# Safeguarding Bulletin

## Lent Term 2023 ~ Issue 02

Dear Parents and Guardians,

Welcome to our newsletter from the Safeguarding Team at Bredon School. Our aim is to provide you with the latest support and advice which could affect you and your children's lives.

### New Guides for WhatsApp and BeReal – NSPCC

This month, the NSPCC has updated its advice on two very popular apps with children and young people - WhatsApp and BeReal.

**WhatsApp** is one of the most popular instant messaging apps, used by over 2 billion people in 180 countries. It allows you to send and receive messages, as well as make voice and video calls. You can connect with people individually or join group chats where lots of people can contribute. For further information, advice and safety tips, please click the link below:

**NSPCC - Is WhatsApp safe for my child?**

**BeReal** is a popular image-sharing app where you can post your own pictures as well as view other people's. Users can only post once a day and are only able to see their friends' images if they have shared their own.

At a different time every day, users receive an alert telling them it's 'Time to BeReal'. This gives them two minutes to take a photo, using both the front and back camera of their device and post it on the app. For further information, advice and safety tips, please click the link below:

**NSPCC - Is BeReal safe for my child?**

### Place2Be: Important Resources for Parents and Carers

This Parenting Smart site is filled with a number of resources for parents and carers of 4-11 year olds. The latest articles on supporting healthy gaming habits, developing a child's talent and safe social media for younger children and preparing your child for secondary school can all be read or watched in under ten minutes. These are perfect for those of you with limited time. For further information, please click the link below:

**Place2Be - Parenting Smart**

## Fraud Update from West Mercia Police - Economic Crime Unit

### DVLA SCAM EMAILS

Please be aware that once again scammers are circulating fake emails purporting to be from DVLA. They often come with the title “Vehicle Tax Status – Unpaid”, and may carry a realistic looking Gov.uk logo, however the sender's email address will certainly not look genuine.

The message will then tell you that your payment has failed so your vehicle is not taxed and you are driving illegally. A clickable link will follow in the message which, once opened, asks the recipient to update their bank details and personal information.

**Please do not click that link**, just delete or mark it as “Spam” and forward a copy to report@phishing.gov.uk

### PAYPAL SCAMS

If you think you have been scammed on PayPal, you can first check to see if the payment is still pending, in which case you can use “Cancel payment” and get an instant refund.

If not, PayPal offers a Purchase Protection plan whereby you can sign into the Resolution centre on www.paypal.com/disputes. You have up to 180 days from the transaction date to use this facility.

Another common type of scam used by fraudsters on PayPal is the “Refund Scam”. The Scammer buys an item from you but makes an overpayment for the goods. Having told you then they overpaid by oversight, they request a refund of that part of the payment.

In many cases they ask for the payment to be sent to a third account after claiming the original account is closed. So the seller sends a refund, delivers the item assuming all is well. But in reality, the buyer is a fraudster and was spending money on a stolen credit card or a hacked PayPal account. In essence, this is just another form of Wire Fraud.

**Take Five To Stop Fraud**

- **Stop:** Taking a moment to stop and think before parting with your money or information could keep you safe.
- **Challenge**: Could it be fake? It’s okay to reject, refuse or ignore any requests. Only criminals will try to rush or panic you.
- **Protect:** If you think you’ve been a victim of fraud, contact your bank immediately and report it to Action Fraud online at actionfraud.police.uk or by calling 0300 123 2040.

For further information, please click the link below:

**Action Fraud**
**Take Five - To Stop Fraud**

# Young People and Money Mules - Metropolitan Police

## Money Mules

**Money Mule activity**, is a fast growing and prolific problem in school, college and university environments; it is a key facilitator for online fraud, other cyber related and traditional crime. It relies on access to bank accounts in order to cash out funds stolen or obtained through crime by Organised Criminal Networks (OCG's). We are finding that young people are often targeted to provide access to their accounts either on the promise of a share of the funds or by coercion.

