

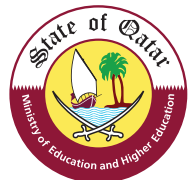


سيف سبيس
Safe Space

DIGITAL LITERACY CURRICULUM



STUDENT'S WORKSHOP GUIDE
SOCIAL ENGINEERING



Workshop Components

Note:

This document is inclusive only of the Workshop Guide. All other components for this workshop are listed below for the trainer's reference and can be found in the Social Engineering Workshop File.

- [Workshop Guide](#)
- [Background Reading for Trainer](#)
- [Background Reading for Student](#)
- [Students Workshop- Social Engineering PowerPoint](#)
- [Workshop Practical Activities for students](#)
- [Workshop Notes for students](#)
- [Workshop Learner feedback for students](#)



Introduction to Social Engineering Workshop

Target Audience:

Students

Workshop Duration:

2.5 hours

Workshop Components:

- [Workshop Guide](#)
- [Background Reading for Trainer](#)
- [Background Reading for Student](#)
- [Students Workshop- Social Engineering PowerPoint](#)
- [Workshop Practical Activities for students](#)
- [Workshop Notes for students](#)
- [Workshop Learner feedback for students](#)

Overview:

The Social Engineering workshop aims to educate and raise the awareness on Social Engineering. The workshop targets students between the ages of 13 and 18. The workshop duration is about 2 hours and a half with a maximum of 25 students. The workshop will highlight the two main categories under which all social engineering attempts could be classified which are technology based deception, and human based deception. Each category will be clarified and discussed using real life examples. The workshop will highlight common behaviours vulnerable to SE attacks along with its impact. To make sure that students understand the concepts of Social Engineering, they will engage in 2 different Practical Activities along with many discussions through the workshop that give them the opportunity to share their thoughts and practice what they're learning in workshop.



Workshop Guide

Social Engineering

Duration:

Around 150 minutes

Requirements:

- Projector
- WIFI for the trainer
- Regular room
- Preferably round tables
- Hand-outs
- Folders

Number of participants:

Maximum 25 students

Purpose:

To educate and raise the awareness on Social Engineering.

Objectives:

1. Define Social Engineering.
2. Highlight human based deception.
3. Highlight computer or technology based deception.
4. Highlight the common behaviors vulnerable to SE attacks.
5. Highlight its impact.
6. Make them able to evaluate scenarios.
7. Help them with some protective mechanisms against SE attacks.
8. Put up a final advice.

Materials to be used:

- Flipcharts
- Markers
- Workshop Guide
- PPT



Action	Trainer	Participants	Materials	Timing
General Introduction to the program and today's topic – Slide 1	This is an opening slide Introduces himself/herself and the program and today's topic DIGITAL LITERACY CURRICULUM. If needed – asks participants to introduce themselves If you think an icebreaker is needed – the trainer does it now.	Listen and introduce themselves.	PPT, ice-breakers ACT1	15 min
Class Objectives – Slide 2	Define class objectives. Walk them through it and highlight the key important areas that you are going to cover.	Listen.	PPT	5 min
Social Engineering Definition – Slide 4-5	Define social engineering as stated by SANs institute and elaborate more on that with further clarifications by your own.	Listen.	PPT	5 min
Social Engineering Concept Breakdown – Slide 5-6	Here you need to highlight the two main categories for social engineering and may need to elaborate but no much as its covered in the coming slides.	Listen	PPT	5 min
Human Based Deception – Slide 6-7	Here you need to highlight the different kinds of human deception techniques, try to bring real life examples in your discussion to elaborate more on the topic.	Listen	PPT	15 min
Computer or Technology Based Deception – Slide 8-9	Here you need to highlight the different kinds of computers or technology based deception techniques, try to bring real life examples in your discussion to elaborate more on the topic.	Listen	PPT	15 min



