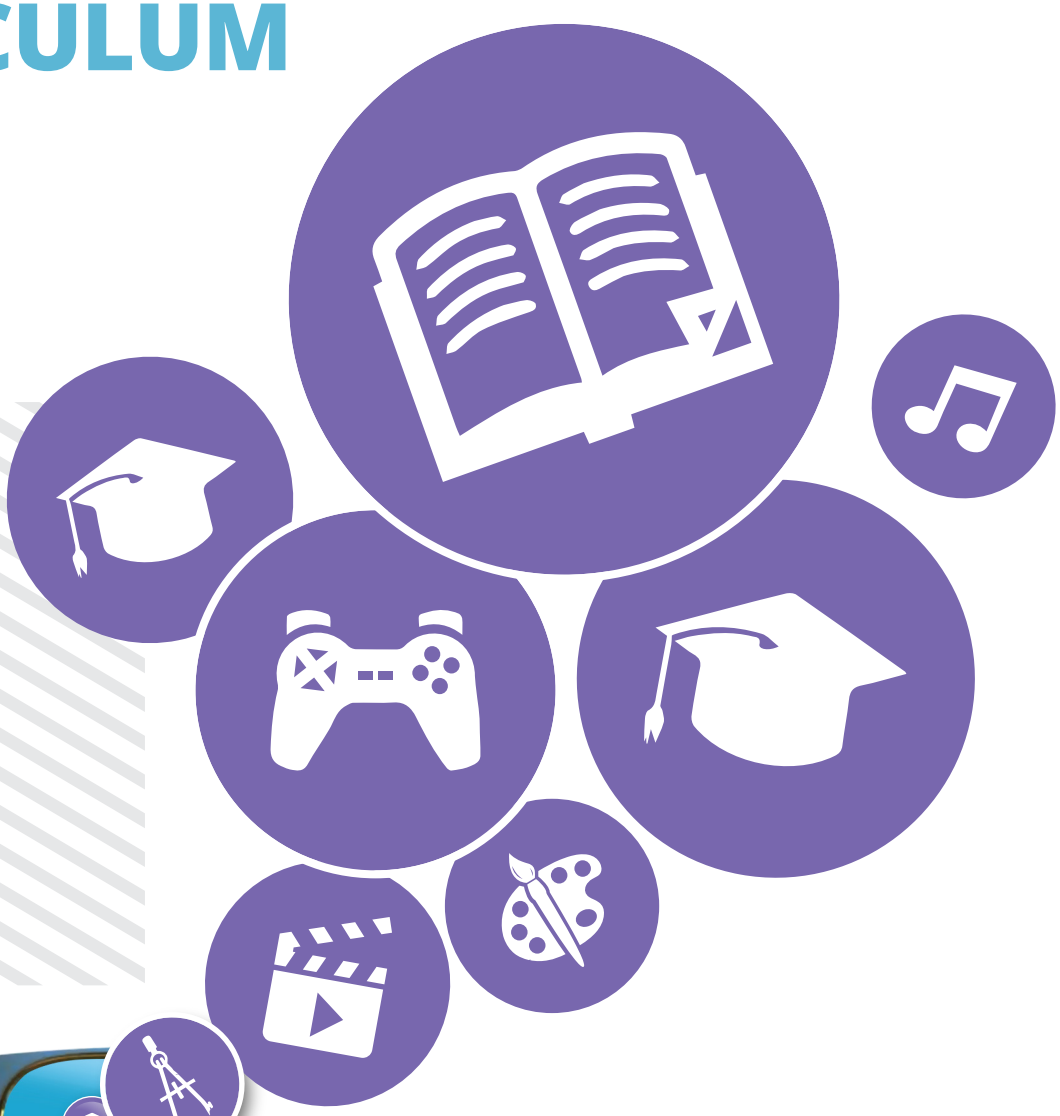
سيف سبيس
Safe Space

DIGITAL LITERACY CURRICULUM



STUDENT'S WORKSHOP GUIDE
IDENTITY THEFT

دولة قطر
State Of Qatar
Ministry of Transport & Communications
وزارة المواصلات والاتصالات

State of Qatar
Ministry of Education and Higher Education

سيف سبيس
Safe Space

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 Identity Theft Workshop File.

- Workshop Guide
- Background Reading for Trainer
- Background Reading for Student
- Identity Theft PowerPoint
- Workshop Practical Activities
- Workshop Notes
- Workshop Learner's Feedback

سيف سبيس
Safe Space

Introduction To Identity Theft Workshop

Target Audience: Students

Workshop Duration: 140 minutes

Workshop Components:

- Workshop Guide
- Background Reading for Trainer
- Background Reading for Student
- Identity Theft PowerPoint
- Workshop Practical Activities
- Workshop Notes
- Workshop Learner's Feedback

Workshop Overview:
The Identity Theft Workshop aims to help the students to understand what Identity Theft and Identity fraud are, the dangers of both, and the best ways to protect their personal information online, and prevent their identity from being stolen. To help students understand the concepts of identity theft, they will engage in 4 Practical Activities that give them the opportunity to practice what they are learning in the workshop first hand.

سيف سبيس
Safe Space

Workshop Guide
Identity Theft

Duration: Around 140 minutes

Requirements:
- Projector
- WIFI for the trainer
- regular room
- preferably round tables
- hand-outs
- activity sheets
- folders

Number of participants:
Maximum 25 students

Purpose:
To educate and raise the awareness on Identity theft.

Objectives:
1. Introduce the meaning of identity theft and fraud.
2. Make them aware of how much valuable information they need to protect.
3. Highlight the common types of ID theft.
4. Spread some caution tips to be considered.
5. Let them judge better in different ID theft situations they may face in life or on the internet.

