nc3.lu
National Cybersecurity
Competence Center
LUXEMBOURG

Be Aware – Cybersecurity for everyone

Script for the sensibilization about cybersecurity

Luxembourg House
of Cybersecurity

Slide 1 :
Presentation of the training, introduction, context. If necessary, one might want to present the company or the department offering the training.

Slide 2 :
The trainer can introduce himself and his curriculum, his CV.

Slide 3 :
Participation Exercise :
Make the audience estimate the value of their phone. Explain them how invaluable there are because they do have lot of personal data which shouldn't be sold.
Explanation of the information security, what it entails and the areas that it concerns.
Participation Exercise :
ask the audience what information security means to them
- ➔ Explain that the security is not a state but a feeling. « We are note secure – we feel secure »

Ask the audience what « information » means and what information is : ask for examples :
- ➔ Explain that information can be medical (like personal example, severe illness …) but it cam be more important : blueprint of drones, military plans, nuclear powerplant construction plan...

Explain the need and importance of protecting information, even those that seem insignificant at first sight. Give the unfortunate consequences of losing the data cited as an example.

Slide 4 :
Generalize the different consequences and types of consequences related to an information security problem, with loss of confidence, economic or legal sanctions. Everyone can be responsible. Explain that these consequences are of professional nature, and also personal.

Slide 5 :
Transition from information security to risk. Express that protecting information is about managing and understanding the different risks. Explanation of the vocabulary used in the field: The treatment of risk. Definition of a risk

Slide 6 :
Break down the risk to better explain it, and do it with an example.
Vulnerability :
Examples :
- ➔ Key under the door mat / flowerpot: Explain a story that could explain a reason to do so, as will give the keys to a close.
- ➔ Human error

Threats :
Examples :
- ➔ Burglar :Indicate how burglars prepare a burglary. Study of habits, lights, surroundings, possible disguise, attempt to knock / ring, attempt to open the door, go behind ... use of the connected world, like connected objects (like a connected toy that speaks to the child , to make him open the door, or flower pots connected to check if the plant is watered ... etc.).
- ➔ Car

Impact :

Examples :

- ➔ Theft of property
- ➔ Injury/Death

Participation exercise :

Reflection with the working group on examples of everyday risk.

Taking the examples show that it is impossible to influence the threats and impacts: it is generally only possible to play on the vulnerabilities.

Slide 7 :

Formalization of existing risks, and examples of categories.

Slide 8 :

Explain by some examples the different common dangers.

Updates :

Technological devices (computer and software, laptop, smartphone and application, car, GPS ...) contain code that is often incomplete, or with unforeseen cases or unforeseen flaws. Need to update to fix existing flaws.

Example :

- ➔ When buying a house, we look at whether it is complete: walls, roof, windows, windows, electricity, plumbing ...). When buying a phone, we are still at the stage where we look at the appearance, the components, which is to ensure the tapestry and finesse of the phone, without looking at more technical details. If a house is worth a certain amount, and a phone is worth much less, it very often contains the data of a life that is invaluable (photos, personal data, user accounts like Amazon or PayPal ...)

Tips to give:

- ➔ Update the different devices and their software, to make sure you have the last possible protection

Coffee break :

Not locking your computer, leaving your phone accessible, it is giving the opportunity to anyone to pretend to be you : Giving access, or trusting blindly can be very dangerous.

Example :

- ➔ Two employees are fighting for a promotion in a field with sensitive data, such as a company's accounting. One of them becomes the superior of the other by the promotion, but he leaves his computer accessible during an absence for a coffee break, with the staff representative. In revenge, his colleague accesses his computer, and sends an insulting email to the management. The management, after knowing the email, requests explanations and testimonials. Due to the confidential nature of the information and the trust granted, the manager is the person who is on a coffee break and has not locked his computer.

Participation exercise :

Name the actors in the story with people from the audience.

Tips to give:

- ➔ Lock your computer and phone in case of absence to prevent identity theft.

Passwords :
The password is like a key protecting a whole virtual life. 80% of the passwords are easily found somewhere on the desk of an individual (photograph, object, document, post-it ...). Sometimes it is also the same password across different accesses.