Action	Trainer	Participants	Materials	Timing
Behaviours Vulnerable to Social Engineering Attacks – Slide 10-11	Highlight the relation between some common vulnerable behaviors and their social engineering attacks related to them or associated with them. i.e. because of too much trust in unknown people you may be vulnerable to phishing attacks.	Listen	PPT	10 min
How much Impact could this have on US – Slide 12	Here and after you have defined the different types of SE attacks and their relation with our behaviour, you may need to highlight its impact on our user lives.	Listen	PPT	10 min
How to Evaluate – Slide 13 & 14	Teach them some questions they need to ask themselves before giving out personal information to people or strangers.	Listen	PPT	10 min
Let's Role Play – Slide 15	Here you need to divide them in groups of five and distribute two scenarios from handouts on each group. Let them role play the scenarios	Listen and participate in the activity.	PPT, Scenarios, ACT2	30 min
How to be protective against social engineering – Slide 16-22	Here you need to highlight and advocate them on how to be more protective when it comes to either online or offline communication by giving them some tips and advice.	Listen	PPT	15 min



Action	Trainer	Participants	Materials	Timing
General Advice – Slide 23-24	Highlight key points on how a person could be little more cautious when it comes to social engineering.	Listen	PPT	5 min.
Any Questions? – 25 th Slide	Encourage participants to ask questions on the topic or even related to safety in general. Pass on workshop Learner feedbacks as well as the articles, FAQ, and tips for them to read when they get back home.	Ask questions if any.	PPT, LEARNER FEEDBACK	10 min



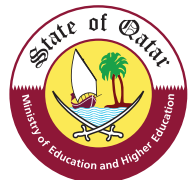


سيف سبيس
Safe Space

DIGITAL LITERACY CURRICULUM



STUDENT'S WORKSHOP
ACT 1. ICEBREAKERS
SOCIAL ENGINEERING



ACT 1.

Icebreakers

Notes for the trainer:

You can choose one of the icebreakers or pick an icebreaker you've previously done in your training practice. You don't have to do the icebreakers and usually with teachers you should choose those not requiring too much energy and moving around – a short conversation or a story from life is better than “hide and seek” or other activities of this kind. Just observe the group and think what they need – do they need more energy or less energy or do they just want you to go on with activities.

The icebreakers are described separately.

Only use icebreakers if you feel they will help you in the workshop. They are not the core of your content – do not fill the workshop just with icebreakers.

Brief description of icebreakers you will find in teacher's materials

Variations:

Treat the list of icebreakers as inspiration. This kind of micro-activities is something each trainer collects and modifies all the time and uses it when appropriate. If you have a group of teachers from the same school do not use icebreakers which are supposed to help the participants memorize each other's names as it is irrelevant, if the group of participants consists of older and experienced teachers – do not try to make them run around and sing as they will probably refuse.

If you feel you have a micro-activity you prefer to use – use it.



1. Names

Participants sit in circle and one by one pronounce their names repeating also all the names of people talking before them. The first one has an extra round repeating all names in the end.

2. Names

Participants sit in circle and one by one pronounce their names saying e.g. Ann – artist – finding words describing them best and starting with the same letter as their names.

3. Names

Participants just pronounce their names one by one.

4. Hobbies

Participants stand on chairs in a circle and given a category – walk on chairs to put themselves in a given order (e.g. size of shoe).

5. Hobbies

All participants draw what is their favorite hobby. Then 4 chosen participants stand in corners of the room and not speaking but just watching the drawings the other participants try to guess with whom they share hobbies. They find place next to the drawing they find describing similar hobby to theirs. STILL NO TALKING! After completing the task the group sits together and discuss the outcomes – how the façade can be misleading ☺.

6. Pure fun

Participants are divided into groups of at least 3 and get a task to build “a machine for...”. Depending on a level of participants’ ability of abstract thinking they either build specific machines i.e. for grass mowing or can build for example a machine for making sun shine.

7. Pure fun

One of participants sits on a chair and four other participants try to lift him/her with their fingers.

8. Pure fun

Guessing characters – participants have sticky notes on their backs with names of characters (from cartoons or from politics or movies etc.). Their task is to guess who they are. They can ask others questions but only can expect a yes or no answer.

9. Feedback

Cigarette – participants write feedback and fold the sheet of paper one by one to form a cigarette at the end. Trainer can decide on the kind of feedback he/she wants.

10. Feedback

Participants draw their hand on paper – just a sketch. Then they write their name on it. Then they are asked to count how many positive features they have and write the number down. Then they are asked to add 2 to the number they’ve written down and this is the number of their features they are asked to name and write down.



