

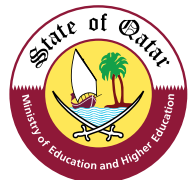


سيف سبيس
Safe Space

DIGITAL LITERACY CURRICULUM



STUDENT'S WORKSHOP GUIDE
INTERNET PRIVACY



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 Internet Privacy Workshop file.

- [Workshop Guide](#)
- [Background Reading for Trainer](#)
- [Background Reading for Student](#)
- [Internet Privacy PowerPoint](#)
- [Workshop Practical Activities](#)
- [Workshop Notes](#)
- [Workshop Learner's Feedback](#)



Introduction To Internet Privacy Workshop

Target Audience: Students

Workshop Duration: 160 Minutes

Workshop Components:

- [Workshop Guide](#)
- [Background Reading for Trainer](#)
- [Background Reading for Student](#)
- [Internet Privacy PowerPoint](#)
- [Workshop Practical Activities](#)
- [Workshop Notes](#)
- [Workshop Learner's Feedback](#)

Workshop Overview:

The Internet Privacy Workshop aims to deliver a holistic overview of what Internet privacy is all about, providing a thorough explanation of privacy settings and how to utilize them to make sure that the student's privacy is secured while browsing the internet. The workshop also provides quick, easy-to-remember tips on privacy that students can refer to after the workshop. Through discussion and group Practical Activities, the students will learn how to create a strong password to protect their online accounts, which will give them the opportunity to practice what they're learning in workshop first hand.



Workshop Guide

Internet Privacy

Duration: Around 160 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 awareness on Internet Privacy.

Objectives:

1. Introduce the audience to Safety and Cyber Safety.
2. Introduce them to Privacy and Privacy Settings.
3. Introduce them to quick tips on privacy.
4. Introduce them to Characteristics of Strong P@ssw0rd.
5. Help them create a strong p@ssw0rd.

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, icebreakers ACT 1	15 min
How to be Safe in Reality – Slide 2	You may want to talk here about safety from a health and life perspective and after that go ahead and ask the participants how different the online world is 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 is Safety online is big concern as Safety in the real world.	PPT	10 min
What is Cyber Safety – Slide 3	First encourage participants to define 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 ACT 2 – 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.	Split into 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	20 min
Workshop Objectives – Slide 5	Define the objectives of today's topic. You may want to give a very brief on Internet Privacy but not much.	Listen.	PPT	5 min

Action	Trainer	Participants	Materials	Timing
Privacy - Definition - Slide 6	Here the instructor is required to introduce Internet Privacy to the participants. Generally talk about privacy that it is the rule a person could have to define what is acceptable and what is NOT.	Listen.	PPT	5 min
Privacy Settings - Definition - Slide 7	Highlight the meaning of Privacy Settings and its relation to our information and accounts.	Listen.	PPT	5 min
What Can We do About it? - ACT 3 (Group Work) - Slide 8	Run the activity and have their answers and at the end highlight that this is how you can set your own rules and remember it's your "online territory".	Split into groups of five and participate in the activity.	PPT, Flip chart, markers, ACT 3	25 min
Quick Tips on Privacy - Slide 9	Walk them through the slide and highlight key tips a person should take care of while using the internet and technology. You may want to practically try some of them on the internet if you have time.	Listen.	PPT	10 min
Characteristics of Strong P@ssw0rd - Slide 10	Here you need to define the Characteristics of Strong P@ssw0rd and before you show them the slide, try having their answers first and then show the slide to confirm understanding or help them find out if they don't understand the clues.	Listen and discuss your opinion.	PPT.	5 min

Action	Trainer	Participants	Materials	Timing
How to Create Strong P@ssw0rd? – ACT 4 (Pair Work) – Password Creation Methodology – Slide 11	Define the two methods and let them pick the one that suits them more and ask them to make up a new strong P@ssw0rd.	Split into pairs and participate in the activity.	PPT, Flip chart, markers, ACT 4	25 min
Brain Storm Privacy – ACT 5 (mind mapping) – Slide 12	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 5	20 min
Any Questions? – Slide 13	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'S FEEDBACK.	10 min



