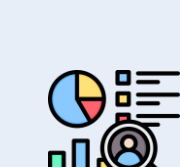
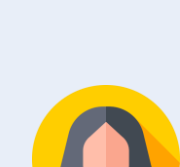


Introduction

- 

In 2022, 39% of all UK businesses identified a cyber attack against their own organisation.
- 

Cyber attacks can not only financially impact an organisation, but can cause the **theft of personal data**, affect critical **national infrastructure**, and have the potential to affect national **democratic processes**.
- 

Despite a great body of technological security research, the most common **vulnerability** remains individual **employees**, through attacks such as phishing and social engineering.
- 

Simulations and **games** are increasingly being deployed in organisations to **educate employees** in security training.

Background

- 

Inoculation Theory pre-exposes a participant to a weakened version of a persuasive argument to **increase resistance to disinformation**.
- 

Researchers have used inoculation theory in both **analog and digital games**, with participants yielding **positive results** identifying false information, and resisting “fake news.”
- 

Phishing attacks are often overlooked as a form of disinformation, and inoculation theory is yet to be utilised to help combat this.

Method

This research focusses on using an **inoculation theory** design approach and **Serious Game design** methods, to create the *disPHISHinformation* game.

To create an activity that is not only fulfilling and enjoyable but also assesses and delivers the ‘serious’ requirements, we have used the **Transformational Framework**.

Work by Aleroud et al. (2017), Rastenis et al. (2020), and Alabdan (2020) has been used to inform game content phishing features (see fig. 1), and a traditional game design process (informed by a focused assessment plan) is currently underway to create an effective prototype.

The Transformational Framework

The **Transformational Framework** is an effective **requirements gathering** approach for Serious Games. As a process, the framework outlines 8 key elements to be considered before the production phase of your game. These elements have been condensed and summarised below.

High-level Purpose

To create a physical gamified activity to deliver phishing training to employees that is more memorable and impactful than traditional approaches.

Audience & Context

All audiences in a professional working environment. This approach should not discriminate players who are not familiar with games or gamification.

Player Transformations

To not only raise security awareness for employees, but train skills in identifying distinct malicious features in phishing attacks.

Barriers

Security training is often seen as unengaging, tedious, ‘required’ training. When done effectively, gamified approaches can break these stereotypical barriers.

Prior Works

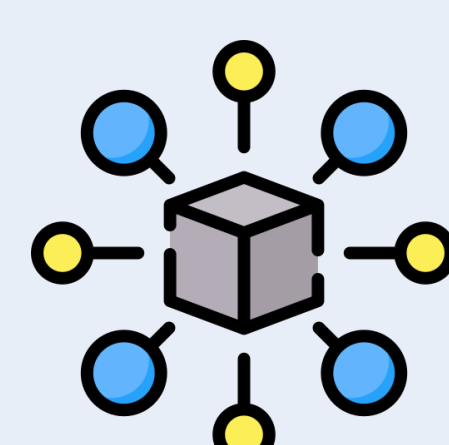
Simulations and games are increasingly being used in organisations for training. Solutions such as Decisions and Disruptions (Frey et al. 2019) and [dox3d!] (Gondree et al. 2013) raise awareness, but do not deliver training policy content.

Expert Resources

Research by Aleroud et al. (2017), Rastenis et al. (2020), and Alabdan (2020) has informed the types and format of content in this initial prototype of the disPHISHinformation game. See figure 1. for further details.

Domain Concepts

The disPHISHinformation game includes concepts from both traditional phishing, vishing and smishing. State-of-the-art attacks such as automated messages and QR codes have also been considered.



EARLY-STAGE PROJECT

The Phishing Game: An Analog Game To Defend UK Organisations From Phishing

Inoculation Theory in Game Design

Inoculation theory has recently been increasingly used in combination with active learning concepts to fight misinformation (Basol et al. 2021, Roozenbeek et al. 2019). Despite these multimedia approaches, there has been little discussion on how inoculation theory can be translated into game design features.

