

# APPLICATION FORM: NMMU ENGAGEMENT EXCELLENCE AWARDS

(CONSULT THE NMMU ENGAGEMENT EXCELLENCE AWARDS POLICY AND READ THE APPLICATION FORM BEFORE COMPLETING THE TEMPLATE IN ORDER AVOID A DUPLICATION OF INFORMATION.)  
COMPLETE THIS FORM IN TYPESCRIPT. PROVIDE ONLY THE INFORMATION REQUESTED.

## SECTION A: Application category

- Indicate with an **X** in the appropriate box the award you are applying for.
- Your application will only be considered for the award you have applied for

- Engagement Excellence Award – Science, Technology and Engineering
- Engagement Excellence Award – Social Sciences and Humanities
- Engagement Excellence Team Award
- Engagement Excellence Project Award – Science, Technology and Engineering
- Engagement Excellence Project Award – Social Sciences and Humanities
- Emerging Engagement Excellence Awards *(note that Professors and Associate Professors are not eligible for this category)*

<b>Surname of Applicant/Team Leader</b>	Van Niekerk	
<b>First Name</b>	Johan	
<b>Initials</b>	JF	
<b>Title</b>	Prof	
<b>Telephone numbers</b>	041 504 3048	
<b>E-mail address</b>	<a href="mailto:johanvn@nmmu.ac.za">johanvn@nmmu.ac.za</a>	
<b>Employment position held at NMMU</b>	Associate Professor	
<b>Faculty</b>	EBEIT	
<b>Department</b>	Information Technology	
<b>Division</b>		
<b>Immediate line-manager</b>	Mrs Karen Church	
<b>Eligibility: Are you permanently employed and/or on a long term (3 years or more) fixed contract?</b> <i>(indicate with an X)</i>	<b>Permanent</b> X	<b>Fixed term contract</b>
<b>If this is an application for one of the Engagement Excellence Project Awards, provide a brief title and description of the project (250 words maximum)</b>	<b>Title:</b>  <b>Description:</b>	
<b>If this is an application for either the Excellence Awards or the Emerging Award, provide a brief description of your engagement activities and initiatives (250 words maximum)</b>	<b>Description:</b>	
<b>If this is an application for the Engagement</b>	<b>Staff:</b>	

**Excellence Team Award, provide**

- the names of all staff members and students participating
- the nature of their involvement
- a brief description of the team's engagement initiatives and activities (250 words maximum)

1. Prof Johan van Niekerk
2. Prof Rossouw von Solms
3. Prof Kerry-Lynn Thomson
4. Prof Mariana Gerber
5. Dr Lynn Futcher

**Students:**

1. Ms Rayne Reid (Doctoral Student and Poster Competition Coordinator)
2. Jason Cross (Provided graphic design services and created digital models for project mascots)
3. Various other students on an ad-hoc basis

**Description:**

**Cyber Safety Calendar Contest**

This project engages with school children, parents and teachers in the NMMM in order to teach the children how to be safe in cyberspace. We give talks at schools, develop and distribute curricula, and host an annual contest for children to create posters showcasing cyber safety awareness messages. Activities for this project is closely integrated with both our teaching & learning, and our research activities. The winning posters created by school children are used in further future awareness campaigns aimed at children. Our primary goal is to foster cybersecurity awareness amongst all South Africans, but for the purposes of this project we focus primarily on school children via various channels.

**Are your Engagement activities/projects/initiatives registered on the Engagement Management Information System (E-MIS) on SharePoint?**

If not, please ensure that they are before you submit this application.

Applications that are not registered and updated on the E-MIS will not be considered for Awards.

The most recent date on E-MIS for each project update (achieved when 'submit' is clicked) must be in 2015.

Provide the exact titles (as featured on the E-MIS) for all of the Engagement activities/ projects/ initiatives with which you are involved.

Visit <http://caec.nmmu.ac.za/Engagement-Information-and-Development/Engagement-Management-Information-System>

**Titles:**

1. Cyber Safety Calendar Contest
- 2.

**SECTION B: Engagement categories**

- You are required to describe and report in detail on a minimum of two engagement categories (these are 1, 2, 3 and 4 below) in order to be considered for an award.
- If you or your team are involved in three or four of the engagement categories, report in detail on all of these categories.
- Applications that describe and can provide evidence of engagement activities across all four categories are encouraged.

- *Refer to section 5 of the attached Engagement Excellence Awards policy which provides a guideline on the specific activities you should report on under each of the categories you have chosen.*

**Report on your:**

**1. Engagement through Community Interaction, Service and Outreach:**

Members of our team visited several schools in the Nelson Mandela Metropolis to give cyber safety talks to school children and/or to promote the calendar contest (i.e. Brylin, Pearson, Framesby, Collegiate, and more). In addition to school visits, talks on this topic were given at other appropriate forums. These included:

- Multiple Cybersafety talks to Learners at the Nelson Mandela Bay Science and Technology Centre in Uitenhage during the SciFest week
- a Cybersecurity talk to the Learners (Grade 11) of the NMMU-FamHealth Youth Leadership Academy in Gelvandale, Port Elizabeth.
- a Cyberbullying talk to social workers, teachers and psychologists at a Child Mental Health Symposium at the NMMU.
- a Guest lecture on Cybersafety to Media Studies students
- an Invited Talk on Cybersafety for the Youth to the South African Online User Group's (SAOUG) annual congress at the CSIR (This group consists of librarians from all universities in South Africa)

Approximately 25 Teachers from +- 20 schools in the Nelson Mandela Metropolis received a cybersafety curriculum and supporting material that we provided free of charge. This curriculum includes 24 lessons with supporting material in the form of videos, learning objectives, assignments.

Members of the group regularly give cybersecurity talks on radio. In 2014 specifically several talks were given on Radio Namakwaland.

**Report on your:**

**2. Engagement through Teaching and Learning:**

The poster project is closely integrated into several of our formal subject offerings. Firstly, the poster contest is used as a case study for students who take the B Tech subject "Information Security IV" in order to teach these students about awareness campaigns and the role these play in both societal and organizational security. Students from this class create awareness material in the form of posters, as well as other content that forms part of the curriculum provided to schools, as assignments for the subject.

The related online Security Education and Training NMMU SLP (SEAT) is also used by these B Tech students and their feedback is further used to improve SEAT. SEAT is made available to participating teachers, parents, and children free of charge.

Secondly, many B Tech students create additional material for this engagement campaign, as their primary 4<sup>th</sup> year projects. For example, in 2014 more than 10 students each developed an interactive e-book/game specifically for use in this project. These e-books/games taught many underlying cyber safety lessons in innovative ways to children. (See screenshots in attached portfolio)

**Report on your:**

**3. Engagement through Profession/Discipline-Based Service Provision:**

We see ourselves as both IT security professionals and as professional educators. As such the creation and distribution of the curriculum to teachers can be seen as a provision of our professional services.

More directly, the NMMU SLP we use for this project, Security Education and Training (SEAT), is also provided to various external parties in order to help foster a wider cybersecurity culture in South Africa. During 2014 this course was completed by a class of university students from UJ as part of their information security course.

During October 2014 we hosted a cybersecurity awareness week at the NMMU targeting staff, and indirectly their children, with our awareness material (The same material we use for schools). Many children are put at risk through unsafe computers provided by their parents. We had more than 50 staff members who completed our SEAT SLP. We also partnered with ICT services to provide a bring your own device facility for staff to bring their own computers from home, to be cleaned from malware and to have new anti-malware software etc installed.