A decorative graphic consisting of several parallel diagonal lines in shades of gray, located on the left side of the page.

11. Feedback

The trainer puts a bowl in an exposed place and asks the participants to put their feedback to it on sticky notes each time they feel they want to.

12. Miscellaneous

Participants get in pairs and speak about each other for one minute, the other taking notes. The task is then to draw all the things heard and show to the group and let them guess what is drawn.

13. Anti – stress

What makes you angry in... (school, work etc.)? Write it down individually. We'll not read it. It's for you to realize. Now tear the papers into as small pieces as you can. And imagine some funny creature. Now stick the pieces on paper to form the creature you thought of 😊.



سيف سبيس
Safe Space

DIGITAL LITERACY CURRICULUM



STUDENT'S WORKSHOP
ACT 2. GROUP WORK
SOCIAL ENGINEERING



ACT 2. Group Work

Topic:

ACT 2- Role Play Social Engineering

Title:

Activity Title – Role Play

Objectives Covered:

Get participants familiar and able to react with different kinds of social engineering attacks.

Time:

30 minutes

Resources:

PPT, Scenarios from hand-outs – Slide 15.

Notes For The Trainer:

Ask participants to split in groups of five. Distribute two scenarios to each group. Give them two to three minutes to think about the scenarios given and let them choose one or two of the group to present scenario 1 and another one or two to present scenario 2. Give each group five minutes to present the outcome of the two scenarios given (two and a half minute for each scenario).

Conclude the role play activity, and move on to the next slide.

Variations:

If it's a small group, let them role play four scenarios and explain the rest to them.

If you find some groups struggling in role playing the scenarios, encourage them, and take part in of the scenarios given.

If you have enough time, and you're in a computer lab, ask them to look for more situations a person could get exposed to online or offline from social engineering. Ask them to present the outcome with possible solutions to the situations.



Scenarios

Social Engineering

Scenario 1:

You received a call from the school administrator claiming that your account information needs to be updated, and he/ she asked for your account credentials to verify and update your account. How will you react and what kind of measures will you take right after the call?

This scenario involves two people, receiver (student) and caller (so called IT administrator).

Scenario 2:

You received a call from someone claiming to be your Dad's bank, and he/ she asked you for some information about you or your Dad. What are the possible consequences, and how you should you react? And what kind of measures you will take right after the call?

This scenario involves two people, recipient (student) and sender (so called banker).

Scenario 3:

Someone identifies him/ herself as related to your classmate and wants to enter the school premises with you. What are the possible consequences, and how you should you react?

This scenario involves two people, (student) and (so called classmate relative).

Scenario 4:

You found a USB stick in the computer lab of the school and on the USB stick, there was written "Win the Prize" or "Nice Gift" or something like "for my girlfriend". What are the consequences, and how you should you react?

This scenario involves two people, a person who left the USB stick and the other who found it in the lab.

A decorative graphic consisting of several parallel diagonal lines in a light gray color, slanted from the top-left to the bottom-right.

Scenario 5:

Someone asked you for your phone because his/ her phone battery drained or died. What are the possible consequences, and how you should you react?

This scenario involves two people, recipient and requester.

Scenario 6:

Somebody you don't know well offered to drive you home. What are the possible consequences, and how you should you react?

This scenario involves two people, a person who offered a ride, and the recipient.

Scenario 7:

You are standing right at the ATM machine to withdraw some cash and before your start typing some information you found somebody standing close to you. What are the possible consequences, and how you should you react?

Scenario 8:

You're home alone and you got a phone call from somebody you don't know and he asked after your Dad for some URGENT issue related to work or something. What are the possible consequences, and how you should you react?

Scenario 9:

You have your phone with no password protection and you left it unattended at the lab or in the bathroom during break time. What are the possible consequences, and what you should have done differently to eliminate the risk?

Scenario 10:

You finished your assignment at the computer lab and saved it and printed it. What are the possible consequences, and what you should have done differently to eliminate the risk?

