STAYING SAFE IN A CONNECTED WORLD

Action Fraud
National Fraud & Cyber Crime Reporting Centre
0300 123 2040

GET SAFE ONLINE .org

WELCOME

- Detective Inspector Gav Callow
- Isle of Man Constabulary Cyber

THIS SESSION AIMS TO COVER:

Introduction – IOMC Cyber Strategy

Basics of online safety

How to keep your family safe online

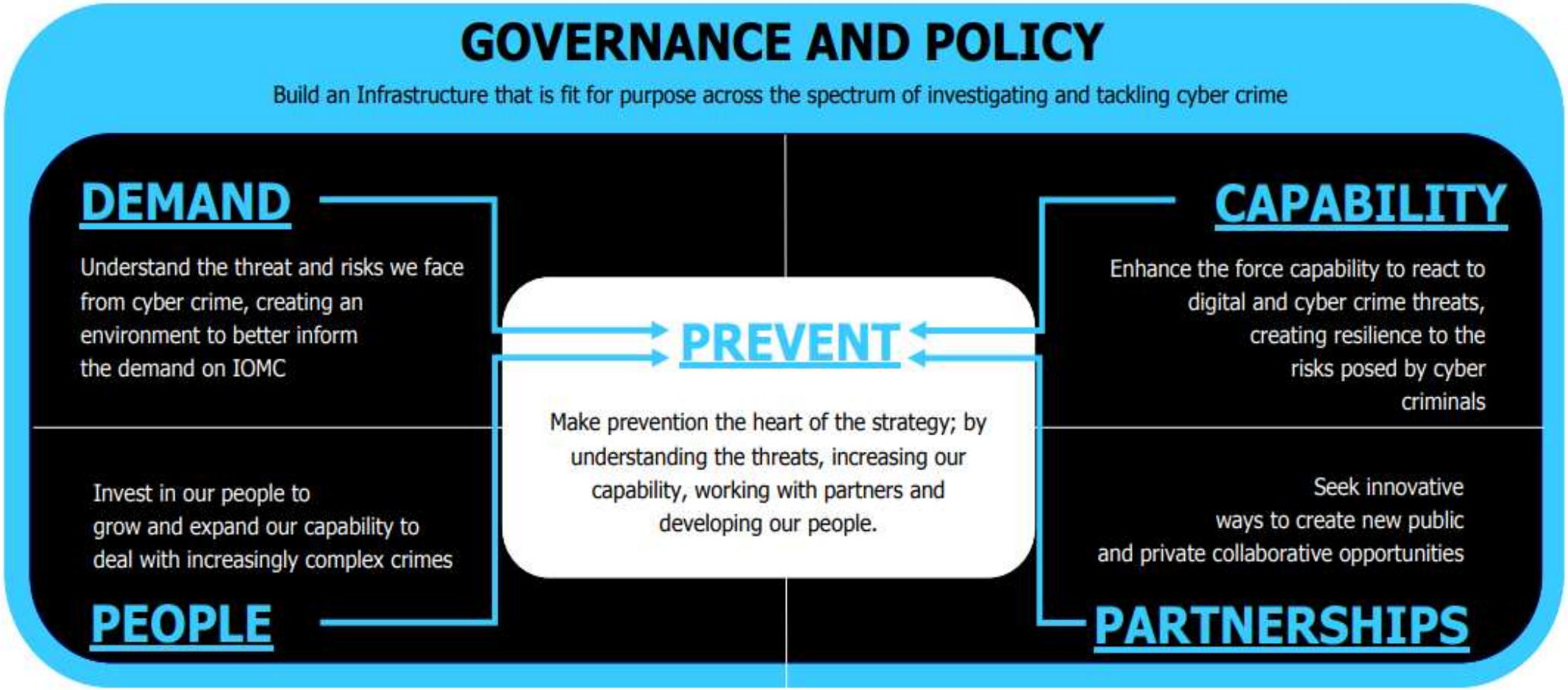
How to have helpful conversations about online safety within the family

Online cyber safety resources

INTRODUCTION:
SINCERE PROJECT, GETSAFEONLINE.ORG, IOMC CYBER STRATEGY

- SENTER - **Strengthening European Network Centres of Excellence in Cybercrime.**
- **SINCERE – Small Islands Virtual Centre of Excellence. Isle of Man, Jersey, Guernsey and Gibraltar.**
- **IOM Constabulary Cyber Strategy -** https://www.iompolice.im/media/1316/cyber-crime-strategy-2019-2023-final.pdf

3. Cyber Strategy Aims



GET SAFE ONLINE PARTNERSHIP

- HSBC have sponsored the GSOL for the SINCERE group – IoMC, SoJP, GP, RGP
- Access via the main website www.getsafeonline.org or via the IoMC website https://www.iompolice.im/
- Contains information about keeping safe online for individuals, families and businesses.