Report on your:

**4. Engagement through Research and Scholarship:**

Our members are very active in research directly related to this project. Ms Rayne Reid's PhD focuses specifically on the problem of fostering a cybersecurity culture in South Africa and her research has been applied in many ways during this project. We also have several other post graduate students who work on problems related to this project.

The following publications that are directly relevant to this project were made during 2014:

1. Reid, R. & Van Niekerk, J. (2014). Snakes and ladders for digital natives: information security education for the youth. *Information Management & Computer Security*, 22 (2).
2. Reid, R. & Van Niekerk, J. (2014). Brain-compatible, Web-based Information Security Education: A Statistical Study. *Information Management & Computer Security*, 22, (4).
3. Reid, R., Van Niekerk, J. (2014). Towards an Education Campaign for Fostering a Societal, Cyber Security Culture. 8th International Symposium on Human Aspects of Information Security & Assurance. 8-10 July 2014, Plymouth, UK.
4. Von Solms, S., Von Solms, R. (2014). Towards Cyber Safety Education in Primary Schools in Africa. 8th International Symposium on Human Aspects of Information Security & Assurance. 8-10 July 2014, Plymouth, UK.

All of the above papers reported on various aspects of the campaign itself, or on awareness material that was developed specifically as part of this project. Paper 1 above relates to a cybersafety game we developed during prior years, paper 2 reports on the refinement of our SEAT course, paper 3 on changes we made in the overall campaign, paper 4 reports on the development of the curriculum we distributed to teachers.

**SECTION C: Descriptions**

**1. Describe the impact your Engagement activities have made on stakeholders/beneficiaries/communities and provide details on how these activities are acknowledged/recognized by:**

<p>1.1. External communities/stakeholders/beneficiaries: (not staff and students of NMMU)</p>	<p>Teachers in the Metropolis have been enabled to teach children about cyber security. See the two</p>
-----------------------------------------------------------------------------------------------	---------------------------------------------------------------------------------------------------------

	<p>newspaper articles acknowledging our efforts in the attached portfolio of evidence.</p> <p>During 2014 almost 300 learners from 5 schools submitted entries to our contest. This was less entries than 2013 due to us running the contest too late in the year. However, 36 prize winners were identified from these and received their prizes during the ceremony we held in 2015.</p>
<p>1.2. Internal communities/stakeholders/beneficiaries: (staff and students of NMMU)</p>	<p>More than 50 staff members completed our SEAT course during the awareness week in October.</p> <p>Many of our current (2015) masters students registered specifically to work in cybersecurity due to their exposure to this project in their B Tech. Ms Zola Nogaga, for example is now working towards her Masters with the development of a curriculum more suitable for high school children as her research topic.</p> <p>This project makes topics like information security awareness much more practical for our B Tech students since they are actively involved in creating the material we use for this project.</p>
<p><b>2. Describe how your Engagement activities contribute towards faculty/department/entity engagement goals and objectives. (Refer to your Department/Faculty/Entity's strategic plan here)</b></p>	
<p>The EBEIT faculty has as one of its strategic objectives to "Strongly connect industry and community engagement to on-campus research and educational strengths."</p>	
<p>This project is a perfect showcase of such a strong connection. We are exceptionally well established as researchers in information and cyber security. Three of the project members are NRF rated researchers in this field and all of the members publish in this field on a regular basis. We also have a very strong history of teaching excellence in information security. This project leverages both these strengths and applies our research and educational expertise directly to a problem that has been identified as a national priority.</p>	
<p><b>3. Describe how your Engagement activities contribute towards the achievement of the NMMU Vision 2020 Engagement Strategic Goals and Objectives. (Refer to the attached NMMU Engagement Strategic Goals and Objectives)</b></p>	
<p>This project aligns exceptionally well with the Ubuntu core value. A very large cyber security problem in our schools is the problem of cyber-bullying. Our awareness education thus also have a large component to try to address cyber-bullying and to make school children aware of the long-term implications of their online behavior, the ethics of using cyber space, etc. Ubuntu is a fundamental building block in becoming a responsible cyber citizen.</p>	
<p><b>4. Describe how your Engagement activities contribute towards: (Refer to any relevant media coverage, representation on boards or committees, scholarly publications, conference presentations etc.)</b></p>	
<p>4.1. Addressing the needs of society and various external communities served by NMMU:</p> <p>Cybersecurity awareness for citizens, industry and government at all levels has been identified by the Department of Science and Technology in a draft National Cybersecurity Research, Development and Innovation Agenda as one of the national priorities. This project is one of a very small group of such projects nationally that are well established and can be shown to be successful. This is the only such project in</p>	

the Nelson Mandela Metropole.

Through this project we provided teachers from about 20 schools with a cybersafety curriculum and supporting material. See the attached press clippings.

The following publications stemmed directly from the project:

1. Reid, R. & Van Niekerk, J. (2014). Snakes and ladders for digital natives: information security education for the youth. *Information Management & Computer Security*, 22 (2).

2. Reid, R. & Van Niekerk, J. (2014). Brain-compatible, Web-based Information Security Education: A Statistical Study. *Information Management & Computer Security*, 22, (4).

3. Reid, R., Van Niekerk, J. (2014). Towards an Education Campaign for Fostering a Societal, Cyber Security Culture. 8th International Symposium on Human Aspects of Information Security & Assurance. 8-10 July 2014, Plymouth, UK.

4. Von Solms, S., Von Solms, R. (2014). Towards Cyber Safety Education in Primary Schools in Africa. 8th International Symposium on Human Aspects of Information Security & Assurance. 8-10 July 2014, Plymouth, UK.

#### **4.2. Profiling and promoting the NMMU as an engaged university:**

Through our visits to schools, engagement with teachers, talks on radio, and other activities we constantly promote the image of the NMMU as engaged. All our awareness material also carries the NMMU logo.

#### **5. Describe how you have successfully integrated engagement into the Teaching and Learning and Research functions of the university. (Refer to sections 5.1, 5.2 and 5.3 of the Engagement Excellence Awards Policy as a guideline)**

The poster project is closely integrated into several of our formal subject offerings. Firstly, the poster contest is used as a case study for students who take the B Tech subject "Information Security IV" in order to teach these students about awareness campaigns and the role these play in both societal and organizational security. Students from this class create awareness material in the form of posters, as well as other content that forms part of the curriculum provided to schools, as assignments for the subject.

The related online Security Education and Training NMMU SLP (SEAT) is also used by these B Tech students and their feedback is further used to improve SEAT. SEAT is made available to participating teachers, parents, and children free of charge.

Secondly, many B Tech students create additional material for this engagement campaign, as their primary 4<sup>th</sup> year projects. For example, in 2014 more than 10 students each developed an interactive e-book/game specifically for use in this project. These e-books/games taught many underlying cyber safety lessons in innovative ways to children. (See screenshots in attached portfolio)

Our members are very active in research directly related to this project. Ms Rayne Reid's PhD focuses specifically on the problem of fostering a cybersecurity culture in South Africa and her research has been applied in many ways during this project. We also have several other post graduate students who work on problems related to this project.

The following publications that are directly relevant to this project were made during 2014:

1. Reid, R. & Van Niekerk, J. (2014). Snakes and ladders for digital natives: information security

education for the youth. *Information Management & Computer Security*, 22 (2).

