

# INFO2222

**Computing 2 Usability and Security**

Week 2: Analysis

# Week 2 – Analysis

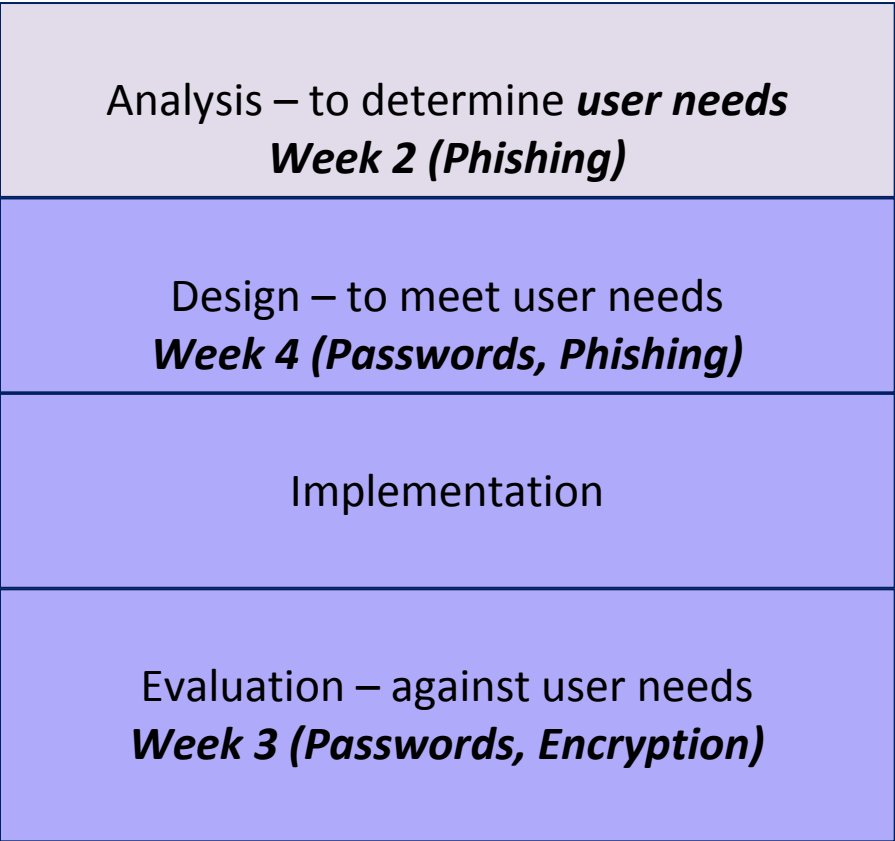
- [Brief discussion of Mini-Assignment 1]
- How can we take a **Soft Systems Method (SSM)** to identify the broad foundation for determining user needs?
- What are the three key methods for **learning about user needs and preferences**, taking account of their context?
- Explain how **high level user goals** come from studies of user needs.
- What is a **persona**?
- Explain how **high level user goals** are refined into **detailed tasks** - to drive the design (Week 4) and evaluation (Week 3) of interfaces.
- How do **mental models** link to user needs studies?

Where does this fit into the  
semester big picture?



People:  
Psychology  
Physiology  
Context

**Week 5**



Privacy  
Integrated  
Case study  
**Week 6**

All the key ideas will be illustrated in  
terms of the Assignment 1 problem

.... phishing

# Preliminary class activity

**Based on the mini-assignments**

# Sharing the mini-assignment

(more to come on this in the lab)

- Work in groups of 2-3
  - Show your homework to the others in your group
  - Discuss similarities and differences in security concerns you identified
- We will then consider some of lists others have made ...

# The 4 Top Security Concerns On The Minds Of Millennials

Larry Alton, Dec 26, 2017, Forbes

- The security of cloud service providers
- Personal passwords and account management
  - “ [4 percent of millennials](#) use between 3 and 5 distinct passwords for their accounts, rather than one, and they’re the generation who uses two-factor authentication the most, at 40.4 percent.”
- **Awareness and education of current threats.**
  - “Millennials would rather learn about current threats, and increase their knowledge, than work blindly, and they seek more education and training because of it.”
- External trust.
  - .... Putting their faith in major brands

Assignment 1 is all about helping users do this



# 5 information security threats that will dominate 2018

By [Thor Olavsrud](#), Senior Writer, CIO | Nov 20, 2017

About the Information Security Forum (ISF), a global, independent information security body that focuses on cyber security and information risk management