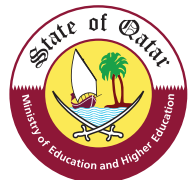


سيف سبيس
Safe Space

DIGITAL LITERACY CURRICULUM



STUDENT'S WORKSHOP
READING FOR TRAINERS
SOCIAL ENGINEERING



Background Reading For Trainers

Note:

The objective of the background reading is to provide trainers with detailed content regarding the topics they will be explaining and sharing with the audience.



Social Engineering Biggest Cyber Security Threat

When you hear of frauds, tricking or duping people of their money by using fake credit cards or breaking into Government websites or one's private social media sites, you cannot remain unaffected. You may wonder how these people do this when there are so many IT Security tools being used. It is here that one gets to know what 'Social Engineering' is.

The term 'Social Engineering' to a normal person could mean something beneficial, something to do with the 'social' aspect of Engineering (like electrical, mechanical or chemical engineering). But it has another meaning which refers to the different methods used to manipulate people to gain access to buildings, systems or share confidential information to commit fraud. The most harmless way of using social engineering is seen in any household - a child getting her way through her father to buy her a favorite toy. The same principle of manipulation is applied to different situations with different people.

Kevin Mitnick¹ the reformed computer criminal who is now a Security consultant states that "The weakest link in the security chain is the human element." The only purpose of a social engineer is to gain the trust of an individual for crucial information to make financial gain or steal one's identity or prepare themselves for a more targeted attack.

The Forbes² magazine predicted Social Engineering to be the greatest Cyber security threat in the year 2013 and we have been a witness to many such attacks on corporate organization and social media sites.

With Information Technology spreading its wings over all the aspects of human interaction in the areas of education, banking, shopping, social media etc., the threat of social engineering too is equally felt. The social engineer tries to build trust and gather information by various means or even develop a relationship, whereby he can exploit it to share or perform actions that could serve his purpose.

¹ <http://resources.infosecinstitute.com/social-engineering-art-human-hacking/>

² <http://www.forbes.com/sites/ciocentral/2012/12/05/the-biggest-cybersecurity-threats-of-2013-2/>



The different ways a social engineer tricks people:

- **Pretexting** is the most commonly and widely used technique wherein a person assumes a false or fake identity to gather personal information.
- **Shoulder Surfing** is mostly done when someone watches over the shoulder while keying in the password on a laptop/banking transaction/using an ATM card etc.
- **Diverting Theft** also known as corner game, is when the person convinces a courier or transport company that he is actually the intended person to receive the consignment.
- **Dumpster Diving** is when someone goes through the trash to gain information via bits of paper with passwords/address/e-mail id's.
- **Phishing** is an Internet fraud where an e-mail appears to come from a legitimate business—a bank, or credit card company requesting “verification” of personal information and warning of serious consequences if it is not provided.
- **Tailgating** is when a person gains entry into a physical facility through bluffing or fooling a legitimate person.
- **Baiting** uses an infected CD or device left unattended at a place to arouse the curiosity of a person to verify the contents on a system, thereby compromising the system.
- **Quid pro quo also known as “give and take policy”** is said to be used when the person offers help usually a free gift or technical support in-exchange for personal information.
- **Fake Pop-ups** are designed programs that appear in between legitimate work, informing the person to re-enter his ID and password to resume work due to network connectivity, thereby capturing personal information.

In summary, the above methods are used to get your personal details which you would never reveal under ordinary circumstances. If companies like Google and media sites like Facebook were not spared by the cyber-attacks, less prepared people will only be caught unaware. Being aware of ‘Social Engineering’ not only alerts you about the schemes used by ill-intentioned people but also prepares you to defeat their plans. As Miguel de Cervantes quotes “Forewarned, forearmed; to be prepared is half the victory.”



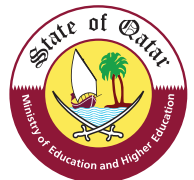


سيف سبيس
Safe Space

DIGITAL LITERACY CURRICULUM



**STUDENT'S WORKSHOP READING
FOR STUDENTS**
SOCIAL ENGINEERING



Background Reading For Students

Note:

Have the students read the background before coming to the workshop or prior to kicking off the workshop session.



