Dio Parents Online Safety Talk 5th March 2019

PAULA GAIR
www.deriskme.com/dio
help@deriskme.com
@deriskme.com

What is Online Safety?

Enjoying the benefits of technology without compromising your own, or another persons safety, online or offline:

- Cyberbullying / Social Exclusion
- Offensive / Inappropriate Content
- Technology Balance / Screen Time
- Privacy / Digital Footprint
- Cyber Security
- Behaviours - Respect, Resilience, Responsibility and Reasoning

Digital Curriculum 2020

The goal of this change is to ensure that all learners have the opportunity to become digitally capable individuals.

This change signals the need for greater focus on our students building their skills so they can be innovative creators of digital solutions, moving beyond solely being users and consumers of digital technologies.

- Ministry of Education

Screentime

Passive <u>consumption</u>: watching TV, reading, and listening to music

Interactive <u>consumption</u>: playing games and browsing the Internet

<u>Communication</u>: video-chatting and using social media

Content <u>creation</u>: using devices to make digital art or music

Screentime

- Apple screen time settings (via family sharing)
- No screens an hour before bed / or after dinner if trouble going to sleep
- Blue light keeps us awake
- No screens at meal times
- Behaviour - sleep / meals / sports / friendships / school

Cyber Bullying

- On and offline closely related
- Cyber bullying is more detrimental than real world bullying
- Social exclusion is a form of bullying
- Many children don’t tell anyone
- Teach the girls to stand up / speak up for others as well
- Sending a message of support makes a huge difference
- Watch for behaviour change (including device use)
- Devices out of bedrooms at night

Cyber Bullying

- Positive communication - stand up for each other
- Online and Offline are the same
- Digital footprint / privacy
- Websites / apps / games / social media
- Report content or issues - ask for help

Inappropriate Content

- Safe search mode
- Child only search engines
- iPad settings to restrict adult content
- Mobile device management (eg Family Zone)
- Talk about what to do if you see something inappropriate
- YouTube / YouTube Kids

Digital Footprint

Don’t share:

- Name
- Address
- Phone Number
- Email Address
- School / Sports teams
- Photos
- Passwords

Social Media / Gaming

- Age limits
    - Commonsense Media Reviews
- ‘Friends’ and ‘likes’
- Digital Footprint
- Multiplayer games
- Compare and despair

Gaming Positives

Playing with others / team environment

Talking / communications

Accomplishment

Creativity / imagination

Autonomy / independence

Being good at something / improving

Strategy / problem solving

Relaxation / stress relief

Gaming Negatives

Screen time / problematic internet use

Interactions with strangers

In game bullying / harassment

Gambling / Gamblification eg‘ loot boxes’

Security vulnerabilities

Anxiety

Fortnite

Made over $1.2 billion since launch

(Free game, in app purchases)

$2m/day (record day July 13th 2018 $3m)

125 million people have played

iOS 15m in 3 weeks / 100m in 90 days / downloaded 82.6M on iOS

68% have made in app purchases (36.7% had never before)

Ave spend pp $84 (USD)

$100million prize money 2018/19

10 M players attended a virtual concert with DJ Marshmello

https://youtu.be/ZyBb6Ha1Un4

S.M.A.R.T

Safe: Keep safe by being careful not to give out personal information when you're chatting or posting online. Personal information includes your email address, phone number, password and school.

Meet: Meeting someone you have only been in touch with online can be dangerous. Only do so with your parents' or carers' permission and even then only when they can be present. Remember online friends are still strangers even if you have been talking to them for a long time.

Accepting: Accepting emails, messages or opening files, images or texts can lead to problems - they may contain viruses or nasty messages.

Reliable: Someone online might lie about who they are and information on the internet may not be true. Always check information.

Tell: Tell a parent, carer or a trusted adult if someone, or something, makes you feel uncomfortable or worried, or if you or someone you know is being bullied online.

4 R’s of Online Safety

Respect - I treat myself and others the way I like to be treated

Responsibility - I am accountable for my actions and I take a stand when I feel something is wrong

Reasoning - I question what is real

Resilience - I get back up from tough situations

Digital Parenting

Set clear expectations / Family Contract

Try what they’re doing / get involved

Keep talking - have lots of conversations / ask questions

Supervise but don’t spy

Another trusted adult ?

Don’t threaten to take away ‘the internet’ / device

Digital Footprint / Privacy

Focus on behaviour

Reward good behaviours

Report problems / get help fast

Digital Parenting

Sharenting?