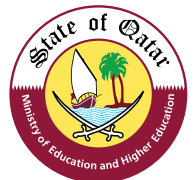


سيف سبيس
Safe Space

DIGITAL LITERACY CURRICULUM



STUDENT'S WORKSHOP
ACT 1. ICEBREAKERS
INTERNET PRIVACY



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. ☺

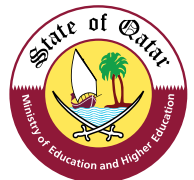


سيف سبيس
Safe Space

DIGITAL LITERACY CURRICULUM



STUDENT'S WORKSHOP
ACT 2. GROUP WORK
INTERNET PRIVACY



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 would they need to be safe online. After that, ask each group to list at 8 online threat and to describe each of the threats into 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 for them one of the threats and encourage them to write and explain the rest. Let them think of what could happen or

happened to them bad 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 is it 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 we 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.

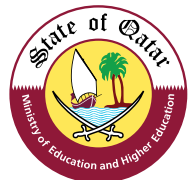


سيف سبيس
Safe Space

DIGITAL LITERACY CURRICULUM



STUDENT'S WORKSHOP
ACT 3. GROUP WORK
INTERNET PRIVACY



ACT 3 – (Group Work)

What Can We Do About It?

Topic:

ACT 3 – What Can We Do About It?

Title:

What Can We Do About It – Group Work

Objectives covered:

1. Participants will be able to define and highlight the difference between public and private information.
2. Participants will be able to decide what information they can share and what can't be shared.
3. Participants will be able to define the level of access for each of their relatives, friends and others.

Time:

25 minutes

Resources:

PPT, Flip-chart, Pen/marker for each group – Slide 8.

Notes for the trainer:

These are questions to be listed on the slides and they should write their answers on the flip chart that is being passed to them.

- Classify information between (Private / Public).
- What to Publish?
- What to keep locked?
- Define who could see what?

Divide them into groups of five and pass on flip chart, pen or marker. Ask each group to take ten minutes to go through the list of questions to define how they could secure their privacy online and offline. The objective is to help them find all the ways they could utilize to secure their privacy, help them define the difference between their private/ public information, let them decide what should be published and what should be kept private, define access rights. Ask all groups to pick one to present the outcome in three minutes.

Highlight at the end that this how you can set your own rules. Remember it is your “online territory”.

Do not rely on what “everyone says”. Use your own judgment and sense of modesty.

Variations:

If you see a group struggling to find answers, try to help them find some, but don't provide so much support and let them think of how they should treat their information.

If you're conducting this session in a lab environment, ask them to login to their account on FB and let them find and list all the privacy settings available and to define the function of each setting if applicable.

If it's a small group, encourage discussion and login to your FB account and show them all the settings and before you go through this, list all answers for predefined questions, so basically walk them through the list and then check all the settings and highlight important parameter to be set. Also, if that's the case, try to show a good model by having all the settings set up before class to show them that this is how it should be configured.

Exceptions:

Public Information:

- Profile picture.
- Basic information like interests and achievements.
- Places you may want to or visited before.
- ...and many more!

Private Information:

- Date of birth.
- Religious interest.
- Pictures with family and close friends.
- ...and many more!



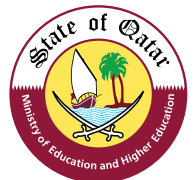


سيف سبيس
Safe Space

DIGITAL LITERACY CURRICULUM



STUDENT'S WORKSHOP
ACT 4. PAIR WORK
INTERNET PRIVACY



ACT 4 – (Pair Work)

How To Create A Strong P@ssw0rd

Topic:

ACT 4 - Password Creation Methodology

Title:

How to Create a Strong P@ssw0rd – Pair Work

Objectives covered:

1. Participants will get to know different ways of creating a strong password – “easy to remember, hard to guess”.
2. Participants will be able to use one of the methods highlight to create a very strong password.