Materials to be used:
- Flip-charts
- Lesson Plan
- Markers
- activity sheet
- Handouts
- PPT

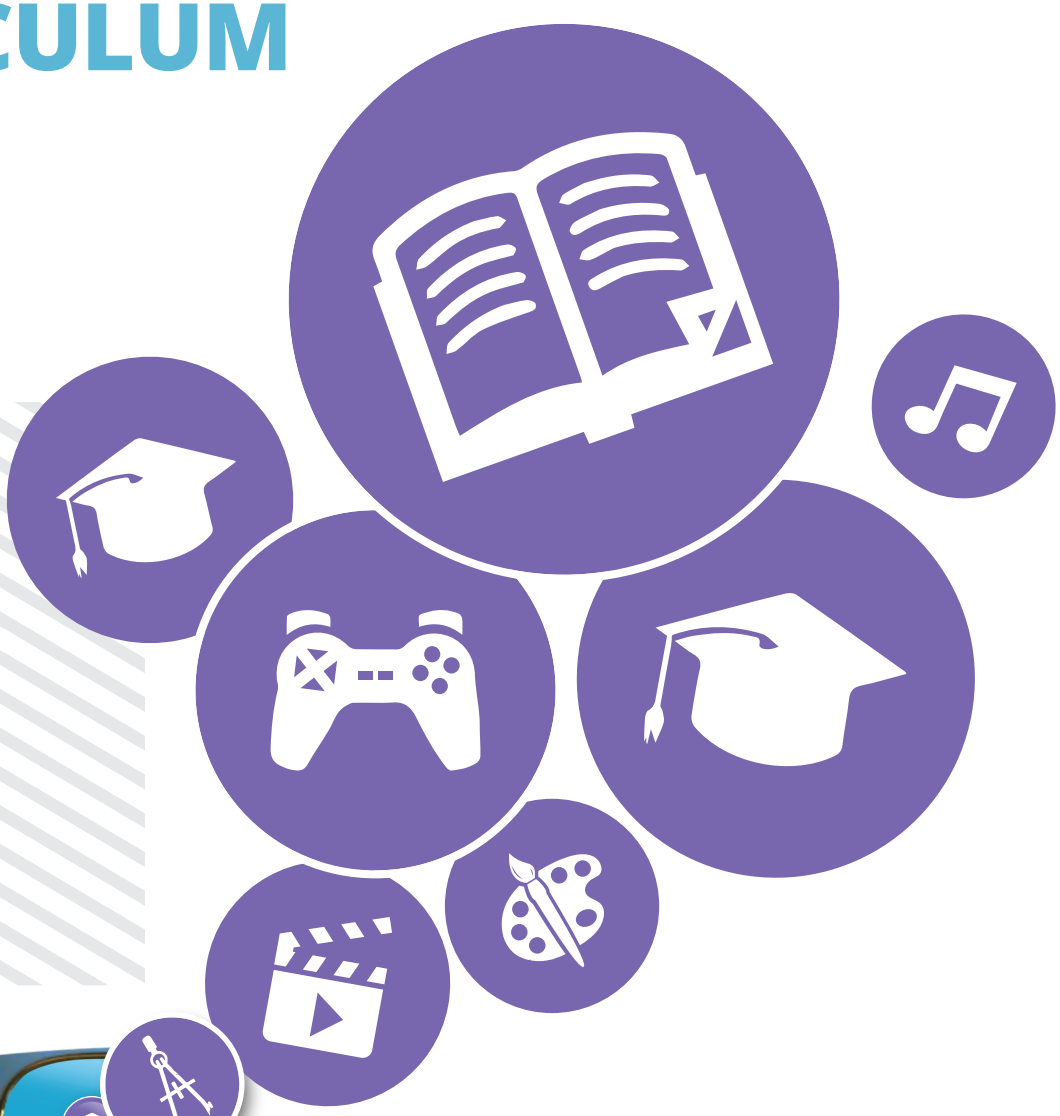
Action	Trainer	Participants	Materials	Timing
General Introduction to the program and today's topic – Slide 1	This is an opening slide. Introduces himself/herself and the program and today's topic DIGITAL LITERACY CURRICULUM. If needed – asks participants to introduce themselves If you think an icebreaker is needed – the trainer does it now.	Listen and introduce themselves.	PPT, Icebreakers ACT 1.	15 min
How to be Safe in Reality – Slide 2	You may want to talk here about safety from health , traffic, and life perspective and after that go ahead and ask the participants how different is the online world from the real world and if it is important to be safe in the online world as well as being safe in the real world.	Listen and discuss why Safety online is as big a concern as Safety in the real world.	PPT.	10 min
What is Cyber Safety – Slide 3	First encourage participants to define what could be a cyber-safety definition. Ask them what they think before you show them the scientific definition.	Listen and discuss.	PPT.	10 min
Is Cyber Safety Important? – List Online Threats (Group Work) – Slide 4	Asks students to divide into groups of 5 and pass on a flip chart sheet and encourage them to write down why would they think we need to be safe online and based on their answers, say YES, that means there are threats and accordingly ask them to list at least 8 online threats.	Get split in groups of 5. Write down why they think it is important to be safe online. List at least 8 online threats.	PPT, Flip chart, markers, ACT 2 – List Online Threats (Group Work).	20 min
Workshop Objectives – Slide 5	Define the objectives of today's topic. You may want to give a very brief introduction to Identity theft but not much.	Listen.	PPT.	5 min

Action	Trainer	Participants	Materials	Timing
Identity Theft – definition – Slide 6	Here the instructor is required to introduce Identity theft.	Listen.	PPT.	5 min
Identity Fraud – definition – Slide 7	Here the instructor is required to introduce Identity fraud.	Listen.	PPT.	5 min
Information You Have and They Look For – Slide 8	Highlight most of the valuable information a person can hold and ask them to offer more.	Listen and participate.	PPT.	5 min
Common Types of ID Theft – Slide 9	Highlight Common types of ID theft attacks.	Listen.	PPT.	5 min
Things Might Put Us in Danger – Slide 10	Highlight bad practices that might keep us at risk of being exposed to identity theft.	Listen and participate.	PPT.	5 min
Caution Tips – Slide 11	Highlight key areas to raise their awareness on how to protect themselves from identity theft crimes.	Listen and participate.	PPT.	5 min
Different Situations and How to React – Slide 12	Pass on the five questions from the hand-outs and ask them to split in groups of five and ask each group to present their outcome. Conclude and discuss the outcome.	Participate in the group work activity.	PPT, Flip-chart, ACT 3.	20 min

Action	Trainer	Participants	Materials	Timing
Brain Strom Identity Theft (mind map) – Slide 13	Encourage students to participate in the mind mapping game to wrap up all what was covered and they have learned.	Participate in the mind mapping game. Ask questions at the end if any.	PPT, ACT 4 – Brain Storm Identity Theft (Mind Mapping).	20 min
Any Questions? – Slide 14	Encourage participants to ask questions on the topic or even related to safety in general. Pass on Learner Feedbacks as well as an article 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
IDENTITY THEFT

دولة قطر
State Of Qatar
وزارة المواصلات والاتصالات
Ministry of Transport & Communications

State of Qatar
Ministry of Education and Higher Education

سيف سبيس
Safe Space

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.