## Fraudsters' Techniques

- A direct approach and openly ask if you want to make some 'easy money' or spin you a lie about needing to use your bank account.
- Posts on Social media sites offering 'Squares' 'Flips' 'AC fraud' 'easy money'
- Airdop contact on your smart device
- Fake job adverts offering working from home on 'money transfer jobs'

## Consequences

- Breaching your Bank Terms & Conditions
- Your Bank account will be closed
- You will be reported to Credit Agencies, this report lasts for 6 years!
- As your Credit Rating will be tarnished, you will have difficulty in getting a financial loan for mobile phone/car/rent/mortgage
- Criminal Proceedings, subject to arrest, charge and Criminal Conviction
- Social effects, perceived by family, employment opportunities and travel

## Tips to keep safe

- Never give anyone details of your Bank Account, PIN number, passcode or password – Bank Accounts are private
- Take time to understand what you are being asked to do, don't be lured or coerced into receiving money into your bank account, however plausible it sounds.
- Research any company (home or overseas) that makes you a job offer and ensure their contact details are genuine.
- If you have been approached, break off all contact with the fraudster, don't receive or move any more money and seek advice
- Report the matter to Action Fraud/Police, Fearless.org or CrimeStoppers on 0800 555 111.

**If the offer sounds too good to be true, it most probably is!**

Report to ACTION FRAUD - 0300 123 2040

Get Safe Online - www.getsafeonline.org

www.met.police.uk/littlemedia

## Children's Mental Health - Royal College of Paediatrics and Children's Health (RCPCH)

The Royal College of Paediatrics and Child Health (RCPCH) have produced a podcast on the increase in mental health issues in young people. It discusses the roles of paediatricians in children and young people's mental health journeys and how they can be part of the safeguarding 'jigsaw'. To listen to the podcast and hear how five child health professionals are tackling the issue through advocacy and innovation, please click the link below:

**RCPCH - Shining a Light on Children's Mental Health**

*Additional Source: NSPCC*

## Thrive Online - Childnet

Thrive Online has been created to help educators, parents and carers to support children and young people aged 11 and over with Special Educational Needs and Disabilities (SEND). Childnet has created a set of free, adaptable resources that cover the important topics of healthy relationships, digital wellbeing and online pornography and are designed to equip and enable parents and carers, to support young people aged 11 and over with SEND. For more information, please click the link below:

**Thrive Online - Childnet**

## Sexual Abuse Online: Helping My Autistic Child - The Mary Collins Foundation

Research suggests that parents and carers worry about online sexual harm and what to do if it happened to their child. When you are caring for an autistic child, it can feel like there are lots of extra things to think about. How we respond to an autistic child who might have been sexually harmed online can impact their recovery so it's important to send the right messages from the start. For further information, advice and safety tips, please click the link below:

**Sexual Abuse Online: Helping My Autistic Child - The Mary Collins Foundation**

## Ten Top Tips for Stronger Passwords - National Online Safety

According to a Google survey, more than half of us (52%, to be exact) routinely re-use the same passwords, with around one in ten employing a single password across all of their online accounts. What that means, of course, is that any hacker successfully cracking our password would find themselves with access to not simply one of our online accounts, but several (at least).

That, along with the fact that many people's favoured passwords aren't exactly impenetrable, makes it easier to see why some sources put the number of online accounts being broken into at around 100 per second. Yes, you read that right: 100 per second.

For further tips on setting more secure passwords, please see the poster on the next page:

# Ten top tips for STRONGER PASSWORDS

Passwords continue to be the most common way to prove our identity online. A combination of a username and a password known only to the user provides access to our online accounts and data – and hopefully keeps unauthorised individuals out. As a security measure, though, passwords are relatively weak. People are often predictable in how we choose our passwords, for example – making them less secure. With increasing volumes of usernames and passwords being leaked online, what can we do to keep our data more secure? Here are our top tips for stronger passwords.

## BE UNPREDICTABLE

We often choose passwords which are easy to remember: featuring the name of our favourite sports team or favourite film, for instance. Those are predictable passwords. Cyber criminals will routinely try various combinations of passwords relating to sports teams, actors, musical artists and the like – and they often focus on these during major sporting events or around high-profile movie releases.

