Creative Brief

Proposer: Dr Lynsay Shepherd, Abertay University.

Concept: Gone Phishing

Phishing emails generally attempt to persuade recipients to reveal private or confidential information such as passwords or bank details, placing users at risk of identity theft, and significant financial loss. In Britain alone, users have lost millions of pounds to scams and phishing attacks. Since the beginning of the COVID-19 pandemic, incidences of cyberattacks and cybercrime have increased considerably, including a sharp rise in phishing attempts.

'Gone Phishing' seeks to raise awareness of how to spot phishing emails and explores the devastating consequences these emails can have on the victim, in terms of monetary and emotional impact. The game should be aimed at the general public (adults 18+). Scenarios included must be informed by trusted academic sources.

Purpose:

Modern society depends upon the Internet, allowing users access to online services such as social networks, banking applications, and e-commerce websites. However, the Internet is also used by cybercriminals looking to exploit vulnerable users. Successful phishing scams can be costly for victims, both in terms of monetary and emotional damage. Following the onset of the COVID-19 pandemic there has been a massive rise in cybercrime. The most common type of fraudulent behaviour online over the last 18 months has been phishing, which has risen by 600% worldwide.

To combat phishing attempts, email clients make use of spam filters to quarantine suspicious emails. However, these filters are not always successful; consequently, users require additional assistance to help them detect phishing emails in the form of anti-phishing tools and security education.

To ensure users behave in a safe and secure manner online, it is important for them to have an understanding of basic security measures. However, users often do not know how to make their online interactions secure.

Thus, the purpose of the project is two-fold:

- Educate users on the dangers of phishing emails, and how to spot features of phishing emails.
- Improve cybersecurity awareness and help users engage in secure interactions.

Audiences:

The prototype game must be accessible and must not require any prior knowledge of cybersecurity or techniques for spotting phishing emails.

The target audiences are:

- Adults over the age of 18 who wish to improve their security awareness.
- Researchers focussing on the human aspects of cybersecurity.

The prototype should be accessible via the web, and work on desktop, tablets, and mobile devices. This will be used for educational and research purposes.

Deliverables Needed:

- A playable game prototype which is accessible via the web
- Project documentation, including a manual for the game

Influences/Tone/Image:

Much of the existing material designed to educate users about phishing is composed of simple text-based websites. Whilst these websites contain a wealth of informative content, they are not engaging.

There are several existing games which have been used to help educate users about phishing such as Anti-Phishing Phil which is limited in functionality (https://dl.acm.org/doi/pdf/10.1145/1280680.1280692) and Phishy (https://dl.acm.org/doi/pdf/10.1145/3270316.3273042), which is geared towards enterprise users and focuses on phishing websites rather than phishing emails.

The tone of ‘Gone Phishing’ is open to interpretation and creative approaches are encouraged.