2. Reid, R., & Van Niekerk, J. (2014). Brain-compatible, Web-based Information Security Education: A Statistical Study. *Information Management & Computer Security*, 22, (4).

3. Reid, R., Van Niekerk, J. (2014). Towards an Education Campaign for Fostering a Societal, Cyber Security Culture. 8th International Symposium on Human Aspects of Information Security & Assurance. 8-10 July 2014, Plymouth, UK.

4. Von Solms, S., Von Solms, R. (2014). Towards Cyber Safety Education in Primary Schools in Africa. 8th International Symposium on Human Aspects of Information Security & Assurance. 8-10 July 2014, Plymouth, UK.

All of the above papers reported on various aspects of the campaign itself, or on awareness material that was developed specifically as part of this project. Paper 1 above relates to a cybersafety game we developed during prior years, paper 2 reports on the refinement of our SEAT course, paper 3 on changes we made in the overall campaign, paper 4 reports on the development of the curriculum we distributed to teachers.

**6. Provide details of scholarly outputs/contributions made to a body of knowledge as a result of your engagement activities.** *(Refer to publications, new teaching programmes, technical reports, conference proceedings, etc.)*

Many additional papers can also be listed. The list below contains ONLY 2014 publications.

1. Reid, R. & Van Niekerk, J. (2014). Snakes and ladders for digital natives: information security education for the youth. *Information Management & Computer Security*, 22 (2).

2. Reid, R., & Van Niekerk, J. (2014). Brain-compatible, Web-based Information Security Education: A Statistical Study. *Information Management & Computer Security*, 22, (4).

3. Reid, R., Van Niekerk, J. (2014). Towards an Education Campaign for Fostering a Societal, Cyber Security Culture. 8th International Symposium on Human Aspects of Information Security & Assurance. 8-10 July 2014, Plymouth, UK.

4. Von Solms, S., Von Solms, R. (2014). Towards Cyber Safety Education in Primary Schools in Africa. 8th International Symposium on Human Aspects of Information Security & Assurance. 8-10 July 2014, Plymouth, UK.

**7. Describe the important role performed by you or the team in:**

**7.1. The leadership and management of the engagement activities and initiatives:**

The cyber safety calendar contest project is managed and run exclusively by our team. This project was initiated by us in 2011 and mostly financed through personal research funds. 2014 was the first year where we received NMMU engagement funding for this.


**7.2. The level and extent of partnerships/collaborations/networks/linkages formed internally and externally:**

**a. Internally** *(inter-departmental, inter-faculty and interdisciplinary):*

During 2014 we collaborated with Bev Ericson from PR and with ICT services staff to host an

	internal version of cybersafety awareness week. Through this more than 50 staff members completed the SEAT SLP and were issued certificates for this course.
<b>b. Externally</b> (at local, national and international level):	We collaborate, and share resources, with researchers from UJ and from UNISA who have similar cybersecurity engagement projects. All UJ information security students also complete our SEAT course. Our project mascot, Cyber Sid, was originally developed by researchers at UNISA who granted us unlimited use of the mascot for cyber security education. We further develop Cyber Sid and created a female counterpart Cyber Sindi which is used by all three institutions. Together with UJ and UNISA we formed SACSAA, the South African Cyber Security Academic Alliance (Cyberaware.org.za)

**SECTION D: Signature**

Applicant Signature		Date	15/03/2015
---------------------	------------------------------------------------------------------------------------	------	------------

**SECTION E: FOR OFFICE USE**

*(Administered by the Centre for Academic Engagement and Collaboration and the NMMU Engagement Committee)*

Resolution regarding application from Awards Committee:	
Feedback to applicant:	

**SECTION F: Portfolio of Evidence**

Attach any relevant documents as a portfolio of evidence to support your application. **Limit this portfolio of evidence to a maximum of 20 pages.** This can include photographs, promotional material, commendations from stakeholders/beneficiaries etc., publication references, (extracts from) annual or project reports to funders/sponsors etc., or any other relevant materials that may serve as evidence.

**List of supporting documents submitted along with this application as addendums:**

Please ensure that the documentary evidence below is clearly cross-referenced with the relevant section and number in the application template, for example Section B1 or Section C4.

1. Portfolio.doc
- 2.
- 3.
- 4.



Teacher Training day at NMMU in 2014



# Cyber Safety for Primary School Learners



**Nelson Mandela  
Metropolitan  
University**

*for tomorrow*

Dear Teacher

Cyberspace has brought many advantages to all of us. Most of us, learners, teachers and parents, have grown almost totally dependent on cyberspace for our everyday recreation, social networking, communication, etc. We can hardly imagine a day without cell phones, the Internet, Google, Facebook, YouTube and many more Internet and cyber-based services.

Unfortunately, along with all of these advantages in cyberspace came a whole series of cyber related risks. Sharing too much private information, cyber bullying, exposure to paedophiles, sexting, losing money are merely a few of these modern-day cyber-related risks we need to contend with and educate our children about.

The Group for Research in Information and Cyber Security (GRICS) at the NMMU has developed a curriculum to teach cyber safety to learners in Primary Schools. The goal of this curriculum for teaching cyber safety is basically twofold;

- i. to empower teachers at primary schools to offer such cyber safety lessons and
- ii. to educate learners of age groups 10 to about 14 the basic principles of cyber safety relevant to their typical activities in cyberspace.

To offer this curriculum, the following need to be noted:

- i. The material will provide introductory information to the teacher to present suitable content to learners and facilitate discussion afterwards on a specific cyber safety topic.
- ii. The curriculum is divided into two age groups; ages 10 - 12 and 13 and older respectively. For each age group a number of lessons on specific topics are prepared. Some of these lessons may overlap to some extent to reiterate some aspects.
- iii. Each lesson is made-up of three pages. Page 1 is a lesson plan for the teacher, page 2 an assessment exercise for the learners and page 3 a memorandum of the exercise. Ideally teachers should print and duplicate the assessment exercise for the learners to complete after they watched the video and discussed the lesson.
- iv. To offer the content, a school does require a computer that is linked to an Internet connection and ideally a data projector with audio.
- v. The intellectual property (IP) of this curriculum belongs to the NMMU.

The curriculum is making it easy for teachers to present, discuss and assess various aspects of cyber safety with their learners in class or in an IT laboratory. The teachers will also be educated to some degree in the process to be able to assist learners with cyber safety issues and problems like; cyber bullying, sexting, etc.

Although this material is the property of the Nelson Mandela Metropolitan University, please feel free to use, copy and distribute the material to interested parties.