Time:

25 minutes

Resources:

PPT, Flip chart, Pen/ marker for each group
– Slide 11.

Notes for the trainer:

First you need to teach them how to create a strong password in ten minutes and to do so you have to show them the two methods below and try to apply both on your passwords before you give the class, so you get more familiar with the topic.

Variations:

If the session is being conducted in a lab environment, ask them to login to their machines and look for more techniques and/ or methods on creating a strong password and let them use it and/ or present it to the class.

If it's a small group, walk them through the exercise yourself. Encourage them to contribute and let them shout out the answers while you write them on a flip chart or on the board.



Method1 (5 minutes):

Ask yourself the following questions where you can add more as such if you like:

- What street did you grow up on?
Abbas el Akaad street
- What is your best friend's name?
Ahmad Tarek
- What is the name of your first school?
MES
- How old are you?
13
- What is your birth date?
1990
- What is your pet's name?
Fluppy
- What is your father's middle name?
Tarek
- ...any many more!

After that and after you write all the answers (as highlighted in **blue-bold** above), pick the first two initials of each of the answers and put them together in capital form, so you'll get something like the following.

ABAHME1319FLTA

After that, set one or two rules and you're done!

First rule is to have one symbol between each of the two characters i.e. AB@AH...

Second, is to have one capital one small, i.e. Ab@Ah...

You will get something like the following.

Ab@Ah@Me@13@19@Fl@Ta

Note that you can have your own set of questions with you own set of rules.

Golden Rule → questions are public, rules and answers are private. No one will get to know the password without knowing the answers and the rules.

Good work! 😊

Method2 (2 minutes):

Write your old password, while shifting one key to the right, so if your password is "strongpassword" you should get something like the following:

"dytpmh[sddept"

Divide them in groups of two and ask each group to take five minutes to use any of the methods to create a **really** strong password. Pass on a flip chart and a pen or a marker. Ask them to present the outcome in one minute to the group.

At the end highlight how important it is to have a strong password and ask them to go back to their homes and do the same on your own.



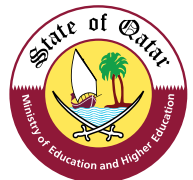


سيف سبيس
Safe Space

DIGITAL LITERACY CURRICULUM



STUDENT'S WORKSHOP
ACT 5. MIND MAPPING
INTERNET PRIVACY



ACT 5 – (Mind Mapping) Brain Storm Privacy

Topic:

ACT 5 – Brain Storm Privacy

Title:

Brain Storm Privacy – Mind Mapping

Objectives covered:

Participants will be able to identify:

1. the meaning of Privacy.
2. the importance of having privacy controlled.
3. the different methods for creating a strong password to ensure privacy.
4. tips on privacy.
5. characteristics of a strong password.

Time:

20 minutes

Resources:

PPT, flip-chart, pen or a marker – Slide 12.

Notes for the trainer:

The trainer starts the mind mapping with Privacy at the centre and starts by asking questions like what is meant by privacy? If it is important then Why? How do we ensure privacy? What are the different methods of creating a strong password? Fill in the gaps on the mind map on a flip chart /or board and by that the trainer makes sure everyone has understood the lecture and is ready to apply 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 Privacy for you to get started:

<http://www.mindmeister.com/26313716/online-reputation>

Variations:

If you see them struggle finding an answer try reminding them with 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 Privacy at the centre or fill in some and encourage the students to fill in the rest.

If there is a computer system, 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>

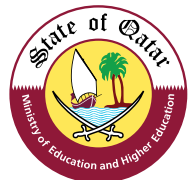


سيف سبيس
Safe Space

DIGITAL LITERACY CURRICULUM



STUDENT'S WORKSHOP
READING FOR TRAINERS
INTERNET PRIVACY



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.