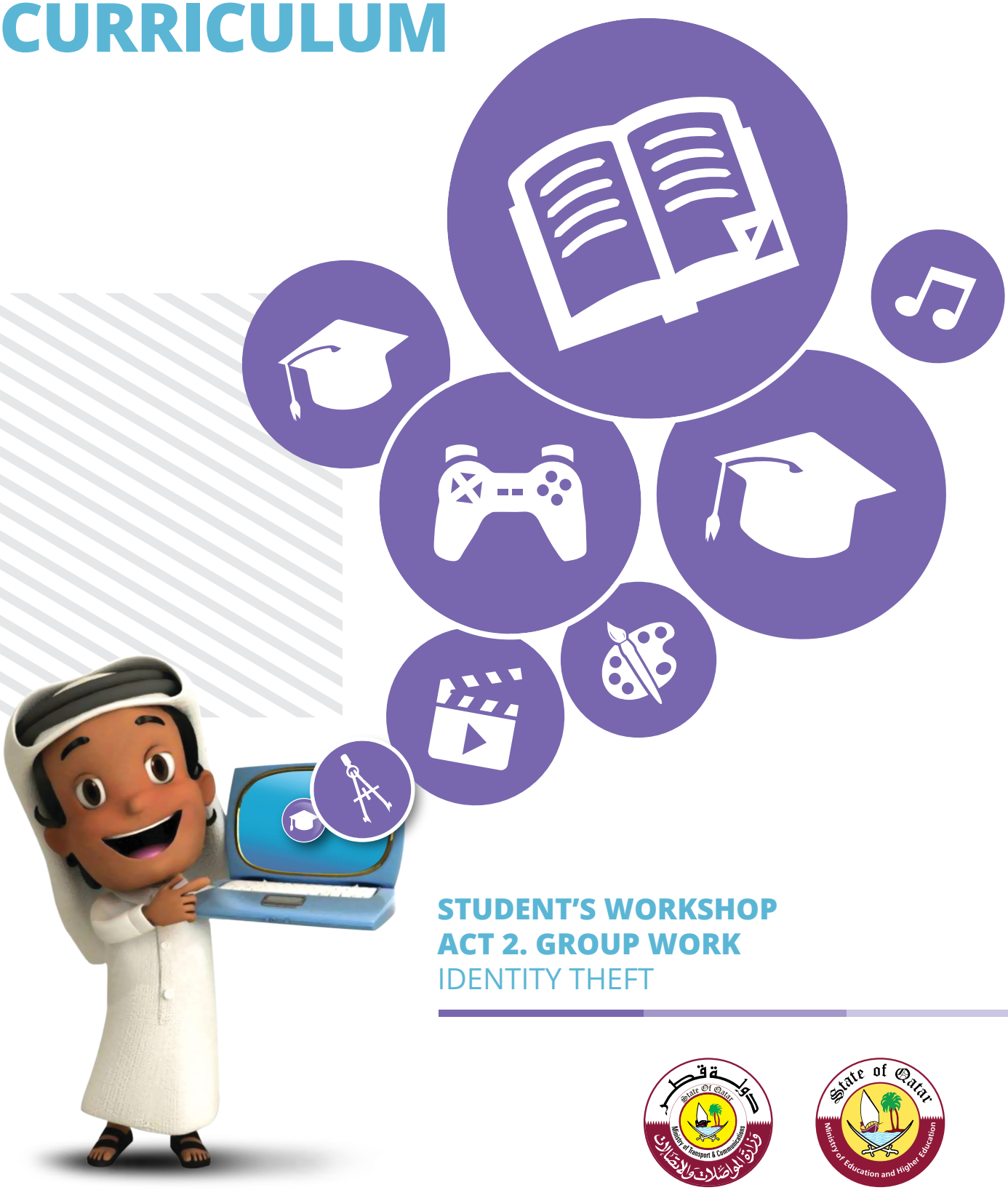
11. **Feedback**
    The trainer puts a bowl in an exposed place and asks the participants to put their feedback to it on sticky notes each time they feel they want to.

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
IDENTITY THEFT

State Of Qatar
Ministry of Transport & Communications
دولة قطر
وزارة المواصلات والاتصالات

State of Qatar
Ministry of Education and Higher Education

سيف سبيس
Safe Space

ACT 2 – (Group Work)
List Online Threats

Topic:
ACT 2- List Online Threats

Title:
List Online Threats – Group Work

Objectives covered:
1. Participants will be able to explain why would they need to be safe online.
2. Participants will be able to list a couple of online threats.

Time:
20 minutes

Resources
PPT, flip-chart, pen/marker for each group – Slide 4.

Notes for the trainer:
Divide students into groups of 5. Pass on a flip chart and a pen to each group. Encourage them to write down why safety is so important and why they would need to be safe online. After that, ask each group to list 8 online threats and to describe each of the threats in a brief sentence. You should not expect them to write exact terms, but mostly the things they face online that could hurt them or their family and to categorise them in a list of things.

Variations:
If a group seems to be willing to complete the task but you notice they didn't understand it – assist them. Write one of the threats for them and encourage them to write and explain the rest.

Let them think of what could happen or has happened to them before and ask them to categorise that as one of the threats.

If the group is small, ask participants to shout out the reason of why it is important to be safe online and a number of online threats while you write them on a flipchart and then walk them through the list.

