netsafe

NETBASICS

www.netbasics.org.nz

NETBASICS E-SECURITY
Lesson Plans

Contents

NETBASICS E-SECURITY

Before you start

This unit of work has been developed for use in conjunction with the Netbasics animated episodes located on the NetBasics in a box DVD.

NetBasics comprises a set of 11 animated episodes that run for around one minute each. The stories follow the members of the Jones Family through a typical day of online activity. Each episode is designed to show how users' computer activities can expose them to a number of security vulnerabilities, and reinforce positive steps they can take to protect their computers and data.

Background

e-security or internet security covers a range of activities to keep computers safe from viruses and other malware. Effective e-security enables users to protect electronic information including personal details and financial information.

The Netbasics resources will educate students about keeping computers and electronic information safe. The episodes explore fundamental e-security concepts and the role human behaviour plays in their effectiveness. The resources focus on the practical steps students need to take to protect their computers and information.

More about Netbasics

The Netbasics episodes use three sets of characters to show the relationship between computer threats, technology solutions and user behavior.

- **The Jones Family**: Each member of the family has a favorite online activity and each family member's actions contribute to the computer's vulnerability.
- **The Security Threats**: There is an army of threats including malware, spyware, viruses, online tricksters and scammers working hard to create havoc inside the family's computer.
- **The Security Team**: Anti-virus, anti-malware, and software updates are fighting a losing battle to keep the family's computer secure.

As different characters interact in the episodes, they show how certain computer threats operate, the importance of computer security solutions and how the Jones Family's apathy contributes to their computer and data vulnerability. Students will learn the important balance between technology and user behaviour to ensure computer security. A full description of the characters and their behaviors is provided in Appendix A.

Each episode is supported by a More Information section which explains the key cybersafety issues covered in the episode.

Unit of work overview and objectives

This unit of work aims to help students to:

- Identify risks to computers and personal information, including financial details
- Identify software, hardware and behavior required to keep computers and finances safe

By the end of this unit of work, students will be able to:

- Identify the main e-security risks
- Identify hardware and software strategies to keep computers and finances secure
- Identify individual and family behaviours necessary to keep computers and finances secure

Lesson duration

The time allocated to this lesson will depend upon the prior knowledge and skill levels of your students. It comprises three activities and an optional extension activity, each designed to take approximately 45 minutes.

Required resources

- NetBasics in a Box DVD to show students the Netbasics episodes either on individual computers, an Interactive Whiteboard.
- Appendix A Character outlines for teacher background
- Appendix B Episode descriptions for teacher background
- Appendix C Netbasics Master Grid
- Appendix D Worksheets 1–3

Learning activities

Activity 1—Current e-security knowledge

This activity helps students understand how their current online interactions can put their computers and information at risk and begin to identify key risks and protection strategies from a real life perspective.

What you will need:

- Access to Netbasics episodes 1 and 11 on the NetBasics in a box DVD
- Worksheet 1: Audit of e-security knowledge (Appendix D)

Ask students to watch episodes 1 to 11 of Netbasics to set the scene for the activity.

Using **Worksheet 1** ask students to work in pairs to brainstorm their existing e-security knowledge, previous threats they have encountered and measures they or their parents have used to prevent or address threats. Follow this up with a classroom discussion.

Alternatively a classroom discussion can be used to brainstorm the risks associated with each activity listed in **Worksheet 1**, with students encouraged to share examples of e-security gone wrong, e.g. viruses corrupting files, school work lost, computers having to be repaired/replaced. Also explore what they or their parents have done to prevent risks to computers.

Teacher notes:

Discussion questions

The following questions can be used to guide class discussions in conjunction with working through the activities listed in Worksheet 1.

Has anybody or their parents ever experienced issues from a virus infecting their computer? How did it get there? (downloads, no virus protection, file sharing etc.)

Do people have tips for ensuring computers are protected when undertaking different activities online? What has and hasn't worked online? (anti-virus protection, anti-spyware protection, firewalls, strong passwords) Do students know what each of these things do?

Activity 2—Exploring character behaviours

This activity helps students examine the relationship between the technology and the human factors that contribute to computer security.

What you will need:

- Access to Netbasics episodes 1 to 11 located on the Netbasics in a box DVD
- Worksheet 2: Technology+Behaviour=Security Grid (Appendix D)
- Appendix C Netbasics Master Grid

Assign student pairs or groups one member of the Jones Family: Jenny (Mom), Jacquelyn (Grandma), Neville (Dad), Raymond (the dog) or Sophie (little girl) to pay special attention to while viewing Netbasics episodes 1-11. Pairs and groups should also explore the More Information sections for the episodes, and the Your Computer Security tab at the top of the screen.