- **Crime-as-a-service**
- **The IoT**
- **Supply chain (e.g. Target)**
- **Regulation**
- **Unmet board expectations**

# Top Online Threats To Your Cybersecurity And How To Deal With Them

Forbes, April, 2017, [R.L. Adams](#), Contributor ,

#1 – Ransomware

**#2 -- Phishing schemes**

#3 -- Man-in-the-middle (MIIM) attacks

#4 -- Ad fraud

#5 -- Social media schemes

#6 -- Bitcoin scams

**#7 -- Social engineering**

#8 -- Targeting employees to compromise corporate networks

#9 -- Tracking movements for physical targeting

#10 -- Customer service interception

Assignment 1 is all about phishing and social engineering

How can we take a **Soft Systems Method (SSM)** to identify the broad foundation for determining user needs?

This is the foundation for understanding the problem (before starting to consider possible solutions).

# Background

A little history and grounding for the  
approach you learn and use

# SSM – Soft Systems Methodology

Checkland, Peter, and Jim Scholes. *Soft systems methodology: a 30-year retrospective*.  
Chichester: John Wiley, 1999.

Old work. But useful and influential (6500 Scholar Citations March 2018)

The challenge of **understanding**  
and describing **the problem**

We use an approach based on  
methods from Information Systems  
and Systems Analysis

The challenge of understanding  
and communicating problems



# From the 1960's...



How the customer explained it



How the project leader understood it



How the engineer designed it



How the programmer wrote it



How the sales executive described it



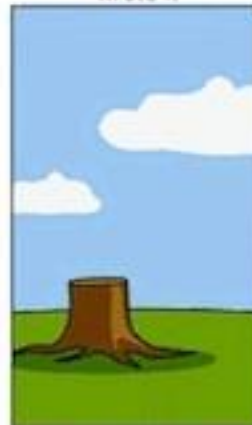
How the project was documented



What operations installed



How the customer was billed



How the helpdesk supported it



What the customer really needed

The swing problem is not a “soft” problem... and even so, it illustrates the many problems in understanding user needs – as well as communication between various stakeholders who create new systems

# Soft Systems

- The opposite of “hard” or “strictly defined” systems
  - eg first year programming assignments are not “soft” as there is a clear, tight specification and it is clear (though not necessarily easy) how to test a potential solution (eg auto-grading with well-designed tests)
- Soft systems that people, organisations, culture, context..... and problems that need to be tackled in light of these aspects
  - eg find a way to protect people from scams based on phishing

# Beware difference between:

## “complex systems” and “Complex Systems”

- Intuitively ... systems are complex if they have
  - many components,
  - complex relationships between components
  - (or both)
  - And they involve people - multiple stakeholder groups
- This is somewhat similar to **but has important differences from** the academic field called “Complex Systems”
  - eg. predicting weather ... very complex but not generally considered a “soft” system

# Take away messages so far

Communication is important and hard

Terms with specific meanings so far:

Soft systems – are complex (small c)

# Important characteristics approaches to tackling Soft Systems

- We do not aim for “**optimal**” solutions
  - because the problems are so complex that there is usually no way to define or recognize an “optimal” solution
- The goal is to find “**satisficing**” or “**good enough**” solutions
  - We still need rigorous ways to measure these
- Good enough solutions are often created by **iterative** approaches – by creating a solution and testing it to gain understanding of how well it works and how to improve it
  - eg Agile software methods and many HCI design approaches
- Introducing a **change** can alter the system in complex ways that we had not anticipated
  - eg people may change the way they work and interact with each other

# SSM

- Soft Systems Methodology
- An approach for tackling problems involving soft systems
- A starting point for working out **what the problem is** ... [heading to identifying users' needs]
- And the key **factors** and **stakeholders**
- Elements we consider: **Situation of concern**, CATWOE which we modify to **SSM2222**

# We start with: Situation of Concern

Statement of the problem we need to address

Our running example as used in Assignment 1.

**The University of Sydney is concerned about phishing**



# 1. Learn more about phishing broadly

To tackle problems like this, you need to become passionate about understanding the problem and learning about it .... Week 1 provided some introductions and the lab and mini-assignments build on this

“The email system is the central battleground against **phishing** and **social engineering** attacks, and yet email providers still face key challenges to authenticate incoming emails. As a result, attackers can apply **spoofing techniques to impersonate a trusted entity to conduct highly deceptive phishing attacks.**”

Hu, H. and Wang, G., 2018. Revisiting Email Spoofing Attacks. *arXiv preprint arXiv:1801.00853*.

