Designing an intervention for security fatigue in the corporate environment

Alexandra Neagu
5233194

February 18, 2024

1 Introduction

A challenge in user-centred security is the prevalence of "security fatigue" among users. Security fatigue refers to a state of weariness or reluctance that individuals experience when consistently confronted with security measures, such as passwords, two-factor authentication, and other security protocols. This phenomenon arises due to the increasing complexity and frequency of security-related tasks that users encounter in their daily digital interactions [2].

In today's interconnected world, individuals are bombarded with security measures across various digital platforms and services, ranging from personal email accounts to online banking systems. Users are required to create and remember multiple passwords, respond to authentication prompts (e.g., reCAPTCHA), and stay updated on the latest security practices. The overwhelming nature of these security requirements can lead to security fatigue, wherein users become apathetic or indifferent towards security protocols, potentially compromising their overall security posture.

This challenge is exacerbated by the fact that many users lack a comprehensive understanding of the potential risks associated with their digital activities [3]. Additionally, the constant need to update passwords and respond to security alerts can be time-consuming and mentally taxing, contributing to a decline in user compliance with recommended security practices.

Beyond its impact on daily digital interactions, security fatigue poses a more severe challenge in corporate work environments, where employees regularly engage with digital platforms like email systems, collaboration tools, and enterprise resource planning (ERP) systems [17]. The demand for heightened security is critical to safeguard sensitive company information, intellectual property, and client data. However, the constant barrage of security protocols can lead to fatigue and various security issues. Take the example of *multiplicity of credentials*, where employees managing multiple sets of credentials for various systems may succumb to password overload, increasing the risk of weak passwords or reuse [1]. Similarly, in *high-stakes information handling*, necessary security measures may be perceived as barriers, contributing to resistance and fatigue among employees dealing with confidential information. Additionally, the rise of *remote work* introduces challenges in ensuring secure behaviours without burdening employees accessing corporate networks from various locations and devices [14].

2 Background

In the intricate landscape of corporate work environments, the intersection of heightened security demands and the imperative for maximized productivity has given rise to a pivotal concern — security fatigue among employees. This weariness and reluctance toward stringent security measures disrupt the balance organizations strive to maintain. Delving into the background of this complex issue is essential for devising a deployable intervention design to address the profound issue of security fatigue in the corporate context.

As previously stated, the challenge organizations face regarding security fatigue is striking a balance between robust security measures and user-friendly practices, as they aim to safeguard sensitive information while maintaining optimal workflow efficiency. At the core of the security-productivity nexus lie the user costs, which encompass a spectrum of elements critical to the success of both security protocols and daily work tasks. These user costs are multifaceted and can be categorized into various dimensions, including cognitive, temporal, and emotional aspects.

Employees often grapple with the cognitive burden imposed by the multitude of credentials required to access various corporate systems. Remembering complex passwords, undergoing frequent authentication processes, and navigating through disparate security measures demand significant cognitive effort [9]. This cognitive load can lead to security fatigue, where users experience weariness and reluctance towards adhering to stringent security practices.

Time is a precious resource in any corporate setting, and the temporal costs associated with security measures can be substantial. From the time spent resetting passwords to responding to security alerts, employees may perceive security tasks as impediments to their daily workflow. Balancing the need for robust security with the necessity for time-efficient processes becomes a delicate challenge in the corporate context.

Security measures can also evoke a range of emotions among employees, from frustration and anxiety to indifference. The constant need to stay vigilant and the fear of unintentional security breaches contribute to emotional costs. Moreover, employees may feel overwhelmed by the responsibility of safeguarding sensitive information, especially in an era where cyber threats are ever-present [16].

Understanding the connections between user costs, the tasks users need to solve, and various contributory factors is essential to unravel the complexities that surround the problem of security fatigue in corporate environments. Revisiting the tasks introduced earlier, our focus now shifts to a comprehensive analysis of how these perceived user costs influence an individual's capability, opportunities, and motivation to execute these tasks. This examination is crucial in discerning the collective impact on the overall operational efficacy of a corporation.

