The Boomer Challenge

Parent & carer guide

The Boomer Challenge

The Boomer Challenge is a fun, interactive, educational online game for children 8 to 12 years of age.

The game's key message is that in the online world, users should always be sceptical about interactions with others – even if they think they know them.

It's important to ***recognise*** *the signs that something could be dodgy,* ***react*** *by walking away and* ***report*** *immediately to a safety helper.*

The Boomer Challenge encourages safer online interactions, normalises risk assessments and empowers online decision-making.

The format allows children to engage in decision making processes and explore the consequences their choices, providing them with a better understanding of online safety.

This game has been developed for children to use unsupervised.

Why is it called the Boomer Challenge?

The story follows a boy called Millsy and his 18 year old sister Kristy, who are participating in a recorded video challenge where they try to teach their grandparents how to navigate the internet safely.

The use of 'Boomer' reflects the joking way that some children refer to older people, especially their struggles with technology. It also captures their general feeling of knowing more than the oldies about the world, and particularly, the internet.

Millsy finds out that teaching someone to navigate the internet safely is not always as easy as it seems, and that dodgy tricksters have many ways of hiding in plain sight online. Millsy and Kristy need to help their grandparents think critically about online interactions, avoid scams, embarrassing videos and other online problems.

The key messages and teachable moments are transferable lessons, providing knowledge that will help children interact online, in any platform, in a safer way.

Who is The Boomer Challenge for?

It is designed for children 8 to 12 years of age, but older kids and adults also find it entertaining!

Parent & carer guide

The Boomer Challenge

How to play the Boomer Challenge

Children play through the perspective of Millsy, who is trying his hardest to help Grandma and Grandpa learn how to use different platforms on the internet.

The various story paths and decision points encourage children to play and replay to explore alternative courses of action.

Children will watch a 9 minute introduction animation before being presented with four scenarios.

Path 1. Grandma uses email

Path 2. Grandpa on social media

Path 3. Grandpa games

Path 4. *Grandma creates an online photo album - available soon.*

Within each path there are decisions that will be faced.

At the end of each path, children can choose whether to replay the path, or try another and teach Grandma and Grandpa something new.

TIP: Encourage children to try all choices for each path to ensure they are aware the different things that can happen in the online world.

Introduction

The introduction sets the scene by introducing the characters and introducing Millsy's top safety tips which are used as core learnings throughout the game.

Talking points

Why did Kristy think it is important to create a strong and secure password? What is a strong password?

A strong password helps to protect your personal information and data and can help prevent hackers accessing your account.

Why does Kristy want Grandma and Grandpa to be sceptical online?

Being sceptical is the ability to doubt whether something is true and questioning something online that sounds 'too good to be true'.

Path 1. Teach Grandma email

Grandma wants to learn how to send internet letters, so Millsy shows her how to send an email. Grandma receives an email from someone who she assumes is her cousin Rob. Rob needs assistance and urgently asks for Grandma to send money. Millsy has to help Grandma and give advice on the safest course of action to take. Is it really Rob?

Luckily Kristy is not too far away to provide help if Grandma and Millsy make an unsafe choice.

Talking points

Grandma thought she knew who Rob was, what are some clues we can look for to identify if someone is real or fake?

It's not just strangers we need to be careful about online. Sometimes dodgy tricksters can pretend to be someone we know so we have to look for other clues.

Kristy thought it was odd that a family member would ask for help through an email, and wondered why they didn't call or ask for help in person?

Always be sceptical if anyone asks you for anything online. Look at how they have contacted you, the words that they have used, and if there is anything personal within the message.

What are some alternative motives of people who contact you online?

To get personal information like your name, number, address, photos, bank details, details for your friends and family.

Path 2. Teaching Grandpa social media

Grandpa has used social media on his phone before but is excited to use it on his laptop. Grandpa is a bit confused that his friend Norm has sent him another friend request, he thought they were already friends. Millsy helps Grandpa decide if it's really his friend Norm.

Talking points

Why should we check Norm's identity before accepting the friend request?

Dodgy tricksters can assume the identity of a family member or a friend, to try to trick us into risky behaviour.

The Boomer Challenge

Grandpa accidentally accessed his camera, and the dodgy trickster was able to film him without him knowing.

Did you know that people can screen cap? Do you know how content can be used or shared and how difficult it is to get back?

The dodgy trickster was able to threaten Grandpa with sharing the video to his workplace, sporting club and friends. How could they identify these people?

There may be clues in your photos that tell a dodgy tricksters where you go to school, work or live.

What should Grandpa do to try to get the video removed online?

Private photos and videos can still be copied and shared. Talk to a safety helper who can report the video to eSafety or to the social media platform where the video was posted to.

Path 3. Teach Grandpa online video games

Millsy is excited to show Grandpa how to play games and offers to teach him. They use Millsy's account.