“By a **careful design and timing of a message**, it should be possible to make virtually any person click on a link, as any person will be **curious** about something, or **interested** in some topic, or find themselves in a life situation that fits the message’s content and context. For example, the message might come from a known sender, or refer to a previous experience in a plausible way.”

Benenson, Z., Gassmann, F. and Landwirth, R., 2017, April. Unpacking Spear Phishing Susceptibility. In *International Conference on Financial Cryptography and Data Security* (pp. 610-627). Springer,

Security experts recommend that IT departments regularly carry out **penetration tests** that use social engineering techniques. This will help administrators learn which types of users pose the most risk for specific types of attacks while also identifying which employees require additional training. **Security awareness training** can go a long way towards preventing social engineering attacks. **If people know what forms social engineering attacks are likely to take, they will be less likely to become victims.**

<http://searchsecurity.techtarget.com/definition/social-engineering>

# Some key concepts

- Phishing
- Social engineering
  - “Social engineering is an attack vector that relies heavily on human interaction and often involves *tricking people* into breaking normal security procedures... [such as]
    - appeal to authority
    - appeal to greed
    - rely on people's willingness to be helpful.”  
<http://searchsecurity.techtarget.com/definition/social-engineering>
- Pure technical approaches are not enough
- Penetration tests
  - a.k.a. white hat attacks or “red teaming”
  - e.g. testers send test phishing mail and track whether people are caught
- Security awareness training

**Assignment 1 is all about security awareness training**

# Spear Phishing

Case study from research literature

“phishing emails were sent to 593 employees, who were asked to provide personally identifiable information (PII) - **personalised spear phishing** email opening was randomly used in half of the emails.

Bullee, Jan-Willem, Lorena Montoya, Marianne Junger, and Pieter Hartel. "Spear phishing in organisations explained." Information & Computer Security 25, no. 5 (2017): 593-613.

# Employee response?

19% provided their PII in a **general** phishing email,

29% in the **spear** phishing condition



2. Learn more about phishing as it affects “The University of Sydney”

# So who is “The University of Sydney” (aka UoS)?

A great question

And in Assignment 1, you will focus on just the parts of UoS concerned with phishing attacks on **students**

# Official and actual processes at UoS

- UoS policies highlight the importance of **education** as critical for addressing problems of phishing
- **Core technical protection** is a toolset called Mimecast.
  - Mimecast sits between the University mail system and the outside world, anything coming in or going out via our core domains passes through it.
  - Lots more at <https://www.mimecast.com/content/phishing-protection/>
- We will focus on the **education** aspects in Assignment 1 ... as that is the usability half of INFO2222

# Mimecast

- Technical solution
- Aims to prevent phishing email from ever reaching a user's mailbox

# Even Mimecast's web site says:

“For many organizations, phishing protection involves educating users to spot the signs of a potentially fraudulent email.”

2016 Data Breach Investigations Report

# Some official teaching materials

From UoS websites

# What do phishing emails look like?

Here is an example of a recent phishing email:

*"Your mailbox has exceeded the storage limit which is 20GB as set by your administrator, you are currently running on 20.9GB, you may not be able to send or receive new mail until you re-validate your mailbox. To re-validate your mailbox please click the link <http://qu3hb.9hz.com>*

*Thanks SystemAdministrator"*

# What is spear phishing?

The concept of spear phishing is the same as phishing, except that instead of sending as many emails as possible for maximum gain, the attack will send a specially crafted email to very select individuals.

With these attacks, the malicious individual will research their targets (e.g. by seeing their Facebook or LinkedIn profiles) and, based on their research, will then create a highly-customized email that appears relevant to their targets. Spear phishing is often used to target individuals with more access into University systems or with the ability to release funds.



