UNIT 4.4

We are online risk managers

Understanding risk and prevention of information loss

1 About this unit

UNIT SUMMARY

In this unit, children will use their knowledge of online safety to work out what has happened to a family member's bank account. They will learn that **hacking** can be a criminal activity and clicking on links in suspicious websites or emails can introduce viruses to devices, putting personal information at risk and stopping the device from working. They will learn ways to protect their devices and accounts and use this information to create a family protection plan to share at home.

REPORTING ROUTES

In Year 4, children should know a range of ways to report concerns and inappropriate behaviour through:

- talking to a trusted adult
- calling Childline (0800 1111).

These points should be re-emphasised in any teaching and learning where children are working online.

If any safeguarding issues or concerns arise during this unit, you must follow your School Safeguarding Policy.

ONLINE SAFETY FOCUS

In this unit, children will:

- understand the risks involved in clicking on and opening links on suspicious websites and in emails
- understand that hacking can be illegal and has consequences for the **hacker**
- develop awareness of viruses and what to do if they think their account has been compromised.

ENGAGING PARENTS AND CARERS

- In this unit, children will share what they have learned in this lesson by creating a family protection plan for online activity.
- Consider running an online safety session for parents outlining the risks associated with suspicious links and weak passwords. You may wish to invite a member of the local police school liaison team to reinforce the importance of data protection.

TEACHER KNOWLEDGE

- This session is designed to give children confidence in their own responses to unexpected online activity as well as introduce them to different risks involved in internet use. The purpose of this is to widen their knowledge of potential risks before they are exposed to them.
- Hacking is not always a criminal offence. Many large corporations now pay specialists to try to hack into their systems to find any weaknesses to attack.
- Whilst the focus of this unit is about protecting our information from people we don't know, it is worth exploring with pupils that they also need to behave responsibly, e.g. not access / remove others work on the school network (a much simpler form of hacking).
- It is worth knowing the difference between hacking and **phishing**: phishing is masquerading as a trustworthy source to get information (for example, via email) and hacking is gaining unauthorised access to data in a system or computer.
- Review definitions of the following terms using the glossary on page 64: **anti-virus software**, **hacker**, **phishing**, **spyware**, **trojan**, **virus**, **worm.**

CROSS-CURRICULAR LINKS

Computing

Use technology safely and respectfully, keeping personal information private; identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies

2 Getting ready

ONLINE SAFETY PRINCIPLES

Think about how you can embed the online safety learning and outcomes from this unit within your whole-school online safety strategy through:

- whole-school e-team engagement
- online safety displays
- use of a website online safety area
- Twitter tweets. For example: 'This half term our Year 4 pupils are finding out how our information can be stolen online and how to prevent this.'
- a school newsletter. You may wish to paste the following advisory text for parents and carers into your school newsletter, or send home in book bags (see editable *Newsletter text* on My Rising Stars): 'This half term, Year 4 pupils have been finding out ways that people might try to steal our personal information such as hacking, phishing or the use of viruses. All children have been asked to talk to their parents about these risks and share a family action plan they have created to help everyone in your household to protect personal information. Please support their learning by adding to this action plan where appropriate.'

THINGS YOU NEED

- A copy of the online safety rules created in Unit 4.1

THINGS TO DO

- Familiarise yourself with the steps of this activity before running this online safety session.
- Print and photocopy *My family protection plan* photocopiable master – one per child.

MY RISING STARS RESOURCES

- *My family protection plan* (.pdf)

OTHER RISING STARS RESOURCES

- This lesson links closely to *Switched on Computing Unit 2.4 – We are researchers* and *Unit 3.5 – We are communicators*.
- This unit builds on *Switched on Online Safety Units 2.3*, *2.4* and *3.3*.

INCLUSION/THINGS TO CONSIDER

- Be aware that some children may have no experience or awareness of hacking. Be clear that hacking is potentially illegal and causes stress and upset to the victim.

