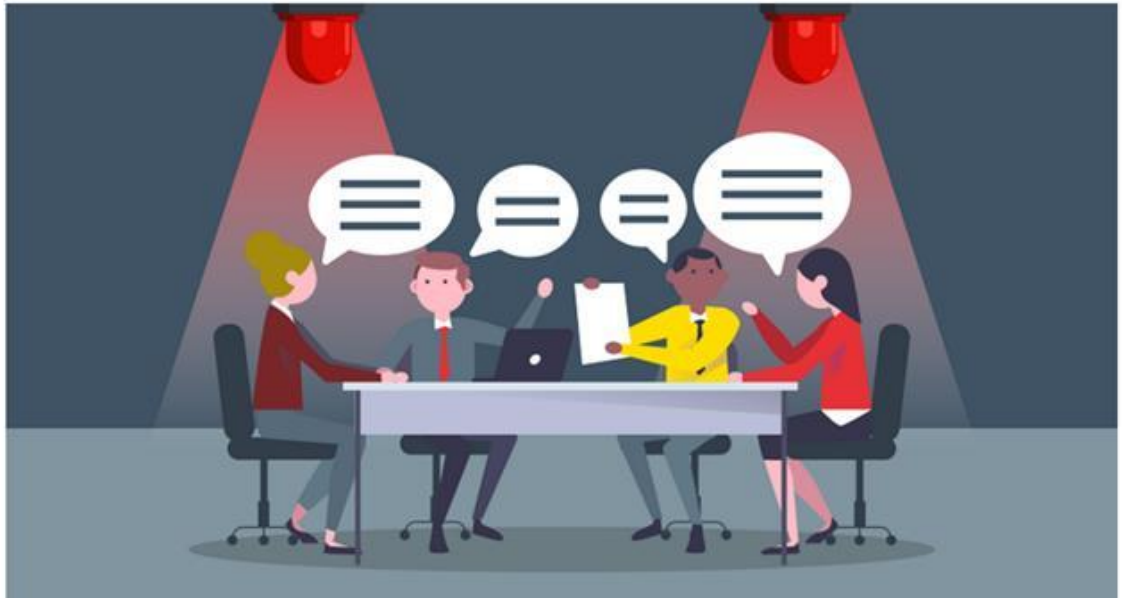
Eramus+KA229. Mobility in Tortosa.

ICT activities. Workshop.

We are discussing the topic in six international groups.

ICT Security rules for students' firms A role-playing game. Are you ready for an attack?



We have four moments, with x minutes for each one. The last one will be the output of the activity.

1st What has happened? The situation / problem is...
[8 minutes]

2nd Which process has failed? Where is the problem?
[8 minutes]

3rd Can we find out a solution?
[8 minutes]

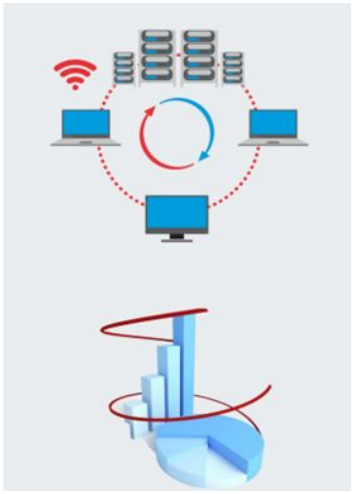
4th Have we learnt anything?
[10 minutes]

OUTPUT

- Each group shows and explains their solutions to the others.
[from 2 to 3 minutes each group]

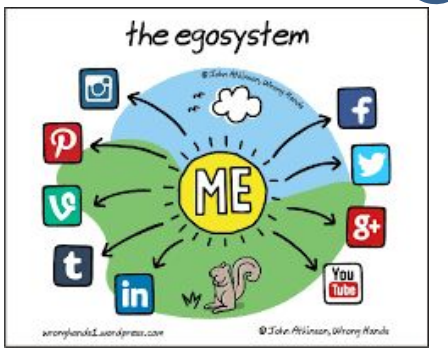
The scene:

Imagine your practice firm, your office with…



- Our practice firm has an office, there are laptops, Wi-Fi and internet connection.
- Our company uses cloud computing and social networks.
- We use the information to send e-mails to clients and suppliers.
- We have a web or e-commerce.
- The workers write the invoices, send e-mails to the management company…

1st The problem / input: someone makes a social engineering attack against our practice firm.



