploiting the chaos to trick the victim into clicking on a malicious authentication link.

  
**2023 MFA -> Phishing email attack on LA COUNTY MENTAL HEALTH SERVICES**

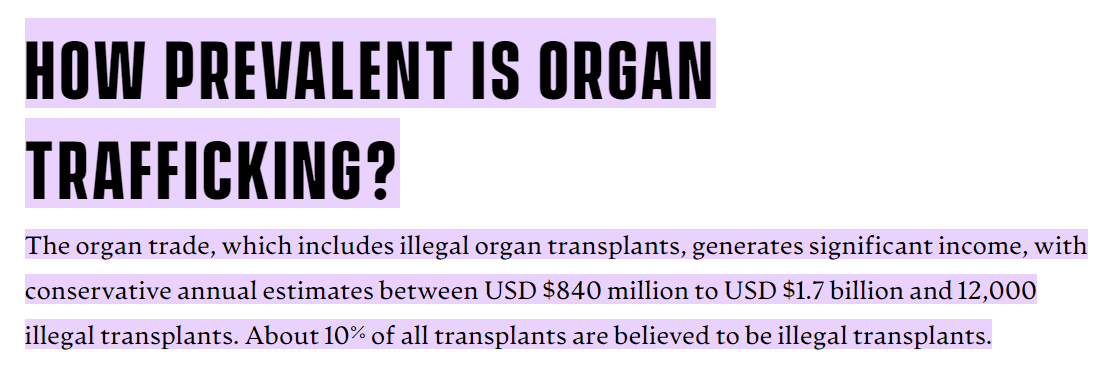
* In 2024, the victims/ zombies (DDOS language, zombies are malicious nodes that trigger attack on the target) are changes but the attack pattern is same as 2023 MFA attack.

**  
2024 MFA -> Phishing email attack on LA COUNTY MENTAL HEALTH SERVICES**

In this analysis, it's crucial to highlight several key conclusions.

* Firstly, **there's no evidence of immediate misuse of the breached information**. However, the nature of the data, particularly containing sensitive health records, patient information, addresses, phone numbers, and even Social Security Numbers (SSNs), raises significant concerns. **The likelihood of this data being unofficially circulated on the dark web is high.** This situation creates a serious risk, especially considering the potential for exploitation in activities such as organ trafficking.

The below data was taken from the internet

  
**Source: EXODUS ROAD**

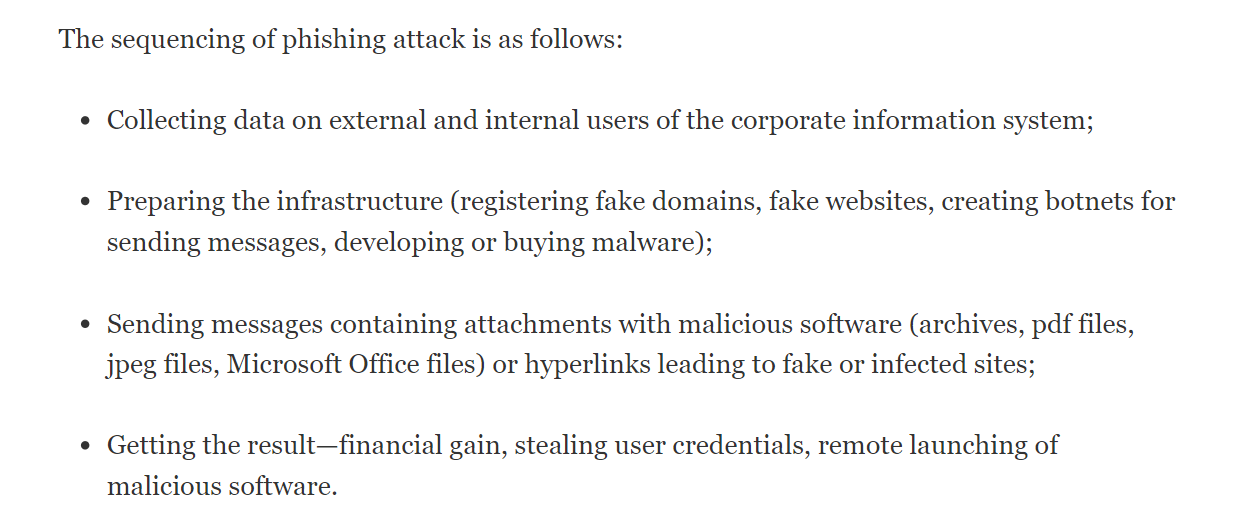
* Secondly, repeated breaches in public health services **erode patient trust,** leading to reluctance in sharing sensitive data. This loss of confidence undermines healthcare effectiveness and necessitates urgent improvements in cybersecurity and **transparent communication to rebuild trust.**

**REFERENCE PAPER SOLUTIONS**

PAPER 1: Ivanov, M. A., Kliuchnikova, B. V., Chugunkov, I. V., & Plaksina, A. M. (Year of publication). Phishing Attacks and Protection Against Them. Publisher: IEEE.

