



# Cyber Awareness, Scams & Fraud

Cyber Protect Officer - Samantha HANCOCK  
(Force HQ)

101 extn 330 7916 or 07814 226278

[samantha.hancock@leicestershire.pnn.police.uk](mailto:samantha.hancock@leicestershire.pnn.police.uk)



@EMCyberSecure



Leicestershire Police Cyber Aware

# *#Tell2*



# **Remember A, B, C**

**A – Accept nothing**

**B – Believe no one!**

**C – CONFIRM EVERYTHING!**

# Our first line of defence .... Devices!

## SUPPORTED Op SYSTEMS

- Ensure you have an up to date, supported Operating System. If using Windows Vista, XP or Windows 7 .... you need to upgrade immediately as these no longer receive security patches!!

## ANTI-VIRUS SOFTWARE IS A MUST

- Ensure that laptops or computers have the default AV running – For Windows this is Defender. NCSC advise that Mac users may wish to install additional AV for Apple Macs. Provided that Android and iPhone users only install apps from Play Store and Apple store, no additional AV is required.

# !! CRITICAL !!

WHATEVER SOFTWARE, APPS OR PROGRAMS WE USE  
**MUST** BE UPDATED AS SOON AS YOU ARE  
ALERTED TO NEW VERSIONS OR PATCHES BEING MADE AVAILABLE

# Password security



- **DO NOT** reuse passwords – you need a different one for each platform!!
- How to remember them all?!

Password Manager ...      Password Hints ...

- **DON'T** use words/names/information that may be in the public domain or easily worked out from social media content, or ancestry sites, eg maiden names; Date/Place of birth; children's names; pets names; teams you support etc
- Your most important passwords are Password Manager and Email accounts

*Current best practice advises THREE RANDOM WORDS*

*CurtainTreeWallpaper*

*If you need to add complexity Curt4inTr33Wallpaper£*

- **ALWAYS** log out of sites and apps, don't just close the window or app – it doesn't end the session!

# Passwords

ARE LIKE

## PANTS



Should only be used ONCE

Never SHARED

Not left out where others can see them!

# Are you aware of exactly how much information there may be about you online?!





# Looking after your personal information



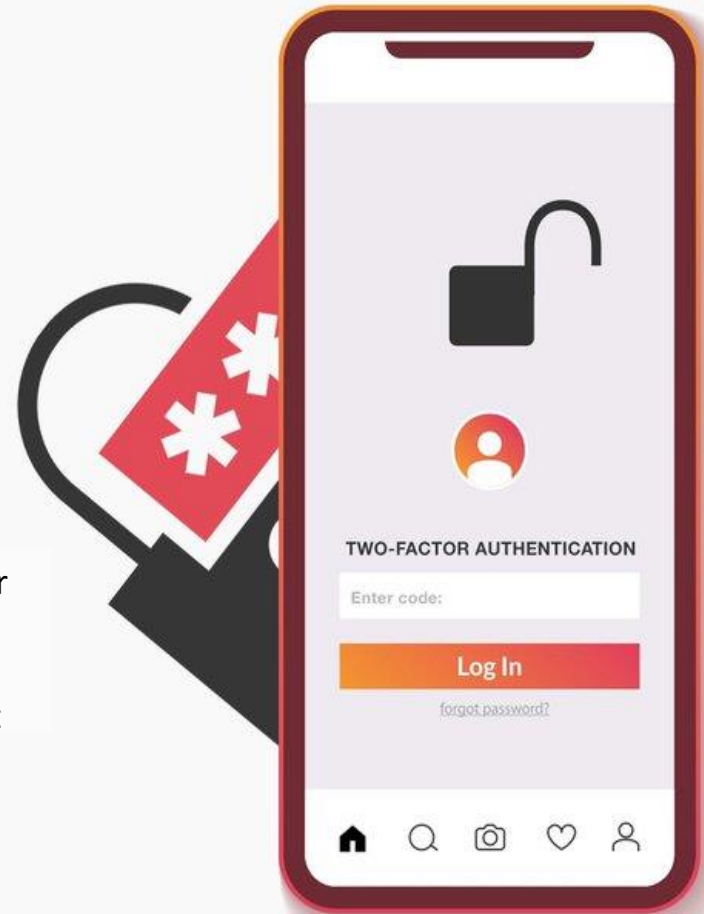
- Limit the amount of information made publicly available
  - see how much information you can find on yourself online
- BEWARE CONSENTED DATA!! Carefully read options when subscribing for anything – they can be misleading. Ensure you opt OUT of sharing your information
- Check [www.ukphonebook.com](http://www.ukphonebook.com) and [www.192.com](http://www.192.com) for your information – it may be a lot more than you realise, including DOB, occupation etc
- Be aware that your phone may be geo tagging your photos!
- Make sure you back up your data (ie photos and contact details etc) on all devices
- Consider installing or activating tracking software/apps in the event of loss or theft
- Wherever possible, accept Multi Factor Authentication (MFA or 2FA) for apps or sites you log in to, especially Social Media and Email accounts



#2FACTOR

# Two-factor authentication

Two factor authentication (2FA) offers an additional layer of protection to your accounts, even if your password is stolen. You should enable it on your important accounts such as email, social media, online shopping and payment services.