Returning to the issue of *multiplicity of credentials and task dependencies*, employees managing multiple sets of credentials face a direct challenge in tasks requiring access to various corporate systems. This challenge arises due to contributory factors such as the decentralized nature of corporate systems and the array of tools used by different departments, amplifying the cognitive burden. The diversity of tools, essential for meeting specialized requirements, introduces complexity, resulting in a mosaic of credentials. This complexity not only obstructs initial access but pervades daily operations, impacting tasks from accessing collaborative platforms to retrieving crucial information. The cumulative effect is an increased cognitive burden that hampers the fluidity of work-related activities [4].

Cascading from issues of *high-stakes information handling*, as seen in the task

of retrieving information from databases, are deep-rooted emotional costs. Tied to tasks involving the access and management of sensitive data, these costs are driven by the fear of security mistakes and the emotional toll of safeguarding critical information [7]. Contributing factors include industry nature, regulatory requirements, and organizational culture surrounding data protection. In high-stakes sectors like finance, healthcare, or technology, where the gravity of information handling is amplified, employees experience heightened emotional pressure. The fear of compromising financial data, sensitive patient information, or proprietary technologies adds an extra layer of emotional burden to their daily tasks.

Lastly, it is important to consider that with the increasing prevalence of *remote work*, the temporal costs associated with security measures become more pronounced. Employees accessing corporate systems from various locations and devices face challenges related to the time required for authentication processes and the adaptation of security protocols to different work environments. Contributory factors include the need for seamless remote access, varying network conditions, and the diversity of devices used by employees [6].

2.1 User costs incurred by corporations in the context of security fatigue

The concept of security fatigue doesn't solely affect individual employees; rather, it permeates throughout the entire organizational structure, imposing tangible costs on corporations striving to maintain robust security postures.

Security fatigue elevates the risk of inadvertent security breaches as employees may exhibit a lack of attentiveness and diligence in adhering to security protocols. The organization faces heightened vulnerability to cyber threats, potentially leading to data breaches, intellectual property theft, or other malicious activities that could result in severe financial and reputational consequences. The costs associated with rebuilding trust among clients, partners, and stakeholders can be substantial, impacting the organization's brand equity and market standing.

As employees grapple with security fatigue, the cognitive and temporal costs associated with security measures contribute to diminished productivity. Increased time spent on authentication processes, password resets, and navigating through complex security protocols results in workflow disruptions, hindering the organization's efficiency and potentially impacting bottom-line results. This often leads to an uptick in IT support requests related to password resets, account lockouts, and user queries about security measures. The organization incurs additional costs associated with providing adequate support and resources to address these issues, diverting valuable IT resources from more strategic initiatives.

Security fatigue can contribute to overall employee dissatisfaction and burnout, impacting job satisfaction and potentially leading to increased turnover rates [13]. The costs associated with recruiting, onboarding, and training new employees can be substantial, making it imperative for organizations to address

security fatigue as a part of employee retention strategies.

To mitigate security fatigue, organizations must invest in continuous training programs to enhance employee awareness and cybersecurity literacy [15]. While a necessary investment, the costs associated with developing, implementing, and regularly updating such programs add to the financial burden on the organization.

In summary, the interconnected nature of user costs, tasks, and contributory factors in corporate security environments underscores the necessity of a targeted intervention to address security fatigue.

3 Intervention Design

To address the challenge of security fatigue in corporate work environments, we propose an intervention plan that integrates elements from existing intervention frameworks while introducing novel components tailored to the identified problem. Our intervention focuses on two key behavioural aspects: improving security awareness through adaptive security education and simplifying the authentication process.

3.1 Adaptive security education

Old behaviour: Employees currently undergo generic, one-size-fits-all security training, often detached from their specific roles and digital literacy levels. This approach contributes to a lack of engagement and fails to address individualized needs, fostering security fatigue [12].

New behaviour: The intervention proposes a shift towards adaptive security education that tailors content based on employees' roles, digital literacy, and historical security behaviours. Gamified learning modules, short videos, and interactive content will replace traditional training methods, making security education engaging and directly applicable to daily tasks [5].

By aligning security education with employees' unique needs and roles, the intervention reduces cognitive costs by delivering relevant information. Adaptive learning minimizes the time employees spend on training, addressing temporal costs too. This personalized approach also addresses emotional costs by fostering a sense of empowerment and relevance in security practices.

3.2 Streamlined authentication processes

Old behaviour: Employees currently grapple with managing multiple sets of credentials, leading to cognitive overload and temporal costs. Traditional password-based systems contribute to security fatigue and hinder seamless access to corporate systems.