As you know, social engineering in the context of information security, refers to psychological manipulation of people into performing actions or revealing confidential information. Phishing is an example of social engineering.

- ✔ When we come back after holidays, we see that the figures in the bank statement aren't as we expected.
- ✔ We phone the bank and they say to us: «these banking movements have been done with the correct accreditation».
- ✔ We have a talk with the other employees: «Have you seen anything strange? One of them explained that, some days before, the boss had sent an e-mail and asked him to give his bank credentials immediately.
- ✔ The e-mail had the name and the phone number of the boss and it wasn't the first time that the boss asks the employee for his credentials (username and password for the bank account). The text of the mail includes information about the employee (his name and surname and his role in the company).

2nd The workshop process: what element or which process has failed? [each international group deals with the problem following the second and third steps]

Problem	A robbery	A break down	Malware	A bad behaviour
Cloud computing				
Laptop				
Smartphone				
Privacy in Social Networks				
Public information on the website				
Password not secure enough in e-mails				
Smartphone not blocked				
Not updated software				

3rd Can we find out a solution?

- Can you phone someone for help? Do you know who to call?
- Maybe the employees need a continuous training or learning in ICT security?
- Can we check our public information settings in social networks?
- If we want to go to the police office, have we got any evidence?

_____
_____
_____

4th The output: have we learnt anything?

What we must do is…	What we shouldn't do is…	How can we avoid this kind of problem in the future?

Each group explains and shows their solutions.

This is **the workshop result**.

Most of the solutions of the six international teams focus on:

What we must do is…	What we shouldn't do is…	How can we avoid this kind of problem in the future?
• Call the bank, stop each fraudulent transaction and review the previous ones or close these bank accounts.	• Post too much personal information or share too much sensitive data, especially in social networks.	• Looking that e-mail is correct and after have confirmations.
• We must go to the police. We have got the evidence (wrong e-mail account).	• Trust every mail that comes to us and send private information by email.	• Use own devices.
• Have an strong password and change it regularly and protect our personal inform alias.	• Trust all the people on the internet.	• Take note and do not repeat the same mistake

The solutions of the teams. Part II:

What we must do is…	What we shouldn't do is…	How can we avoid this kind of problem in the future?
• Be more careful and learn about security.	• Leave the email account open.	• Some of the answers in the first column are had been repeated in this third by the groups.
• Have different passwords for different accounts.		

A proposal of solutions by the experts is…

What we must do is…	What we shouldn't do is…	How can we avoid this kind of problem in the future?
1. Phone the bank and cancel the wrong bank movements or transactions.	5. Hide the problem.	9. Have a contact list for ICT security.
2. Phone the police to report the incident.	6. Try find a solution by your own / alone.	10. Make an analysis risk; we must have an incident record.
3. Give personal credentials (ID identity cards) and permission only to the employees who are in charge of the section (bank accounts, clients information...).	7. Look for someone to put the blame on before a good analysis.	11. Make a method, a protocol for each kind of incident.
4. A continuous training for strong passwords, social engineering, etc.	8. Give credentials to all the employees for all the services.	

In conclusion:

What we must do is…	What we shouldn't do is…	How can we avoid this kind of problem in the future?
The groups identified most of the things we should do: numbers 1, 2 and 4.	All students solutions are valid tips.	Perhaps we need to clarify that there are short-term solutions (first column) and others in the medium and long term (third column).
Only the third point remained to be determined: "give personal credentials (ID identity cards) and permission only to the employees who are in charge of the section (bank accounts, clients information...)."	Solutions 5 to 7 of the experts are interesting not only for a social engineering attack. On the other hand, number 8 is a more concrete advice for our companies.	

In conclusion. Part II:

What we must do is…	What we shouldn't do is…	How can we avoid this kind of problem in the future?
– A continuous training for strong passwords, social engineering, etc.	- Look for someone to put the blame on before a good analysis	
	- Give credentials to all the employees for all the services	