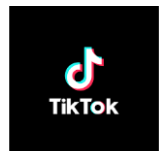


@cyberprotectuk

Easy to follow steps to 2FA : <https://twofactorauth.org>

# How secure is your Social Media?

- It's SOCIAL media, don't have your employer or job title listed
- We strongly advise that you opt for "Friends only".
- **Be a good friend** and change your settings to 'hide' your friends list to protect their security too. Also helps prevent account cloning issues – do the same for contact details!
- Be mindful that "friends" settings can affect your own security
- It is advised you turn app location settings off when you post to social media as it indicates your current location .... AND where you are NOT!
- Remember regularly checking in to places, regardless of your settings 'checking in' is publicly viewable
- Change your settings so that you control what others post about you!
- Social media checklists :  
<https://www.saferinternet.org.uk/advice-centre/teachers-and-school-staff/teaching-resources/social-media-checklists>



# Be aware of data breaches & protect your passwords!



[www.haveibeenpwned.com](https://www.haveibeenpwned.com)

A website that allows you to check if your personal data has been compromised by data breaches.

We recommend opting for "Notify me". You will now receive notifications about future breaches. Once signed up, you will receive an email message any time their personal information is found in a new data breach.

*This service often alerts users to breaches long before it reaches the news, meaning that you can take action immediately instead of your accounts being at risk for months without you knowing.*



**Canva:** In May 2019, the graphic design tool website Canva suffered a data breach that impacted 137 million subscribers. The exposed data included email addresses, usernames, names, cities of residence and passwords stored as bcrypt hashes for users not using social logins. The data was provided to HIBP by a source who requested it be attributed to "JimScott.Sec@protonmail.com".

**Compromised data:** Email addresses, Geographic locations, Names, Passwords, Usernames



**Data Enrichment Exposure From PDL Customer:** In October 2019, security researchers Vinny Troia and Bob Diachenko identified an unprotected Elasticsearch server holding 1.2 billion records of personal data. The exposed data included an index indicating it was sourced from data enrichment company People Data Labs (PDL) and contained 622 million unique email addresses. The server was not owned by PDL and it's believed a customer failed to properly secure the database. Exposed information included email addresses, phone numbers, social media profiles and job history data.

**Compromised data:** Email addresses, Employers, Geographic locations, Job titles, Names, Phone numbers, Social media profiles



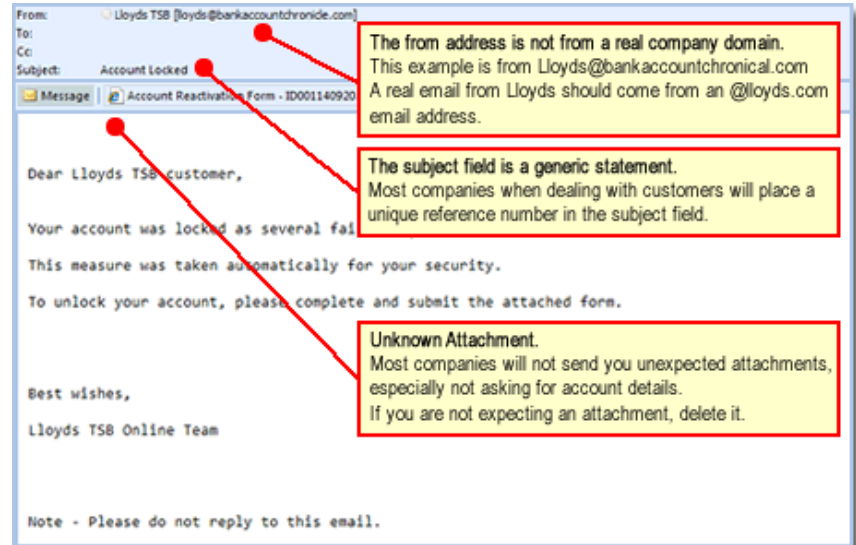
**LinkedIn:** In May 2016, LinkedIn had 164 million email addresses and passwords exposed. Originally hacked in 2012, the data remained out of sight until being offered for sale on a dark market site 4 years later. The passwords in the breach were stored as SHA1 hashes without salt, the vast majority of which were quickly cracked in the days following the release of the data.

**Compromised data:** Email addresses, Passwords



**MyFitnessPal:** In February 2018, the diet and exercise service MyFitnessPal suffered a data breach. The incident exposed 144 million unique email addresses alongside usernames, IP addresses and passwords stored as SHA-1 and bcrypt hashes (the former for earlier accounts, the latter for newer accounts). In 2019, the data appeared listed for sale on a dark web marketplace (along with several other large breaches) and subsequently began circulating more broadly. The data was provided to HIBP by a source who requested it to be attributed to

# Phishing



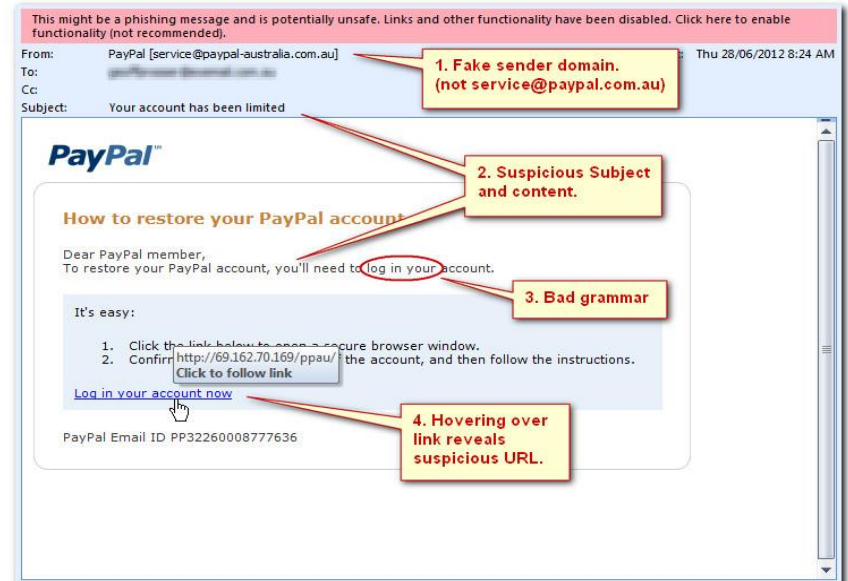
Take many plausible forms

Appear authentic

***! Always a sense of urgency to make you act quickly !***

All designed to trick you in to parting with sensitive data OR contain malware

***GOLDEN RULE – NEVER click on a link to log in or resolve an issue!***





# HOW TO PROTECT YOURSELF AGAINST PHISHING

ATTACHMENTS • LINKS • YOUR INFORMATION

Fraudsters will often create authentic looking emails purporting to be from genuine companies, or even someone you know, in order to defraud you. The emails are designed to infect your devices with malware, or to steal sensitive information such as your financial details or passwords.