USEFUL LINKS

- Useful information about what can go wrong on the internet: www.thinkuknow.org.au/youth/what-can-go-wrong
- BBC One Direction parody song about sharing information online: www.youtube.com/watch?v=GHW6O3Mf0qE
- Beware what you download – Lady Jane Grey gets spam and junk mail: www.bbc.co.uk/cbbc/watch/p01g2ppl
- Hacker's top 5 tips for internet safety: www.bbc.co.uk/cbbc/findoutmore/stay-safe-facts

3 Running the lesson

Resources

- *My family protection plan* photocopiable master – one per child.

Possible outcomes

- Children will use their existing skills and newly-learned knowledge to develop a family protection plan for online activity.
- They will then take this plan home to share and develop with their family.

Step 1: Introducing the session

- Explain to the children that in this online safety session they are going to use all their internet safety skills to work out what to do when something goes wrong online and personal information is at risk.
- Explain that sometimes things go wrong on the internet and it feels like we have no control over them. We do. We have control over how we respond.

Step 2: Information loss: hackers

- Ask the children to recap their online safety rules created in *Unit 4.1*. Remind them that they are skilled online detectives, information protectors and code masters. They have learned lots of skills to help them understand when something doesn't seem right and how to respond to it.
- Explain that the internet is changing all the time so they are going to discuss a scenario that they haven't specifically learned about to see if their skills work!
- Split the children into smaller groups for discussion and read out the following scenario: *A family member has an email from their bank showing they bought lots of things online. They didn't order anything. What has happened here?*
- Give the children time to discuss in their groups and then ask for their suggestions of what might have happened. If appropriate, explain that the email account has been hacked. A hacker has used software to get access to personal information online. Hacking can be a criminal offence (see *Teacher knowledge*).
- Ask the children what advice they would give to a family member who has been hacked. Give the children time to discuss the situation and ask for their responses. If necessary, explain that their family member needs to report the incident to the bank and change their passwords for every online account.
- Ask the children to recall their own learning and offer advice on how the family member can better protect their information, for example, developing and using strong passwords which are different for every account.

Step 3: Information loss: viruses

- Explain to the children that there is one more step their family can take to protect their information. They should run **anti-virus software** on their devices in case the hacker still has access to their personal information.
- Explain that anti-virus software protects devices from all sorts of harmful software like **worms**, **trojans** and **spyware**. These are viruses that can stop computers from working and risk personal information.
- Ask the children if they can think of any ways they might inadvertently get a virus on their computer. If necessary, prompt them to recall *Unit 3.3 – We are internet detectives*. Clicking on a link on a website can cause this.
- Explain that clicking on a link in an email can also cause a virus to be downloaded on a computer. How can they prevent this happening?

Step 4: Developing a response

- Explain that we now believe the family member had their account hacked and their personal information was taken. Hackers were the problem. They used the information to buy goods online without the account holder's knowledge, causing them stress and upset.
- Ask the children to discuss how the hackers may have got access to the account, i.e. weak or shared passwords, no anti-virus software, same password for every account.
- Finally, ask them to decide what action they or their family should take to ensure it doesn't happen again.
- Hand out a copy of *My family protection plan* photocopiable master to each child. Ask the children to use all the information they have learned today to create a protection plan that reminds family members how they can keep their information safe from online attack. Encourage them to be creative in how their present this information; they might like to write a set of rules, create a poster with pictures or even create a comic strip.
- Encourage children to take the family action plan home to share with grown-ups at home.

Step 5: Summing up

- Reinforce that sometimes unexpected things happen on the internet, causing loss of personal information or computers not to work properly. We can take steps to limit unexpected events by protecting our personal information with strong passwords, using anti-virus software and not clicking on links on suspicious websites or in emails. If something unexpected does happen, we will use our knowledge of internet safety to respond appropriately and to quickly minimise loss or damage.

4 Taking it further

- Ask the children to take home their online protection plan and share it with their family. Encourage parents to help children to develop the plan further together, thinking of extra preventative measures to help protect personal information online.