Internet Privacy For Trainers

Protecting Student's Privacy Online:

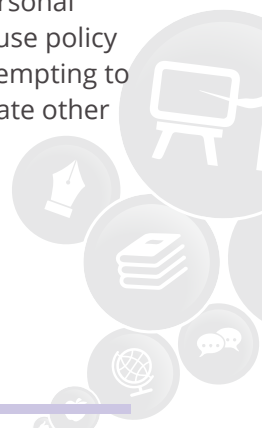
Information Technology has penetrated schools. This poses advantages as well as threats for a school administration, where they need to protect their students from risks on the web. When it comes to privacy issues, schools are more targeted as most of the easily identifiable personal information of the student is held by the school administration.

The Internet has become part of a school's curriculum. Having said this, educators have to be careful about the student's Internet usage at school. Educators have to upgrade their understanding with the advancements happening in the technology world. The present generation of students is far ahead when it comes to awareness and understanding of latest technology and educators have to get to that level to address the needs of the students. The same process must be discussed with parents to ensure a standard policy is followed both at school and home. Educators have to coordinate with the school administration to implement technology, protective measures, and develop Internet safety plans that address unauthorized disclosure, use and sharing of personally identifiable information on the Internet. Educators and school administrations have to consider a variety of aspects in order to establish an Internet safety and security plan to be followed by both staff and students.

To meet this requirement they need to address the following issues:

- Educators and school administrations have an obligation not to disclose student records¹. Many Internet companies offer services to schools that provide online access to student records. Contract with those companies must be reviewed properly before providing access to student records.
- Disclosure of student name, class and pictures of school with students should not be posted online. In this regard, school authorities should work with parents and take their consent and assistance in protecting the privacy of students.
- Educators must follow a standard guideline (sending encrypted email messages) when student's confidential information is transmitted via email to other educators or school staff.
- Educators must instruct students not to disclose their personal information over emails or on Websites. They should be taught about protection of personal privacy. The Internet acceptable use policy should restrict students from attempting to do such things as well as not violate other student's privacy.

¹ www.educationworld.com/a_tech/tech120.shtml



- Educators must learn to distinguish between Internet companies who offer legitimate Internet services that benefits student's education requirements' and those that do not. There are companies that are just on the lookout to access student information and sell it to online brokers for business purposes. Educators must discern between these and also train the students to know whom they are dealing with on the Internet when it comes to sharing their privacy.

These are some practices which educators and school administrations have to work on in implementing a standard Internet privacy policy. These policies must be explained to the entire staff and make them to comply with it to ensure protection of student as well as the school's reputation.

Ensuring Student's Online Privacy:

The days where traditional schools had black boards, paper and pen as learning tools are almost reducing now. These have been replaced by LCD screens, projectors, computers, and laptops. Everything is being digitized. Certain schools have become completely digital allowing students carry laptops and computer tablets instead of books. The Internet is rapidly changing the way education is being conducted. Everyone is becoming dependent on the Internet and hence people prefer to adapt to the transformation this digital age is bringing forth.

With new changes come new threats, as privacy of information may not be the same. As educators you need to counsel your students in conducting correct online practices.

Students are using the Internet to get access to information that will help them in completing their assignments. Parents trust and provide children with access to the Internet as children mention it is a requirement to complete school assignments. Though children start with the right intentions when using the Internet, they may later on may be misled with the features available on the Internet. Because the Internet offers so much facilities to browse information of any kind, chat with anyone from anywhere, post videos and pictures, etc. which all may not be suitable for children.

Educators should also be careful in protecting the student's information that is provided to them. School administration should have stricter polices in protecting students and staff information for maintaining school's reputation.

As educators you have to evaluate the amount of web exposure each student requires as part of their academics. The practices that schools are taking in protecting the privacy of students, similarly students should also be made aware of privacy safety. They need to be exposed to the good side and bad side of the Internet. As educators you need to speak with the school management and arrange for workshops on acceptable Internet usage. These workshops must be attended by both parents and students so that parents will also know what facilities they need to provide to their children.