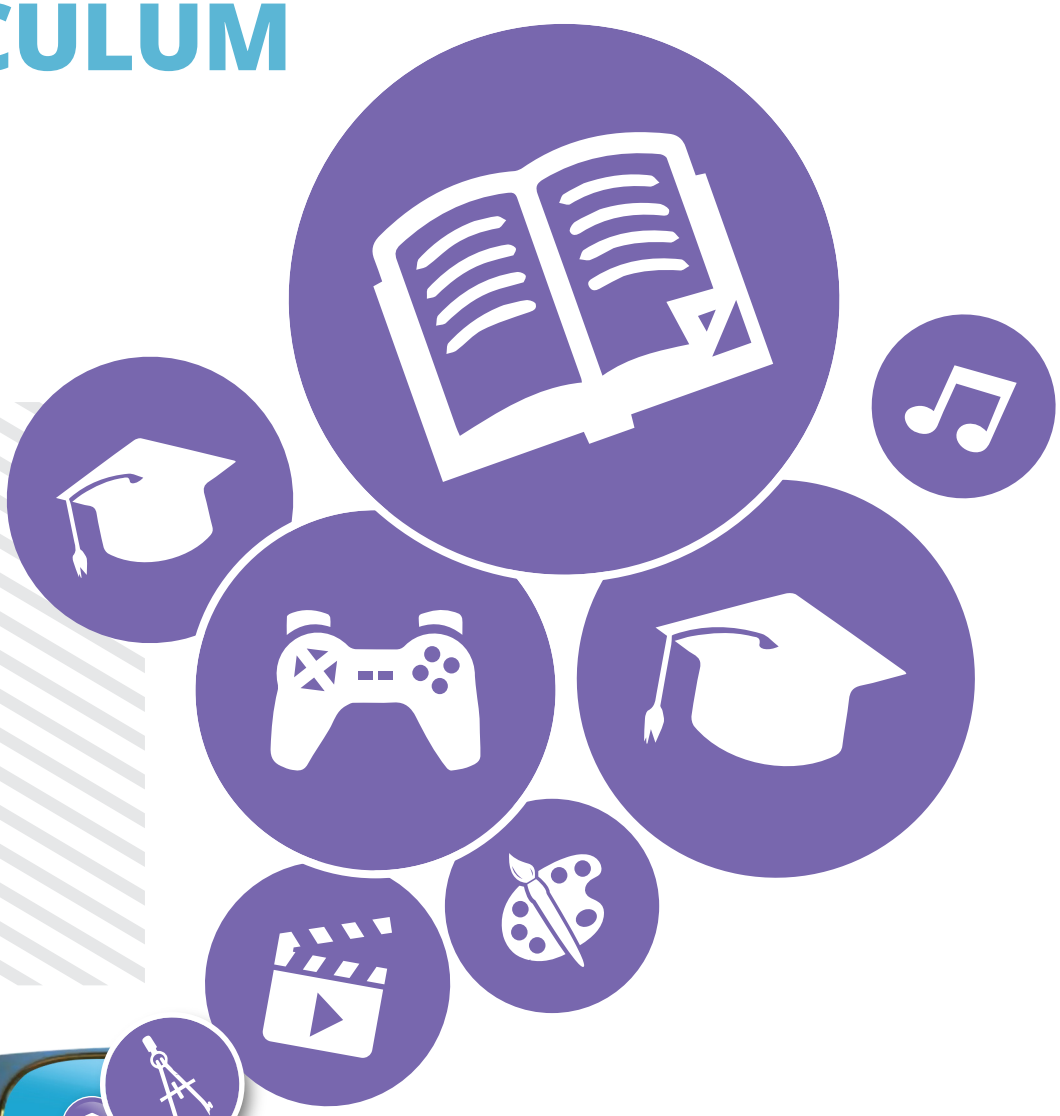
If computers are available and you have enough time, divide them into groups of five and ask them to look online for online threats and a definition of online safety in five minutes and then present the outcome to the rest of the group in three minutes.

If the session is being conducted in a library, divide them into groups of five and ask them to look for books on safety and pick any number of online threats and a definition on online safety in five minutes and then present the outcome to the rest of the group in three minutes.

Expectations:
Why is it important to stay safe online? In the same way you learn about safety when you leave the house, it is important to learn how to stay safe online. These are skills that will stay with you for life.

سيف سبيس
Safe Space

DIGITAL LITERACY CURRICULUM



STUDENT'S WORKSHOP
ACT 3. GROUP WORK
IDENTITY THEFT

State of Qatar
Ministry of Transport & Communications
دولة قطر
وزارة المواصلات والاتصالات

State of Qatar
Ministry of Education and Higher Education

سيف سبيس
Safe Space

ACT 3 – (Group Work) Different Situations and How to React

Topic:
ACT 3 - Different Situations and How to React

Title:
Different Situations and How to React – Group Work.

Objectives covered:
1. Participants will be able to judge properly when exposed to identity theft crimes online or in the real world.
2. Participants will get to know many different identity theft scenarios and proper ways of dealing with them.

Time:
20 minutes

Resources
PPT, Flip-chart, Scenarios or questions from handouts, Pen/marker for each group – Slide 12.

Notes for the trainer:
Divide participants in groups of five. Pass on all the five questions to each group with a pen or a maker. Ask them to take 10 minutes to answer the questions. Let them pick one of the group to present the outcome in less than a minute while you write the letters (a, b, or c) on the white board in the table below.

N.B. Draw the table as the following to discuss the outcome with all the groups.

	G1	G2	G3	G4	G5
Question 1	a	b	c	b	a
Question 2	b	c	b	b	b
Question 3	b	b	c	b	b
Question 4	a	b	a	c	a
Question 5	c	c	c	c	c

Conclude the activity in 5 minutes by showing the right answers to all the questions and explain the reason behind each answer or reaction to the situation.

Variations:

If you find a group having difficulty in answering the questions, try helping them.

If it's a small group, show them the questions with the answers on the slide show and let them give the answers while you write them on the white board.

If you have enough time and you're in a computer lab, let them search for more situations and present them to the rest of the group.

An alternative is to give each group one question instead and in two minutes they're supposed to answer and present the outcome to the rest in which all groups will get to know all the situations and their correct answer or the right way of dealing with each of the situations.

سيف سبيس
Safe Space

Questions & Answers For Different Situations and How to React?

Question 1: Bothered by faked banking banter?

You receive an email from your bank informing you that it suspects an unauthorized transaction on your account. To protect your account, the email advises you to click on a link to verify your identity. Should you do so?

1. No way – the whole thing sounds 'phishy'! If you're concerned about your account, contact your bank directly using a phone number or web address you know is genuine.
2. Yes. If someone is using your bank account, you don't have a second to lose. Immediately click on the link to verify your identity.
3. Yes – but first you should make sure the message looks like its legitimate.

Question 2: Attack of the Pop-ups?

You're surfing the web when you see a pop-up message from your Internet Service Provider (ISP) saying that it needs you to click on a link to verify or update your account information. Should you comply?

1. It sounds like a reasonable request, so click on the link to see what type of information they need from you, and follow the instructions.
2. Just say no. Legitimate companies, including ISPs, never ask for this information via pop-up ads or email.
3. Reply immediately. If you don't cooperate, you could run the risk of losing all you email messages, and possibly even being permanently disconnected from the internet.

