Protecting and Valuing Identity

Cyber Safety Education for Parents and children 8 to 10 years

The world is at their fingertips, so let's keep an eye on them

John Parsons C21

Facebook: www.facebook.com/johnparsonsS2E

Website: www.Citizen21.co.nz

Please read the questions and answers before you let children read this information, confirming the content is consistent with your family values. *Note question 5 refers to pedophiles. You may wish to talk to your young children in more detail or less about this subject before they read the questions and answers.*

Your child will test your knowledge on cyber safety by asking you a set of questions from this resource, allowing them to become the teacher. The question sheets are separated into week 1, 2 and 3, Answers should be recorded separately. *You could complete each section once a week as a family and include family and friends outside of your bubble via the internet.* Why not invite grandparents to also participate in this question and answer activity perhaps via Skype, Facebook or a similar online platform. It is important to stay connected to family and friends who are living in other locations. We must maintain physical separation but not cyber separation.

Encourage teenagers in the home to use this resource to teach their brothers and sisters about online safety.

Please feel free to help them by discussing the questions and possible answers.

Once a week for the next few weeks I will be uploading a short format video on cyber safety for parents and their children to watch. You can access the videos through my Facebook page.

John Parsons
Safeguarding Children & Adults Online
Citizen21
www.citizen21.co.nz
info@citizen21.co.nz

Question 1: Why should we never submit to blog sites, chat rooms or social networks, information that tells the general public when we are on holiday?

Answer: Knowing when people are away and for how long (as well as where they live) is a gold mine for burglars. Homes have been burgled because of content uploaded by unwitting victims, their friends and or family members.

Question 2: What is an Internet predator?

Answer: A person who preys on someone by using any form of Digital Communication Technology (or any other means) to cause harm.

Question 3: How could a minor's social network profile harm their future prospects for employment?

Answer: Employers are utilising online background checks as part of their employment process. When a person young or older submits a CV to a potential employer, most employers will use Google and other IT technologies to search for information on the job applicant. If the content found is negative this can reduce the person's chance of getting the job.

Question 4: What is Identity Theft?

Answer: Identity Theft is a crime that can be committed by numerous types of individuals or organised criminals. Information unique to the individual is stolen for the purpose of committing a crime. The type of information stolen is wide in range and includes bank account information, credit card details, Social Security numbers, passwords, user names, passport numbers and even medical records. Some of this information can then be used by the criminal to purchase goods in social networks looking for unsuspecting victims who may have uploaded information about themselves, their friends and or family.

Question 5: What is Online Grooming?

Answer: Online grooming refers to the tactics used by some adults who try to trick and deceive minors, often by befriending them, using digital communication technologies such as mobile phones, chatrooms and social networks. That's why Parents, Grandparents and adults that look after young children, want to look at their children's devices to see who they might be connected to. It's actually showing how much they love their children.

Question 6: What is Net Burn?

Answer: Net Burn is the painful effect of over-exposure in cyber space of a person's personal life. It also occurs when a young person (or older) or their friends use the Internet without concern for negative impacts to record detailed accounts of their personal life. It often includes derogatory images of the person, inappropriate language or lack of respect for other people.

Question 8: What is Cyberbullying?

Answer: When a person deliberately and repeatedly uses Digital Communication Technologies to psychologically distress another person. The cyber bully may be an individual, or a group may be involved. Often this type of bullying can cause devastating consequences for the victim. Information uploaded by the bully can be available for a long time, leaving the victim feeling extremely vulnerable long after the bullying has stopped.

Question 9: If you see somebody being bullied, what can you do to help them?

Answer: Never get involved and never become a bully yourself. Even if *friends* try to get you to join in - don't. If you see or hear of somebody being bullied go and talk to a teacher or a trusted adult at home about it. If somebody comes up to you and says they are being bullied take them to a teacher or a trusted adult and support them especially if you are not at school. Most of all, the best

thing you can do is support the victim and help them talk to an adult about the situation.

Question 10: Before we take a picture or video of a friend or even a stranger, what should we do?

Answer: Ask for their permission. Remember people are unique and when we ask for permission we are respecting and protecting them.

Question 12: Why is a person's online identity so valuable?

Answer: Everybody is unique: our identity includes our family name, our brothers and sisters, where we live, what school we go to and much, much more. Our online identity helps tell the rest of the world who we are and what we are like. When we have a positive online identity it helps us as we go forward into the future. It even helps our family members because we often have the same last name as the rest of our family. People like employers will form ideas about us at interview time based on what they find on the Internet about us. So if it's inappropriate behavior like bullying, or saying nasty things about people it could reduce our chances of getting the job we want.