Rossouw von Solms (Prof)

**Acknowledgement:** Ruan Koen & Ryno Schoeman (BTech: IT students for the content)

© NMMU

## Table of Contents

### **Age: 10 – 12 years**

[Lesson 1- Phishing attacks and Viruses](#)

[Lesson 2- Web Information](#)

[Lesson 3- Sharing personal information](#)

[Lesson 4- Cyber Bullying](#)

[Lesson 5- Summary of SMART lessons](#)

[Lesson 6- Password protection](#)

[Lesson 7- Viruses and Antivirus Software](#)

[Lesson 8- Accepting friend requests](#)

[Lesson 9- Privacy Settings](#)

[Lesson 10- Cyber Bullying](#)

[Lesson 11- Meeting online friends in real life](#)

[Lesson 12- Online Game Addiction](#)

[Lesson 13- Illegal Downloads](#)

[Lesson 14- Cyber Bullying](#)

### **Age: 13 – 15 years**

[Lesson 15- Online privacy](#)

[Lesson 16- Cyber Bullying](#)

[Lesson 17- Share with care](#)

[Lesson 18- Online safety](#)

[Lesson 19- Safe social networking](#)

[Lesson 20- Cyber privacy](#)

[Lesson 21- Cyber Bullying](#)

[Lesson 22- Online posting can haunt you in the future](#)

[Lesson 23- Be careful of online friends](#)

[Lesson 24- Sexting](#)

## Lesson 10:

### Cyber Bullying

#### Overview:

Cyber bullying is the deliberate act by an individual or a group, through the use of information technology communication mediums such as social media, emails, instant messaging etc., to cause harm to another. With the increase of access to technology, cyber bullying has become a common trait among teenagers. The internet allows a smokescreen behind which aggressors of cyber bullying can hide whilst bullying their victims.

Some victims are negatively influenced by cyber bullying which can have a significant effect on them, such as an increase feeling of sadness, loss of interest in activities and a lower self-esteem. This lesson will focus on cyber bullying in order to explore why it is wrong, what should be done if you are a victim and what will happen should you be the aggressor of cyber bullying.

This lesson is all about cyber bullying. It emphasises the importance of reporting cyber bullying to a parent or teacher.

Learning Objectives:	Primary: Create an understanding of what cyber bullying is and why it is wrong.
	Secondary: <ol style="list-style-type: none"><li>1. Create an understanding of what cyber bullying is and why it is wrong.</li><li>2. Know what should be done when you're a victim of cyber bullying.</li></ol>
Materials:	Video: Funmoods - Online Safety- Little Red Riding Hood- Chapter 3 <a href="https://www.youtube.com/watch?v=eIYv-pZVgyo">https://www.youtube.com/watch?v=eIYv-pZVgyo</a>
Procedure:	<ol style="list-style-type: none"><li>1. Overview of privacy. Recap Lesson 9.</li><li>2. Watch video</li><li>3. Reflect on video with class discussion</li><li>4. Explain main lesson concepts</li><li>5. Do class assessment to measure understanding and insight</li></ol>
Discussion:	Questions for class discussion: <ol style="list-style-type: none"><li>1. What are some examples of cyber bullying?</li><li>2. Why is it wrong to bully someone online?</li><li>3. Why shouldn't you keep quiet about being bullied?</li><li>4. What should you do when you see someone being cyber bullied?</li><li>5. To whom should you report cyber bullying?</li></ol>
Assessment:	Worksheet: True/False for bullying activities and essay.

## Lesson 10: Memorandum

True/False Questions:

*Instruction: State whether the action is a form of cyber bullying by writing true or false.*

ACTION:	TRUE/FALSE
A Facebook friend making a joke about your bad hair day on Facebook.	<i>True</i>
A Facebook friend spreading rumours about you on his wall every day.	<i>True</i>
A friend asking for you Twitter password.	<i>False</i>
A Facebook friend uploading an edited picture of you after a birthday party.	<i>False</i>
A Twitter follower constantly making bad comments about your tweets and embarrassing you.	<i>True</i>
A stranger on Facebook repeatedly sends you nasty messages.	<i>True</i>
A Facebook friend tags you in pictures of funny animals, saying you look like them.	<i>True</i>

Essay:

*Instruction: Shortly tell someone why cyber bullying is wrong and what they should do if they are a victim.*

- Cyber bullying can influence someone else emotions. Make them sad
- Words can hurt someone.
- Cyber bullying can leave someone not wanting to take part in social activities or even go to school.
- Some have committed suicide of being a victim of cyber bullying.
- They can get into trouble when they cyber bully.
- You should not take bad comments or any form of cyber bullying literally.
- Save evidence if you get cyber bullied.
- Don't reply to the person who cyber bullies you. Ignore them.
- Delete and block the person who cyber bullies you.
- Speak to your parents/guardians or teacher when you get cyber bullied.

## Lesson 10: Assessment

True/False Questions:

*Instruction: State whether the action is a form of cyber bullying by writing true or false.*

ACTION:	TRUE/FALSE
A Facebook friend making a joke about your bad hair day on Facebook.	
A Facebook friend spreading rumours about you on his wall every day.	
A friend asking for your Twitter password.	
A Facebook friend uploading an edited picture of you after a birthday party.	
A Twitter follower constantly making bad comments about your tweets and embarrassing you.	
A stranger on Facebook repeatedly sends you nasty messages.	
A Facebook friend tags you in pictures of funny animals, saying you look like them.	

Essay:

*Instruction: Shortly tell someone why cyber bullying is wrong and what they should do if they are a victim.*

---

---

---

---

---

---

---

---

---

---

Examples of Posters (4 of 14) created for parents and grandparents

8

**MAY VICTIMS**  
PAUL BOCCI

**CYBER-BULLYING**

**What is it?**  
It is the use of electronic communication to bully a person, typically by continually sending messages of intimidating or incriminating nature.

**How does it happen?**  
It happens in situations in which someone attempts to maintain control over others, by manipulation and mental domination. Social networking, instant messages and emails are methods of communication which the bullies may use to keep hampering and teasing their victims.

**Who are the targets?**  
It can happen to any child, especially teenagers who lack self-esteem and self-confidence. Teenagers with limited social experience and tact tend to believe that this controlling and possessive behavior is romantic.

**Tips for prevention**  
Keep the computer in a common area of the home. Do not allow it in your child's bedroom. Monitor your child's online activities. Build trust with them. Set time limits and explain your reasons. Be reasonable to your children and discuss rules towards online safety and internet usage.

5

**MAY VICTIMS**  
PAUL BOCCI

**SEXTING**

**What is it?**  
Sexting is the online messaging and sharing of sexual explicit text and images.

**Where does it occur?**  
It is an activity that occurs online, usually promoted by sexual content like images and videos. It is prominent on chat rooms and social networking sites like Facebook and Twitter.

**Who is involved?**  
This type of behavior is common amongst teenagers and young adults.

**Where are the risks?**  
It encourages teenagers to engage in premature sexual activities. The images that they share through these mediums may be distributed without their consent and will exist in cyberspace forever.

**Tips for prevention**  
Talk to and show interest in your child's personal life, as this will give them the trust and courage to talk to you about issues like these. You can also set up parental controls on the devices that they use to connect to the internet to prevent them from engaging in such behavior. Such parental controls may include blocking certain sites or installing parental control software.