# What do spear phishing emails look like?

Here is an example of a recent spear phishing email:

*"Please let me know if you are available to process a bank transfer. And so, what are the information you will be needing to process it?"*

*Regards*

*Dean*

*The University of Sydney*

*Sent from my iPhone"*

# What should I do if I receive a phishing email?

Here is what to do if you receive a phishing email:

- **Do not respond to these emails and do not visit websites with an unusual or unfamiliar web address**
  - Although it may seem innocuous, the website may deliver malware and infect your machine simply by clicking on it
- **Immediately contact the University Service Desk** if you receive a message soliciting private information by [sending the relevant email as an attachment](#) to the email address [ict.support@sydney.edu.au](mailto:ict.support@sydney.edu.au)
- **If you believe you have fallen victim to an attack immediately [reset your UniKey password](#) and contact the University Service Desk on 9351 2000, select option 2 for ICT.**
- **If you believe a colleague has fallen victim to an attack immediately contact the University Service Desk** by phone on 9351 2000, select option 2 for ICT

NOTE:

Please be aware that **the University would never ask you to provide your private information by asking you to respond directly to an email.** If we require your details or need you to confirm the validity of your UniKey account, we will ask you to contact the University Service Desk and speak to one of our staff.

For more information about spam email, refer to [What should I do if I receive spam email?](#)

Summary so far

# Elaborating on the situation of concern at UoS

1. Study literature **to gain insights about the problem in broader contexts and organisations**
  - eg study the state of the art in phishing attacks, phishing prevention ... we have done a little of this and hope you are inspired to learn much more
2. Study the **particular context** to gain insights into the particular concerns at the University of Sydney
  - eg study the current strategies for teaching about phishing, the problems that have occurred
3. Key approaches:
  - Helping people learn to identify phishing email PLUS
  - Technical solution to automatically stop phishing email

.... moving on from the Situation  
of Concern (aka the problem)

Identify what you will change  
(**Transformation**) and the **stakeholder**  
people and organizational units involved

# Transformation

Assignment 1 transformation is:

**To provide new approaches to phishing education for students at University of Sydney**

CATWOE – part of SSM method to study the particular context to gain insights into the situation of concern

CATWOE structures thinking about key elements ... starting with the original and then the INFO2222 form

# CATWOE – original

Purple is for elements that are usually people

- **Customer**
- **Actors**
- **Transformation – what effect is intended for the new system to address the situation of concern**
- Weltanschauung (worldview)
- ***Owner***
- Environmental constraints



# Our form of SSM - SSM2222

Purple is for elements from CATWOE

- **Situation of Concern**
- **Transformation**
- **Key stakeholders (was Client, Actor, Owner)**
  - **Worldview (Weltanschauung)** of each stakeholder ...  
as a part of the description of their **mental models**
  - Broader aspects of mental model
  - Context and **environmental constraints** for each stakeholder

# Our form of SSM - SSM2222

Purple is for elements from CATWOE

- **Situation of Concern**
  - Phishing is a problem for the University of Sydney
- **Transformation**
  - To provide new approaches to phishing education for students at University of Sydney
- Stakeholders ... now we consider this

# Stakeholders relevant to Asst 1

- The attackers
- The ICT Service (the group responsible for ICT infrastructure and security)
- Senior University Leaders (set the policies and oversee the ICT services)
- Services that ICT/UoS could purchase to provide training
- **Students**

# Assignment 1 analysis of stakeholder group - students

Purple is for elements from CATWOE

- **Worldview (Weltanschauung)** of each stakeholder ... as a part of the description of their **mental models**
- Broader aspects of mental model
- Context and **environmental constraints** for each stakeholder
- We return to this later in this class – in conjunction with “personas”
- You will work on this in the lab

# Stakeholder analysis for students – some potentially relevant aspects

- **Worldview (Weltanschauung)** of each stakeholder ... as a part of the description of their **mental models**
  - All students want to *learn* within the formal degree program; many students also want an *active on-campus experience*; many students want *full social lives*; many want to get *work experience*; many want to *gain a broader education*; based on earlier slides on broad concerns about security, many students *want to learn about security* in general and phishing in particular is relevant for this analysis
- Broader aspects of mental model
  - A core aspect here is students' *knowledge about phishing* - this needs to be defined in detail; technical expertise and confidence...
- Context and **environmental constraints**
  - Students are likely to be *very busy and time poor*

This list is a starting point for actually  
conducting user research to learn  
about user needs

# Assignment 1 analysis of stakeholder group - students

- We return to this later in this class – in conjunction with “personas”
- You will work on another example in the lab

What are the three key methods for  
**learning about user needs and  
preferences**, taking account of their  
context?



