CSAW CAC² Qualification Report

Team Mashers

Tiziano Caruana
Sapienza University of Rome
tizianocaruana@gmail.com

Ryan Shaikh Mohammed
Roma Tre University
ryan.shaikh03@gmail.com

***Abstract*—Despite increasing investments in cybersecurity and the pursuit of technical talent, the most effective attacks remain surprisingly simple. Phishing, through emails and SMS, continues to be the primary threat, affecting even newer generations. This persistent cycle demonstrates that even younger users are vulnerable to technically trivial yet easily scalable tactics. It is hence crucial to develop educational projects aimed at 'breaking the chain', informing the non-technical public before it's too late.**

We'd like to create a memorable and engaging visual experience using vibrant graphics for both posters and social media. By tapping into the power of surprise and cultural references, we want to leave a lasting impression on our audience.

***Index Terms*—Cyber Security Awareness; Phishing; Awareness Campaign; Digital Literacy;**

I. The Cybersecurity Threat Landscape

Cybersecurity is a constantly growing sector. More and more companies are investing increasing amounts of capital to defend themselves against digital attacks [1], more universities are offering courses to allow students to specialize in this field, and throughout all this, hackers continue to improve their techniques [2], automate their attacks, and search for 0-days[1] that allow them to discover profitable and widely replicable attacks [3].

The cost of a data breach is often unsustainable for companies [4], which may have difficulty finding qualified personnel [5] or affordable courses that are up to the dangers.

Many people, from movie fans to business owners, imagine cybersecurity as a dramatic battle where skilled hackers breach impenetrable corporate defenses using complex vulnerabilities.

But "reality is often disappointing": the most common cyber attack is phishing [6] (over 90% of attacks), an easily replicable attack that can be used even by technically unskilled cybercriminals [7], which makes us understand how the weak point of computer systems is the humans who use them. As Kevin Mitnick states, no matter how complex or trivial a system is, the human will almost always be the weak link in the system [8].

II. Understanding the Vulnerable Targets

When talking about social engineering and phishing[2], there are many types of attacks to analyze and discussions to open [9], but to stay within the scope of the Cybersecurity Awareness Communication Challenge, this report will focus on attacks that concern single individuals taken "randomly". In other words, we will leave out the types of attacks that have high-profile individuals as "targets", who may represent particularly appealing victims for social engineering attack [10].

According to private research, digital natives are the most likely to open phishing emails, in the 18-39 age range. One might imagine that this is due to a greater dependence of new generations on digital services, but in reality, this data has also been found when analyzing subjects who have been part of the same awareness campaigns and data collection. So, receiving emails and messages with the same content, the most sensitive age range remains the same [11].

In addition to this data, it's noted that more than half of internet users fall within the same age range [12]. It's then understood how important it is to warn this generation about the dangers that sharing information online can pose, or even simply being an active user of the network.

III. Identifying the Right Audience

While general awareness campaigns can be effective, we believe targeting specific demographics is crucial for addressing social engineering issues [13].

We have therefore tried to identify a fairly specific category of people who are highly likely to be users of social media, online forums, and/or frequenters of digital communities.

After navigating through a sea of data for a while, we found some interesting data: in the United States, more than 70% of anime viewers are under 35 years old, with numbers suggesting a significant increase in viewers in the coming years [14]. The numbers are less marked, but still surprising, for Europe [15]. In addition to this, it should be taken into account that many streaming services dedicated to anime also act as social media and that fandoms of this category of cartoons proliferate on the internet [16].

This group likely overlaps significantly with internet users, though specific research is lacking.

[1]Technical vulnerability typically unknown to the vendor and for which no patch or other fix is available.

[2]Social engineering is the broader term, referring to any psychological manipulation to trick someone into revealing confidential information or performing actions against their better judgment. In the case of a phishing attack, the attacker uses some form of messaging platform to send links, malicious attachments, or other types of deceptive, enticing, or threatening content to the recipient in order to get them to do the attacker's bidding.

The target audience for the awareness campaign is therefore defined as that of internet users and, even more specifically, that of young anime viewers under 35.

IV. Our Campaign Strategy

The idea of our team was to create graphics featuring some characters generally known in the target audience as icons or characters of interest.

It is important to use particularly famous characters that can attract the attention of people who may know them through general culture.

Using Japanese-style artwork in advertising is proven effective but not yet overused, offering a unique opportunity to engage the target audience with novel, inclusive content [17].

The graphics are suitable for use both in the form of posters and for posting on social media. Thanks to these graphics, if accompanied by appropriate descriptions, it would be possible to create new awareness pages on social media. However, we believe that the surprise effect would be even greater if a public and/or established institution were to propose the campaign, increasing the impact.

The posters can instead be attached in a less planned way, taking advantage of bulletin boards or, if allowed, walls of any public institution buildings such as schools, universities, hospitals, etc.

The use of awareness posters is among the most widespread types of ”cybersecurity training”, surpassed only by significantly more expensive alternatives [18].

The project's innovation is applying this communication method to raise cybersecurity awareness.

Italy has two excellent examples from this point of view. Two projects have been activated, one by AVIS FVG (Italian Blood Volunteer Association of the Friuli-Venezia Giulia region), and one by the Air Force.

Following the first, a ”notable recovery” in plasma donations was recorded, part of the focus of the awareness campaign, while during the second, the Air Force recorded a significant increase in views and, less markedly, in subscriptions to their information channel on air transport engineering.