Your privacy settings

Set a good example (digitally distracted parents)…

Model positive behaviours

Conversation starters

Tools and Technologies

Harmful Digital Communications Act (NZ)

Family
Online Safety
Institute

GOOD DIGITAL PARENTING

Family Online Safety Contract

Parent's Contract

I know that the Internet is an important resource for my children and that being familiar with it is a necessary skill. It can also be a wonderful place to visit, but I know that I must do my part to help keep my kids safe online.

If my child does something that I do not approve of online we will have a calm conversation about my expectations and the reasons for our Internet rules. I understand that just taking away the Internet will not solve the problem.

I will set reasonable rules and guidelines for computer use by my children, including how much time they may spend online; I will encourage them to participate in offline activities as well. We will discuss these rules and post them near the computer as a reminder.

I will not overreact if my child tells me about something "bad" he or she finds or does on the Internet.

I will get to know the services and websites my child uses.

I will try to get to know my child's online friends and contacts just as I try to get to know his or her offline friends.

I will try to put the home computer in a family area rather than in my child's bedroom.

I will report suspicious and illegal activity and sites to the proper authorities and learn how to report abuse when necessary.

I will learn about parental controls for filtering and blocking inappropriate Internet material from my children.

I will talk to my children about their social networking profiles; what they can and cannot post, who they should allow as friends and how to behave appropriately in their online interactions.

I will frequently check to see where my kids have visited on the Internet and I will talk to them if I see something I'm concerned about or that I think is inappropriate.

If my child continues to break our Internet rules after we have discussed them I will impose penalties for their actions including taking away his or her computer, cell phone or other devices until the behavior changes.

Family technology contract

Parenting Place

In our family, we...

✕ Cross out ones that don't apply

Will always acknowledge if someone speaks to us even if we are watching a brilliant movie and it's the best part

Will say, "Excuse me" If we want to talk to someone who is using a device or watching TV, or if we burp

Look at the person who is talking to us and not at our device

Will let someone know that we want to talk to them and then give them a fair amount of time to finish what they are doing if it cannot be paused

Won't use any device during meals together

*unless you consider cutlery a device

Will share cool things that we have found online with our family

*including but not limited to memes, photos of fridges and mum's research into the family tree

Believe that online connection can never replace real life connection

Will have times where no one is allowed to use their device

I, _____ agree to the following terms and conditions of the technology contract -

✕ Cross out ones that don't apply

Technology contract

Parenting Place

I will never change the default browser of the computer to Internet Explorer

I will not give personal information to people I meet online unless I'm entering a competition and I'm certain it's not a scam and the Nigerian prince seems really legit

I will ask before I download an app

I will ask before creating a social media profile

I will only ever change the volume to multiples of two or five on shared devices

I won't arrange to meet with someone I've met online unless I've discussed it with my parents

I will always find out if my phone number spells something weird

https://phonespell.org

I will never take part in bullying or abusing anyone IRL (in real life) or online

I will tell parents about anyone who sends explicit messages or content or wants me to send explicit messages or content

I will always tell a parent about anyone who bullies IRL (in real life) or online

Privacy and Security Settings

- Check by app (settings / privacy / type of access) and device
- https://myaccount.google.com
- Facebook / Instagram / Snapchat settings

Parental Controls

- Active supervision
- Family Contract
- iPad / iPhone iOS12
- Don’t spy but do check up
- Friend your children on social media
- Safe Search options
- Family Zone app / box and app

iPhone/iPad Settings

- Family Sharing - approve apps remotely
- Auto-Updates
- Air-drop / bluetooth / wifi / hot spots
- Settings / Screentime / Content and Privacy Restrictions
- App Store purchases - installing / deleting apps / in app purchases
- Allowed Apps - can switch off mail / camera / siri etc
- Content Restrictions - block explicit content (including web and Siri), limit adult sites, whitelist favoured sites
- Share my location
- Game centre (multiplayer games / adding friends)
- Privacy - review which apps use location / camera etc

Cyber Security

- Email - the key to everything
- Passwords - Password Manager / Secure Passwords
- 2FA - SMS / Authenticator / Yubikey
- Home network - default password / guest network
- Travelling /public wifi - VPN / Data Blocker
- Back Ups - Encrypted / Unencrypted
- Private searching - DuckDuckGo (with safe search)
- Antivirus / Internet security