**Inference from the paper**: This paper states the different kinds of attacks on web applications especially types in phishing itself. There are types of phishing like spear phishing, vishing, smishing and as discussed in the attack scenario, attacker needs to do a lot of social engineering on the victim to use phishing techniques.

This paper also stated about clickjacking, classic clickjacking, crypto-jacking and many others. The common principle of phishing is to manipulate. Strategy of phishing according to this research paper



* **Email Attachments:** Phishing attackers often send emails with attachments containing keyloggers or ransomware. Ransomware, in particular, comes in two forms: blockers, which restrict access to data until a ransom is paid, and encryption-based ransomware, which encrypts data and demands payment for decryption. It's worth noting that despite paying the ransom, around **20% of victims are unable to recover their data according to Kaspersky labs.**
* **Malicious File Formats**: Phishers frequently utilize common file formats like PDF, Word, or Excel to deliver their malicious payloads. These files may contain embedded scripts, such as **Macro (VBS scripting)**, which can automatically execute functions like autorun (). This tactic often results in privilege escalation or denial-of-service attacks, effectively turning the victim's system into a "**zombie**."
* **Cloud Service Threats**: Phishing emails originating from cloud services like **Dropbox** pose a significant threat. Since cloud services are widely used and not easily stopped by standard antivirus scans, malicious emails containing forms and malware files can easily evade detection.
* **Banking Trojans**: Phishing emails may entice users to download banking Trojans, such as **Remote Access Trojans (RATs**). These trojans are designed to surreptitiously obtain banking information and personal data from the victim. **Notable examples include Dyre, Trick-Bot, Carbanak, Dridex, and Riltok.**
* **CSRF Attacks**: **CSRF attacks** exploit the trust a website has in a user's browser by tricking the user into executing unwanted actions while logged into the target website. This could result in unauthorized transactions, data theft, or other malicious activities.

**SOLUTIONS FROM THIS PAPER**

• Regularly update the software, including licensed antivirus software.

• Check the sender addresses and also verify the attachments; don’t run any executables from the mail unless we receive confirmation of legitimacy.

• Use two-factor authentication, including hardware tokens that generate a unique password for the current session.

• Malware can be obfuscated, so there is a chance of executables in .pdf, .jpg, .PNG, and other formats. Therefore, don’t click or download any attachment without a thorough idea.

• Backup important files.

• Double-check for confirmation if the email is from your friend; this may or may not be legitimate.

• Don’t call the phone numbers given in the attachments because this can lead you to “**VISHING**.”

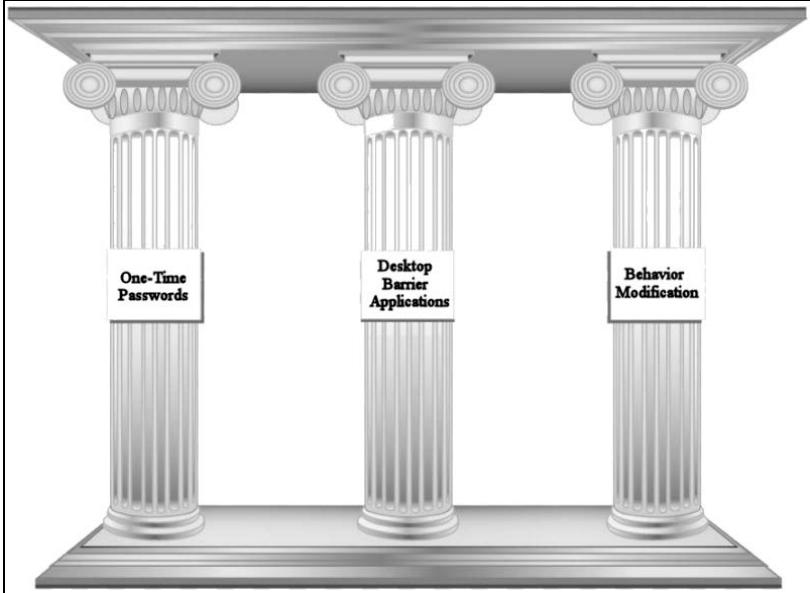
• Don’t reply to suspicious emails.