Get Safe Online

Get Safe Online is the UK's leading source of information and advice on online safety and security, for the public and small businesses. It is a not-for-profit, public/private sector partnership backed by a number of government departments, law enforcement agencies and leading organisations in internet security, banking and retail.

For more information and expert, easy-to-follow, impartial advice on safeguarding yourself, your family, finances, devices and workplace, visit www.getsafeonline.org

www.getsafeonline.org

CYBERCRIME?

The internet is a fantastic resource and is part of our everyday life but…

- Organised Crime Groups
- Nation States – China, Russia, North Korea, Iran
- Terrorist Groups - ISIS
- Hacktivists – Anonymous, LulzSec
- Hackers – White, Grey and Black Hat. Script Kiddies
- Insider – Disgruntled Employee, partner, friend
- CSE/Bullying/Abuse/Drugs/Crime/Gangs-

THE MAIN CYBERCRIME TYPES

NCA - https://nationalcrimeagency.gov.uk/what-we-do/crime-threats/cyber-crime

"Cyber criminals seek to exploit human or security vulnerabilities in order to steal passwords, data or money directly. The most common cyber threats include:

- Hacking - including of social media and email passwords
- Phishing - bogus emails asking for security information and personal details
- Malicious software – including ransomware through which criminals hijack files and hold them to ransom
- Distributed denial of service (DDOS) attacks against websites – often accompanied by extortion"
- CSE/Bullying/Abuse/Drugs/Crime/Gangs-

BASICS OF ONLINE SAFETY

Pa55$w0rds

Complexity- alpha numeric, special characters, length

Passphrases – monkey kitchen apple, 18 characters

Email account password separate to other accounts, avoid repetition

Multi factor authentication – Google authenticator

Always change the default password!

Can't remember all your passwords – use a password manager

Never disclose your passwords!

Change key passwords periodically

https://youtu.be/opRMrEfAIiI

JIMMY
Kimmel
LIVE!

NATIONAL CYBER SECURITY CENTER (NCSC) TOP 10 HACKED PASSWORDS WORLDWIDE 2019

1. 123456 (23.2m)
2. 123456789 (7.7m)
3. qwerty (3.8m)
4. password (3.6m)
5. 1111111 (3.1m)
6. 12345678 (2.9m)
7. abc123 (2.8m)
8. 1234567 (2.5m)
9. password1 (2.4m)
10. 12345 (2.3m)

NATIONAL CYBER SECURITY CENTER (NCSC)

- **Top 5 names**
- ashley (432,276)
- michael (425,291)
- daniel (368,227)
- jessica (324,125)
- charlie (308,939)

- **Top 5 football teams**
- liverpool (280,723)
- chelsea (216,677)
- arsenal (179,095)
- manutd (59,440)
- everton (46,619)

- **Top five fictional characters**
- superman (333,139)
- naruto (242,749)
- tigger (237,290)
- pokemon (226,947)
- batman (203,116)

EMAIL ACCOUNTS

- Keep them safe
- Other accounts (social media, gaming, banking, etc.) rely on your email should you forget your password and allow you to reset them
- Don't use your email password for any other service/application
- https://haveibeenpwned.com/

UPDATE

- Keep your devices up to date
- Auto update
- Antivirus
- Operating systems – Windows 7 out of support Jan 2020
- Broadband router - VPNfilter

BE CAUTIOUS

- Phishing – Vishing – Smishing
- If it sounds to good to be true it is
- Email is responsible for 92.4% of malware. It is followed by the Web for a measly 6.3%, and others 1.3%. (**Verizon 2018 Data Breach Investigations Report**)
- Bank account details
- Malware, Ransomeware

From: Mrs.Juan <test@test.com>
Sent: Tuesday, October 15, 2019 11:26:00 AM
Subject: Attention: Beneficiary2
Attention: Beneficiary

We are not sure you received our previous message but we wish to us this medium to officially inform you that following the ongoing review of all unclaimed and delayed funds by the United Nations and the World Bank, your payment file was forwarded to our office for immediate payment of your long delayed funds starting with a first transfer of US$10,000,000.00 with reference No. NG/FM14FGN, to your bank account.