If you have been a victim of fraud or cyber crime, please report it to Action Fraud at [actionfraud.police.uk](http://actionfraud.police.uk)



## ATTACHMENTS

Don't open the attachments in any unsolicited emails you receive.



## LINKS

Don't click on the links within any unsolicited emails you receive.



## YOUR INFORMATION

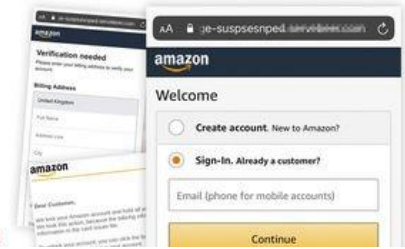
Never respond to emails that ask for your personal or financial details.

Action Fraud  
Met Police  
Cyber Aware

## SCAM WARNING

### Over 270 reports about fake Amazon emails

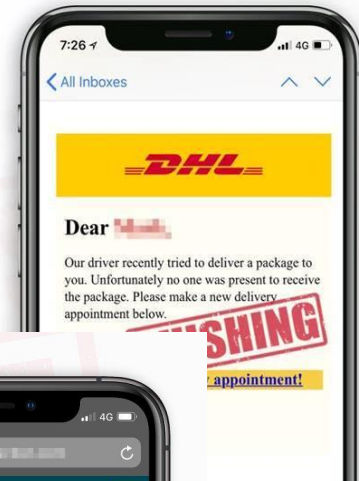
Action Fraud has received over 270 reports in 24 hours about fake emails purporting to be from Amazon. The emails state that there is an "account issue" and ask the recipients to "verify" their Amazon account. The links provided in the emails lead to genuine-looking phishing websites that are designed to steal Amazon login credentials, as well as personal and financial information.



### Watch out for these fake DHL emails.

This email contains links to a phishing website designed to steal personal information and details about which utility providers you use. That information can later be used to create highly personalised phishing attempts against you.

Criminals can spoof email addresses to make it appear as though an email was sent by a person or company you know. Don't click on the links or attachments in unsolicited



## SCAM WARNING

### Fake TV Licensing emails received by thousands

Action Fraud has received more than 5,000 reports about fake emails and texts purporting to be from TV Licensing. The messages contain links to genuine-looking websites that are designed to steal personal and financial information.

Always question unsolicited requests for your personal or financial information in case it's a scam. Never automatically click on a link in an unexpected email or text.

Met Police Action Fraud @cyberprotectuk



## Member Sign In

Email

Password

Remember me

Secure Server

**NETFLIX**  
Update your payment information!

**PHISHING**


We face some difficulties with the current billing information of your own. We will try again, but please at the same time you update your payment details.

Update Account now

TV Licensing email sent from [Name] <[Email]>

# Missed Delivery Scam Emails


Mail 3G 17:41  
yourincome.org

 **dpd** Your delivery

Options for tracking number: 1550488005

The first and second delivery attempt was free. To schedule a new delivery, a shipping fee must be paid.


Pick up (from €60.55)

 **€0.00**

DPD Pickup


The shipment is available until 25/04/2020 for collection at:  
Unit 9, Rosemount Business Park  
Dublin, D11 X8PX

Schedule a new delivery (from €2.20)

 **€2.20**

Track & Trace

Find package with the Royal Mail App




Hello [redacted]

Your Parcel Number #LZ8942357486EN is on the way

Your package is stopped at our post. A £ 1.00 shipping fee has been paid.

If shipping cost is not paid, the package will be returned to the sender.

With the free Royal Mail App, you can see the current status of your package and the next step.





Package Information:

Status: Parcel being held at Terminal 2

Parcel number: #LZ8942357486EN

Weight: 0,467 kg





Unsuccessful delivery attempt

Package from: HM Revenue & Customs  
Package type: Large letter  
Delivery date & time: Friday, 13 November 2020 11:15

We attempted to deliver your package at 11:15 on Friday, 13 November 2020 but no one was available.

Your parcel was returned to our depot and you need to reschedule your package delivery.

Please reschedule your package delivery by pressing 'Reschedule Now' and one of our drivers will attempt to deliver your package.

[Reschedule Now](#)

Thank you,  
The Royal Mail Team

This is an automatically generated email, please do not reply to it.

Copyright 2020. All rights reserved.

Royal Mail is a trading name of Royal Mail Group Ltd. Registered in England and Wales. Registered number 4138203  
Registered Office: Victoria Embankment, LONDON EC4Y 0HQ. VAT Registration Number GB 243 1700 02.



# Covid vaccine invitations

In order to roll out the Covid vaccine programme swiftly, many people are being invited to book their appointments by clicking on a link in a text message or email from surgeries etc.