# Three key methods for **learning about user needs and preferences**

Study peoples' **behavior**

Study what people **say**

Study **trustworthy previous work**  
reporting the above

# 1. Study peoples' behavior

What do people **actually do** in the context of the situation of concern? To learn this we need to observe users with approaches such as:

- **Automated monitoring** approaches – use software to track behavior (eg penetration-style white-hat testing to see who is tricked by phishing email)
- **Ethnographic** approaches – observe people in context – comes from anthropology where an observer immerses themselves in a community to gain a deep, qualitative understanding of them
- **Laboratory studies** – observe people out of context by bringing them into a lab

# Automated monitoring approaches

- Widely used by security specialists in, or hired by, companies eg <https://www.wombatsecurity.com/>
- This can be a starting point for **embedded training**:
  - where a user is taught about phishing when they fall for a penetration-style white-hat test, this becomes a teachable moment (assuming it is not too irritating for a busy user)

# Ethnographic methods

- Give much richer data than simple monitoring of online behavior
- Works only if the observer can be present at relevant time (eg observing when people read their email – but that typically poses a privacy problem in this case)
- Ethnographic studies need training (like that anthropologists do to do effective observations, recording the observations, analyzing and interpreting the data collected)

# Study what people say

- Ask people in context
  - what they do
  - why they do it
  - what they like/dislike about the current situation
  - **questionnaires**, interviews, in-context notification with question to answer
- Ask people out of context
  - After lab studies
  - Interviews, focus groups, questionnaires for small groups
  - Crowd-source studies (eg Amazon Mechanical Turk)
- Hybrid
  - study what people say to others eg on social media

# Ask people ... phishing

- Conduct tests to discover what people know (and don't know)
- Ask people what they believe they know and whether they need to learn more
- Ask people about their concerns, the reasons they consider them important (as in Mini-Assignment 1 for this week)
- Organise group discussions (as in this week's lab).

# 1. Study the work of people who did #1/2

**Where** to find relevant work?

- Research publications
- Commercial and Practitioner publications
- HCI specialized versus domain specialized

**What** to find?

- Identify the places, publications
- Identify the leading experts
- Seminal work
- Reviews and overviews and expert opinion pieces
- Important breakthroughs

# Observing versus asking....

- The challenge of lack of **self-awareness** of mental models
- The challenge of **self-censorship**
- The challenge of **politeness**
- Some people **joke or lie for various reasons**
- In general, you need to be aware of these aspects when interpreting what people say



# Is more better?

- Ethnographic (small numbers of people) versus monitoring (can study many)
- Small-scale interviews (small numbers of people) versus crowd-source questionnaires (can study many)
- Ideally, you would do both – gain large amounts of quantitative data and smaller amounts of higher quality qualitative data

# Study trustworthy previous work

Where can you find such work?

What are the top academic forums?

What are the commercial forums?

NOTE the categories: usability – usable security –  
usability aspects of phishing

“By a **careful design and timing of a message**, it should be possible to make virtually any person click on a link, as any person will be **curious** about something, or **interested** in some topic, or find themselves in a life situation that fits the message’s content and context. For example, the message might come from a known sender, or refer to a previous experience in a plausible way.”

Benenson, Z., Gassmann, F. and Landwirth, R., 2017, April. Unpacking Spear Phishing Susceptibility. In *International Conference on Financial Cryptography and Data Security* (pp. 610-627). Springer,

# Please to learn about HCI

- Many blogs eg <https://www.nngroup.com/>
- Many government website eg <https://www.usability.gov/>
- Academic literature
  - Start with Google Scholar
  - CHI, Ubicomp, ToCHI
  - Metrics on top places to publish HCI
  - [https://scholar.google.com.au/citations?view\\_op=top\\_venues&hl=en&vq=eng\\_humancomputerinteraction](https://scholar.google.com.au/citations?view_op=top_venues&hl=en&vq=eng_humancomputerinteraction)

# Usable security

Societies eg <https://www.antiphishing.org/>

eg “APWG is the global industry, law enforcement, and government coalition focused on unifying the global response to cyber crime through development of data resources, data standards and model response systems and protocols for private and public sectors.”

Leading commercial groups

- They publish helpful “whitepapers” with recent information (eg wombat earlier)

Commentators

- eg Bruce Schneier: “Only amateurs attack machines; professionals target people. “

Academic research at intersection of HCI and security

- SOUPS <https://www.usenix.org/conference/soups2018>
- <http://cups.cs.cmu.edu/soups/>
- Search for key terms (eg phishing) and identify top research groups

Explain how **high level user goals** come from studies of user needs.