However, we are surprised to receive another application this morning from your representative, MR.KRAUS MULLER,stating that you authorized him to transfer the funds to another bank account in Germany and that you were recently involved in an auto accident and cannot walk right now.

Could you please confirm immediately, your relationship with MR.KRAUS MULLER and also, confirm if the bank account in Germany as shown below is now your new bank account information to receive your funds this week from our paying bank

CREDIT SUISSE, D-80321 BREMEM,GERMANY
ACCOUNT NO: 098-11180933-109
IBAN: CH55 0910 3045 6011 91110 0
SWIFT CODE: AREZCHZZ8OU

Kindly get in touch with us today by email with your telephone number to confirm this information to avoid wrong transfer of your funds, so that we can proceed with the transfer of the US$10,000,000.00 to your correct bank account as scheduled.

Yours sincerely,
MRS.JUAN HENRY
Director,Anti-Fraud Unit.
Financial Services Regulation Committee
Plot 33,ATB Way Cadastral Zone,Abuja,NG

KEEPING YOUR FAMILY SAFE ONLINE
BE A SWITCHED ON PARENT

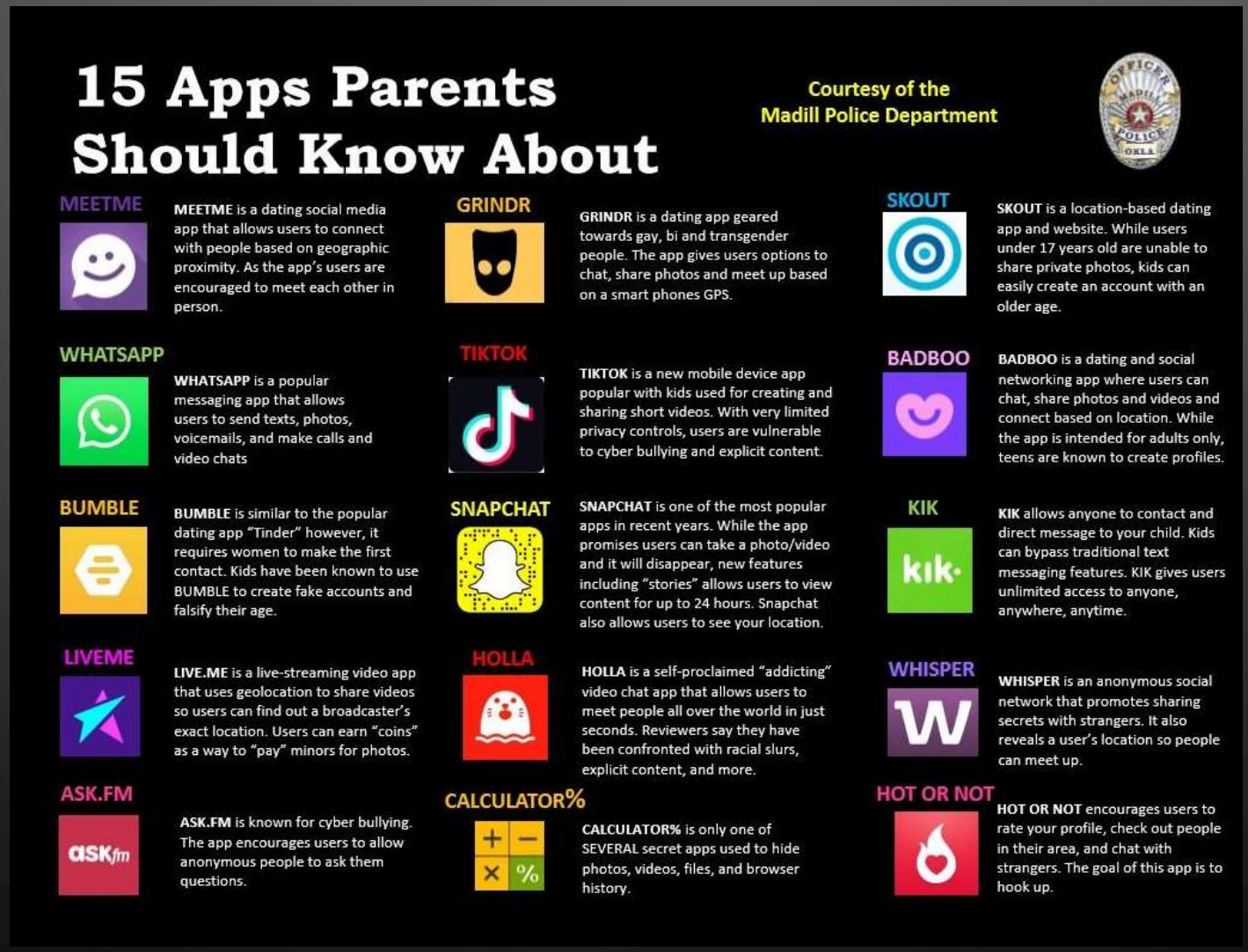
WWW.GETSAFEONLINE.ORG/SAFEKIDSONLINE
#SAFEKIDSONLINE