Question 3: So you swallowed the bait, now what?

Despite all your precautions let's say you suspect that you've been 'phished' – and provided personal or financial information to someone masquerading as your ISP, bank, online payment services, or even a government agency. What should you do?

1. Not to worry. Because you gave your information in good faith, there's no way doing so could cause any problem.
2. Contact your local marine sports licensing board to see whether the company has a valid phishing license.
3. First, file a complaint at ftc.gov or at a police office. Then, since phishing victims can also become victims of ID theft, visit the FTC ID theft website for more information: **www.consumer.gov/idtheft**

Question 4: Is it safe?

Let's say you work for an organization with an excellent IT department. Your network administrator sends you an email warning of a security breach and asking you to confirm your password by entering it into a secure website. What should you do?

1. Don't share your password. Report the incident by calling your IT department.
2. Don't enter your password on the site. Instead, send your reply by email to the sender.
3. Immediately enter your password on the site. You can always trust emails from your own organizations.

Question 5: A Shocking Statement?

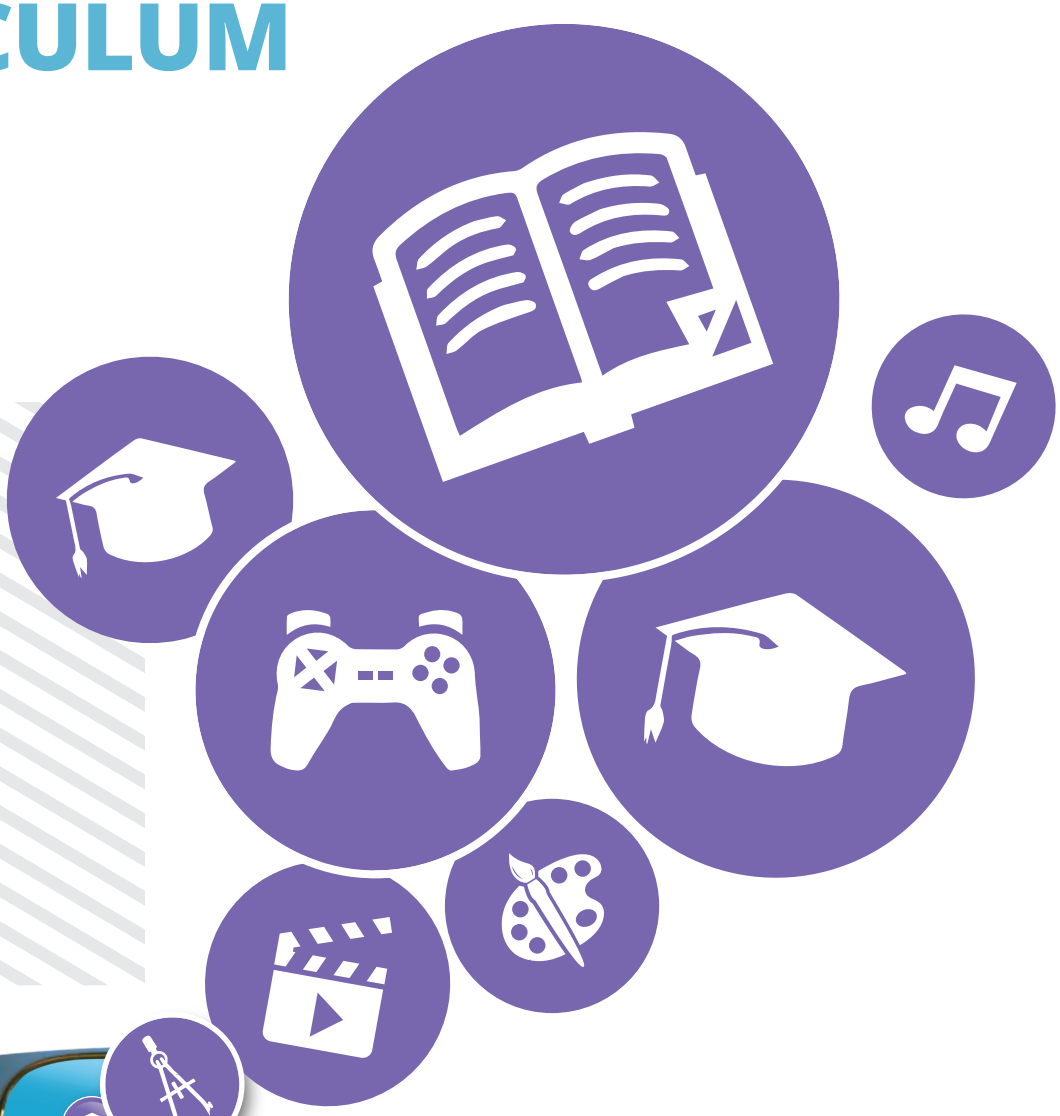
A security firm sends you an email and suggests several ways to avoid getting hooked by a phishing scam, including reviewing credit card and bank account statements as soon as you receive them. How can this help you avoid being scammed?

1. It's a quick way to make sure you're solvent. If you have money in the bank, or credit, you're still a player!
2. By reviewing your statements for unauthorized charges, you can know quickly whether someone has started using your account. If this happens, you can alert authorities and stop the problem before more damage occurs.
3. It's not that it helps directly, but it will give you something to do while waiting to see if the scammers have drained your account.

Ref: "Phishing Scams (Game)": **http://www.onguardonline.gov/media/game-0011-phishing-scams**

سيف سبيس
Safe Space

DIGITAL LITERACY CURRICULUM



STUDENT'S WORKSHOP
ACT 4. MIND MAPPING
IDENTITY THEFT

دولة قطر
State Of Qatar
وزارة المواصلات والاتصالات
Ministry of Transport & Communications

State of Qatar
Ministry of Education and Higher Education

سيف سبيس
Safe Space

ACT 4 – (Mind Mapping)
Brain Storm Identity Theft

Topic:
ACT 4 – Brain Storm Identity Theft

Title:
Brain Storm Identity Theft – Mind Mapping

Objectives covered:
Participants will be able to identify:
1. The meaning of identity theft and fraud.
2. How much valuable information they need to protect.
3. The common types of ID theft.
4. Some caution tips to be considered.
5. The right reaction to different situation they may face in life or on the internet.