New behaviour: The intervention advocates for the implementation of biometric authentication and single sign-on (SSO) solutions. Biometrics, such as

fingerprint or facial recognition, enhance security while simplifying the authentication process [11]. SSO reduces the number of credentials employees need to remember, streamlining access to various corporate systems.

This intervention directly tackles the multiplicity of credentials, reducing the cognitive load on employees. Biometric authentication enhances security without compromising user experience, and SSO minimizes temporal costs associated with frequent logins. The streamlined authentication process also aligns with the diverse devices used in remote work, addressing challenges posed by varying network conditions and device diversity.

3.3 Research gap

Existing intervention frameworks often focus on either security education or authentication methods independently. The intervention proposed in this paper uniquely combines these elements to address security fatigue more efficiently. The integration of adaptive security education and streamlined authentication processes creates a comprehensive approach that aligns with the identified user costs, tasks, and context of corporate work environments.

3.4 Critical changes and feasibility

Critical changes for the success of this intervention include an organizational commitment to adapting security training methods, investing in technology for biometric authentication, and implementing SSO solutions. Feasibility is supported by emerging technologies, increased awareness of user-centric security, and success stories from organizations adopting similar strategies.

3.5 Improvements and possible challenges

The proposed intervention aims to significantly enhance security behaviours within corporate work environments by addressing critical user costs.

The integration of adaptive security education customizes training content, reducing cognitive load linked to generic training. This ensures employees encounter only pertinent information, fostering a more focused and efficient learning experience. Simultaneously, streamlined authentication processes, including biometric authentication and single sign-on adoption, diminish cognitive and temporal costs tied to managing multiple credentials. This friction reduction in access procedures directly enhances daily task efficiency. The adaptive nature of security education, tailored to individual roles and digital literacy levels, ensures heightened user engagement. Employees are more likely to actively participate in training when it directly aligns with their responsibilities.

The holistic approach of the intervention extends beyond individual behaviour change to cultivate a security-aware culture within the organization. By instilling a sense of empowerment and relevance through adaptive security education, employees become active participants in the organization's security posture. The streamlined authentication processes reinforce the importance of

security without compromising user experience, contributing to a culture where security is perceived as an integral aspect of daily operations.

However, despite the promising improvements, several challenges may surface during the initial implementation of the intervention. Employees may exhibit resistance to the shift from traditional, one-size-fits-all security training to adaptive education. Resistance may stem from familiarity with existing processes, fear of the unknown, or perceptions of additional workload. Overcoming this resistance requires effective change management strategies, communication, and emphasizing the benefits of the new approach in terms of relevance and efficiency.

Implementing biometric authentication and single sign-on solutions introduces technical complexities related to integration with existing systems, compatibility with various devices, and ensuring a seamless user experience. These challenges necessitate careful planning, robust testing, and collaboration with IT departments to mitigate potential disruptions and ensure a smooth transition.

The dynamic nature of cybersecurity threats requires ongoing adaptation of security measures. The intervention may face challenges in keeping pace with emerging threats, necessitating a continuous improvement cycle. Regular updates to adaptive security education content and the agility to integrate new authentication technologies are essential to maintain the intervention's effectiveness over time.

3.6 Relating the intervention to the Fogg Behaviour Model

The proposed intervention framework aligns seamlessly with the Fogg Behavior Model [10], incorporating key elements of motivation, ability, and prompt to influence behaviour change in the context of security fatigue within corporate work environments.

Adaptive security education leverages personalized and role-specific content to enhance employees' **motivation** to engage with security practices. By aligning training with their specific needs and tasks, the intervention capitalizes on intrinsic motivators, making security education more compelling. Streamlined authentication processes, including biometric authentication and single sign-on solutions, significantly enhance the **ability** of employees to comply with security measures. These measures simplify the authentication process, reducing the cognitive load and making it more feasible for users to adopt secure behaviours.

The intervention identifies **opportune moments** within the corporate workflow to intervene. Adaptive security education can be seamlessly integrated into onboarding processes, ensuring that employees receive tailored training at the commencement of their roles. Implementation of streamlined authentication processes occurs during routine system access, minimizing disruption to daily tasks.