The NHS :

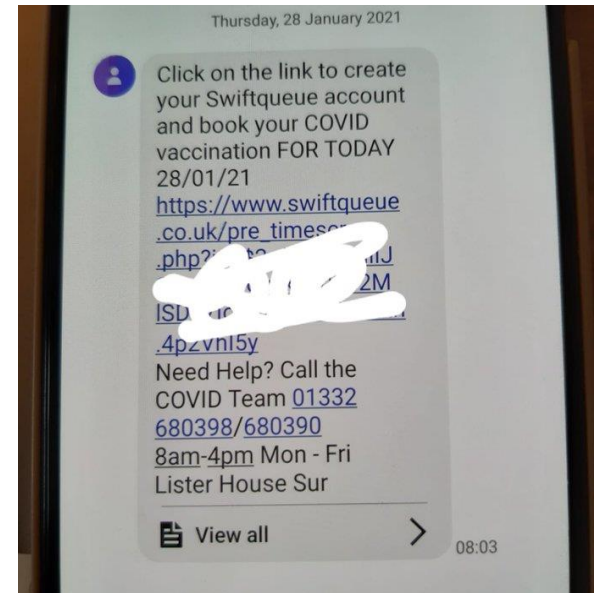
- will NEVER ask for payment - the vaccine is free
- will NEVER ask for your bank details
- will NEVER arrive unannounced at your home to administer the vaccine
- will NEVER ask you to prove your identity by sending copies of personal documents, such as your passport

If you reach a point where you are asked for any of the above, please stop and close the webpage.

**\*\* YOUR HELP PLEASE \*\***

We are aware that our social media messages may not reach some of older and more vulnerable members of the community and we ask you please to talk to relatives and neighbours and ensure they know the above.

<https://www.nhs.uk/conditions/coronavirus-covid-19/coronavirus-vaccination/how-you-will-be-contacted/>



## By letter, text or email

If you're invited to have your vaccination at a larger vaccination centre or at a pharmacy, you'll get a letter.

If you're invited to have your vaccination at a local centre such as a hospital or GP surgery, you'll usually get a text or email. You may sometimes get a letter.

You can choose to go to a larger vaccination centre or pharmacy, or wait to be invited to go to a local NHS service. More places are opening all the time.

## Spotting a scam

The COVID-19 vaccine is free of charge on the NHS.

The NHS will never ask for:

- your bank account or card details
- your pin or banking password
- copies of personal documents to prove your identity such as your passport, driving licence, bills or pay slips

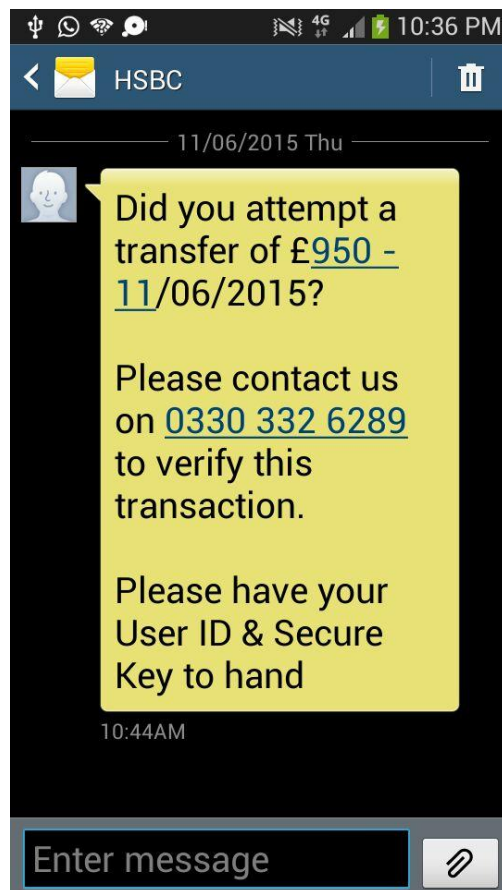
If you think you have been a victim of fraud or identify theft, report it to Action Fraud on 0300 123 2040.

# And it's not just emails ....

< Messages PayPal Details

Text Message  
Yesterday 14:20

PayPal - Your account  
has been locked  
Please click on the link  
below to restore your  
access:  
<http://i.imgur.com/...>  
PayPal Team



*... and not just SMS ...  
Caller ID can be spoofed too!*



# Reporting suspicious emails and text messages

actionfraud.police.uk/report-phishing

## Spotted a suspicious email?

**ActionFraud**  
National Fraud & Cyber Crime Reporting Centre  
actionfraud.police.uk

**Cyber Aware**

If you have received an email which you're not quite sure about, forward it to the Suspicious Email Reporting Service (SERS)

[report@phishing.gov.uk](mailto:report@phishing.gov.uk)

## Fake; Spam and Scam Text Messages / SMS



SMS SPAM (also known as smishing) can be more than just annoying – it may contain suspicious content.

Many carriers will let you report SPAM by simply forwarding the message to '7726' (which is the keys for SPAM on most phones).

Check the sender's details and the service.



**ALWAYS TRUST YOUR INSTINCTS**

**NOT THE CALLER**

**NOT THE TEXTER**

**NOT THE EMAILER**

If you don't think they are who they say  
they are, always take time to stop and think.

