

Cyber Safety in Action – Teacher’s resource

These scenarios and activities are designed to reinforce Internet Safe Education key messages. Gender neutral names are used in the scenarios. Please assign pronouns if that works better for your students. (Provision made for single gender schools.)

Key Messages

- The internet is PUBLIC and PERMANENT
- My identity is paramount
- Online contacts remain strangers
- Online rules and laws are real
- I take action when things go wrong online



1 – Freddie turns 18 and applies for a car loan. Freddie discovers they have a poor credit score and is declined a loan. Freddie has never had a loan or a credit card. What might have happened in this situation?

- Discussion points
 - Someone with the same name may have applied for credit and not paid their debts but it is more likely that their identity was stolen.
 - This is the best case outcome. Other outcomes include debt collection letters or tax bills.

Child identities are valuable commodities because the theft is rarely identified until the child turns 18 and applies for credit. How can your identity be stolen online?

- Online shopping scam – False store front collects financial credentials
- Phishing scam – click through from email, text, app to a phishing site that collects your financial credentials then uses those to access bank accounts or purchase in legitimate websites.
- Forged website – eg bank site that collects your sign in data

What are some ways we can protect ourselves from online identity theft?

- Check URL. Look for ‘https’. Make sure the URL is spelt correctly.
- Don’t click through from an email, forum, or message. Be cautious when using a search engine, still check the URL if you are entering private data.
- Use secure networks – not public access wifi like on a train.
- If shopping on a phone, use the app rather than the website as the apps tend to be more secure.
- Use PayPal if over the age of 18.
- Use a prepaid card – reduces the amount another person can steal.
- Use double verification methods.
- Don’t overshare online. Social media can be used to put together parts of the identity puzzle that allows your identity to be stolen. Advancements in AI make deep fakes of you or your voice possible if your social media presence gives sufficient material to work with.

2 – Activity – Presentation to middle school. Your digital footprint – keep it clean.

Small groups (3 – 5 students). You are going to present to middle school students about the importance of carefully curating their digital footprint. You will create the outline for ONE topic/reason/strategy. (Useful if students think of different things in each group.) Think about fun ways to get the key message across. We are more likely to act on advice when the presentation of the facts elicits an emotion and/or the consequences feel real and potentially important.

You can get creative, for example use

- **stories/examples of things that can go wrong or**
- **5 years from now what are you going to be doing (applying for a job) and why that matters or**
- **what would your grandma say.**
- **Teacher notes – allocate time to storyboard one idea. Feedback to the larger group.**

Now consider your digital footprint. Have you taken your own advice? Are there cautionary tales in your online presence? You are 5 years ahead of the younger middle school students. How will your online presence impact your employability now and possibly in another 5 years? What would your grandma say?

- **Not necessarily expecting a response. This is a reflective practice. You could, time permitting, encourage them to make some notes about how well they have implemented this own advice and what they may be able to do about it now. Eg remove content, improve security settings**

Teacher guidance – Employment screening checks look for -

- **Social media - evidence of toxic, inappropriate, discrimination (race/ gender/ religion/ sexuality) and potentially discriminatory beliefs/actions. Bad mouthing teachers or other employers or inappropriate sharing of information. Too frequent posting online. An individual's online identities are used to check more broadly on the internet for further evidence of beliefs and conduct, such as friend's accounts and who they follow online.**
- **Illegal activity such as drug use, underage drinking, sexualised images, links to pornography.**

3 - Sam receives a message with a nude image of themself. Sam knows this photo. It was on social media where Sam had been wearing clothes. The clothes had been removed and now it looks like a deliberate nude photo. The message says – ‘Looking good. If you don't want everyone to see this version on Instagram, click this link and follow the instructions.’ How is Sam likely to feel?

- **Discussion points**
 - **Decide whether small group or large group will work better for your class.**
 - **NOTE the wording does not elaborate on Sam's gender. Let it play out and see how many of the students assume Sam is female. The reality is this happens to all genders. Gender is irrelevant in this instance. The offender is looking to extort for financial gain. Interesting to see whether the students think boys will feel differently about it than girls. Bring it back to digital footprint – parents, employers, future partners, and grandparents.**
- **What do you think this person wants?**
 - **Sextortion is a form of blackmail and image-based abuse. The demand is usually for money, cryptocurrency, gaming credits or gift vouchers. This has become such a**

problem that stores that sell gift cards will make enquiries when someone buys many cards all at once. This is happening now in Australia. Remind them of the importance of considering whether what they see or read is 'genuine' online.

- **What can Sam do?**
 - Collect evidence immediately – screenshot the identifying information (when, where, who, what – time, date, phone number or platform, name, image)
 - Remember that there is no reason to feel shame or fear. You have been targeted by a criminal. Tell an adult. Contact a 24/7 helpline if you feel you need more support.
 - Report to eSafety and police. This is a criminal offence and the offender can be prosecuted.
 - Stop all contact. Block. Delete. Do not pay or send intimate content (if that's what they request).
 - Blackmailers are often playing a numbers game. They will often ignore those who don't engage.

This is happening now. AI and deep fakes are convincing and pretty easy to create. Encourage a conversation about not believing what you see or hear and encourage students to be discerning and sceptical.

4 - What do you do if something upsets you or makes you uncomfortable online?

- Preferred responses – (encouraging strong self-regulation practices. Online problems are the same as physical world problems. Get offline to feel better.)
 - Same as when anything else upsets you, regardless of whether it is online.
 - Think of 3 things that make you feel lighter or happier or more peaceful. Do one of those.
 - Talk to someone you trust. Cuddle your pet. Listen to music and dance and sing. Colour in. Shoot some hoops. Go for a ride or a swim. Read a book you love. Do something that makes you feel happier or lighter. You can change your day when you change your mood.
 - Play Tetris or poyo poyo = therapeutic impact on trauma¹
 - Deliberately choose to do things that make you feel better and ask for a hug from someone in your family when you need one.
 - Everything is easier when you feel better and there is help – you just need to ask.



¹ <https://pmc.ncbi.nlm.nih.gov/articles/PMC7828932/> 2020 Journal of Psychiatry and Neuroscience