• If the email seems suspicious or the communication appears dubious, report it to cyber support or technical support but do not provide workplace data.

**Paper 2**: **Miller, B., Miller, K., Zhang, X., & Terwilliger, M. G. (Year of publication). Prevention of Phishing Attacks: A Three-Pillared Approach. Journal Name, Volume (Issue), page numbers.**

Inference from the paper: This paper gives us the “**THREE PILLARED APPROACHES**” for the phishing attacks

1. One-time password
2. Multi-level desktop barrier applications
3. Behaviour modification.

  
**3-PILLAR APPROACH**

* Initially, OTP is the first pillar. Upon entering the username and password, attackers can somehow use social engineering or brute force to gain access to the victim’s account. Thus, OTP can be one level of security that can be added, redirecting customers to another page for authentication. As mentioned earlier, this can be compromised by fake OTP traffic sent to the victim, where the attacker initially obtained the user credentials or due to late OTP entry leading to session expiry.
* Second pillar deals with multi-level desktop application.

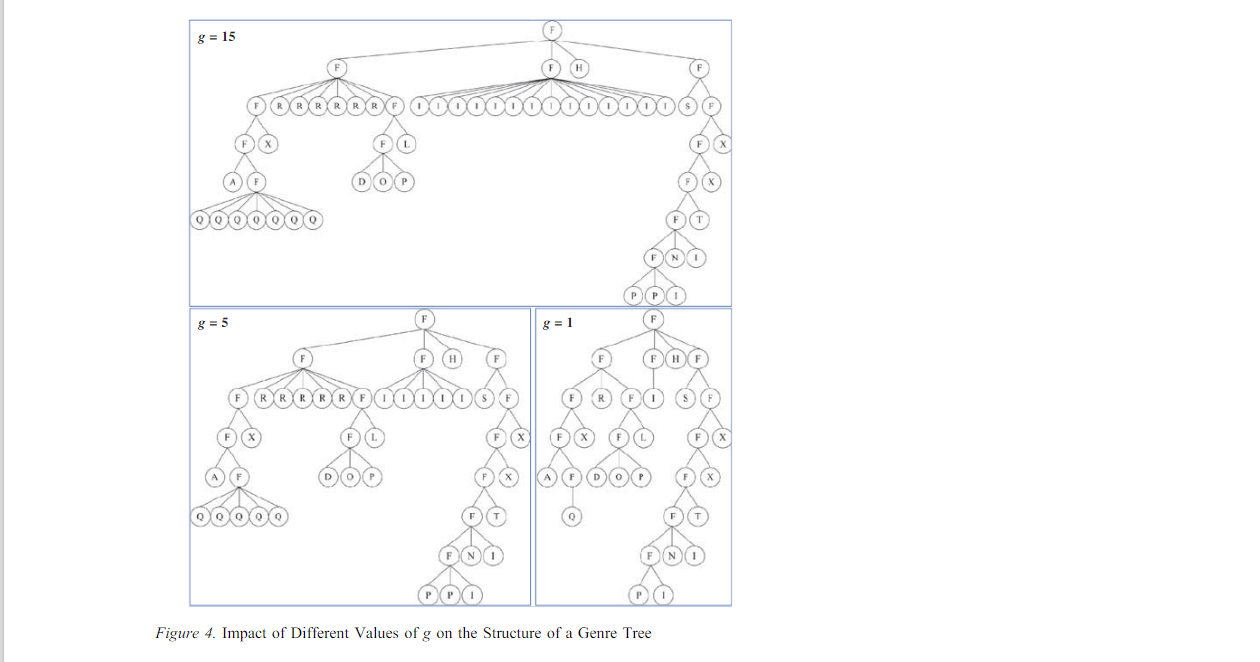
Kaur and Kalra (2016) propose a five-level desktop barrier application designed to prevent users from opening suspicious webpages. Phishers are motivated by recognition, monetary gain, or identity improvements (Kaur & Kalra, 2016).

In this application, there are several verification barriers in place. First, there is the **whitelist barrier**, which sorts out suspicious websites. Following this is the **text field barrier**, which alerts when an insert text field is found on the webpage. Next is the **anchor tag endorsement barrier**, which triggers an alarm if the login does not lead to expected pages such as login, sign-in, or sign-up, but instead to some other page. Then, there is the **null link barrier**, which prevents attackers from keeping the victim static on one website to gather more data. Finally, there is the **website identity barrier**, the final step where the verification of the website link occurs, checking how frequently the website redirects to the original page, as most phishing pages redirect to other malicious pages.

