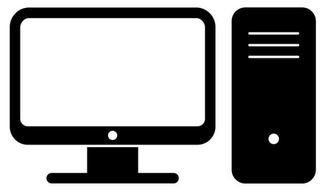
Natasha Churchill (s4901667)

An Approach for Creating a Contextual Cyber Security Awareness for Tourism

Overview

In the travel industry there has been a shift in how holidays are booked with the number of holidays now being booked online. This shift has led to holidaymakers falling for online holiday booking while navigating the online booking process.



In 2017, 83% of holidays were booked online (ABTA, 2018)

Types of holiday booking fraud:

- Fake / misleading marketplace listings
- Fake booking websites
- Fake emails relating to the booking of a travel product
- Fraudulent social media adverts and pages

An Approach for Creating a Contextual Cyber Security Awareness for Tourism was created to reduce the number of holidaymakers falling for holiday booking fraud in the tourism industry. It can be used by holiday providers and other entities to provide measures for holidaymakers and holiday providers to follow, and should be more effective than current solutions (National Institute of Standards and Technology, 2018).

Objectives

- Review current threat landscape of the tourism industry by performing threat analysis and impact assessment
- Identify requirements of approach by reviewing the threat landscape
- Design and implement an approach which identifies and responds to holiday booking fraud
- Test and evaluate the approach to identify if the approach is fit for purpose

Background

Holidaymakers vulnerability

Drawn to cheap deals

Naivety due to lack of knowledge

Sophisticated attack methods

Internet provides anonymity to its users

Social engineering and phishing techniques (Jagatic et al. 2007)

Current solutions

Fail to reach target audience

Only basic and general tips provided (ABTA, n.d.)

Prosecution and jurisdiction issues

Methodology

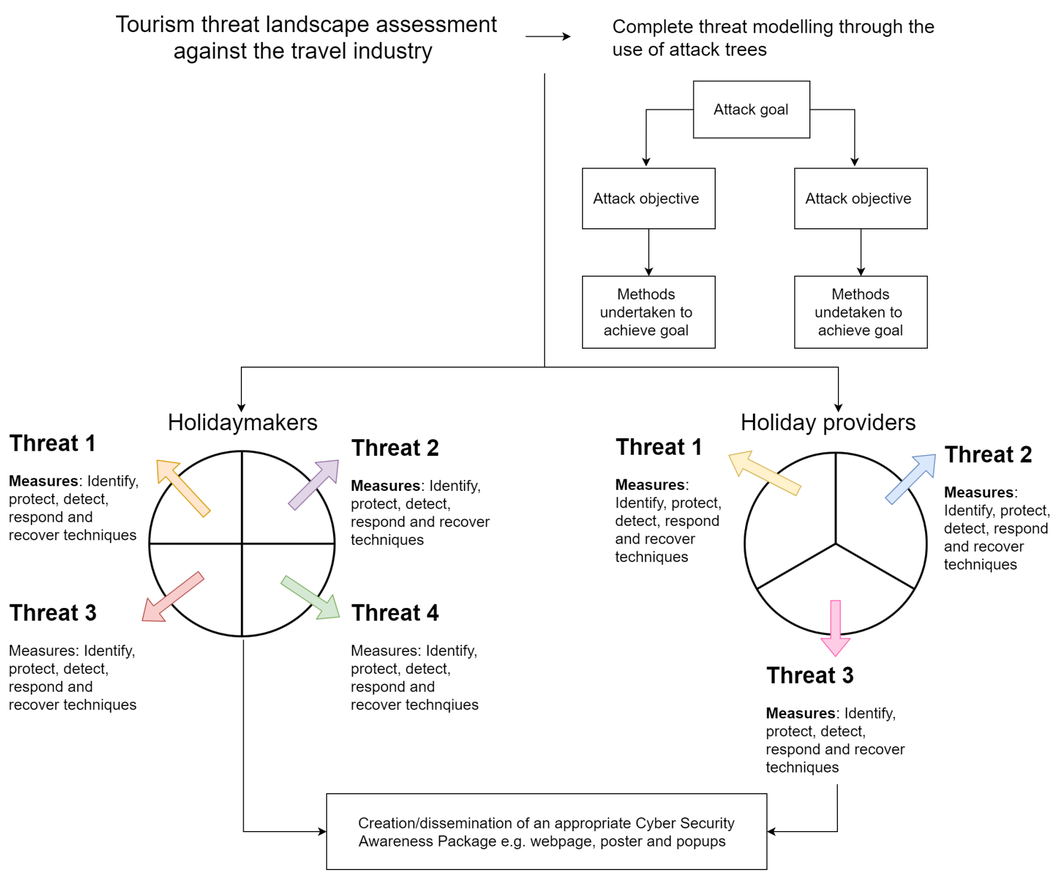
- Undertake a threat landscape to understand the threats, actors and victims within the tourism industry
- A threat landscape was performed using mixed research methods allowing benefits of both quantitative and qualitative to be utilised
- Primary research was undertaken to evaluate first hand how holidaymakers and holiday providers view and are impacted by holiday booking fraud, along with a review of current solutions
- Requirements identified through the background study and primary research were categorised using MoSCoW so important requirements are meet
- To evaluate the approach, a Cyber Security Awareness Package was created using the approach and tested through a usability test to ensure the approach meets the requirements and provides an effective solution

Proposed Solution

Tourism threat landscape assessment:
Undertaken to identify the threats, trends and vulnerable assets which occur throughout the holiday booking process relating to the holidaymaker falling for holiday booking fraud, through the use of attack trees

NIST framework application:
Holidaymaker and holiday provider threats identified in the holiday booking process are applied to the NIST framework, to identify measures which will reduce the occurrence and impact of holiday booking fraud

Creation/dissemination of an Appropriate Cyber Security Awareness Package:
Once the threats and mitigation measures for holidaymakers and holiday providers have been completed, the information needs to be outputted through the development of a Cyber Security Awareness Package to allow the information to reach its designated target audience



References

ABTA, n.d. *How to avoid travel-related fraud* [online]. London: ABTA Ltd. Available from: https://www.abta.com/tips-and-advice/planning-and-booking-a-holiday/how-avoid-travel-related-fraud [Accessed 29 Oct. 2019].
ABTA, 2018. *Holiday Habits Report 2018* [online]. London: ABTA Ltd.
Jagatic, T., Johnson, N., Jakobsson, M. and Filippo, F. (2007). Social Phishing. *Communications of the ACM*, 50(10).
National Institute of Standards and Technology, 2018. *Framework for Improving Critical Infrastructure Cybersecurity*. Maryland: National Institute of Standards and Technology.