# To create the system for the transformation....

- Identify user's core goals, based on all methods
- Assignment 1 – evidence in earlier slides suggest that
  - students want to learn about phishing risks
  - In studies many people can be fooled by phishing email (and associated websites)
  - We use this as a starting point

What is a **persona**?




# From usability.gov

- “create **reliable and realistic representations** of your **key audience segments** for reference ...
  - Represent **a major user group** for your system
  - Express and focus on the **major needs** and **expectations** of the **most important user groups**
  - **how they're likely to use the system**
  - Aid in uncovering **universal features and functionality**
  - Describe **real people** with **backgrounds, goals, and values**”

*[with site replaced by system]*

In INFO2222 personas, we combine

- HCI personas
- SSM2222 - Information Systems perspective including the organisations, culture, broader environment

<b>Persona:</b>	USDA Senior Manager Gatekeeper
<b>Photo:</b>	
<b>Fictional name:</b>	Matthew Johnson
<b>Job title/ major responsibilities:</b>	Program Staff Director, USDA
<b>Demographics:</b>	<ul style="list-style-type: none"> <li>• 51 years old</li> <li>• Married</li> <li>• Father of three children</li> <li>• Grandfather of one child</li> <li>• Has a Ph.D. in Agricultural Economics.</li> </ul>
<b>Goals and tasks:</b>	<p>He is focused, goal-oriented within a strong leadership role. One of his concerns is maintaining quality across all output of programs.</p> <p>Spends his work time:</p> <ul style="list-style-type: none"> <li>• Requesting and reviewing research reports,</li> <li>• preparing memos and briefs for agency heads, and</li> <li>• supervising staff efforts in food safety and inspection.</li> </ul>
<b>Environment:</b>	He is comfortable using a computer and refers to himself as an intermediate Internet user. He is connected via a T1 connection at work and dial-up at home. He uses email extensively and uses the web about 1.5 hours during his work day.
<b>Quote:</b>	"Can you get me that staff analysis by Tuesday?"

# Why is a persona useful?

- Builds on our ability to think about people, when we “know” them
- Valuable as a communication tool for the design team and other stakeholders
- Helps in discussions in design group and making design trade-offs eg
  - Alice would not want.... but Bob would (based on Alice and Bob preferences in their personas)
  - Carol would not understand ... (based on Carol’s background knowledge in her persona)
- Designs can be constantly evaluated against the personas

# Elements in the INFO2222 Asst 1 persona

- \*\*\* Name, position in The UoS
  - (in Asst 1: students at UoS)
- \*\*\* Photo
- Mental model
  - Worldview
  - detailed goals
  - Current knowledge (technical generally and phishing in particular)
- Context and environmental constraints for each stakeholder (eg things about this student that would impact the mail they are likely to receive)

\*\*\* Elements needed because that helps the design team talk and think about this hypothetical person

# How to create a persona2222

1. Start with user needs research (as earlier in this class: observation, asking, literature that already did this)
2. Summarise this to identify key similarities and differences between people for each main attribute - in terms of the aspects of the user's mental model (worldview and broader aspects, especially goals)
3. Identify the key groups that should be considered and define a persona for each, justifying the choice with information from Step 1

Explain how **high level user goals** are refined into **detailed tasks** - to drive the design (Week 4) and evaluation (Week 3) of interfaces.

# Starting with high level goals...

Assignment 1 – evidence in earlier slides suggest that

- students want to learn about phishing risks – and how to recognize and avoid them

Decomposing this goal:

- Your next mini-assignment will help you identify the precise attributes of email that a student needs to learn to recognize as suspicious
- Your group will need to design good ways to teach people how to check each of these



# How do **mental models** link to user needs studies?

One core goal of user needs studies is to learn about the mental models of the intended users and people involved in your system.

# User needs research aim to get evidence to about user's mental models

## Mental model

- Worldview
- Detailed goals
- Current knowledge (technical generally and phishing in particular)

... need to ask + observe what people actually do + and draw on research from those who have done this (earlier in this class)

# Week 2 – Analysis – what you now know

- **Soft Systems Method (SSM)** to identify the broad foundation for determining user needs
- Three key methods for **learning about user needs and preferences**, taking account of their context
- Explain how **high level user goals** come from studies of user needs.
- What is a **persona**?
- Explain how **high level user goals** are refined into **detailed tasks** - to drive the design (Week 4) and evaluation (Week 3) of interfaces.
- How do **mental models** link to user needs studies?