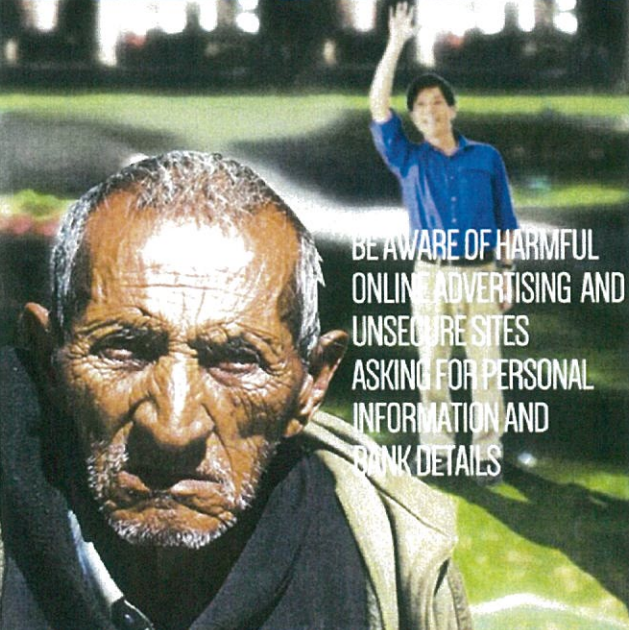
**STAY SAFE ON THE WEB**



BE WARY OF ONLINE GAMBLING SITES ASKING BANKING DETAILS  
AVOID SITES THAT ARE CLUTTERED WITH ADVERTISEMENTS

**IT'S ALL FUN AND GAMES...  
UNTIL SOMEONE LOSES THEIR PENSION**

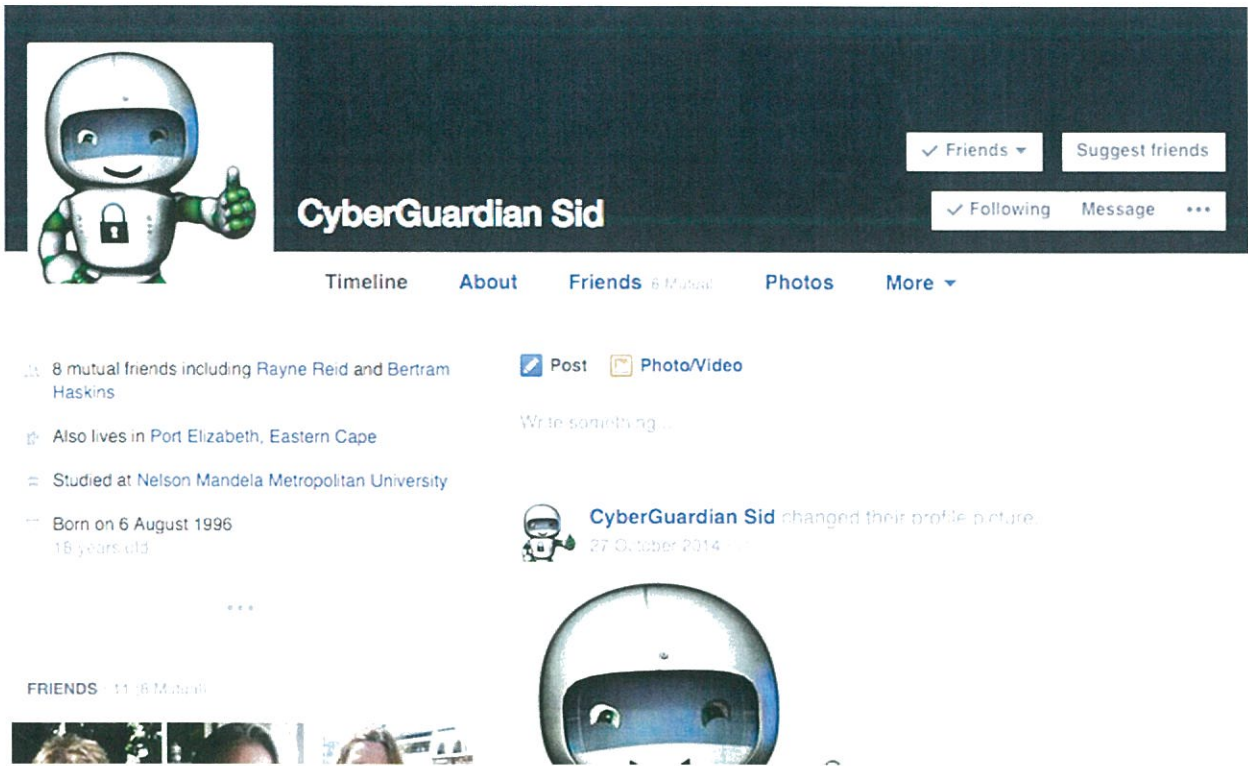
**STAY SAFE ON THE WEB**



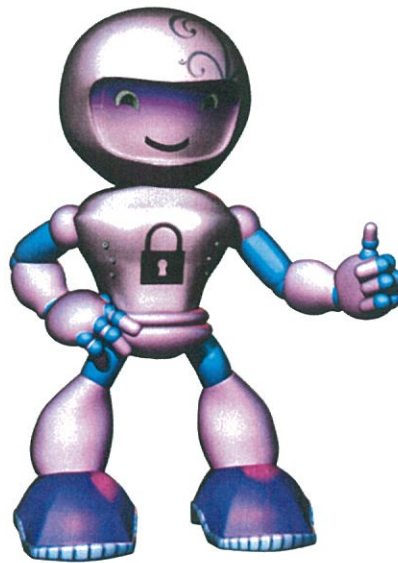
BE AWARE OF HARMFUL  
ONLINE ADVERTISING AND  
UNSECURE SITES  
ASKING FOR PERSONAL  
INFORMATION AND  
BANK DETAILS

**IGNORE ONLINE ADS LIKE YOU  
IGNORE YOUR SON-IN-LAW**

# Cyber Sid and Cyber Sindi characters and 3D Models developed for use In awareness material during 2014



The image shows a screenshot of a Facebook profile for a character named CyberGuardian Sid. The profile picture is a 3D model of a white robot with a blue visor and a lock icon on its chest. The name 'CyberGuardian Sid' is displayed in white text on a dark background. Navigation options include 'Timeline', 'About', 'Friends', 'Photos', and 'More'. Interaction buttons for 'Friends', 'Suggest friends', 'Following', and 'Message' are visible. The profile information section lists 8 mutual friends, including Rayne Reid and Bertram Haskins, and mentions the character lives in Port Elizabeth, Eastern Cape, and studied at Nelson Mandela Metropolitan University. A post from October 27, 2014, shows the character changing their profile picture to a close-up of their face.





# Cyber safety awareness on the rise

Chanice Koopman

NELSON Mandela Bay teachers are being taught to deal with cyber bullying – a major concern in an increasingly technological society.

The teachers attended a lecture at the Nelson Mandela Metropolitan University (NMMU) yesterday where they were given a free curriculum with 24 lesson plans addressing cyber safety, associated discussion questions and assessment worksheets.

The curriculum aims to empower teachers to educate pupils between 10 and 14 on basic cyber safety principles relevant to their typical cyberspace activity. NMMU Professor Rossouw von Solms said cyber safety education and awareness was common in many other countries.

"Cyberspace has brought many advantages to all of us and most of us, pupils teachers and parents have grown almost totally dependent on cyberspace for our everyday recreation, social networking and communication," Von Solms said.

"The proposed curriculum makes it

easy for teachers to present, discuss and assess various aspects of cyber safety with their pupils in class or in an IT laboratory. Teachers and pupils can learn together about the risks associated with online activities. Typical topics that are covered for include cyber bullying, sexting, safe social networking, privacy settings on Facebook and sharing sensitive information."

Pupils will then be given a chance to showcase their artistic side at the annual cyber safety poster competition where they will design posters depicting a cyber-safety message.

Winners of this competition will be announced next month and winning posters will be used in further cyber safety campaigns. Cape Recife High School teacher Bardiwe Huebsch said the curriculum was a necessity in this advanced technological era.

"These lesson plans will be a great way for us as teachers to educate pupils."

