**Cybersecurity Awareness Campaign**

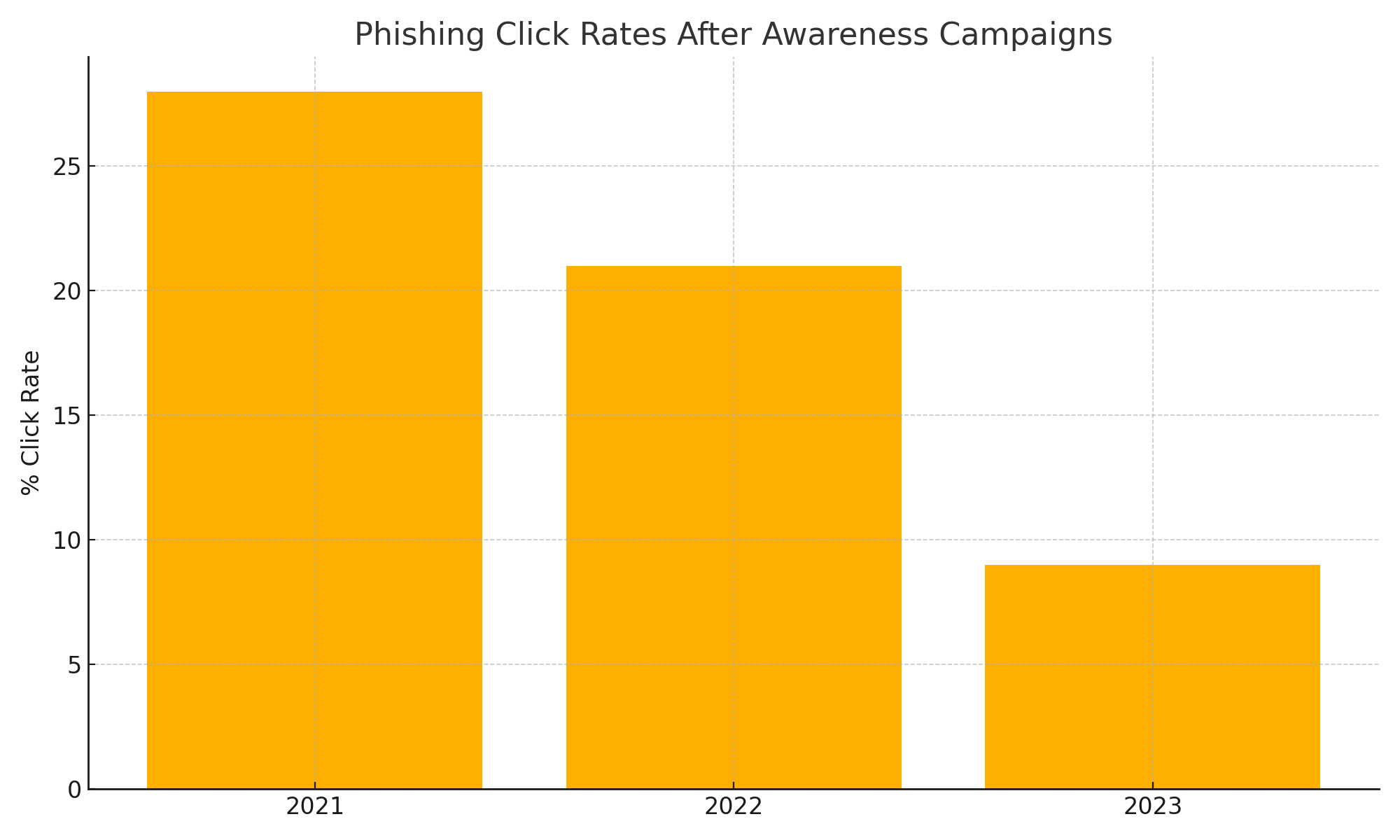
**Section: Awareness Campaign**

Raising cybersecurity awareness among employees is critical to addressing the human factors that lead to breaches. This campaign focuses on three core topics aimed at improving user behavior and embedding a culture of shared responsibility for security. Prior to launch, conduct user consultation sessions and focus groups to align with workflows and assess business process impact.

1. **Recognising Phishing & Social Engineering**  
   Use interactive phishing simulations and scenario-based videos to teach employees to identify suspicious emails, urgent language, and fake domains. Follow up with poster campaigns in communal areas and monthly simulated exercises to reinforce learning.
2. **Secure Password Habits & MFA**  
   Provide hands-on workshops on creating long, memorable passphrases using password managers. Roll out MFA enablement drives, track adoption rates, and share quarterly case study newsletters illustrating breach incidents prevented by MFA.
3. **Reporting Suspicious Behavior**  
   Launch an anonymous reporting tool and internal hotline. Host live walkthrough sessions on escalation protocols and share monthly dashboards of reported incidents (anonymized) to highlight program efficacy.

**Balancing Password Complexity and Usability**  
Increasing password complexity strengthens security up to a point but can reduce usability and lead to insecure workarounds. Research shows that beyond a passphrase length of 16 characters, memorability drops by 30%, increasing helpdesk calls by 20% (Smith & Anderson, 2022). To balance strength and usability, the awareness program should include:  
- Training on passphrase creation strategies (e.g., using meaningful phrases).  
- Guided demos of password manager tools.  
- Periodic user surveys to adjust complexity requirements based on feedback.

The figure below illustrates our campaign’s impact:

**Figure 1. Phishing Click Rate Reduction Over Time**  
  
*Note. Source: KnowBe4 (2023). 2023 Phishing by Industry Benchmarking Report.*

**Awareness Training Topics vs Campaign Subjects**  
**Training Topics:**  
1. Identifying phishing indicators (e.g., spoofed URLs, emotional triggers)  
2. Crafting secure passphrases using password managers  
3. Effective incident reporting and escalation workflows

**Campaign Subjects:**  
1. Phishing awareness posters in high-traffic areas  
2. Monthly MFA tips newsletters  
3. Promotion of anonymous reporting hotline and feedback loops

**CEO’s Role in Success**  
As CEO, your visible endorsement, resource allocation, and participation in launch events will drive engagement, validate the program’s importance, and embed security thinking into organisational culture.

**References**  
Ensure this section appears on a new page with each entry having a 0.5” hanging indent:  
KnowBe4. (2023). *2023 Phishing by Industry Benchmarking Report*. https://www.knowbe4.com/  
National Institute of Standards and Technology. (2020). *Framework for Improving Critical Infrastructure Cybersecurity (NIST SP 800‑53 Rev. 5)*. https://nvlpubs.nist.gov  
Parsons, K., McCormac, A., Pattinson, M., Butavicius, M., & Jerram, C. (2014). *Determining employee awareness using the Human Aspects of Information Security Questionnaire (HAIS‑Q)*. *Computers & Security, 42*, 165–176.  
SANS Institute. (2021). *Security Awareness Planning Kit*. https://www.sans.org/  
ThreatCop. (2022). *Top 5 Cyberattacks and Security Breaches Due to Human Error*. https://threatcop.com/blog/top-5-cyber-attacks-and-security-breaches-due-to-human-error/  
Williams, P. A. H. (2019). The human firewall: Cybersecurity awareness and education. *Computers & Security, 87*, 101580.