## AVOID GETTING PERSONAL

Many of us use passwords relating to our family, such as children's names or favoured holiday destinations. The problem here is that we also typically post about our holidays and our family on social media – making that information potentially visible to cyber criminals and supplying them with clues which could help them in narrowing down possible passwords we might have set.

## NEW PLATFORM, NEW PASSWORD

Where cyber criminals gain access to an online service through a data breach, they often use the data they've stolen to try and access the victim's other accounts. This is because the criminals know that, for convenience, people often use the same password across different services. When we reuse passwords, our security is only as strong as the weakest site where we've used it.

## LONGER IS STRONGER

Our passwords are often stored by online services in an encrypted format, in case the service suffers a data breach. The strength of this encryption, however, is dependent on the length of the password you've selected. If your password is only a short one, cyber criminals are significantly more likely to be able to break the encryption and identify your password.

## CHECK SOCIAL MEDIA VISIBILITY

Staying up to date with friends and relatives on social media is part of everyday life now. We need to ensure, though, that we limit who can see our posts via each platform's privacy settings. It's also wise to consider what we're posting and if it's *really* safe to share online. If we restrict what cyber criminals can see, we reduce the chance of them using that information to identify our passwords.

## 'DOUBLE LOCK' YOUR DATA

It's possible that cyber criminals may eventually discover your username and password. Enabling multi-factor authentication (MFA) on your accounts, however, reduces the chance of them obtaining access to your data, as they'd also require a code which is provided via an app, SMS message or email. MFA isn't infallible, but it *does* definitely provide extra protection and security.

## DELETE UNUSED ACCOUNTS

Data breaches occur when cyber criminals gain access to an online service and all the data contained within it – including usernames and passwords. Whenever you stop using a service, it's wise to make sure that you delete your entire account and not just the actual app. If the service no longer has your data, there's zero risk of it being leaked should they suffer a data breach in the future.

## TRY PASSWORD MANAGERS

Even though most of us have numerous online accounts to manage these days, it's advantageous to avoid password re-use. Specialist password management software (like Dashlane or OnePassword, among others) can help by storing a different password for every online service that you have an account with: the only one you or child will need to remember is the single master password.

## GET CREATIVE

The British government's National Cyber Security Centre (NCSC) recommends the 'three random words' technique. This method helps you create a password which is unique, complex and long – yet which is memorable enough to stay in your mind ("FourBlueShoes", for example). The NCSC website, incidentally, also offers plenty of other useful information relating to personal cyber security.

## STAY VIGILANT

The best way to protect your accounts and your data is to be vigilant and careful. If you receive an email or text message that's unusual or unexpected, treat it as suspicious until you're able to verify whether it's genuine and safe. Starting from a position of vigilance and caution will reduce the likelihood of you or your child being tricked by a malicious email, text or phone call.

## Meet Our Expert

A Certified Information Systems Security Professional (CISSP), Gary Henderson is the Director of IT at a large boarding school in the UK, having previously taught in schools and colleges in Britain and the Middle East. With a particular interest in digital citizenship and cyber security, he believes it is essential that we become more aware of the risks around technology, as well as the benefits.

Source: https://www.ncsc.gov.uk/

National Online Safety®
#WakeUpWednesday

## Children's Health and Wellbeing - NSPCC and Barnardo's

Barnardo's have published a report on the impact of the cost-of-living crisis on children and families in the UK. The report includes findings from a YouGov poll of 1,000 parents in England, Scotland and Wales and findings from a survey of 316 children aged 11 to 25 in the UK. Findings include: almost 1 in 3 parents said their child's mental health had worsened due to rising costs of living; and additional financial pressures were impacting parent's mental health and capacity to support their children. Recommendations include that the UK government should publish an annual report and an action plan on reducing child poverty. To read the news story, download the report, and / or seek support, please click on the relevant the link below:

**Barnardo's - Read the news story: A crisis on our doorstep**
**Barnardo's - Download the report: A crisis on our doorstep (PDF)**
**Barnardo's - Cost-of-living crisis: Where to Get Support if Your Family is Struggling**

*Additional Source: NSPCC*

Best wishes,

Charmain Eaton
**Deputy Head (Safeguarding),**
**Jarrett Housemistress & CCF Contingent Commander**