Using **Worksheet 2** ask groups to answer specific questions for their character and fill in the yellow spaces. There can be more than one answer in several places. **Worksheet 2** can also be customised to increase or decrease difficulty for students.

Ask student groups to share their answers with the class and explore the risks each character is taking online.

Teacher notes

Print Appendix C Netbasics Master Grid to help guide students and discussions.

Discussion questions
The following questions can be used to guide class discussions.

- Why do people have a hard time distinguishing between real web sites and phishing sites
- Which member of the Jones Family is most at risk from their online behaviors?
- What is the weakest link in the Jones Family's computer security system?
- How does Ben save the day for the Jones family
- What are some of the reasons people do not update their security software?
- Why do people create weak passwords or readily give out their passwords?
- In the Netbasics episodes, what threats could be posed by the character "Fiona"?
- What conditions could make computer users be proactive in securing their data and their computer?

Activity 3—Identifying positive steps

Computer users can take some simple steps to reduce the chance their computer and their important personal data will be affected by the most common threats. After viewing all the Netbasics episodes, students create a plan that identifies the steps the Jones Family should take to develop stronger computer security.

What you will need:

- Access to Netbasics located on NetBasics in a Box DVD
- Appendix A Character outlines
- Appendix C Netbasics Master Grid
- Appendix D Worksheet 3 Home e-security plan

Print Appendix A Character outlines and Episode descriptions to guide students in this activity. Students can also explore NetBasics to help guide their work. The More information, Your Computer Security and Protect Your Stuff sections of Netbasics will be particularly helpful during this activity.

Print Worksheet 3 at Appendix D, Home e-security plan for student pairs or groups. Assign student pairs or groups. Ask students to develop an e-security plan for a family member or friend that is likely to need help. Discuss the recommended strategies in a group to ensure students understand what and how their family members/friend family should protect their computers and data.

Alternatively students can complete the plan at home and follow up with a class discussion about their outcomes.

Teacher notes:

The following discussion points and Appendix C Netbasics Master Grid will help inform your guidance and student discussions.

Students should be able to identify the following key e-security strategies to protect computers and information:

- **Use the latest operating system**
  The newest version of any operating system is generally the safest.

- **Use a firewall**
  A firewall can protect you against hackers, some viruses and some spyware. It can also stop your computer being hijacked and used to infect other machines or send spam emails.

- **Use anti-virus software**
  Anti-virus software can scan a computer and incoming emails for viruses. Make sure your anti-virus software is set to automatically update so it can identify new threats

- **Use anti-spyware software**
  Spyware is software that secretly monitors a user's activity, or collects private information such as credit card details. In most cases a firewall and anti-virus software will not prevent spyware. You need up to date anti spyware software to keep it at bay. Be wary of programs/files you might download and install. They may harbor unwanted extra programs, in particular those from peer to peer sites.

- **Set your computer to automatically update all of the above**
  New ways to compromise your computer and information are constantly being identified by hackers. You need to set your operating system, firewall, anti-virus and anti-spyware software to automatically update. Having this done may also improve your computers performance.

- **Use a STRONG password**
  It is important to password protect your computer to help limit access by unwanted users. Change your password regularly and keep it secret. A strong password is one that is at least 8 characters with a mix of lower

- **Back up data regularly**
  Backing up important data is crucial to any computer security plan. A reliable back up strategy needs to be systematic, organized, documented and include safe storage of the backup medium.

Appendix A

Character outlines

The Characters

The **Netbasics** episodes use three sets of characters to show the relationship between computer threats, technology solutions and user behavior.

- **The Jones Family**: Each member of the family has a favorite online activity and each contributes to the computer's vulnerability.
- **The Security Threats**: There is an army of threats including malware, spyware, viruses, online tricksters and scammers working hard to create havoc inside the family's computer.
- **The Security Team**: Anti virus, anti malware, and software updates are fighting a losing battle to keep the family's computer secure.