The Fogg Behavior Model emphasizes the importance of triggers or prompts to initiate behaviour change. Adaptive security education serves as a **trigger** by delivering relevant and engaging content at the right time, **sparking** employees' interest and motivation to learn. Streamlined authentication processes

act as **facilitators** by simplifying access to corporate systems, reducing the friction associated with multiple credentials and prompting secure behaviour. The introduction of biometric authentication and SSO solutions acts as a **signal** to users that the organization is committed to enhancing security while prioritizing user experience.

4 Deployment

To ensure the successful deployment and long-term effectiveness of the proposed intervention, a strategy for monitoring, maintenance, and ongoing adaptation is needed. This deployment plan is designed to align with the user costs and factors influencing secure behaviour, considering their potential evolution over time within the identified corporate context.

The primary target behaviour is the adoption of secure practices by employees. This encompasses actively engaging in adaptive security education, participating in training modules, and seamlessly embracing streamlined authentication processes. Success is defined by increased security awareness, reduced cognitive and temporal costs, and a measurable decrease in security-related incidents.

In the systematic deployment and monitoring of the proposed intervention, specific criteria and mechanisms have been established to assess its effectiveness and address potential challenges.

Firstly, the monitoring and observation criteria for *adaptive security education* involve a multi-faceted approach. Regular assessments of user engagement metrics, completion rates of training modules, and feedback on content relevance and effectiveness constitute the monitoring criteria. Observation criteria encompass increased participation in adaptive training, positive shifts in employees' security awareness, and a decrease in security-related incidents due to an improved understanding of security practices.

Similarly, for *streamlined authentication processes*, the monitoring criteria include tracking user adoption rates of biometric authentication and SSO, measuring the reduction in password-related support requests, and analyzing the time saved in authentication processes. Observation criteria involve the detection of a significant increase in user acceptance, reduced instances of password-related issues, and the establishment of a streamlined access experience.

A critical aspect of ensuring the long-term success of the intervention involves the consideration of evolving factors. Continuous monitoring mechanisms, such as regular surveys, focus groups, and feedback mechanisms, are in place to spot changes in user perceptions, cognitive load, and temporal costs over time. Furthermore, periodic reassessment of the intervention's alignment with evolving user needs, technological advancements, and emerging security threats allows for timely adjustments to maintain relevance.

The monitoring of the evolution of user costs and factors is essential for gauging the impact of the intervention on cognitive and temporal aspects. For cognitive costs, criteria involve a reduction in reported cognitive overload, im-

provement in users' ability to recall security practices, and a positive shift in the perception of security measures. This is monitored through regular surveys, user interviews, and analysis of support requests related to security education. In terms of temporal costs, criteria include a decrease in the time spent on authentication processes, a reduction in the number of password resets, and improved efficiency in daily tasks. Monitoring involves analyzing system logs, support ticket data, and periodic assessments of time spent on security-related activities.

Factors influencing the success or failure of the intervention are also closely monitored. Organizational commitment, a critical success factor, is assessed by actively monitoring leadership communication, resource allocation, and the inclusion of security metrics in organizational key performance indicators (KPIs). User involvement, another success factor, is monitored by assessing continuous engagement and feedback from end-users through regular surveys, focus groups, and a responsive feedback mechanism. Additionally, technological adaptation, a crucial success factor, is evaluated by regularly conducting technology assessments, security audits, and collaborating with IT departments to identify opportunities for improvement.

The intervention's effectiveness is ensured through vigilant review and adaptation mechanisms. Identifying signs for revisiting is paramount; a decrease in user engagement or non-compliance with authentication processes may indicate reassessment is needed. A surge in security incidents signals potential gaps in effectiveness. Obsolescence or incompatibility of technological components demands a revisit for ongoing relevance. Consistent negative feedback from end-users necessitates adjustments for enhanced satisfaction. Periodic reviews, assessing adaptive security education content, relevance to evolving roles, and emerging threats, drive ongoing improvement. Adaptations encompass updates to training modules, integration of new security practices, and alignment with technological advancements. User-centric assessments, involving continuous feedback and a flexible approach, ensure the intervention remains agile and responsive to evolving needs.

The robustness of this intervention is even further proven by drawing inspiration from comparable interventions successful in other domains. In healthcare, gamification employs interactive and personalized game elements to motivate patients and promote adherence to medical treatments [8]. Similarly, the adaptive training modules in the security intervention tailor content to individual roles and learning needs, creating a gamified learning experience designed to enhance user engagement. The success of gamification in healthcare serves as a pertinent example, reinforcing the versatility and effectiveness of adaptive strategies in influencing positive behaviour change.