Question 13: What does Always respect, always protect mean. *Give one example*

Answer: Always respect, always protect really means following a set of principles that supports the individual, their family and their friends.

Here are 2 examples:

1 If a person has a picture of a friend on their computer and they want to upload it to Facebook, the first thing they must do is ask permission of the person who is in the image. When they do this, they "Respect" and "Protect" that person.

2 One of your friends on the Internet during an online communication asks you "When are you going on your holidays?" and you reply with "I don't talk about that kind of thing on the Internet", you are Respecting and Protecting yourself and your family.

Question 1: How do Internet predators get information that they can use to trick and deceive families and children?

Answer: By searching social networks, chatrooms and Blog sites looking at what people upload to the Internet. People actually make life easy for Internet Predators when they upload personal information.

Question 2: How can a personal family image on the Internet harm a family; example only.

Answer: If a young girl uploads a picture of her older sister providing details of where she works and socializes, this can place the older sister in danger. Often the older sister wouldn't even know this information had been uploaded to the Internet because the younger sister hadn't asked for permission.

Question 3: Name all potential victims when a boy or a girl uploads personal, private or embarrassing images or videos of friends or strangers.

Answer: The victims are numerous and include the person in the picture/video, the mother, father, brother(s) and sister(s) of the person in the image/video. The Internet connects family in numerous ways including surname and other related information. Often images of family and friends demonstrate those connections.

Example: An embarrassing picture of Tommy Tomkins age 10 from Nelson is uploaded to the Internet. Tommy's Dad goes for a job interview and the potential employer searches the Internet looking for any information on Tommie's Dad, George, that he can find. One of the pictures that returns from the Google search is of Tommy Tomkins the son of George. When the employer did the search, he typed in Tomkins of Nelson, so Google simply returned anything with that name in it. The picture of Tommy came back because he has the same last name as his Dad.

Question 4: What is a Server Log?

Answer: A server log is a copy of the information a person sends when using digital communication technology. For example, when a person sends a text message or a photo via a mobile phone the information sent is stored by the Internet Service Provider. So even if the sender and or receiver deletes the massage the ISP sill holds a copy.

Question 5: How can a Server Log help the police?

Answer: Example. A person is being cyber bullied by mobile phone or via the Internet. That person tells the police. The Police can then issue a warrant to the Internet Service Provider (ISP) so that they can access the messages that person has received. They can then get the ISP to track back to find who sent the mean-spirited messages. These Server Logs are used as evidence in court when required.

Question 6: Before we take a picture of a friend or family member what should we do?

Answer: Ask permission. Remember Always respect, Always protect.

Question 7: If a stranger asks a young person, perhaps at the local shopping centre or the local library, “Can I have your email address?” what should they say and then do?

Answer: Say “No,” or just ignore the person walk away and tell your parents or caregivers as soon as possible. You could also tell the librarian.

Question 8: What is a Squeeze Page?

Answer: Often when a child or adult is surfing the Internet, they end up at a web site offering them something for free. A screensaver, a software application or even the chance to win money or a holiday for the family. The website instructs them to download the gift. When the minor clicks the download button another screen appears which requires them to submit personal unique information including email address, full name and home address and in most cases, much more.

This is referred to as a Squeeze page. The minor has been targeted with a gift, providing they supply certain information which is valuable to third party applicants, marketers or even criminals. It is almost impossible to know the true intention of these sites. The gift cannot be accessed or downloaded *until* the information has been supplied. This process also allows identify thieves to covertly place a key logger on your computer during the download of the free gift.

Question 1: If a person is bullied how could they feel? Give three examples

Answers:

1 They could feel very scared or tearful

2 They could feel very alone

3 They could become so unwell that they need to see a doctor

Question 2: Why are some young children at risk on the Internet?

Answer: Because they are on the Internet in large numbers every day of the week and in many cases just because they are too young. They trust people too quickly, who they may have only connected to online.

Question 3: Name four online environments that predators go to in order to look for potential victims.

Answers: Social networks like Facebook, Chatrooms, Blog sites and online games.

Question 4 Describe some of the risks when using chatrooms.