**[takefive-stopfraud.org.uk](https://takefive-stopfraud.org.uk)**



**TO STOP FRAUD™**

# !! WHATSAPP SCAM !!



If you receive a WhatsApp message with a verification code that you did not request, delete the message and **DO NOT FORWARD OR DISCLOSE** to ANYONE

- Message allegedly from someone you know or trust, most likely messaging from a different number
- Request to forward verification code

## ! KEY POINTS !

- NEVER DISCLOSE OR SHARE A VERIFICATION CODE SENT TO YOU BY WHATSAPP (or indeed any platform, no matter how convincing the request)
- IF YOU HAVEN'T ALREADY, CHANGE THE SETTINGS ON YOUR WHATSAPP ACCOUNT TO TURN ON TWO STEP VERIFICATION (Open app, click the 3 dots, settings, account, two step verification – it will require you to create a six digit PIN)

For more information visit <https://faq.whatsapp.com/.../received-verification-code...>



# Public WiFi

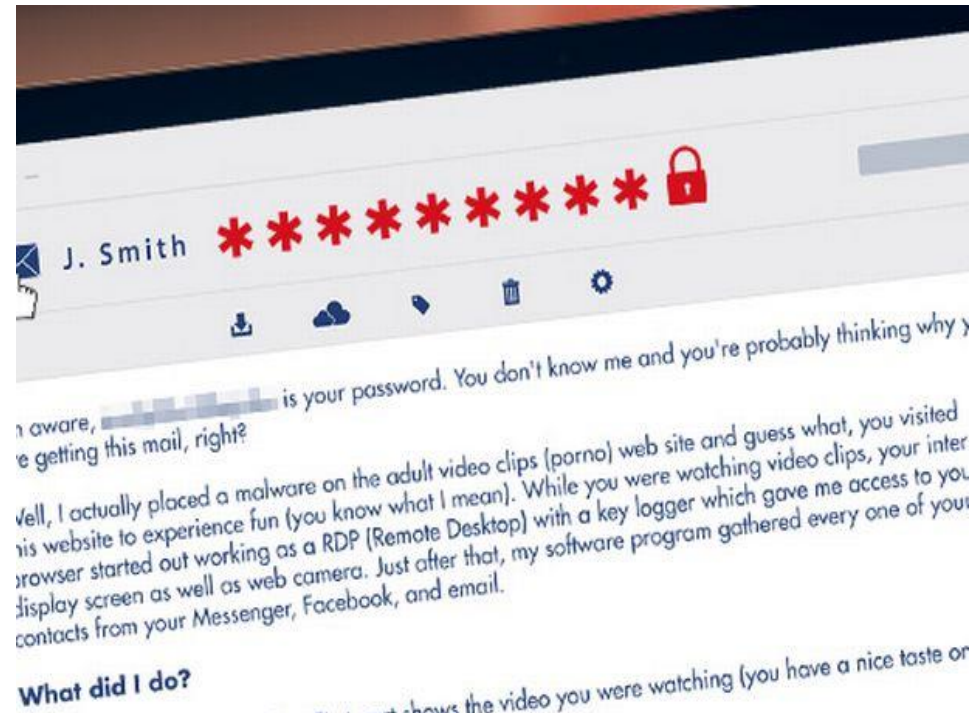
... we all love a bit of free WiFi don't we?

- Potentially, any device connected to a Wi-Fi hotspot can view traffic sent & received by everyone else?
- Do you know even check with the business that it is their WiFi, or is it a fraudsters?!
- If you must use WiFi hotspots, consider installing a **VPN** – Virtual Private Network app
- Your 3G and 4G mobile data is secure!



# Sextortion Phishing emails

- May or may not contain the individuals password or phone number
- Claims to have infiltrated webcam and have footage & copied contacts from social media/email
- BitCoin ransom demanded
- ***DO NOT PAY!!***
- Change the password mentioned on any accounts that use that password





# Computer Software Service Fraud

| How to protect yourself |





Never reveal your personal or financial details as a result of a cold call.


Never install any software or visit a website as a result of a cold call.

Need professional tech support? Ask your friends or family for recommendations and look online for reviews first. Don't contact companies promoting tech support services via browser pop-ups.

# Remote Access

Legitimate companies like Microsoft and Google will never cold call you asking for remote access to your computer or for your financial details. Never grant remote access to your computer to anyone during an unsolicited call.

Always be wary of unsolicited calls, if you're unsure of the caller's identity, hang up.



#Tipoftheweek

**ActionFraud**  
National Fraud Reporting Centre  
0300 123 2040

**CITY OF LONDON POLICE**  
NATIONAL POLICING LEAD OF FRAUD

Be aware of scam calls purporting to be from internet providers, IT support and “Microsoft” etc

Quite simply you should NEVER allow remote connection from an incoming call. Always #HangUp

NEVER install software or visit webpages if instructed – **beware bandwidth test calls!**

More info here : <https://www.actionfraud.police.uk/a-z-of-fraud/computer-software-service-frauds>



# Computer Service Fraud

## How big is the problem?

### November

31 reported incidents - total loss of £8,295

### December

27 reported incidents - total loss £13,285

### January

38 reported incidents - total loss of **£93,260**

### February

29 reported incidents - total loss of £19,000

125 reported incidents in only 4 months, with a total monetary loss of **£133,840**



# Online Banking

- **It is safe!**

- But don't do it on insecure Wifi!
- Use strong passwords
- Only install apps from authorised app stores or official banking sites

- ***The only risk to your accounts is if you respond to rogue emails, texts and phone calls***



**TO STOP FRAUD™**

# Making payments and transferring money

- If using online payment systems, use recognised and trusted ones such as PayPal and WorldPay
- Credit Cards offer the most protection
- Bank transfer payments – the same limited protection as cash, ie none

Beware...there's a problem with the normal payment....