The Jones Family

Character	Online Activities	Online behaviors	Online Risks
Dad Neville Jones Age: 50	Email	Opens links or attachments in Spam; fails to update security software.	Bypasses computer security by downloading malware from spam links or attachments; compromises home computer security by not applying security updates.
Mum Jenny Jones Age 44	Online shopping	Buys from online shops without checking whether the shop's website is trustworthy.	Risks being defrauded by fake websites; may pay for bogus goods; may have credit card information stolen or sold to other criminals to use later on; compromises home computer security by not applying security updates.
Grandma Jacquelyn Jones Age: 78	Investing, email, online banking	Trusts unexpected emails from online businesses requesting important login, password, or pin information.	Risks having banking login / password phished/stolen and used fraudulently; risks loosing other important information by replying to spam emails from fake sites; compromises home computer security by not applying security updates.
Sophie Jones Age: 10	Web surfing, social networking, chatting, gaming.	Chats to total strangers online.	Risks communicating with total strangers who might may harm children by harassing/cyberbullying them, sending them inappropriate material, engaging them in online sexual activity, and seeking to meet and abuse them in person.
Raymond *(the family dog)* Age: 4	Web surfing, peer to peer	Likes pictures of dog food and turns off the firewall to get the best brands.	Compromises computer security by turning off the firewall.
Ben Jones Age: 15	Web surfing, social networking, chatting, researching, gaming, YouTube, trading, peer to peer	Spends all his free time on online games and online chatting, Always connected!	Risks never being seen in a Netbasics episode, because he's always in his room.

The Security Threats

Character	Known aliases	How they operate	Convictions
Viruses	Viruses - W32.Anyvirus.A@mm, topdraw.32.dll, and approximately 923,948,849 others	Viruses infect computers when infected files are downloaded onto a vulnerable computer. They damage computer programmers and files, can slow the computers down. Some viruses may not cause damage immediately but can hide and attack at a later date.	First degree computer slowness, Destruction of important files and data (1st and 2nd degree), deletion of family photographs, murder of the computer operating system, computer crash (in the 1st degree), Illegal backdoor entry.
Spyware	Spyware - Flashget, Zango freezescreensaver.exe, MyWebSearchToolbar	Spyware programs get installed without users knowing. Spyware can 'listen in' and record computer activity including websites visits, password details, and credit card numbers. Spyware can send information to others with criminal intent.	Stealing logins and passwords (1st and 2nd degree), fraud, browser stalking.
Fiona	Unknown - No records on file	Unknown-No records on file.	Unknown-No records on file.
Pixelmania	Virus - Trojan Horse	Trojan horses appear to do one job while they secretly carry out harmful activities. They can create vulnerabilities such as opening up the firewall or disabling security. With a 'back door' criminals can secretly gain control of the computer and use it to send out viruses or steal information.	Harboring known criminals (including various spyware and viruses), Illegal back door creation, aiding and abetting fraud and identity theft.
Masquerade	Social Predator - Scammer, Cyberbully, Predator - Two-face, gemini, Louis XIV, sally_nz, LonelyBoy19	Masquerading criminals pretend to be legitimate so they can trick people into giving them something they want. They may want someone's identity, their money, or they may just want to harm them.	Unknown counts of deliberate deception for unlawful gain, stalking, felonious use of unsolicited email, harassment, GPH and CBH (Grievous Psychological Harm & Cyber Bodily Harm).

Rapid Spawn	Worm-Virus, Zacker, Maldal.exe, Mydoom, Sobig	Worm's reproduce to install themselves on other networked computers. A worm can use a network to send copies of itself infecting other computers. Worms may include malware that damage data and files, or compromise computer security. Worms may use a computer's email program to send copies of itself to other computers outside the network.	Network Attacks, Slow Networks, Spamming malware, Installing "Back Doors", deleting data and files, Installing Spyware, Installing other viruses.
The Prince	Scammer, - 419, The Sting, Honest John,	Criminals pretend to be legitimate websites so they can trick users into entering passwords, logon, or credit card details. They also seek out auction sites, email, and social networking sites to obtain logon details and passwords.	Obtaining goods or services by false pretences, Advance Fee Fraud, Spamming.

The Security Team

Character	Functions	Strengths	Vulnerabilities
S.U.P. Security Update Process	Applies updates to patch weaknesses in the security software.	Marksmanship in troubleshooting computer security weaknesses. Extraordinary engineering abilities to reinforce computer programs to patch any holes.	User apathy in applying update to the computer operating system and other software.
A.S.S. Anti Spyware Security	Identifies and manages spyware activity inside a computer. Cannot recognize viral activity, works in partnership with A.V.A.	Top class detective in identifying spyware files and matching them to the register of known criminals. Received medal of honour for scanning incoming network connections for spyware software.	Weakened by lack of regular spyware definition updates. Reliant on support from A.V. A. and S.U.P. Can be easily overworked by spyware infected peer to peer programmers.
A.V.A. Anti Virus Authority	Identifies and manages viral activity in the computer.	Excellent at identifying virus file definitions. Highly skilled at identifying suspicious viral behavior from computer programs.	Weakened by lack of regular virus definition updates. A.V.A. Is dependant on support from A.S.S. and S.U.P. Can be easily overloaded by firewall failure.