Social Engineering For Students

What Youth Should Know About Social Engineering


Social Engineering is the act of manipulating people into performing actions. The objective is to trick someone into providing their valuable information or access to that information. This technique was mainly used by hackers to gain access to buildings, systems or data by exploiting human psychology rather than breaking in or using technical hacking methods. This technique has been practiced for ages; it was popularized as “Social Engineering” in the 90’s by famous hacker Kevin Mitnick. Currently he is an international information security consultant, and carries out testing a company’s security strengths and weaknesses.

Youth may not take Social Engineering risks seriously because they think that these techniques are mainly orchestrated on large organizations to gain access to their information. However, the fact is that criminals of the present generation are using this technique to gain access to homes and bank accounts primarily for money and teenagers are good targets. Social Engineering criminals are everywhere and are on the lookout to gain information with an objective to trick someone and make a profit out of it. We are prone to or may have become a victim to these attacks without our knowledge.

We may become a target to divulge information about our school, parents, or home etc. Which may not seem suspicious but could be used to carry out a criminal act? Social Engineers are skilled people who gain our trust and confidence. They disguise themselves as normal people and have the ability to extract any kind of information. A major Social Engineering scam that caught the attention of the public in 2010 was the famous WikiLeaks¹ initiated by Julian Assange to gain sensitive information from several countries. These kinds of attacks have caused great threats to an organization’s information and assets for which they are taking security measures to protect them.

¹ <http://news.idg.no/cw/art.cfm?id=57716384-1A64-6A71-CE2AE8785D9CF7BF>





We are prone to social engineering attacks when someone calls us representing themselves as the school's computer administrator to gain your system password. If you are not alert to crosscheck their identity, you may share your system password with the hacker. He may also gain access to our online accounts when we log-in to our account using the same password. The hacker can initiate a cyberbullying act on our contacts and damage our reputation online. This is one such way of getting our information, but social engineers use other ways such as making friendly conversations with you as they enter school pretending to be related to your school mate, thereby gaining entry into the school premises. Such hackers may enter the school premises to steal school related documents or try to gain information about the location of valuable assets to burgle them later.

Another such incident could be on our visit to the mall where someone approaches us to participate in a lucky dip competition by sharing that the winner will get a car, smart device, etc. We get excited about the gift and give our personal information. This technique called "quid-pro-quo", or "give and take policy" may or may not bring us any loss, but the people who are using our information are making profits by selling it to online merchants, data collecting companies, etc.

We have to know that our personal information is our identity and we need to safeguard our information.

Social Engineering Biggest Cyber Security Threat

When you hear of frauds, tricking or duping people of their money by using fake credit cards or breaking into Government websites or one's private social media sites, you cannot remain unaffected. You may wonder how these people do this when there are so many IT Security tools being used. It is here that one gets to know what 'Social Engineering' is.

The term 'Social Engineering' to normal person could mean something beneficial, something to do with the 'social' aspect of Engineering (like electrical, mechanical or chemical engineering). But it has another meaning which refers to the different methods used to manipulate people to gain access to buildings, systems or share confidential information to commit frauds. The most harmless way of using social engineering is seen in any household - a child getting her way through her father to buy her favorite toy. The same principle of manipulation is applied to different situations with different people.

Kevin Mitnick² the reformed computer criminal who is now a Security consultant states that "The weakest link in the security chain is the human element." The only purpose of a social engineer is to gain the trust of an individual for crucial information to make financial gain or steal one's identity or prepare themselves for a more targeted attack.

The Forbes³ magazine predicted Social Engineering to be the greatest Cyber security threat in the year 2013 and we have been a witness to many such attacks on corporate organization and social media sites.

With Information Technology spreading its wings over all the aspects of human interaction in the areas of education, banking, shopping, social media etc., the threat of social engineering too is equally felt. The social engineer tries to build trust and gather information by various means or even develop a relationship, whereby he can exploit it to share or perform actions that could serve his purpose.

