

Cyber Security Awareness Campaigns

Why do they fail to change behaviour?

Introduction

- ↗ Information and Communications Technologies → need for cyber security
- ↙ people do not follow
 - ↗ not aware
 - ↘ do not understand

Cyber security awareness try to influence the adoption of secure behaviour online
→ simply informing is not enough:

- (1) accept that it is relevant to them
 - (2) understand how they are supposed to respond
 - (3) willing to do what is necessary in the face of other demands
- Why is changing cyber security behaviour such a challenge

Cyber Security Awareness Campaigns

- awareness and training programs are crucial, since they carry the information to all users (security requirements and appropriate behaviour)
- needs to be **interesting**, **current** and **simple** in order to effective

“Awareness is not training. The purpose of awareness presentations is simply to focus attention on security. Awareness presentations are intended to allow individuals to recognize IT security concerns and respond accordingly” NIST Special Publication 800-16

Cyber Security Awareness Campaigns

- reason for attacks:
 - hackers are becoming more skilled
 - security interfaces are often too difficult for layman
 - know answers to awareness questions but do not act like it

→ System needs to be understandable and easy to use in order for people to follow it

cyber security awareness as conceived today is not working

Psychological perspective

Factors influencing change in behaviour:

- the messenger
- incentives
- norms
- defaults
- salience
- priming
- affect
- commitments
- ego

Personal factors:

- people disregard security procedures if they perceive them as obstacle

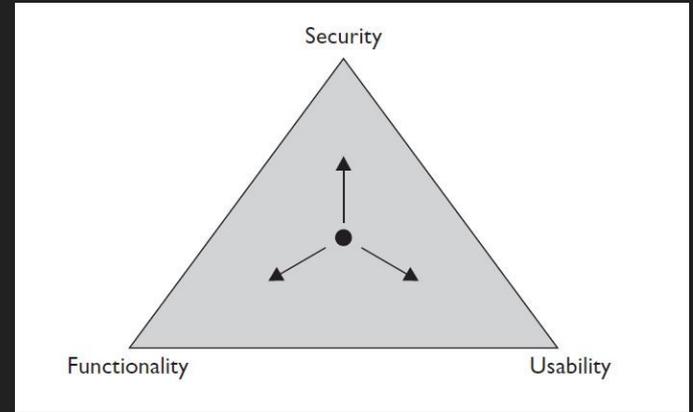
Cultural factors:

individual cultures

- defined by internal attributes (goals, attitudes)
- focus on benefits and positive outcomes

collective cultures

- avoid behaviors that might cause social disruption
- focus on prevention of negative outcomes



Persuasion techniques

- fear
- humour
- expertise
- repetition
- intensity
- scientific evidence

→ persuasion tactics need to be carefully chosen to fit specific situations and target groups

Factors leading to success or failure of cyber security awareness campaign

1. Communication
2. Pitfalls
 - a. not understanding what security awareness really is
 - b. lack of engaging and appropriate materials
 - c. no assessment of the awareness programmes
3. Cultural differences
4. Measuring can be a very complicated process

Cyber security awareness campaigns in the UK (Case Study)

A. The GetSafeOnline Campaign:

- a. jointly-funded by government & private sector
- b. focuses on users at home & in businesses
- c. offers a comprehensive repository of information on threats and how-to advice for protection.

B. The Cyber Streetwise Campaign:

- a. users at home and in businesses
- b. Five basic measures for businesses to boost security
- c. uses positive message to influence the behaviour of users "In short, the weakest links in the cyber security chain are you and me".

Cyber security awareness campaigns in Africa (Case Study)

A. The ISC Africa:

- a. industry and community-wide effort to inform and educate
- b. safe and responsible use of computers and the internet
- c. positive message with collectivist approach *“Working together to ensure a safe online environment for all”*

B. Parents Corner Campaign:

- a. coordinate work of government, industry and civil society
- b. protect children, empower parents, educate children, create partnerships among Shareholders
- c. message with social group approach *‘People aren’t always who they say they are, Think before you post, Just as they would in real life - friends must protect friends’*

Compare Campaigns in the UK & Campaigns in Africa

What do they have in common ?

- They both reflect the cultural aspects
- Both do not offer the possibility of a help-line

What is different ?

- The UK studies = individualist approach
- The African studies = collectivist approach

Suggested factors to enhance the effectiveness of current and future campaigns (Conclusions)

1. Security awareness has to be professionally prepared and organised in order to work
2. Invoking fear in people is not an effective tactic, since it could scare people who can least afford to take risks
3. Security education has to be more than providing information to users – it needs to be targeted, actionable, doable and provide feedback
4. Once people are willing to change, training and continuous feedback is needed to sustain them through the change period
5. Emphasis is necessary on different cultural contexts and characteristics when creating cyber security- awareness campaigns