Appendix B

Netbasics episode descriptions

Below is a brief description of the 11 Netbasics episodes

Number	Title	Description
Episode 1	Trailer	The trailer is an introduction to the Netbasics characters that depict the Jones Family, common security threats, and security solutions.
Episode 2	'The Jones Family goes online'	Online things are not always what they appear to be and users need to be aware.
Episode 3	'Neville reveals his lack of smarts online'	Even with security measures in place, users can be tricked into downloading malicious software in the guise of a normal download. Neville
Episode 4	'Raymond goes a hunting'	A firewall can only protect data when it is turned on. Simply having one installed will not protect data.
Episode 5	'Jenny gets a dose of retail therapy'	User should only trust sites they can verify as legitimate. In this episode, Jenny unwittingly hands over her credit card details to a trickster
Episode 5 *Extended Version*	'A.V.A. puts his body on the line'	The Anti Virus Authority (A.V.A.) is no match for a number of risks and unsavory characters including 'Fiona' !
Episode 6	'Nana meets a nice man from the bank'	Online passwords can protect you. In this episode, Nana is duped into providing hers after reading a scam email masquerading as her bank. Managing and protecting passwords is a vital security activity.
Episode 7	'A.S.S. seeks professional help'	Anti Spyware Security (A.S.S.) software requires regular updates to be effective. Spyware and malware are constantly evolving and security software that is not up to date is vulnerable.
Episode 8	'Sophie gets a new friend'	It is easy to appear to be somebody else online. All members of the Jones family need strategies to help identify what is real online. Sophie's new 'friend" may not be a friend at all.
Episode 9	'S.U.P. is frustrated trying to maintain an orderly computer system'	Internet threats are constantly evolving and users play a vital role in ensuring security software can do its job by having a reliable Software Update Process (S.U.P)
Episode 10	'Computer at War- Worm meets Malware'	Viruses and spyware are different types of malicious software (malware). The threats they pose can have a major impact on a computer and computer data.
Episode 11	'Rewind -Setting right past wrongs'	15 year old Ben becomes the family hero by restoring the family computer's settings.

Appendix C

Netbasics Master Grid

Character	Online Activity	Online behavior	Online Risks	Security Threats	Security Team
Who	*These activities alone are not the risk*	*The risk comes from…*	*What they do (or don't do) to contribute to their vulnerability*	*What are the likely threats?*	*Which member(s) of the security team will be the most help?*
Dad Neville Jones Age: 50	Email	Opens links or attachments in Spam; fails to update security software;	Bypasses computer security by downloading malware from spam links or attachments; compromises home computer security by not applying updates.	Viruses, Spyware	A.V.A.
Mum Jenny Jones Age: 44	Online shopping	Buys from online shops without checking if the shop website is trustworthy	Risks being defrauded by fake websites; may pay for bogus goods; have credit card details stolen or sold to other crims; compromises computer security by not applying updates.	The Prince, Spyware	A.S.S. S.U.P
Grandma Jacquelyn Jones Age: 78	Investing, email, online banking	Trusts unexpected emails from businesses requesting login, pin or password, information	Risks having banking login / password phished / stolen/ used fraudulently; risks loosing important information by replying to spam / fake emails compromises home computer security by not applying updates.	Trickery	S.U.P
Sophie Jones Age: 10	Web surfing, social networking, chatting, gaming.	Chats to total strangers online	Risks communicating with strangers who might may harm children by harassing / cyberbullyling them, sending them inappropriate material, engaging them in online sexual activity, or seeking to meet them in person.	Masquerade Trickery	
Raymond (the dog) Age: 4	Web surfing, peer to peer	Likes pictures of dog food and turns off the firewall to see favourites.	Compromises computer security by turning off the firewall.	Viruses, Spyware	A.V.A. A.S.S.
Ben Jones Age: 15	Web surfing, social networking, chatting, researching, gaming, trading, peer to peer	Spends his free time on online games and online chatting, Always connected!	Risks never being seen in a Netbasics episode, because he is always in his room	?	?

Appendix D Worksheets 1–3

Worksheet 1: Audit of e-security knowledge (EXAMPLE)

In pairs talk through potential risks to your computer security through using the technologies listed. Discuss risks you have encountered, how you knew there was problem, and things you or your family have done to manage risks.

Write main points down in the table below.