# Shopping safely online

***Please beware !Green Padlock! means data is encrypted  
NOT confirmation the site is legitimate!!***

- ***Rule #1 ... if it seems to good to be true....it probably is!***
- *Don't click on links in emails (offers) to take you to shopping websites – search via a browser*
- Use trusted, reputable retailers
- Remember credit cards offer greater payment protection
- Do not reply to unsolicited emails from companies you don't recognise
- Double check all details of your purchase before confirming payment

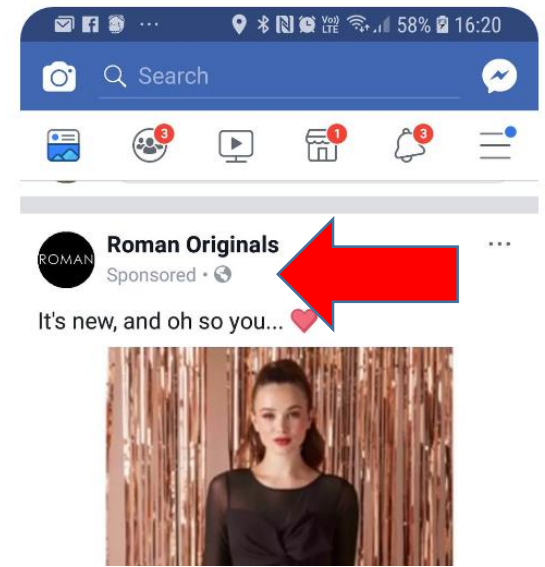
**!! THEN !! ... Before entering payment card details on a website, ensure that the link is secure, in two ways !!**

- There should be a green padlock symbol in the browser window frame
- The web address should begin with 'https://'. The 's' stands for 'secure'.



# Actual reports received ...

- Paid £30 for an iPad ... never turned up
- A really great deal on an iPhone ... turned out to be a Chinese counterfeit
- Beware sponsored Facebook adverts!! Especially if they are “big names at low prices”
- Buying from abroad (and now that includes EU!) – don’t forget you may have to pay import duties to receive your goods!





# “COURIER” Fraud

- The Police will **NEVER** send a courier to collect bank cards or PIN details, no matter what!
- There is no such thing as a “Safe Account”. Banks nor Police will ever ask for funds to be transferred to one – it absolutely **WILL BE** a fraudster
- Police **WILL NOT** ask you to withdraw cash
- Police will **NEVER** ask you to be part of an undercover investigation
- E.G. purchase high value jewellery to be collected





# HMRC / Gift Card Fraud

Predominantly HMRC M.O. threatening warrant for arrest with Police

Any phone call demanding payment by any sort of gift cards is a SCAM

**!! HMRC do not pursue outstanding debts via telephone !!**



# PIN and CODE Rules and reminders

- ✗ **NEVER** click on a link in an email OR a text
  - *if the email relates to an issue with your account or order, log in to your account from a browser or an app*
- ✗ **NEVER** trust a phone number provided within an email or text
  - *Use a trusted number or look one up*
- ✗ **NEVER** respond to unsolicited texts or emails
- ! Card reader codes (or one time codes sent via SMS) are for entering during online banking transactions **ONLY**. **NEVER** disclose these codes to anyone via phone or any type of message.
- ! PIN numbers should only be entered into an ATM, payment terminal or card reader - never disclose to anyone

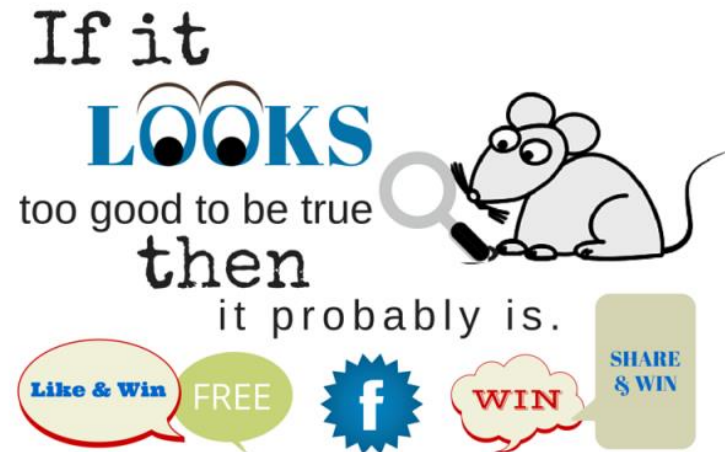


# REMEMBER : You've got to be in it, to win it!!

- ➔ You cannot win a prize, competition, lottery etc if you haven't entered into it! Scams happen in paper format via snail mail too!
- ➔ You should never have to pay a 'release', 'admin' or 'advance' fee to claim a legitimate prize, OR to release online loan funds

Social Media "Give-aways"

A word to the wise .....



# Doorstep Traders & Telesales



**Please encourage everyone to  
make it a RULE not to trade at the door  
or over the phone**

# Beware of telephone cold callers!

- Not everyone is who they claim!
- ALWAYS verify before parting with information
- ALWAYS leave more than 10 seconds after hanging up before dialling out
- Enquire with landline provider regarding free measures to protect against nuisance callers ie Call Guardian / Call Protect
- Call Blockers are good – especially TrueCall



# Current scam calls of note

- Calls regarding Amazon Prime regarding subscription renewal
- Automated calls regarding transactions abroad
- Calls regarding irregularities in relation to your National Insurance number
- Fake investment scams – **always** check FCA register BEFORE investing money  
<https://register.fca.org.uk/s/>
- ANY calls from HMRC regarding outstanding debts
- ANY calls regarding problems with broadband, routers or slow computers





# Romance Fraud



It's real !!