In this paper there is one point of stress, “**BEHAVIOR MODIFICATION**” this points out

* Most of the students rely more on the information on the internet, and there is no checking of legitimate nature of the information
* This finding suggests that women and individuals aged 18 to 25 are less likely to be suspicious of phishing attempts compared to other demographic groups. [**AGE FACTOR**]
* As mentioned earlier, employees or IT people need to know how typical phishing scams and also the typical signs, misspellings (typo squatting case), a high sense of urgency, threats, generic salutations or signatures, requests for personal or work-related information, phone numbers, company logos and many other.
* Concept of salting is found in phishing where the data and background of same colour, manipulating images and many others.
* Other concept is how phishing websites differ and these are types of websites and technique here using is **genre tree kernel.**



****

**Node structure (not completely analyzed)**

Upon, checking other mitigation techniques, there are other categories are:

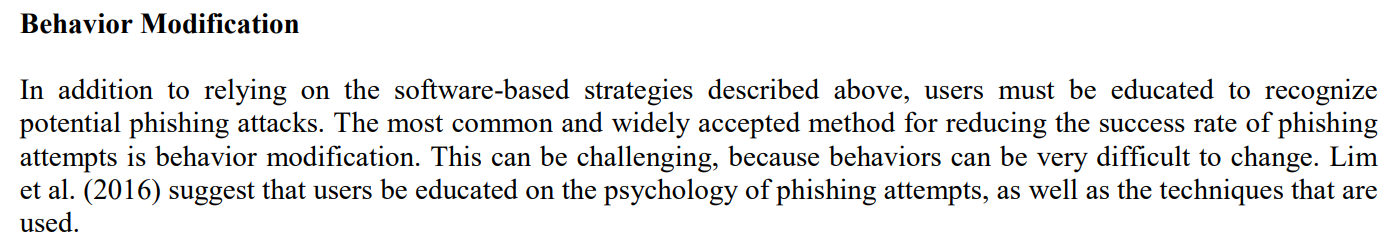
* Organizational which has policy, process control and awareness training.
* Technical include sandbox mechanisms and AAA (Authorization, accounting and authentication)

SOLUTION FROM TEAM

Upon **training the proxy servers which can be a count of n** (depends on the strength) where the traffic can be stopped using URL check, here we can focus on HTTP, TYPO-SQUATTING, also check the amount of traffic in the page which is one of the target points to check the status of the web application also this works with the emails and run the updated anti-virus (also updated defender)

**REFERENCES**

* <https://www.egress.com/blog/phishing/phishing-statistics-round-up#:~:text=Important%20phishing%20statistics%20for%202024&text=94%25%20of%20organizations%20were%20victims,suffered%20from%20account%20takeover%20attacks>.
* <https://pages.egress.com/whitepaper-email-risk-report-01-24.html>
* <https://www.ssa.gov/policy/docs/ssb/v69n2/v69n2p55.html#:~:text=Assigned%20at%20birth%2C%20the%20SSN,track%20an%20individual's%20financial%20information>.
* <https://www.infosectrain.com/blog/phases-of-ethical-hacking/>
* <https://dhs.lacounty.gov/public-and-media-relations/home/notice-of-data-breach/>
* <https://file.lacounty.gov/SDSInter/dmh/1153322_ProjectHoundPressRelease122223FINAL.pdf>
* <https://docs.apwg.org/reports/apwg_trends_report_q4_2023.pdf>
* <https://www.hipaajournal.com/mfa-bypased-cyberattack-la-county-department-mental-health/#:~:text=Los%20Angeles%20County%20Department%20of%20Mental%20Health&text=The%20cyber%20threat%20actors%20bypassed,that%20they%20will%20eventually%20respond>.
* <https://twitter.com/search?q=la%20county%20data%20breach&src=typed_query>
* <https://oag.ca.gov/privacy/databreach/list>
* <https://oag.ca.gov/privacy/databreach/list?field_sb24_org_name_value=Los+Angeles+County&field_sb24_breach_date_value%5Bmin%5D%5Bdate%5D=&field_sb24_breach_date_value%5Bmax%5D%5Bdate%5D=>
* <https://laist.com/brief/news/health/la-county-department-of-mental-health-announces-it-was-victim-of-cyberattack>
* <https://medium.com/@mehervardhan/not-ee-pad-hah-typo-squatting-40fb7a70e39a>

****