School authorities must ensure that the staff too are upgraded with the latest innovations happening on the web and also train staff on the best practices that they need to practice and implement in class with the students.

You need to emphasize students about the importance of protecting their information both online and offline. Students should be taught about safe use of Internet. The web displays so many ads, games and win a gift offers etc., that children are lured into getting those fake benefits in exchange for providing their personal information. Internet companies maintain a digital dossier² on all the people accessing the Internet, which include the websites you access, the friends to whom you send emails, the photos in which you are tagged, and the information you search for on search engines (i.e. Google). Each person's access on the Internet is monitored and then complied to ascertain user choices. This information is then sold to online advertisers and merchants who try to contact us over email promoting their product. It should not come as a surprise when you receive an email promoting a product or service which you have been looking for.

It is said that once your information is on the Internet, you have lost control of the information. It can be used, misused and abused in ways you cannot think of. Educators must guide students by taking the following precautions so that students can maintain privacy while using the Internet.

- Stop clicking on advertisements³ and other offers which are on the web.
- Disable popup windows.
- Delete cookies daily.
- Never asks website to remember passwords.
- Never share personal information on social media sites.

² <http://ideas.time.com/2013/04/30/internet-privacy-a-new-bill-finally-offers-protections/>

³ <http://edition.cnn.com/2013/04/09/tech/privacy-outdated-digital-age>

⁴ <http://www.dailymail.co.uk/news/article-1354515/Teacher-sacked-posting-picture-holding-glass-wine-mug-beer-Facebook.html>

- Create strong passwords for emails and change it once every 3 months.
- Avoid sharing real pictures on the Internet, better to share a drawing.
- Avoid registering for sites which are not secure websites.
- Use secure mail servers for sending and receiving emails.
- Encrypt important documents when sending over email.

For parents:

1. Install parental control software's on the computer.
2. Discuss with educators and block websites which are not right for the children to access.

Educator's role towards privacy protection:

Ashley Payne⁴ a teacher working with Apalachee High School in Winder, Georgia, United States was asked to resign from school because she had posted a picture of herself holding a glass of wine and mug of beer on Facebook. This incident happened in the year 2009 when Ashley was enjoying her summer vacation. Her picture was spotted by a parent on Facebook and she complained about it to the school management. The school authorities gave Ashley a choice to resign or be suspended. Ashley resigned from her job and is now in a legal battle with the school to get her job back.



This incident may not happen in our culture but the moral we can derive is that the Internet cannot protect our privacy. The latest attitude among online users is that we want to post everything on the internet, a vacation picture, family get together, birthday celebration, watching sports at a stadium, etc. The problem that we don't realize is that sometimes the pictures can misrepresent us and reveal a different picture about ourselves, which is not true. Hence it is important to be cautious about your presence on the Internet.

As educators you need to protect your privacy and also train others to do the same. The irony is that now days, if we don't post about ourselves online there are others like friends who post pictures of ourselves on the Internet just for fun. In some cases it might be someone who is against us and can post a picture which can send out a different message on the Internet. It is necessary for us to be careful in all these aspects.

We need to educate our students on the importance of protecting their privacy as well as other's privacy. It's not about changing the student but we need to change the environment that will help educate the student in the right way. As educators you need to be cautious of your online activities. Your behavior and attitude that is displayed online matters. You need to maintain decorum while being online as well as urge your online friends to respect your privacy as you do for them. Be careful to post any real pictures of yourself or write any comment without giving it much thought. All these unprepared online action can later become damaging to your career as well as your character.

A student's perspective of looking at and accessing technology differs from the way we see it. They are not bothered about its consequences and threats. The advantage they see is that they are connected with friends; they can share pictures, videos, text messages and browse for information which is in abundance. They also want this kind of access without parent's and educator's supervision. An Educator's role is to make students aware of online risks and the restrictions that should be implemented while online. Students may not take it in the right spirit. However we have to ensure that they stay safe online.