Example :

➔ Passwords are easily retrievable by asking simple questions. A study was done on the possibility of recovering a password with a password security tester, on the street. The recovery rate is greater than 60%.

Tips to give :

➔ Passwords must be complicated enough, changed from regularilsy, and must not be the default password. They must not be easily guessable. Passwords should not be given to anyone.

Slide 9 :
Plan on the points addressed during the initiation of information security.

Slide 10 :
Explain to what extent it is possible and easy to take advantage of the various points cited to achieve these ends, and this by examples.

Example :

➔ Spam can illustrate the different weaknesses of the man. Curiosity is represented by promotional offers that can make you want to click, venality by sums offered following a tragic story. Laziness is used by easily accessible links, and libido by different advertisements or evocative images. Fear is used by recent threats, such as sextortion, and pity is used by tragic stories. Overall, all these vulnerabilities are primarily human.

Participation exercise :

It is possible to start a story about human vulnerabilities. Explain that one person (A) is in love with another (B), and that she is friends with a last (C). The person who is loved (B) goes on vacation, and has a Facebook profile reserved for friends. The person in love (A) confides in his friend (C), in a bar, where the discussion is heard by an evil person (E). Interrupt here the story, and resume it Slide 12.

Build a spam (simple) with the audience, to show how easily this is possible, but also explain the strings used by hackers.

Tips to give :

➔ Think before replying to a message. Responding to spam means being on a valid email address list that can be a victim of spam. You should never pay because paying is a way to be on a good payroll list, and to be asked for money again, while participating in a criminal activity.

Slide 11 :

Participation exercise :

Ask a person if they would come from a certain city, with the aim of obtaining their address. Innocently ask the neighborhood once the name of the city obtained.

Ask what would happen if a USB key was simply left in front of the premises, presumably abandoned. Explain the dangers of using such a device.

Talk about social engineering. Explain the different possibilities for manipulating the language, and other possible psychological techniques

Example :

➔ Talking about Gilbert Chikli, the "inventor" of impersonation fraud (fraude au président). Explain how to carry out such a fraud, using typical examples of calls or phrases used: "I count on you", "you do not have to talk to anyone about it, it's a secret mission", "I trust you"... Moreover, explain the way of being insistent and not give time to think.

Tips to give :

➔ Communicate any suspicion of such a problem. It is necessary to contact a person by known means in case of suspicion or a strange or challenging case, to ensure that it is the legitimate person who made the request.

Slide 12 :

Participation exercise :

Resume the story left Slide 10. The person-spy (E) will then pose as the friend of the lover (C), and send him a link with the profile of the person party on vacation (B), playing on libido (photo in bikini / shorts) or fear (seen with another person we do not know about photos). Start the video to explain what could happen :

Video : https://www.youtube.com/watch?v=_iqoFbVLUHY

Show how much to pay attention to URLs, before clicking, and always check the sources before any actions. Also explain that a known password will be tested on other services.

Participation exercise :

Prepare them to read quickly what is indicated, and show it as an exercise.

Slide 13 :

Participation exercise :

Quickly make people read the slide in turn, without giving them time to think. Explain that despite the awareness of these phenomena, you should always pay attention, and always look carefully before clicking on a link.

Tips to give :

➔ Always look carefully, and most importantly, take the time to read well.

Slide 14 :

Example :

➔ False refund proposed by the Tax Administration: A false site was reproduced, with the request for a credit card, which could be easily given.

Participation exercise :

Ask if people would be fooled by such fraud, and ask if their parents or grandparents would fall for it.

Slide 15 :

Example :

➔ Example of what can be seen commonly. The first is a computer of a person who has a lot of responsibilities, and therefore, a lot of personal data. The second is visible in a train, when traveling or moving, or all data is visible, and unprotected.

Tips to give :

➔ In public, it is necessary to pay attention to what we allow the external to see and hear. Any information given may be reused against us.

Slide 16 :

Participation exercise :

Ask for the different problems related to this image.

A photograph that has been published on Facebook without taking into account that the screens are visible, that WiFi is accessible on the board, but also that the GDPR is not even respected a priori.