- Beware of the sob story
  - Desperate to visit you but need a loan to pay for the ticket/visas
  - Desperately ill family member who needs help with medical expenses
- Too good to be true business deals – if only they extra up-front money.....
- Beware profiles that immediately tug on heart strings
  - supposed ex-serviceman or woman
  - recently widowed to gain your trust and sympathy
- Alarm bells should ring if anyone is asking for money, especially if you are asked not to tell friends or family!
- NEVER respond to a request for money  
*.... If they're asking for money, it isn't love....*
- Never give out bank account or other details

# Follow up or Recovery Scams



- The person making contact will be aware that you have previously been a victim of a scam and lost money
- Beware also of websites and social media ads claiming to be able to get the money back for you
- Likely to be carried out by the original fraudster
- Will of course have personal details about IP and their previous fraud/scam
- Likely to be seeking an up front payment (again)
- Sadly, often times when you lose money to fraud, it's gone

# Where to report?



Report online

<https://www.actionfraud.police.uk>

Or by phoning [0300 123 2040](tel:03001232040)

WHEN :

Monday to Friday between 8am to 8pm  
Saturday & Sunday - Closed

Textphone users can dial **0300 123 4050**

# Safer Internet Day 2021

## Exploring reliability online

*... not everything is as it appears? .....*



***Do you see a man running ... or a dog...?! ... an old lady, or a young girl...?!***

# SID 2021 : An internet we trust: exploring reliability in an online world

What are the risks of false or misleading online content?

Risks posed by false or misleading content online might include:

- Creating fear, anger and/or panic
- Spending money on products sold under false pretences
- Public opinion affected by inaccurate information
- Personal harm or injury e.g. fake weight loss claims
- Physical damage e.g. inaccurate instructions to fix a broken phone screen
- Negative impact on wellbeing e.g. feeling targeted or powerless or failure/disappointment

The poster features the 'An internet we trust' logo with a magnifying glass icon and the text 'Exploring reliability in the online world'. To the right is the 'Safer Internet Day 2021' logo with a smartphone icon and the 'UK Safer Internet Centre' logo.

### What to trust online? A Parents and Carers Guide

**Q** This sheet aims to give you the confidence and understanding to discuss this year's Safer Internet Day theme, 'An internet we trust: exploring reliability in an online world' with your child.

Some young people will know false and misleading content exists online but some may be new to the idea that you can't trust everything you see on the internet. Regular discussion can help them to develop the habit of questioning and evaluating what they see online.

---

**Q** How are children and young people experiencing false or misleading content online?

Some examples are below, but the best expert on this is your child themselves! Ask your child what they like to do online and where they go to find things out to help start this conversation.

A central diagram shows a cloud of icons representing different types of online content. The icons are: Advertising, Clickbait, Conspiracy theories, Biased reviews and ratings, Edited photos and videos, Inaccurate or exaggerated news stories, Scams and phishing, and Untrustworthy people and messages. A speech bubble icon is also present.

#SaferInternetDay  
1 [www.saferinternetday.org.uk](http://www.saferinternetday.org.uk)

Parents and Carers Pack  
What to trust online? A Parents' and Carers' Guide

# Resources to use with your own youngsters

## UK Safer Internet Centre

<https://www.saferinternet.org.uk/safer-internet-day/safer-internet-day-2021/i-am-parent-or-carer>

## ThinkUKnow

<https://www.thinkuknow.co.uk/parents/>

## Leics Police

Two films made about the dangers that exist online when people hide behind technology and use it to pretend to be somebody they're not.

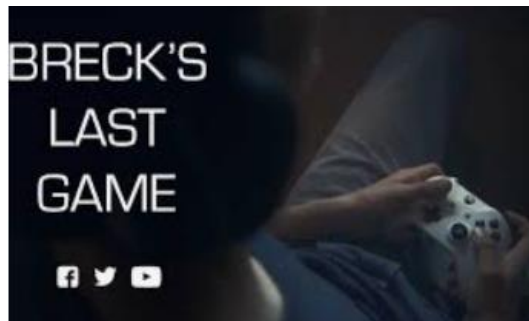
*! The films feature grooming, coercive control and violence and would be rated as a 15 if shown in a cinema !*

Breck's Last Game

<https://youtu.be/hZIYSCE-ZjY>

Kayleigh's Love Story

<https://youtu.be/WsbYHI-rZOE>





# Homeschooling Covid19



# Shake it up ... variety!

*Enlist celebrity help for interest!*

Maths with Carol Vorderman

[www.themathsfactor.com](http://www.themathsfactor.com)

English with David Walliams

[www.worldofdavidwalliams.com/elevenses](http://www.worldofdavidwalliams.com/elevenses)

PE Workouts with Joe Wickes

<https://www.youtube.com/playlist?list=PLyCLOPd4VxBsXs1WmPceksQyFbXTf9FO>



***Don't forget life skills are learning!***

Learning about money – play shop – adding up totals and giving change is maths!

Cooking – learning about the ingredients, where they come from, and nutrition!

Crafts – fun, but also creative and encouraging imagination and fine motor skills!

***BE KIND TO YOURSELF – Most of us aren't teachers!***

# Lockdown Learning: BBC puts school materials on TV, iPlayer and online

BBC Bitesize

<https://www.bbc.co.uk/news/education-55591821>

and

CBBC Daily TV programmes



Did you know you can use games consoles for home learning and internet?

<https://www.wired.co.uk/article/xbox-playstation-online-learning-classroom-teams-zoom>

Need more mobile data?

<https://get-help-with-tech.education.gov.uk/about-increasing-mobile-data>

Useful guidance from Gov.UK

<https://www.gov.uk/guidance/supporting-your-childrens-education-during-coronavirus-covid-19>

# Taking good care of ourselves is as important as learning

## DAILY BINGO

Complete 1 bingo before having free time!