Answers: You cannot know for certain who a person actually is. They could tell you they are 12 years old and they could be 26 and a criminal. Sometimes criminals simply watch what friends say to each other and they are able to extract sufficient information to trick or device a child.
For example, Sally messages her friends that her Dad is a fisherman who goes to sea for four weeks at a time. This means a criminal knows there are times her Dad is not at the house.

Question 5: Describe some of the dangers found when using Social Networks.

Answers: Users put revealing personal details and photos of their day-to-day lives online leaving them vulnerable to attack by criminals. Just like a chatroom, criminals search out and look at the information people upload so that they can commit a crime. The *perception* of safety, security and control leads the users to reveal information that can later be used to trick or deceive them.

Question 6: How can a negative post (information uploaded to a social network or blog site) harm a person; give two examples

Answers: If a young person uploads an image of themselves in an embarrassing or inappropriate situation then an employer might see this image which could reduce their chances of getting a particular job. If a young person bullies another person online, then this could also reduce a person's chances at interview time because employers do not want troublemakers or mean-spirited people in their workplace.

Question 7 Why should we never talk about personal things on the Internet?

Answer: Criminals rely on young people giving out personal information about themselves, their friends or family members. Criminals then use this personal information to trick and deceive children.

Question 8 If a young person feels threatened, embarrassed or just feels that something is wrong when they are using the Internet, a mobile phone or a computer, what should they do?

Answer: If a young person sees or experiences anything online or when using a mobile phone that makes them feel threatened or uncomfortable, they should do their best to tell parents or a trusted adult as soon as possible.

Question 9 Why should a young person never go to meet somebody they have only communicated with via the internet or by phone?

Answer: We can never know for certain who somebody is on the Internet or when communicating with them by phone. Criminals trick young people into meeting them. A YOUNG PERSON SHOULD NEVER GO TO MEET A PERSON THEY HAVE ONLY COMMUNICATED WITH VIA THE INTERNET OR BY PHONE WITHOUT MOM, DAD OR A TRUSTED ADULT WITH THEM?

FOLLOW JOHN PARSONS ON FACEBOOK AND ACCESS VIDEOS ON PROTECTING CHILDREN AND YOUNG PEOPLE ONLINE

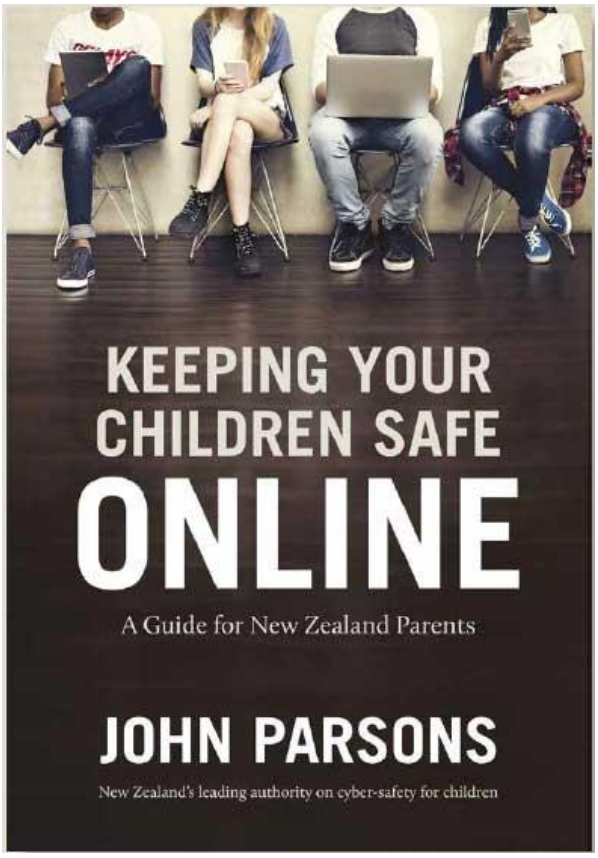
Facebook: www.facebook.com/johnparsonsS2E

PURCHASE JOHN'S BOOK, KEEPING YOUR CHILDREN SAFE ONLINE.

To request a signed copy delivered to your address with free postage

Email: citizen21@outlook.co.nz

$35.00 with free postage anywhere inside New Zealand



Important information

Call 111 in emergencies. If you can't decide whether it's a real emergency and you're still worried, call 111 and ask the Police. They will help you work out what to do.

You could also contact www.netsafe.org.nz if you have concerns about your child's use of Information Communication Technology. Sometimes a chat on the phone with an expert is all it requires to solve a problem or relieve a concern.