Tips to give :

➔ Always ask permission to take an image, but also to disseminate it. In addition, it is necessary to check what is in the photo.

Slide 17 :

List a good many of the pitfalls that can be made on mobile devices. Forgetting and loss of material, discussion in public places, unencrypted data in case of theft, which makes the information accessible to all.

Video : https://www.youtube.com/watch?v=GBUiBEv-cM0

Participation exercise :

➔ Create a WiFi network with the phone, with an SSID similar to existing networks, and show the group that it is visible on their phone, and so show them how easily it is feasible.

Tips to give :

➔ We must not connect to a network that we do not control, and prefer the data of the mobile package. Otherwise, be sure not to send confidential data.

Participation exercise :

➔ Induce a brainstorming exercise, with the main objective of showing how simple it is for realization:

- You are a private investigator, and work on behalf of the state. You have all means, including illegal, to recover a person's medical data. How would you do it?
- Your best friend suspects his / her spouse of having an extra-marital relationship, and asks you to help him discover it. You have all means, including illegal, to do so. How would you do it?

---------- Break ----------

- ➔ Debrief about the different story that could be thought. Those could be written on a board. Eventually, explain the whole story and the consequences of the data leak.

Example :

- ➔ The doctor of the target has been approached under the identity of the WHO (World Health Organization) to get the information needed of the target, after looking some identity information on the people who work there (by looking on Facebook, LinkedIn…) to get some credible detail on the phone call. The phone call explains that a rare disease could hide under the file, and that it should be sent under every detail to define it correctly. (Example of impersonation fraud, or social engineering).
- ➔ The phone of the target has been recovered. The lock code has been found by ask to his spouse, or deduced by her date of birth. Some incriminating message or pictures have been found. Other proofs have been found in the phone (explain how it's possible to get some life information in the device that has all our lives).

Slide 18 :

Participation exercise :

Show a little demo about how it is possible, with online tools, to crack a password. Show how it is possible to access to a robots.txt file, and how that file could bring some information like where are stored passwords. Say that we have got a line of the file, and that we can try to crack it online. Explain that most of the password are the same on every web services, and so an entire life is accessible by just doing some small hack.

Example : 179909b745f81f03f177a3079e0ce5e3:ef749ff9a048bad0dd80807fc49e1c0d

www.bikes.com/robots.txt -> Showing in the disallow the user/password

https://crackstation.net/

Some cases that are real, some leaks of passwords on famous website or applications. Explain that is why it is important to change password between application, but also why you need to change password often.

Participation exercise :

Whom have at least one password on those web sites ? Who keeps using it until the hack announced ?

Tips to give :

- ➔ Change passwords often, and if you have the same password since the hack, change it as quickly as possible.

Slide 19 :

Why hackers do that ? What are their main reasons to break the law ?

Examples of price that your personal data could be sold on the black market. These values are an average.

Slide 20 :

Example of what kind of numbers could be found on a phishing campaign. These number are strictly indicative.

Slide 21 :
Example of how the data are sold by a social network, and where they go. GDPR now broke some parts of this, but only in Europe.
Example :
➔ A personne which write on facebook a comment about sports. Then, Facebook will sell those data to Brokers, who will sell data at some marketing company. Those one should sell their data to local gym center, which could finally send an advertisement to convince the person to get on the gym center.

Slide 22 :
Gold was really precious, petrol was really precious, and now, the new black gold is the datas of every single human on earth.

Slide 23 :
Quick explanation of the Deep Web and the Tor browser. If there is illegal stuff that could be found in the Deep Web (buying illegal products like drugs, organs, guns…), it's mainly a tool to stay anonymous. But, by accepting to participate, it's also accepting to serve as a relay for eventual hackers.

Slide 24 :
Available price that can be found in the Dark Web, and all the product or the services. Prices are lower and lower as time passes.

Slide 25 :
Show how this is easy to buy stolen credit cards, which could be buy by the young people.
Example :
➔ It's not rare to see teenagers, to buy article or services that they can't afford for, buy some stolen credit card, so their parent won't see the bill.
Tips to give :
➔ Children should be accompagnied and guided to explain all the danger linked to the use of internet.