A new player joins the channel, gives Grandpa multiple compliments and asks him to join a separate chat channel. In the other chat channel Grandpa is dared to send a picture of himself in his undies for 1000 gems. Luckily Kristy is hanging around to make sure things don't get out of hand!

Talking points

When Grandpa was playing, did he really know who the other players were?

Someone else might be using a friends account to play online. Millsy's friends may have thought it was Millsy playing the game when it was actually Grandpa – you never know who someone is online. It's not just strangers that we need to sceptical of.

The stranger wanted Grandpa to move out of the game into another chat platform, why do you think they wanted him to do that?

Dodgy tricksters can have many reasons as to why they want you to change platforms – there might be different security measures between platforms, or they want you to use a platform that your parent or carer doesn't know about.

Did you notice what methods the dodgy trickster tried using to get Grandpa to go to the other platform?

Dodgy tricksters have a number of tactics used online to trick kids into making an unsafe choice that they wouldn't normally make. You can have a look at these tactics here (link to parent info sheet).

Path 4. Teach Grandma to image share

Grandma wants to learn how to make an online photo album so she can show off her lovely green lawn. Grandma is contacted by Manure2You offering her a great deal on lawn fertiliser. Grandma decides to take them up on the offer. Millsy and Kristy help Grandma figure out the intention of Manure2You contacting her online.

This situation can be likened to a child being contacted by a *modelling agency* or *designer clothes company*. Whilst in this particular story the dodgy trickster is after money from Grandma, the same technique can be used to trick a child into sending photos.

Talking points

Grandma wanted to comment on a photo. Why did Kristy not want her to post those comments?

Decisions should not be made when we are emotional or under pressure. Comments that you make online might be misunderstood by the other person or you might not be able to delete or remove the comment if you change your mind later.

Grandma reacted quickly to her neighbour's picture online. Why can't we always trust a picture that gets posted online?

Pictures can be edited and don't always represent reality.

How did Manure2You set up the situation knowing Grandma was interested in lawn fertiliser? What are some of your interests that you post about online?

Grandma might have a public profile on the platform and used hashtags which make it easy for dodgy tricksters to search for certain topics.

Manure2You offered Grandma a free deal to make her lawn look the best in the street, why should Grandma be sceptical of this?

People might try to make something seem 'rare or special' to trick us into wanting it more. People might say nice things to us to try to trick us into doing something risky.

Parent & carer guide

The Boomer Challenge

What are the risks to children online?

Over confidence – because children easily adapt to technology there is a risk that they could find themselves on a platform that is not age appropriate and could be exposed to harmful content.

Social - the internet has provided a platform for children to connect with other kids and form relationships with people who they may not know in real life. Children do not view these people as a threat and in some instances, they see their online friends as closer to them than their friends or family.

Emotional - negative online information, harmful content and fake news can be distressing and traumatising for children to process. Knowing how to navigate the internet and seek assistance if they see something that upsets them is crucial.

Physical - there is an assumption that children are physically safe while they are interacting online. However, there is a real threat of physical danger associated with sharing photos or personal information online.

Why do children take risks online that they wouldn't take offline?

Capabilities - children lack the awareness of online risks. In real life they are aware that their physical safety can be threatened by people unknown to them. Online, the threat of someone they have met in a game does not necessarily immediately raise red flags. Also, children often lack the necessary skills to deal with people who may be trying to use persuasive, coercive or manipulative tactics on them.

Opportunities - there are more opportunities to interact with a wide variety of people online and this has become a societal norm. The environmental prompts surrounding online behaviours are not apparent and children often take things at face value.

Motivation - often elements of online games or platforms contain highly addictive reward-based elements. These could be lights, colours, sounds, gems or game levels. The part of the brain responsible for reward-based stimuli is distinct from the part of the brain responsible for rational decision making. This leads to children acting more impulsively and taking more risks online, than they would do in real life.

Children often find that cyber-safety lessons are way below their understanding, so they don't engage with them. The lessons paint the internet in a way that does not represent the experiences of children.

Handling difficult situations

Avoid blaming or shaming the child – it is never a child's fault, and they are not responsible if someone tricks them into doing something online. The key to keeping kids safe online is to keep communication open and let them know they can always come to you or another safety helper if something feels wrong or uncomfortable.

Glossary of terms

Sceptical – not easily convinced, having doubts or reservations that something is true.

Social engineering – is how predators use natural human behaviour to trick someone into doing something they wouldn't normally do. They can pretend to be someone a child knows or may try to make friends with them in a game.

Phishing – is an attack that attempts to steal your money or your identity, by getting you to reveal personal information, such as credit card numbers, bank information or passwords.

Screen capped (or screen grab) – to capture a copy of one's computer screen, whether that is a copy of a picture or a video.

Need support of more information?

- If you believe a child is in danger call **Police 000**
- Resources to teach child safety skills to children and young people are available from the **Daniel Morcombe Foundation website.**

1300 326 435
DanielMorcombe.com.au