Top 25 most common passwords by year according to SplashData

Rank	2011[4]	2012[5]	2013[6]	2014[7]	2015[8]	2016[3]	2017[9]
1	password	password	123456	123456	123456	123456	123456
2	123456	123456	password	password	password	password	password
3	12345678	12345678	12345678	12345	12345678	12345	12345678
4	qwerty	abc123	qwerty	12345678	qwerty	12345678	qwerty
5	abc123	qwerty	abc123	qwerty	12345	football	12345
6	monkey	monkey	123456789	123456789	123456789	qwerty	123456789
7	1234567	letmein	111111	1234	football	1234567890	letmein
8	letmein	dragon	1234567	baseball	1234	1234567	1234567
9	trustno1	111111	iloveyou	dragon	1234567	princess	football
10	dragon	baseball	adobe123[a]	football	baseball	1234	iloveyou
11	baseball	iloveyou	123123	1234567	welcome	login	admin
12	111111	trustno1	admin	monkey	1234567890	welcome	welcome
13	iloveyou	1234567	1234567890	letmein	abc123	solo	monkey
14	master	sunshine	letmein	abc123	111111	abc123	login
15	sunshine	master	photoshop[a]	111111	1qaz2wsx	admin	abc123
16	ashley	123123	1234	mustang	dragon	121212	starwars

UNCOMMON (NON-GIBBERISH) BASE WORD

ORDER UNKNOWN

Tr0ub4dor&3

CAPS?

COMMON SUBSTITUTIONS

NUMERAL

PUNCTUATION

(YOU CAN ADD A FEW MORE BITS TO ACCOUNT FOR THE FACT THAT THIS IS ONLY ONE OF A FEW COMMON FORMATS.)

~28 BITS OF ENTROPY

2^{28} = 3 DAYS AT 1000 GUESSES/SEC

(PLAUSIBLE ATTACK ON A WEAK REMOTE WEB SERVICE. YES, CRACKING A STOLEN HASH IS FASTER, BUT IT'S NOT WHAT THE AVERAGE USER SHOULD WORRY ABOUT.)

DIFFICULTY TO GUESS:

EASY

WAS IT TROMBONE? NO, TROUBADOR. AND ONE OF THE Os WAS A ZERO?

AND THERE WAS SOME SYMBOL...

DIFFICULTY TO REMEMBER:

HARD

correct horse battery staple

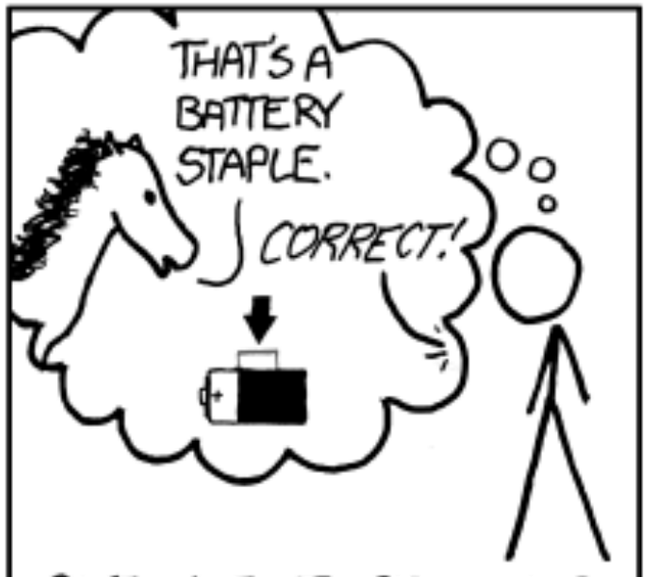
FOUR RANDOM COMMON WORDS

~44 BITS OF ENTROPY

2^{44} = 550 YEARS AT 1000 GUESSES/SEC

DIFFICULTY TO GUESS:

HARD



DIFFICULTY TO REMEMBER:

YOU'VE ALREADY MEMORIZED IT

THROUGH 20 YEARS OF EFFORT, WE'VE SUCCESSFULLY TRAINED EVERYONE TO USE PASSWORDS THAT ARE HARD FOR HUMANS TO REMEMBER, BUT EASY FOR COMPUTERS TO GUESS.

';--have i been pwned?

Check if you have an account that has been compromised in a data breach

email address or username pwned?

264	4,859,717,682	61,452	59,843,767
pwned websites	pwned accounts	pastes	paste accounts

Top 10 breaches

711,477,622 Onliner Spambot accounts

593,427,119 Exploit.In accounts

Actions

- Set up family sharing
- Privacy / Security settings - apps / devices
- Family Contract - choose one and talk to your family
- Find another trusted adult
- Check your social media privacy settings
- Take an interest in what your children are doing online
- Cybersecurity

PAULA GAIR
www.deriskme.com/dio
help@deriskme.com
@deriskme.com