"Cyber bullying is a major problem and kids do not necessarily realise the consequences of giving out personal information, so we do hope that through these lessons they would become more safety conscious," she said.



**SAFETY AWARENESS:** NMMU's Prof Rossouw von Solms, left shares the cyber safety curriculum for primary schools with teachers Paul Critchlow (Mount Pleasant Primary) and Liana Smit (Sunridge Park) PHD student in IT Rayne Reid

PE EXPRESS | WEDNESDAY 22 OCTOBER 2014

## Cyber safety curriculum for primary schools

A CYBER safety curriculum for primary schools to empower teachers in Nelson Mandela Bay to teach learners to be cyber safe was launched at NMMU last week.

The Group for Research in Information and Cyber Security (GRICS) at NMMU has developed a curriculum to teach cyber safety to learners in primary schools.

The goal of this curriculum is to empower teachers to offer cyber safety lessons and to educate learners in the 10 to about 14 age group the basic principles of cyber safety relevant to their typical activities in cyberspace.

"The proposed curriculum makes it easy for teachers to present, discuss and assess various aspects of cyber safety with their learners in class or in an IT laboratory," says NMMU's Prof Rossouw von Solms.

"The teachers will also be educated to some degree in the process of being able to assist learners with cyber safety issues and problems like cyber bullying, sexting, etc.," says Prof Von Solms.

According to Prof Von Solms, no formal curriculum in this regard exists in most South African schools and this cyber safety curriculum is an effort to fill this gap.

Cyberspace has brought many advantages to society and most learners, teachers and parents have grown almost totally dependent on cyberspace for everyday recreation, social networking, and communica-

tion. However, "Along with all these advantages in cyberspace, comes a whole series of cyber related risks. Sharing too much private information, cyber bullying, exposure to paedophiles, sexting and losing money are merely a few of these modern day cyber-related risks we need to contend with and educate our children about," adds von Solms.

During the launch a free curriculum with 24 lesson plans for teachers, associated discussion questions, assessment worksheets and memoranda was made available.

During this workshop the annual Cyber Safety Poster Competition was also launched. The objective of the Poster Competition is for primary school learners to design posters that depict a cyber safety message.

Winners of this competition will be announced at an event in November and winning posters will be used in further cyber safety campaigns.

For more information Prof Von Solms can be contacted at [rossouw@nmmu.ac.za](mailto:rossouw@nmmu.ac.za).

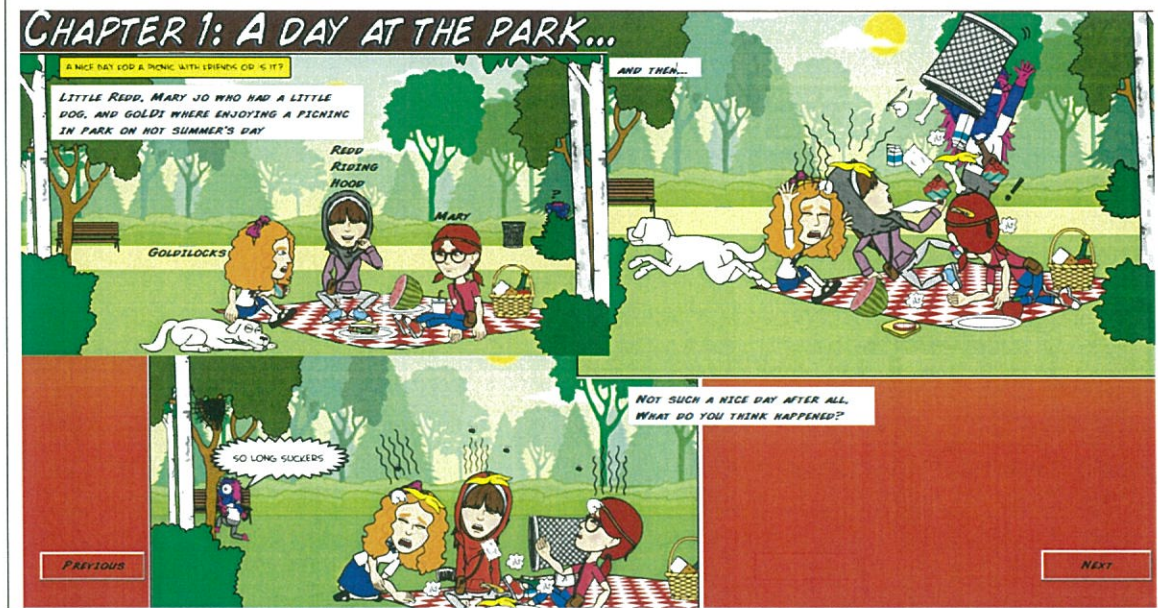
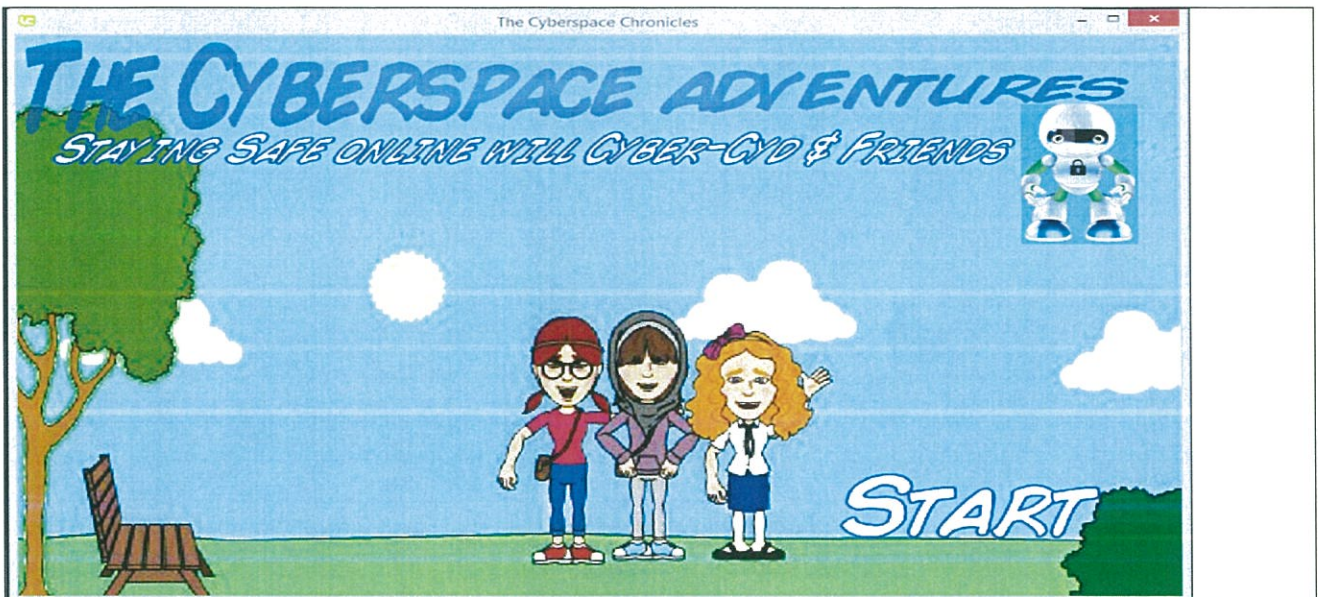
REPORTER

Johan van Niekerk, Kerry-Lyn Botha and Prof Rossouw von Solms of the School of ICT at NMMU with some of the posters designed for previous Cyber Safety Poster Competitions.