- Have regular conversations with your child about the good and not-so good things about the internet
- Set boundaries and rules – only play with people you know, duration online, time of day
- Swap experiences with family and friends – share knowledge, apps, technology
- Parental control software, apps, mobile devices, consoles, family filters (ISP), OpenDNS Family Shield, PiHole
- Tell your children not everyone online is who they appear to be – gaming, social media, video streaming (YouTube, Twitch)
- Oversharing - Live streaming, pictures, videos, personal information. Once it's on the internet, it's out of your control.

BE A SWITCHED ON PARENT CONTINUED

- Messaging apps – Whatsapp, Snapchat, Discord, Viber, Wechat, Messenger, Kik. Messages are recorded, images can be saved. App
- Cyberbullying – Keep a record, 'print screen', mobile phone camera, seek advice
- Protect accounts with good passwords and don't share them.
- www.nspcc.org.uk/preventing-abuse/child-abuse-and-neglect/bullying-and-cyberbullying
- www.childline.org.uk/info-advice/bullying-abuse-safety/types-bullying/online-bullying/
- There is also an excellent article on preventing different kinds of bullying (not just online) at momlovesbest.com/bullying-prevention
- Report inappropriate content or behaviour to the website or social media site where it occurs, and child sexual abuse or grooming to www.ceop.police.uk & Isle of Man Constabulary

HOW MANY DO YOU KNOW?



HOW TO HAVE HELPFUL CONVERSATIONS ABOUT ONLINE SAFETY WITHIN THE FAMILY

- Balanced Approach
- Set boundaries but don't be heavy handed
- See what they are using – are they appropriate for their age?
- Try to understand what they are doing online, try for yourself or research online
- What are your friends and family doing online – compare experience
- Parental controls - computers, mobiles and games consoles, privacy features on social networking sites, and the safety options on Google and other search engines

DISCUSSION QUESTIONS TO HAVE WITH YOUR KIDS

- - What are your friends doing online?
- - What are the newest and best websites and apps?
- - Can you show me your favourites?
- - Do you know what cyberbullying is, and have you ever experienced it in any way? Or have any of your friends?
- - Has anything you've seen online ever made you feel weird, sad or uncomfortable?

SOCIAL MEDIA

- Phishing – links to take you outside of the service to a fake site
- Download malware
- Ask you to call premium rate numbers
- Extortion
- Stealing login details to bank website through fake web link
- Similar techniques to email phishing
- If it looks to good to be true ….. It is

SOCIAL MEDIA CONTINUED

- Check your security settings, is full public access necessary?
- Facebook is the most popular social media app with over 2 billion accounts
- Makes its revenue through advertising
- Social engineering – Cambridge Analytica - misinformation
- Careful what you click on – information from your profile can be collected when engaging with some of the posts.
- Who are your real friends? Who can access your profile?

USEFUL ONLINE RESOURCES

- www.getsafeonline.org
- www.nspcc.org.uk/preventing-abuse/child-abuse-and-neglect/bullying-and-cyberbullying
- www.childline.org.uk/info-advice/bullying-abuse-safety/types-bullying/online-bullying/
- momlovesbest.com/bullying-prevention
- www.ceop.co.uk
- https://www.actionfraud.police.uk

USEFUL ONLINE RESOURCES CONTINUED

- https://haveibeenpwned.com/
- https://www.ncsc.gov.uk/blog-post/passwords-passwords-everywhere
- https://www.iompolice.im/
- https://oursaferschools.co.uk/

ANY QUESTIONS?