Time:
20 minutes

Resources:
PPT, flip-chart, marker – Slide 13.

Notes for the trainer:
The trainer starts the mind mapping activity with Identity theft at the centre and asking questions like what is meant by identity theft and identity fraud and what are the information identity thieves look for? What are the common types of ID theft? What are the different situations a person could face? And how he/ she should react? Get all the answers and fill in the gaps on the mind map on a flip chart /or board . In this way the trainer makes sure everyone has understood the lecture and is ready to apply what they have learnt in the online world.

Let the students shout out the answers while you write them on a flip chart.

An example of a mind map on ID theft for you to get started:
http://www.mindmeister.com/233694760/id-theft

Variations:
If you see them struggle to find an answer try reminding them what was already covered during the day by mentioning titles and an answer or two as a teaser and expect the rest from them. If they weren't helpful enough to remember then do it yourself as a wrap up of what was covered.

You may leave the mind map all blank with You may leave the mind map all blank with ID theft at the centre or fill in some and encourage the students to fill in the rest.

If there is a computer lab, let them bring all the answers they learned from the lesson and ask them to dig for more online.

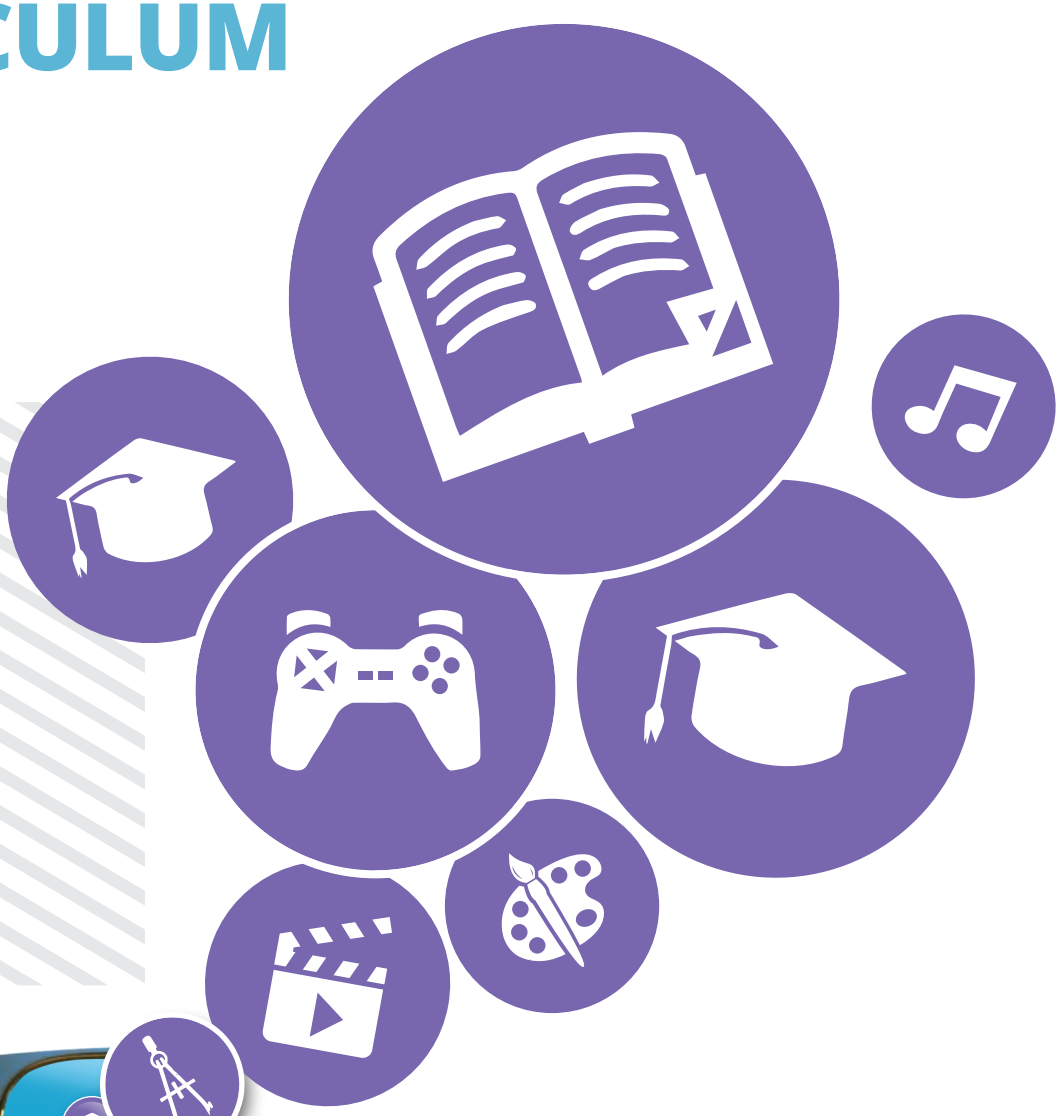
You may want to create the mind map on an online platform using the following information:

Username: safespaceqa2013@gmail.com
Password: safespaceqa2013safespaceqa2013

http://www.mindomo.com/mindmap

سيف سبيس
Safe Space

DIGITAL LITERACY CURRICULUM



STUDENT'S WORKSHOP READING FOR TRAINERS

IDENTITY THEFT

دولة قطر
State Of Qatar
وزارة المواصلات والاتصالات
Ministry of Transport & Communications

State of Qatar
Ministry of Education and Higher Education

سيف سبيس
Safe Space

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.

سيف سبيس
Safe Space

Identity Theft For Trainers

Protecting Student's Privacy Online

Identity theft is becoming a serious problem[1] making children, youth, adults and elderly people irrespective of age, gender and income level become victims of this threat. Anyone holding an identity in this world can be a target. Similarly, identity thieves can also be anyone from our school; friends in our neighborhood, a complete stranger, or people with bad intentions who indulge themselves in such practices. They can be an individual or a group of individuals. They can belong to the same country or orchestrate the entire crime from a different country. Everything amounts to one thing - money. Your information may not appear to have much value to you but for identity thieves it is of great value.

In today's generation, securing our identifiable information is challenging, as it is not just on paper but is also available and accessible electronically. Our identity has its presence in emails, social media sites, chat messengers, etc. Youth especially have to be educated on protecting personal information. In this regard, schools play an important role. Every educator must ensure that students know about protecting their privacy. This generation requires education on identity theft and online safety practices.

