Interview on cyber security awareness

By Rick van Bottenburg

# Introduction

This document details an interview held with cyber security teacher Igor Burger. The purpose of this interview is to confirm previous information found, and to answer the following research question:

*What kind of topics does cyber security awareness encompass, and which of them will be in the game?*

Do you give permission for the interviewer to record audio for the purpose of future reference, where the audio will only be shared with the assessors? Y/N, by:

# Questions

* Can you give a general description of cyber security awareness?

(zie doc)

* What do you think are bigger threats in cyber security, that can be fixed with good awareness? Can you give me the consequences? (follow-up: phishing is popular, but can you give other examples maybe not so well-known?)

Your data can be exposed by hackers and stolen, and they can coerce you to buy it back, or sold to others  
Your data can be locked by ransomware, and if you don’t pay, it may be deleted. (cryptolocker, encrypts your files by opening a file and asking for permission)  
Social engineering  
Becomes more advanced, they get more data about you (like from the hacked companies in the news), and they threaten you with something. (things are getting more difficult)

* What do you think are certain pitfalls that people fall into?   
  Scaring, urgency by coercion, they make use of money and personal data
* Can you think of any guidelines people should follow to avoid being compromised?

(zie doc), domeinnaam is anders, spelfouten (maar dit is niet langer zo), mail zorgt voor urgentie, bank stuurt nooit mails, vragen om op een link of bijlage te klikken, bijlage kan verborgen worden, don’t have images in mails  
Hoe word je aangesproken in een mail? (wordt gegenereerd, dus soms zitten daar fouten in.) Kijk naar de warning boven de mail. Hover with mouse over link to see.

Niet je naam zeggen bij iemand die je niet kent

* What should you do if you are compromised?

Contact bank, for cryptolocker, turn off the pc immediately. Look online if there is a key for the specific cryptolocker; the police tries to crack them  
otherwise, look for snapshots  
(idea, like bomb defusal game you look online for the key)

# Conclusion