² <http://resources.infosecinstitute.com/social-engineering-art-human-hacking/>

³ <http://www.forbes.com/sites/ciocentral/2012/12/05/the-biggest-cybersecurity-threats-of-2013-2/>



The different ways a social engineer tricks people:

- **Pretexting** is the most commonly and widely used technique wherein a person assumes a false or fake identity to gather personal information.
- **Shoulder Surfing** is mostly done when someone watches over the shoulder while keying in the password on a laptop/banking transaction/using an ATM card etc.
- **Diverting Theft** also known as corner game, is when the person convinces a courier or transport company that he is actually the intended person to receive the consignment.
- **Dumpster Diving** is when someone goes through the trash to gain information via bits of paper with passwords/address/e-mail id's.
- **Phishing** is an Internet fraud where an e-mail appears to come from a legitimate business—a bank, or credit card company requesting “verification” of personal information and warning of serious consequences if it is not provided.
- **Tailgating** is when a person gains entry into a physical facility through bluffing or fooling a legitimate person.
- **Baiting** uses an infected CD or device left unattended at a place to arouse the curiosity of a person to verify the contents on a system, thereby compromising the system.
- **Quid pro quo also known as “give and take policy”** is said to be used when the person offers help usually a free gift or technical support in-exchange for personal information.
- **Fake Pop-ups** are designed programs that appear in between legitimate work, informing the person to re-enter his ID and password to resume work due to network connectivity, thereby capturing personal information.

In summary, the above methods are used to get your personal details which you would never reveal under ordinary circumstances. If companies like Google and media sites like Facebook were not spared by the cyber-attacks, less prepared people will only be caught unaware. Being aware of ‘Social Engineering’ not only alerts you about the schemes used by ill-intentioned people but also prepares you to defeat their plans. As Miguel de Cervantes quotes “Forewarned, forearmed; to be prepared is half the victory.”



Social Engineering

Why Would Someone Hack Your Information?

Organizations consider information as the blood of the organization. Any compromise in the access of information may damage the reputation of the organization. Today our information is our identity, thanks to the online services, which are making our identity known globally. Today most of us are known and communicated through our online identities. As Teenagers we are particular about having an online identity and knowingly and unknowingly have created a reputation about ourselves online.

Our online identity helps us to process a lot of work without doing it in a traditional way. Earlier our online identity was used to send emails, share pictures, etc. However the former is done in addition to doing a lot of financial processing. We as teenagers may not be in a profession or hold bank accounts but an online criminal can use our information to do many things which may not be in our favor.

There are different reasons as why someone would steal your information:

The first reason can be '**greed**'; today our information is stolen from us and sold to online merchants who try to send emails or call us to promote their products and services. When we receive such calls we realize that somewhere we have not been careful about our information. There are people who search through trash bins (dumpster diving), peep into other's laptop or smart phone while at a cafeteria, airport, etc. (shoulder surfing) to gain information.

There are organizations that are stealing personal information and selling it to online companies and making good profit. Their greed is never satisfied.

The second reason is '**hatred**'; this is where cyber bullying kind of crimes happen. Sometime some teenagers develop a dislike towards another teenager in the school or playground and they try to harm them secretly. These kinds of attacks are initiated by familiar people or even by complete strangers.. The perpetrator gathers information about the victim from friends and sends a series of hurtful messages to the victim's online account to defame him/her and make them feel miserable.

The third reason is '**necessity**'; this is when someone is in dire need to obtain money by using your information. An identity fraud scam can happen where the perpetrator will use your information and try to apply for a loan which later requires you to repay the loan. This is prevalent these days and such perpetrators are often caught and imprisoned. As teenagers we may not have bank accounts, but they may try to get to our parent's accounts through us.

The point to consider is no wrong activity can be hidden for a long time, everything will be exposed. However till the perpetrator is caught, the victim suffers and it is a threat to others as well. We have to protect our information and also warn others if they are careless of their personal information.

Social Engineering FAQ

Why will a Social Engineer target me, as I'm just a student?

Students believe that social engineers would never target them for their information as they are just students with no bank accounts or assets. In fact, social engineers can steal identities which could be used to purchase a mobile SIM card on the victim's name and the victim will be charged with the bill later on. Hence, never take your information casually but protect it as social engineers are capable of doing anything with your information.

Tips:

1. Don't type in passwords with everyone else looking.
2. Set strong passwords on cell phones and other Internet enabled devices.
3. Never leave any confidential document unattended.
4. Shred documents completely before throwing into trash.
5. Never open email attachments when you are unsure of the sender.