As educators, you have to propose to the school administration to incorporate online safety practices as part of school curriculum. If it already exists, it's good; otherwise this is very much needed as the Internet is accessed by one and all. So, where the Internet is accessible, students must also be educated on both good and bad aspects of the Internet. Students may not know the bad side of it as much of enjoying the good side of browsing, playing games, sending messages, pictures to friends, etc. What they fail to understand is that when we are not careful about our information online then we must be prepared to face negative consequences.

Students must be taught about protecting their identity whether it is on paper or electronically available. Educators have to conduct workshops with students as well as for parents. These workshops should present the current identity thefts and frauds happening around the world, and must be conducted on a regular basis to ensure that school, parents and students have a shared understanding.

[1] http://www.sheknows.com/parenting/articles/968131/teaching-teens-about-identity-theft

Here are some practices for educators to follow:

- Teach students not to share their personal information with strangers.
- Documents that contain personal information must be kept in a safe place.
- If documents containing personal information must be carried daily, have a photocopy of the original.
- Teach students to always have copies of the original documents containing personal information.
- Teach students to change their email passwords regularly and create strong passwords which are difficult to be cracked.
- Teach them not to subscribe for free online games and other services by providing personal identifiable information.
- Teach them never to share any personal information about themselves or family or known people online.
- Ask parents to monitor their children's online activities.
- Teach students to install updated and strong anti-virus softwares on their Internet enabled devices.
- Teach them to shred documents when not needed and never leave sensitive documents unattended anywhere (home or outside).

Teach students that any mail which mentions of their name or family names should not be left unattended. If it is not important, shred it completely and dispose them.

Youth are vulnerable to ID Thefts

The present generation is termed as being a transparent generation. The credit goes to the Internet and mobile communication technology. People are becoming more expressive and are willing to share their name and location with pictures and videos. Then we read on the news about people becoming victims of identity theft. Who should be blamed? Is it technology or the people using the technology?

Yes, it is people who use technology without proper guidelines and controls who contribute. The Internet is an open environment, with no boundaries, if there are to be boundaries and control points; it is with the people who have to place controls and practices. In this regard, youth are mostly vulnerable in losing their integrity. According to a survey conducted by Javelin Strategy[2] and Research technology, some 12.6 million Americans were victimized by ID theft in 2012, the second highest total since the Federal Trade Commission started counting victim in 2003. The criminals made off with $ 3 million more than in 2011.

Computer criminals are gaining the upper hand on many fronts because online users are not careful about their online activities. Identity theft has been in existence since the pre-technology era and still identity theft continues to escalate even in the age of cyber espionage and advanced targeted attacks. The concern with identity theft is that even infants become a victim even though they don't have any assets or a bank balance in their name. Identity thieves try to acquire their name and address and citizenship number (in western countries it is the Social Security Number). Then they create fake identity cards and apply for bank loans etc.

[2] http://www.nbcnews.com/technology/id-theft-rise-again-12-6-million-victims-2012-study-1C8448021

Identity theft is increasing because it is an easy means to success, once an individual's complete personal information is acquired. However the identity thief must be clever enough to follow through. Some are successful in carrying out the crime for a year or so, but some are caught at their first attempt. Having said this, every individual has to be careful about his/her personal information. Children and youth must be educated regarding protecting their privacy. There are companies who provide protection as well as help you to recover from an identity theft crisis. However these companies provide a premium service, which a normal individual cannot afford. For corporates and other industry sectors it is recommended and appropriate.

Our personal information should be our sole responsibility to secure. Every individual has to be careful about his /her personal information both online and in real life. Without our consent no one should be able to use our personal information. Identity theft can be stopped when we are mindful of what we say and provide online and in real life. There are computer criminals out there waiting to lure us and steal our identities; hence we must evaluate everything and everyone before providing personal information.

Protection from Identity theft and other online crimes

Identity theft has become a global problem and hence a global solution is required. Federal Trade Commission statistics reveal that children and youth are greater potential targets for identity theft compared to adults[3]. So when children and youth are considered, their surroundings are also taken into consideration. What are the areas where children and youth are vulnerable to identity theft? Youth spent almost 30% of their daily time in school and the rest at home; they might spend about 5% of their time with friends on a daily basis. Most of the schools have stricter policies that are implemented in school premises, which govern and protect the students and staff.

Schools play an important role in instilling the right behavior in youth. School is the place where a child's lifecycle begins from child to becoming a youth. In this regard educators have a greater role to play and their influence can bring a positive change in every student.

Youth are becoming a victim to online crimes because the discipline they follow at school is not practiced at other places. At school a student's activity is governed and monitored. The same may not apply elsewhere which is making them susceptible to these threats. Identity theft is occurring and prevalent because students are not mindful of their actions and behavior both physically and on the Internet medium.

Now that the Internet is becoming a necessary requirement for school education and mobile communications are becoming a basic necessity for everyone, it is recommended that schools have a subject on Information technology usage and policies. These policies are applicable only in the work place but because of the increase in online crimes and youth are fast becoming a target to ID thefts. It is necessary that youth be educated on IT policies and the risks of compromising their personal information.