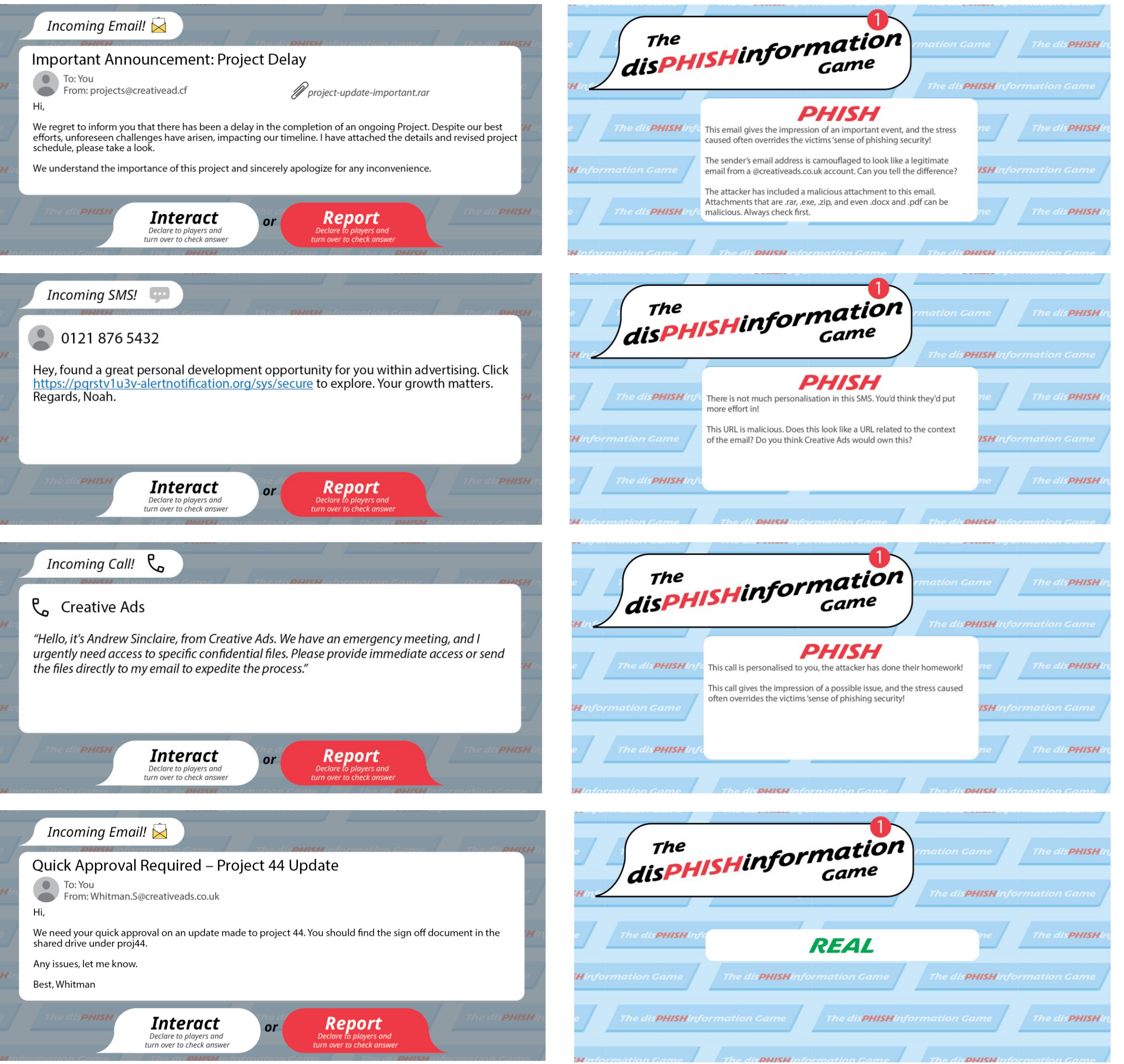
Three core elements to inoculation theory are threat, counterargument, and refutation. These three elements have been incorporated through game mechanics, content, and woven into the game narrative.



The game design is centred around phishing, vishing, and smishing attacks that are sent to players. A variety of different types of attacks (using taxonomies by Aleroud et al. (2017), Rastenis et al. (2020), and Alabdan (2020)) simulates content commonly observed by SMEs. Game content is distributed from a catalogue of different phishing features. These can be seen in fig. 1.

Attack Platforms	Attack Presented as:	Sender's Email/Number	Attack Type
Phishing	Benefit for Recipient	Owned	Behavioural
Smishing	"legitimate" request	Camouflaged	Shortened URL
Vishing	Important information	Hacked legitimate	Bad domain name
	Possible failure		Hostname obfuscation
			Encoded URL obfuscation
			Malicious Attachment

Figure 1: Catalogue of phishing attack features from which game content is sourced.



References

Aleroud, A., & Zhou, L. (2017). *Phishing Environments, Techniques, and Countermeasures: A Survey*.
Rastenis, J., & Ramanauskaite, S. (2020). *E-mail-Based Phishing Attack Taxonomy*.
Alabdan, R. (2020). *Phishing attacks survey: Types, vectors, and technical approaches*.
Basol, M., Roozenbeek, J., Berriche, M., Uenal, F., McClanahan, W. P., & Linden, S. van der. (2021). *Towards psychological herd immunity: Cross-cultural evidence for two prebunking interventions against COVID-19 misinformation*.
Roozenbeek, J., & van der Linden, S. (2019). *Fake news game confers psychological resistance against online misinformation*.
Frey, S., Rashid, A., Anthonyamy, P., Pinto-Albuquerque, M., & Naqvi, S. A. (2019). *The Good, the Bad and the Ugly: A Study of Security Decisions in a Cyber-Physical Systems Game*.
Gondree, M., & Peterson, Z. N. J. (2013). *Valuing Security by Getting [dox3d!] Experiences with a network security board game*.

Poster icons from Flaticon (icon:author). Pie chart: Pixel perfect, research: Uniconlabs, avatar: Freepik, vaccine: Freepik, gamepad: Stockio, spam: Freepik, structure: Freepik.



Niklas Henderson
Postgraduate Researcher
University of East Anglia
N.Henderson@uea.ac.uk
[@14hendersonn](https://twitter.com/14hendersonn)