The project would be easily implementable in both its branches. We are talking about minimal expense in case it was decided to use the graphics to create posters, and zero expense in the case of starting a social campaign (assuming that a person or team is already in charge of managing digital channels).

V. Project Summary and Implementation Strategy

To conclude the discussion as a whole, we define more clearly the strategy of our communication project:

- Create graphics suitable for social media posts containing awareness messages accompanied by famous characters from the world of Japanese animation;We're creating a memorable and engaging visual experience using vibrant graphics for both posters and social media. By tapping into the power of surprise and cultural references, we want to leave a lasting impression on our audience.
- Print posters to be attached to bulletin boards in educational institutions and places of interest for the 18-35 age group. Having even just one volunteer in every French university would mean potentially reaching almost 3 million students;
- Spread the message on social media channels of public institutions to increase surprise and thus impact on the audience. If this were not possible, establish an independent communication strategy based on creating social profiles specifically for the campaign;
- Measurement and evaluation. A critical point of the campaign, being a low-cost initiative;
  Regarding posters, surveys could be conducted in the places where they have been displayed, to estimate the number of people reached and how much the campaign has been noticed and appreciated. Questions could be asked such as ”What do you think was the main message of the campaign?” or ”Do you remember the behaviors that the campaign recommends adopting?” To increase the accuracy of responses and avoid self-exclusion of less interested subjects, it would be appropriate to conduct face-to-face surveys.
  For social media, comments, likes (which give an idea of how much the campaign has been appreciated) and views (the number of people who have been reached) are available;

We would aim to capture the target's attention through vivid colors and marked expressiveness of the characters. In doing so, we wouldn't keep the message in the background, delivering it with strong words and a cheerful font. This would create a sharp and ironic contrast, which we believe could leave a lasting impression on the viewer.

REFERENCES

[1] Statista, "Cybersecurity market size, share & trends analysis report by solution, by security type, by deployment, by enterprise size, by end-use, by region, and segment forecasts, 2022 - 2030." https://www.statista.com/outlook/tmo/cybersecurity/worldwide, 2024. Accessed: (2024-08-07).

[2] IEEE, "As hackers get smarter, cyber security experts turn to new ideas." https://innovationatwork.ieee.org/as-hackers-get-smarter-cyber-security-experts-turn-to-new-ideas/, 2020. Accessed: (2024-08-07).

[3] J. Greig, "Zero-days exploited in the wild jumped 50 Accessed: (2024-08-07).

[4] IBM, "Ibm report: Escalating data breach disruption pushes costs to new highs." https://newsroom.ibm.com/2024-07-30-ibm-report-escalating-data-breach-disruption-pushes-costs-to-new-highs, 2023. Accessed: (2024-08-09).

[5] M. Meineke, "The cybersecurity industry has an urgent talent shortage. here's how to plug the gap." https://www.weforum.org/agenda/2024/04/cybersecurity-industry-talent-shortage-new-report/, 2024. Accessed: (2024-08-09).

[6] S. Morrow, "Over 90 percent of cyber attacks begin with phishing." https://www.titanhq.com/phishing-protection/over-90-percent-cyber-attacks-begin-phishing. Accessed: (2024-08-07).

[7] L. Seltzer, "Phishing is still easy—and effective." https://ransomware.org/blog/phishing-is-still-easy-and-effective/, 2023. Accessed: (2024-08-09).

[8] K. Mitnick, *The Art of Deception*. John Wiley & Sons, 2002.

[9] E. Woollacott, "What is social engineering? types of attacks to beware of." https://www.forbes.com/sites/technology/article/what-is-social-engineering/, 2024. Accessed: (2024-08-09).

[10] IBM, "What is whale phishing?." https://www.ibm.com/topics/whale-phishing/, 2024. Accessed: (2024-08-09).

[11] SoSafe, "Digital natives more likely to open harmful phishing emails than their older colleagues." https://sosafe-awareness.com/company/press/digital-natives-more-likely-to-open-harmful-phishing-emails-than-their-older-colleagues/, 2022. Accessed: (2024-08-09).

[12] A. Petrosyan, "Distribution of internet users worldwide as of february 2024, by age group." https://www.statista.com/statistics/272365/age-distribution-of-internet-users-worldwide/, 2024. Accessed: (2024-08-09).

[13] EACEA, "Awareness raising campaigns for stakeholders' behavioural change." https://climate-adapt.eea.europa.eu/en/metadata/adaptation-options/awareness-campaigns-for-behavioural-change, 2023. Accessed: (2024-08-09).

[14] A. Eser, "Anime popularity in america - statistics & facts." https://worldmetrics.org/anime-popularity-in-america-statistics, 2024. Accessed: (2024-08-07).

[15] Statista, "Europe leads a new anime boom, but there's room for growth." http://www.ampereanalysis.com/insight/europe-leads-a-new-anime-boom-but-theres-room-for-growth, 2023. Accessed: (2024-08-07).

[16] Z. Ahmad, "Exploring the impact of social media on anime fandom: A study among university of ilorin undergraduates," *Journal of Global Business and Social Entrepreneurship*, 2024.

[17] Z. Ahmad, "The implementation of japanese animation (anime) in advertising," *Jurnal Indonesia Sosial Sains*, 2024.

[18] A. Borgeaud, "Cybersecurity training use among employees worldwide, by type." https://www.statista.com/statistics/1376495/cybersecurity-training-use-employees-worldwide-by-type, 2024. Accessed: (2024-08-07).