PHOTO SUPPLIED



Examples from livecode interactive e-book project (note this is incomplete examples)



# CHAPTER 2: CYBER-CYD TO THE RESCUE!



HI GUYS MY NAME IS CYBER CYD. WHAT HAPPEND RED, MARY AND GOLDI WAS WRONG. DO YOU KNOW WHAT HAPPENED. I THINK WE SHOULD INVESTIGATE

WHERE SHOULD WE START?

FACEBOOK  
LITTLE-RED RIDING HOOD  
GOLDILOCKS



DO YOU KNOW WHERE TO START? GREAT. LETS LOOK AT THE CLUES

CLUE 1

CLUE 2

Public

**Goldi Locks**

Me and my frnds are going to have a picnic today I'm sooo excited — 🥰 feeling excited with Mary Joh Lamb and Little-Red Riding Hood at Enchanted Gardens

Like Comment Share

You and Mary Joh Lamb like this

Boogie Wolf Mann mmmmmm  
Like

Boogie Wolf Mann "mahn that's nice"  
Like

Mary Joh Lamb Cant w3  
Like

CLUE 3

Private Chat

Little Red Riding Hood

Hi Goldi Locks! I saw your post and I'm so excited for you! I hope you have a great picnic! I'll be there to see you!

Like Comment Share

SO MANY CLUES DO YOU HAVE AN IDEA? LET ME GIVE YOU ANOTHER CLUE: PRIVACY, CYBERBULLYING, PERMISSION. REMEMBER THESE WORDS

NEXT

# CHAPTER 3: THE BIG BAD...



MEANWHILE IT SEEMS THE DISASTER PICNIC HAS BEEN POSTED ON FACEBOOK, DID REDD REALLY POST THE PICTURE?



OH NO WHY DID REDD DO THAT?

WHY CAN'T I LOG INTO MY FACEBOOK ACCOUNT. I HAVE TO DELETE THAT PICTURE

Little Red Riding Hood

hahahahahahaha look at Goldi Locks Mary Joh Lamb

Like

I Little Red Riding Hood hahahaha  
Like

Mary Joh Lamb N03000000 Red how can you be so mean?  
Like

Boogie Wolf Mann hahahahahahahahaha what a bunch of losers  
Like

Boogie Wolf Mann You guys are so dumb I posted this photo  
Like

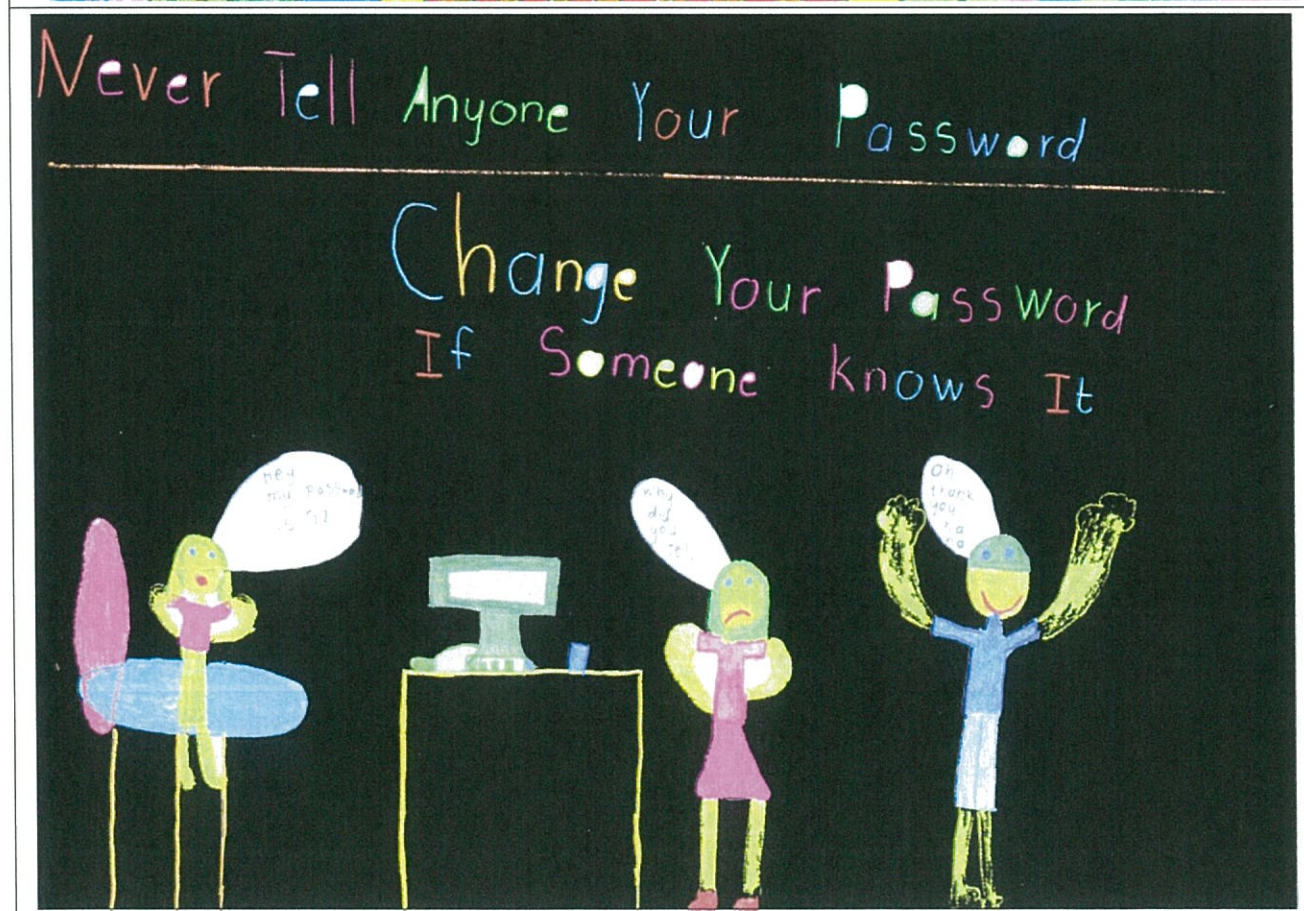
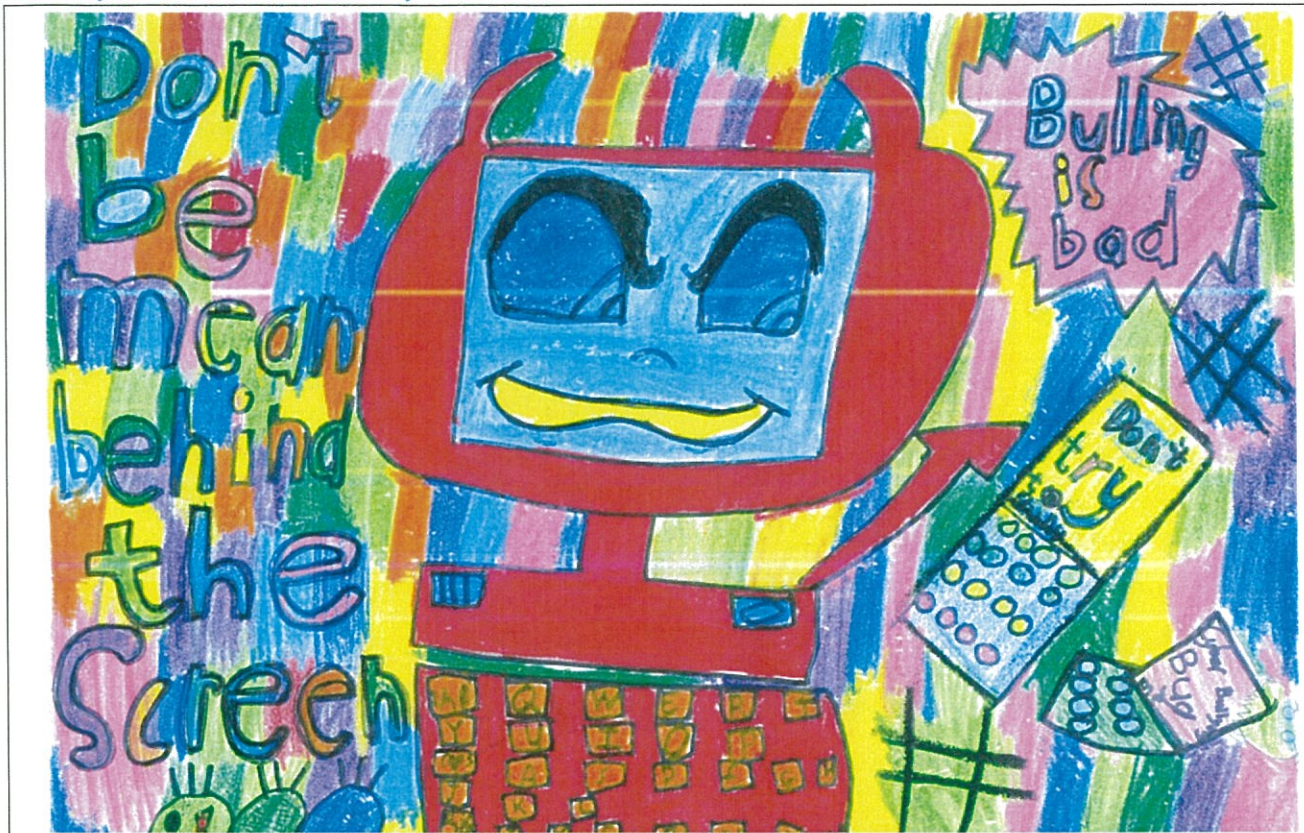
Goldi Locks T0000000000 how can you be so mean  
Like