Favorite Online Activities	**Potential Risks**	**Ways to stop risks** **Software** **Hardware** **behaviour**
Email		
Online shopping	e.g Dodgy site steals credit card details.	e.g. • Use anti-spyware, firewalls, anti-virus • Check site is secure… valid security certificate, https:// address.
Web searches		
Peer to peer		
Chat / IM		
Downloading music/games/movies		
Location check-in / geo location		
Gaming		
Social networking		

Worksheet 2: Technology + Behaviour=Security Grid (EXAMPLE)

Note for teachers:

There can be more than one answer in several places. The Netbasics Master Grid at Appendix C provides the answers to this table. You may also like to fill in some squares to help students along.

For students:

For your character write down:

- are their any risks to the computer security because of the online activity of your character?
- how does the character make the risk worse?
- why doesn't your character understand the risks?

Character	Online Activity	Online behavior	Online Risks	Security Threats	Security Team
Who	**Favourite online activities**	**What are the potential risks?**	**What behaviour makes the risk worse**	**What security issues might happen as a result (e.g., virus, spyware, masquerade, trickery)?**	**Which member(s) of the security team will be the most help?**
Dad Neville Jones Age: 50	Email				
Mum Jenny Jones Age: 44	Online shopping				
Grandma Jacquelyn Jones Age: 78	Investing, email, online banking				
Sophie Jones age: 10	Web surfing, social networking, chatting, gaming.				

Raymond *(the family dog)* **Age: 4**	Web surfing, peer to peer				
Ben Jones Age 15	Web surfing, social networking, chatting, researching, gaming, YouTube, trading, peer to peer				

Worksheet 3 Home e-security plan - EXAMPLE

For students:
Develop the following e-security plan for a family member or friend that you think might be leaving themselves open to e-security risks, guiding them with the software and behaviour they need to put in place to protect themselves.

Name of e-security target:

Online Activities	**Potential Risks**	**Ways to stop risks** **Software** **Hardware** **Behaviour**
Email		
Online shopping	e.g Dodgy site steals credit card details.	e.g. • Use anti-spyware, firewalls, anti-virus • Check site is secure 'valid security certificate, https:// address.
Web searches		
Peer to peer		
Chat / IM		
Downloading music/games/movies		

Appendix E

WORKSHEET TEMPLATES

Worksheet 1: Audit of e-security knowledge

In pairs talk through potential risks to your computer security through using the technologies listed. Discuss risks you have encountered, how you knew there was problem, and things you or your family have done to manage risks.

Write main points down in the table below.

Favorite Online Activities	**Potential Risks**	**Ways to stop risks** **Software** **Hardware** **behaviour**
Email		
Online shopping	e.g Dodgy site steals credit card details.	e.g. • Use anti-spyware, firewalls, anti-virus • Check site is secure… valid security certificate, https:// address.
Web searches		
Peer to peer		
Chat / IM		
Downloading music/games/movies		
Location check-in / geo location		
Gaming		
Social networking		

Worksheet 2: Technology + Behaviour=Security Grid

For students:

For your character write down:

- Are their any risks to the computer security because of the online activity of your character?
- How does the character make the risk worse?
- Why doesn't your character understand the risks?

Character	Online Activity	Online behavior	Online Risks	Security Threats	Security Team
Who	**Favourite online activities**	**What are the potential risks?**	**What behaviour makes the risk worse**	**What security issues might happen as a result (e.g., virus, spyware, masquerade, trickery)?**	**Which member(s) of the security team will be the most help?**
Dad Neville Jones Age: 50	Email				
Mum Jenny Jones Age: 44	Online shopping				
Grandma Jacquelyn Jones Age: 78	Investing, email, online banking				
Sophie Jones age: 10	Web surfing, social networking, chatting, gaming.				
Raymond *(the family dog)* Age: 4	Web surfing, peer to peer				
Ben Jones Age 15	Web surfing, social networking, chatting, researching, gaming, YouTube, trading, peer to peer				

Worksheet 3 Home e-security plan

For students:

Develop the following e-security plan for a family member or friend that you think might be leaving themselves open to e-security risks, guiding them with the software and behaviour they need to put in place to protect themselves.

Online Activities	**Potential Risks**	**Ways to stop risks** **Software** **Hardware** **Behaviour**
Email		
Online shopping	e.g Dodgy site steals credit card details.	e.g. • Use anti-spyware, firewalls, anti-virus • Check site is secure 'valid security certificate, https:// address.
Web searches		
Peer to peer		
Chat / IM		
Downloading music/games/movies		
Location check-in / geo location		
Gaming		
Social networking		