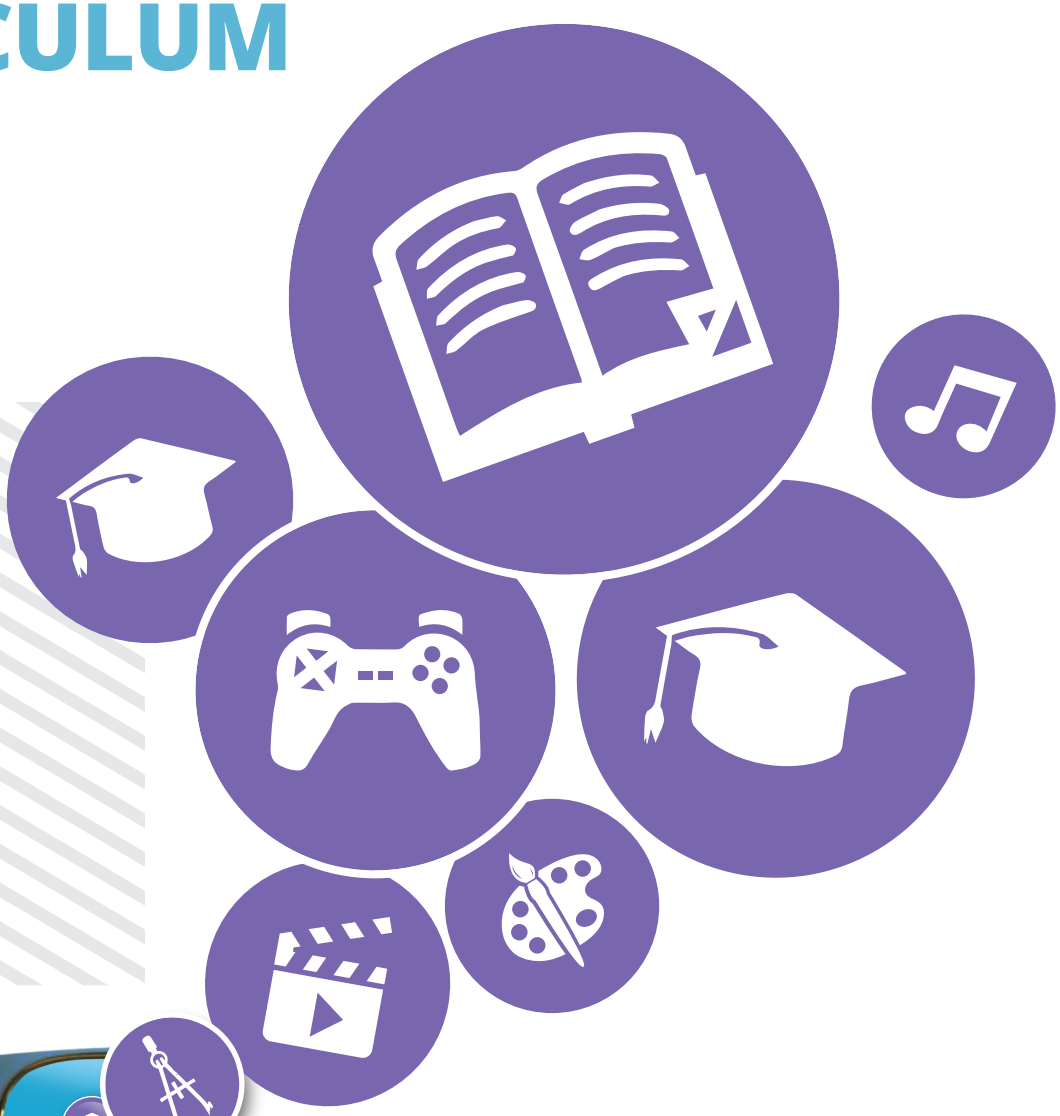
[3] http://www.ikeepsafe.org/be-a-pro/online-security/do-i-need-to-protect-my-childs-identity-online/

When youth are exposed to the dangerous side of the Internet, they will automatically know how to protect their information. Schools should have a subject on identity theft and other online crimes as part of their curriculum each year of their academic growth. Schools are conducting workshops and campaigns to promote awareness among students regarding protection of identity. As educators you should propose the need to have the subject of Internet threats and countermeasures as part of the school curriculum.

As educators you have to discuss these practices and threats with student's parents. Organize workshops with parents and students and elaborate on identity theft and other online crimes. Learn with them how online companies are making a business out of our information. Prepare an action plan where parents, students and educators commit with regard to best practices for protecting identity theft. These workshops should be interactive with role-plays to explain parents and students how an identity thief collects your information. These role-plays may include an incident at a shopping mall asking you to fill a form and win a prize, or an online stranger who gets lures you by sharing their false information and gathering our real information. These kinds of role-plays and reconstruction of real incidents in the form of drama can help students and parents understand the need to protect their identity as priority.

سيف سبيس
Safe Space

DIGITAL LITERACY CURRICULUM



STUDENT'S WORKSHOP
READING FOR STUDENTS
IDENTITY THEFT

State Of Qatar
Ministry of Transport & Communications
دولة قطر
وزارة المواصلات والاتصالات

State of Qatar
Ministry of Education and Higher Education

سيف سبيس
Safe Space

Background Reading For Students

Note:
Have the students read the background information document before coming to the workshop or prior to kicking off the workshop session.

سيف سبيس
Safe Space

Identity Theft For Students

Introduction to Identity Theft

ID theft can happen to anyone and at any time. As teenagers you are at risk of becoming an Identity theft (ID theft) victim. This is because you own and carry so much information with you without knowing what risks you may have to face when your information falls into the wrong hands. For a long time, Identity Theft was not given much thought. But in recent years, things have had to change due to the fact that it has become quite evident, that Identity Theft has become the fastest growing crime compared to other crimes in the world.

Now though, every country has set up specific organizations to curb and stop ID theft crimes. If you are unaware of such agencies, first register a police complaint. They will guide you on the right procedure to follow for resolving your problem. It's good there are agencies and organizations to approach when in trouble, but have you questioned why this trouble has come upon you. As teenagers you have to be aware of what personal information is and how your personal information can be stolen from you. This article will illustrate what is identity theft and what identity thieves want from you.

What is Identity theft?
Identity theft occurs[1] when someone steals your personal information and uses it to pretend to be you without your knowledge.

What is identity fraud?
Identity fraud happens when the person who has stolen your information uses it to cheat people and get money.

What information of yours is considered as personal information?
Personal information refers to any data about an individual that could potentially identify a person. In your case, personal information may include any of the following:

- Full Name
- Email address
- Date of birth
- Place of birth
- Residential address
- Telephone number
- Qatari ID number

[1] http://www.consumer.ftc.gov/features/feature-0014-identity-theft

Common Types of Identity Theft:

- Creating user names in another person's name.
- Applying for a loan in another person's name.
- Applying for credit cards fraudulently on another person's name.
- Create a fake identity on the Internet.

How can your identity be stolen?

1. An identity thief may steal your wallet or purse, if your wallet contains an identity card, driver's license (in the case of adults) bank related cards, phone book, etc. then the thief can collect information about your name, address, bank account, contact numbers, etc.
2. You may prefer maintaining easy passwords for your convenience such as date of birth, place of birth, vehicle number etc., and an Identity thief may use your personal details to guess easy passwords and gain access to your email account.
3. You may participate in a survey or competition at a mall and fill out your personal details which may be stolen later.
4. When you don't shred documents which contain personal information, an identity thief can search through trash bins and gather information pieces to create a false identity which he/she can use it for their gain.

Your identity is unique; safeguard it throughout your life.