HMMM SOMETHING FISHY IS GOING ON WHO IS THE BOOGIE WOLF MANN?. I THINK WE ARE GETTING CLOSER GUYS

NEXT

Example Posters entered by school children





# Cyber Phishing

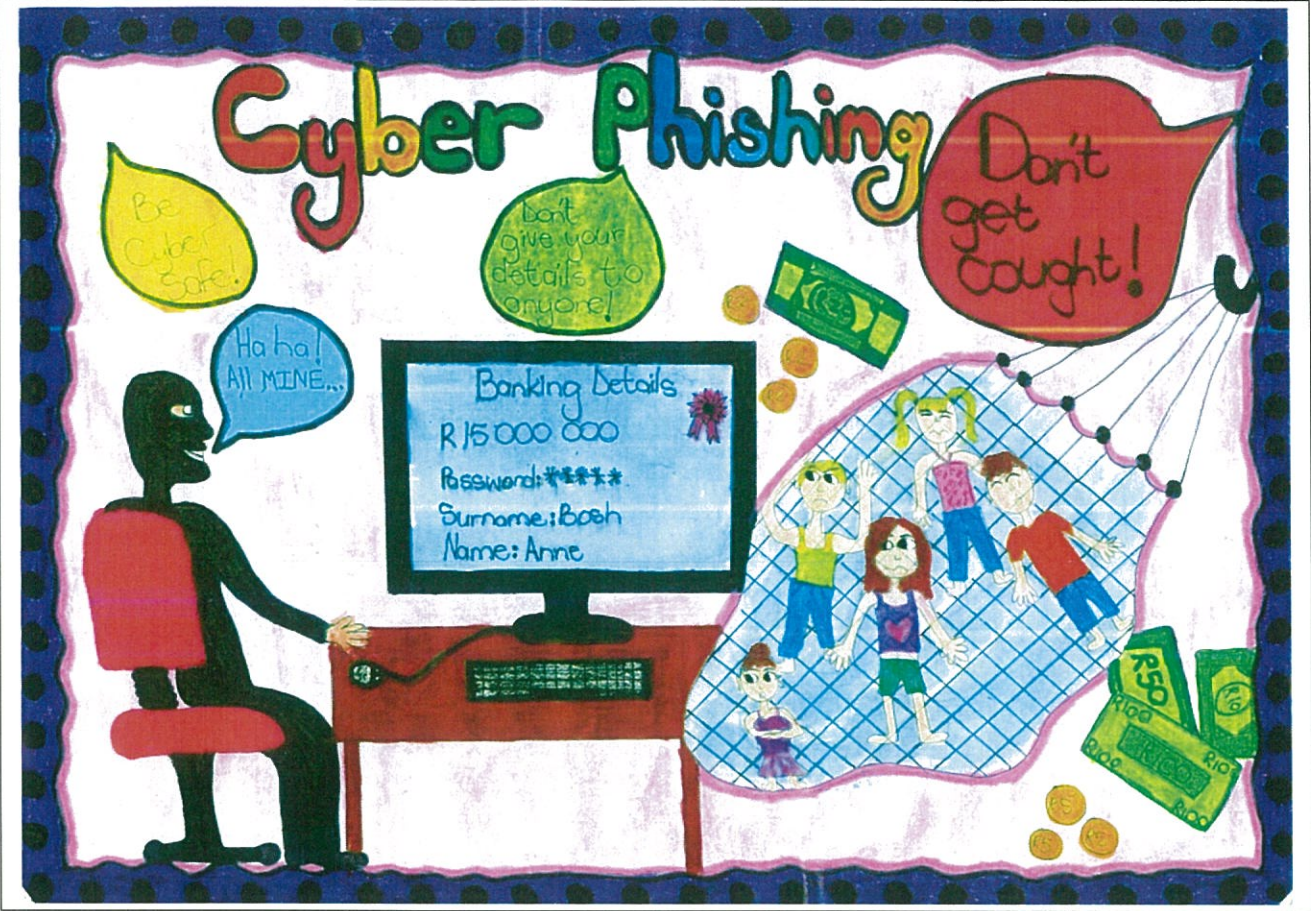
Be Cyber safe!

Don't give your details to anyone!

Don't get caught!

Ha ha! ALL MINE...

Banking Details  
R 15 000 000  
Password: \*\*\*\*  
Surname: Bosch  
Name: Anne



2014 Competition Prize giving (Was held in 2015)







# NMMU Cyber-Security Team

Prof Rossouw van Sofine



Prof Johan van Niekerk



Prof Penny-Lynn Thomason



Dr Lynn Furcher



Dr Melissa Carter



Prof Johan Van Niekerk  
visiting a school



**Nelson Mandela  
Metropolitan  
University**

*for tomorrow*



Learners participating in  
cyber-security talk



Poster Competition



Security-Awareness Board Game



SACSAA Website



Awareness Flyers