Students should be taught about their online sharing practices, the online friends they maintain and keep including in their list of friends. Students should know that once they lose control of their privacy online, it is difficult to restore it again. Their intentions with which they share information online with others may not be interpreted correctly and can be misused in different ways. Have regular presentations on importance of student's privacy, show videos of victims of privacy invasion and the consequences of it. Have discussions with the students and know from them how they can recover from privacy compromises.

The same practice should be proposed to the school administration for school staff. All educators should know about privacy issues and there should be some collective best practices adopted and implemented in schools to ensure that educators are cautious of their privacy invasion online. When Educators are effective, students are efficient and the school is safer for growth and education.

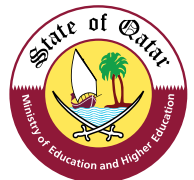


سيف سبيس
Safe Space

DIGITAL LITERACY CURRICULUM



STUDENT'S WORKSHOP
READING FOR STUDENTS
INTERNET PRIVACY



Background Reading For Students

Note:

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



Internet Privacy For Students

Introduction to Internet Privacy

What is Internet privacy?

Internet privacy involves controlling the information that an online user reveals about themselves and determining who has access to that information.

Risks to Internet Privacy

Online hackers depend on the following to extract user information¹:

- Internet Service Provider Is a business or organization that provides internet access to users.
- Cookies: Also known as browser cookies are created and stored on the user's computer when a user opens a web page.
- Data Logging – records the time when users access their computer.
- Spyware programs: software that is installed on a computer without the user's knowledge and steals information on the computer covertly.
- Web bugs: Also known as 'tracking bug' is a program embedded on the web page and is usually invisible to the user but tracks user's activities on the web page.
- Social engineering: Is the method of psychologically manipulating people to reveal their personal information.
- Phishing: Sending fraudulent emails to a user for example, representing a bank and collecting their personal information.

- Malicious proxy server: Proxy server is a server that protects your identity while surfing on the internet, and malicious proxy server is a server that poses as protecting your identity but steals your identity.
- Search engines: (Google) a web search engine used for researching information on the web.
- On-line social networks: (Facebook, Twitter) are online platform to build social relations and social networks, such as chatting, sharing interest, pictures, videos, viewpoints etc.

Responsible teenagers are careful to protect their personal identification documents such as birth certificate, academic documents, driver's license etc. They don't leave them unattended, share them with all or leave them unguarded. This same principle should be applied to the way personal information is shared online in order to restrict others from illegally using the information to impersonate or humiliate you.

Identity theft is on the rise and online hackers who engage in stealing another person's personal information can use this information to create bank accounts, apply for loans and take advantage of other benefits that you are entitled to.

¹ www.hiz.hr/icttrain/content/trainings/Privacy+on+the+Internet.ppt

Steps to protect your privacy:

1. Check twice or three times before you post any information pertaining to family or friends online.
2. Adjust your privacy settings on social networking sites to avoid unwanted attention from others.
3. Check the website privacy policy, prior to providing your contact information or email address.
4. Maintain at least two email accounts, one for social purposes and another account for professional and educational purposes.
5. Create strong passwords for email accounts you regularly use and keep changing them on a periodic basis to prevent unauthorized access.

Treat your personal information as you would treat your money – don't leave it lying around for others to take.

**The Internet² needs to know how to forget, all it knows is how to remember.
That's not very human** – Andrew Keen,
author and expert on digital economy.

Tips on Privacy

1. Remember that you should decide on what information³ you would reveal about yourself, when, why and to whom.
2. Ensure social network privacy settings are set to the most restricted levels.
3. Self-reflect before you self-reveal, think twice before you share anything about yourself.
4. Learn to respect other people's privacy online.
5. Geo locations apps should not be installed or used on the digital devices.

² <http://edition.cnn.com/2013/04/09/tech/privacy-outdated-digital-age>

³ <http://www.commonsemmedia.org/advice-for-parents/protecting-personal-privacy-online>