Slide 26 :
Participation exercise :
Do you recognise these tools ? Are you using them in your everyday life ? If you do, your credits card information could be stolen.
How those credit card could be stolen. That could be stolen in the web site were those information are stored, or by different physical way like cash dispenser or electrical payment terminal.
Example :
➔ It's also possible to stole money with contactless payment. Get into the metro, with a payment terminal NFC, and you can stole 30€ per non-protected card if you are enoughly close.

Slide 27 :
Explain the Blippar application, which can show where two people have met by crossing the localisation historic of the two phones.
Participation exercise :
With the group, show and show them the IPhone localisation. Go into « *Settings* » > « *Privacy* » > « *Location Services* » > « *System Services* » > « *Frequent Location* ». These recorded locations could be used by applications from which we accept blindly the terms of use without reading them. Explain that the Android phone send the same kind of historic, as Google send you a mail of different locations seen during the month.

Slide 28 :

Exemple :

- ➔ Some aberrations, like nude selfies which are made to assure credits.

Insist also on the importance to protect and explain children and teenagers about this kind of practices, and how it's complicated to delete data whenever they are stored somewhere, even in a phone or in a laptop.

Slide 29 :

Explain the problem of the Internet of Things. All connected objects could be attacked from a way to another, or could give some information. Explain that not so many of builders are worried about the protection of the data, because they are focus on other problems.

Example :

- ➔ It's possible to access data from a Pacemaker, to read them, but also mainly modify them. They do not have enough protection.
- ➔ A connected flower pot could give some information to a rubber, like the absence of the people in their house.

Slide 30 :

Example :

- ➔ Another example of hacking, with connected cars. The problem here is that the builders won't protect their product, and do not think about security at the beginning. The task get more complicated just after (Security by Design).

Slide 31 :

Sometimes, targets of the hackers are not active people, but also children or older people. Toys are only an example. A hacker will attack on the weak point of someone, and it's important to know that most of the weak point are childs.

Example :

- ➔ Some rubbers have used a connected toy, making it cry, and have told a story to the children. His wife were crushed by a car, and his kids search for the house of the kid. The toy ask to the kid to open the door without telling it to his parents. Then, rubbers won't have to enter by breaking it.

Slide 32 :

Some items become more and more connected, sometimes in a useless way at the first thougth, but gain access for even more people than their owner.

Example :

- ➔ Sometimes some real hostage-taking are made, like decreasing the temperature of a house easily when it's connected, in winter, to make them paid some ransom, or give some information of a company.

Slide 33 :

Example :

➔ Some cameras which ensure out protection (and sometimes, personnal protection) are accessible on internet, and could sent some informations that are private, or really sensibles. The password are rarely changed, and hackers know it, so they always try to enter it on the first try. Some website list those cameras which are not well protected or are easily accessible.

Tips to give :

➔ Globally, default access should be changed, and a better protection should be use to protect a product.

Slide 34 :

Example :

➔ Another example on drones, even the ones from the american army that could be hacked, contains lot of precious and sensitive data. Most of the time, they have some cameras that are permanently activated, and that can give some information of what is buy, by who and where. Even the first flight has been diffused.

Slide 35 :

Show the law to show that hacking something is forbidden, and shouldn't ever be done.

Participation exercise :

Ask to someone randomly in the public to try to enter a code on a phone which is not his/her (example : the one from the teacher). Explain that this simple gesture costs as much as entering in the phone. Explain all the different sentences.

Slide 36 :

How this is possible to protect ourselves. This slide is really important, as it explain the main and best practices, and explain that people shouldn't be deconnected, but should protect themselves by following easy lives rules.

Exemple :

➔ Take again the beach example. At the beginning, danger of the beach where unknown : wind, tides, danger of the sun … But when people have learned the danger, they do not stops to go on holiday at the beach, they do have taken precaution, like have solar cream, look at the danger flags … It's the same on internet, people should just take precations, witohout denying all advantages that internet give.

Tips to give :

➔ Resume all tips that were given during the presentation

Slide 37 :

Explain some general advices on what should generally be done.

Slide 38 :

Get and answer all the questions asked.