In conclusion, the identified challenge of security fatigue in corporate work environments necessitated a user-centred intervention that addresses cognitive, temporal, and emotional costs associated with security practices. The proposed intervention combines adaptive security education and streamlined authentication processes, leveraging the Fogg Behavior Model to influence behaviour change. Through systematic deployment, careful monitoring, and collaboration

with stakeholders, the proposed intervention strives to create a secure and user-friendly corporate environment, mitigating security challenges and fostering a culture of proactive security awareness.

References

[1] Steven Furnell. "Authenticating ourselves: will we ever escape the password?" In: *Network Security* 2005.3 (2005), pp. 8–13. ISSN: 1353-4858. DOI: https://doi.org/10.1016/S1353-4858(05)00212-6. URL: https://www.sciencedirect.com/science/article/pii/S1353485805002126.

[2] Steven Furnell and Kerry-Lynn Thomson. "Recognising and addressing 'security fatigue'". In: *Computer Fraud Security* 2009.11 (2009), pp. 7–11. ISSN: 1361-3723. DOI: https://doi.org/10.1016/S1361-3723(09)70139-3. URL: https://www.sciencedirect.com/science/article/pii/S1361372309701393.

[3] Cormac Herley. "More is not the answer". In: *IEEE Security & Privacy* 12.1 (2013), pp. 14–19.

[4] M Angela Sasse et al. "The great authentication fatigue–and how to overcome it". In: *Cross-Cultural Design: 6th International Conference, CCD 2014, Held as Part of HCI International 2014, Heraklion, Crete, Greece, June 22-27, 2014. Proceedings 6*. Springer. 2014, pp. 228–239.

[5] Filomena Faiella and Maria Ricciardi. "Gamification and learning: a review of issues and research". In: *Journal of e-learning and knowledge society* 11.3 (2015).

[6] Malik Shahzad Kaleem Awan, Pete Burnap, and Omer Rana. "Identifying cyber risk hotspots: A framework for measuring temporal variance in computer network risk". In: *computers & security* 57 (2016), pp. 31–46.

[7] Mark A Geistfeld. "Protecting Confidential Information Entrusted to Others in Business Transactions: Data Breaches, Identity Theft, and Tort Liability". In: *DePaul L. Rev.* 66 (2016), p. 385.

[8] Daniel Johnson et al. "Gamification for health and wellbeing: A systematic review of the literature". In: *Internet interventions* 6 (2016), pp. 89–106.

[9] Marios Belk et al. "The interplay between humans, technology and user authentication: A cognitive processing perspective". In: *Computers in Human Behavior* 76 (2017), pp. 184–200.

[10] BJ Fogg. "Fogg behavior model". In: *URL: https://behaviormodel. org (visited on 12/14/2020)* (2019).

[11] Wencheng Yang et al. "Security and accuracy of fingerprint-based biometrics: A review". In: *Symmetry* 11.2 (2019), p. 141.

[12] Zheyu Tan et al. "Adaptive security awareness training using linked open data datasets". In: *Education and Information Technologies* 25 (2020), pp. 5235–5259.

[13] Hao Chen et al. "Understanding employees' adoption of the Bring-Your-Own-Device (BYOD): the roles of information security-related conflict and fatigue". In: *Journal of Enterprise Information Management* 34.3 (2021), pp. 770–792.

[14] Jason RC Nurse et al. "Remote working pre-and post-COVID-19: an analysis of new threats and risks to security and privacy". In: *HCI International 2021-Posters: 23rd HCI International Conference, HCII 2021, Virtual Event, July 24–29, 2021, Proceedings, Part III 23*. Springer. 2021, pp. 583–590.

[15] Zuopeng Zhang et al. "Cybersecurity awareness training programs: a cost–benefit analysis framework". In: *Industrial Management & Data Systems* 121.3 (2021), pp. 613–636.

[16] Jurgita Lapienytė. *25 million free VPN User Records exposed — Cybernews*. Nov. 2023. URL: https://cybernews.com/security/25-million-free-vpn-user-records-exposed/.

[17] URL: https://www.cloudflare.com/the-net/security-fatigue/.