READ 20 MIN	WRITE A LETTER OR TEXT A FRIEND	MOM'S CHOICE	PLAY WITH YOUNGER SIBLING OR PET	COOK SOMETHING
SERVE A FAMILY member	BOARD OR CARD GAME	PRACTICE MUSIC OR SPORT	EXERCISE 20 MIN	WRITE A LETTER OR TEXT A FRIEND
PRACTICE MUSIC OR SPORT	EXERCISE 20 MIN	HUG MOM OR DAD	BOARD OR CARD GAME	SERVE A FAMILY member
PLAY WITH YOUNGER SIBLING OR PET	BUILD A LEGO CREATION	WRITE A LETTER OR TEXT A FRIEND	MOM'S CHOICE	READ 20 MIN
MOM'S CHOICE	PLAY OUTSIDE	READ 20 MIN	COOK SOMETHING	PRACTICE MUSIC OR SPORT

*Build in :*

- Work / school breaks
- Rewards
- Screen breaks
- Physical activity (daily exercise?)
- Relaxation / Meditation

**But most of all,  
don't forget,  
the most important thing  
is we just have to make it through  
these difficult times!**



- Infographics on a huge number of social media platforms and games
- Advice on mental health and self confidence
- Give them a follow on social media too!

At National Online Safety we believe in empowering parents, carers and trusted adults with the information they need to help an informed conversation about online safety with their children, should they feel it is needed. This guide focuses on one platform of many which we believe trusted adults should be aware of. Please visit [www.nationalonlinesafety.org](https://www.nationalonlinesafety.org) for further guides, hints and tips for adults.

**NOS** National  
Online  
Safety  
#WakeUpWednesday

# REMOTE EDUCATION 10 TOP TIPS FOR PARENTS

Remote education ensures continuous learning outside the classroom. For parents and carers, remote education isn't always straightforward and there can be a number of factors they need to consider, especially around ensuring their children feel comfortable and are familiar with the whole concept. That's why we've created this guide to help parents and carers support their child in getting the most out of their remote education experience.

## 1. TAKE AN ACTIVE INTEREST IN YOUR CHILD'S LEARNING

As a parent or carer, your school may have explained how remote education works already, but children may still need help. Take an interest in their learning and help support them whenever they need a helping hand.

## 2. MONITOR YOUR CHILD'S COMMUNICATION AND ONLINE ACTIVITY

It's important to remind your child that despite being at home, the same level of behaviour and conduct must be in place every day at school. Encourage them to remain polite, remember their username and not to post or send any negative comments just because they are behind a computer.

## 3. ESTABLISH A DAILY SCHEDULE AND ROUTINE

Working from home and trying to learn in a more casual setting that children might associate more with play and a degree of freedom might take a bit of getting used to. Try to stick to a daily routine and use the timetable/schedule that schools have sent home to help children keep on top of their daily learning.

## 4. ENCOURAGE SCREEN BREAKS AND PHYSICAL ACTIVITY AWAY FROM DEVICES

Remote learning will inevitably require more interaction with computers, laptops and tablets. Teachers will inevitably advise on screen breaks; however, it doesn't hurt to keep a check on their time online or encourage them to get some fresh air/exercise.

## 5. ENSURE YOUR LEARNING DEVICE IS IN PUBLIC SPACE IN THE HOME

It's important to consider where your PC or laptop is placed if live video is being used. Try to keep the background neutral, with no personal information visible and ensure learning devices out of the bedroom as this could be deemed inappropriate.

## 6. IMPLEMENT SAFETY CONTROLS AND PRIVACY RESTRICTIONS ON APPS AND SOFTWARE

Dependent on how your school implements remote education, your child may be required to download certain software or apps. Whilst these are likely to be relatively safe to use, like any other new app or platform, parents should still implement safety controls as a precaution.

## 7. ENSURE YOUR CHILD ONLY USES OFFICIAL SCHOOL COMMUNICATION CHANNELS

It's important that all communication with teachers and school staff is directed through approved school channels, whether that be through the school's online portal or the relevant secure messaging app.

## 8. FAMILIARISE YOUR CHILD WITH RELEVANT SCHOOL POLICIES

Schools should have a policy on remote education that they can share with parents. Familiarise yourself with this and ensure you know what is expected of teachers and your child during lessons, both online and offline.

## 9. MAINTAIN FEEDBACK WITH TEACHERS

Engage in communication with teachers where possible, and try to feed back progress and development as well as any helpful suggestions around the learning process, the transparent but respectful professional and only use official channels to communicate.

## 10. MONITOR YOUR CHILD'S WELLBEING AND MENTAL HEALTH

Remote education will likely mean that your child won't get the same level of social interaction and might not see their friends as much. Keep a check on their wellbeing and try to encourage them to get out as much as they can. Whilst learning from home might seem fun and exciting to start with, missing out on seeing their friends every day might take its toll.

[www.nationalonlinesafety.org](https://www.nationalonlinesafety.org) Twitter - @nationalonlinesafety Facebook /NationalOnlineSafety Instagram - @nationalonlinesafety

Source: Remote education good practice UK guidance | Published: 11 February 2020 | Version: 1.0 | Page 10 of 10

Users of this guide do so at their own discretion. No liability is entered into. Current as of the date of release: 04.11.2020

# Neighbourhood Link – free service, sign up!

[www.neighbourhoodlink.co.uk](http://www.neighbourhoodlink.co.uk)

The screenshot shows a web browser window displaying the Neighbourhood Link website. The browser's address bar shows the URL <https://www.neighbourhoodlink.co.uk/>. The website has a dark blue header with the text "Neighbourhood Link" and "Local news for Leicester, Leicestershire and Rutland". To the right of the header are social media icons for Facebook, Twitter, and Instagram, along with a "Select Language" dropdown menu. Below the header is a navigation bar with links: HOME, ABOUT, REGISTER, OUR ALERTS, FAQs, and CONTACT. The main content area features a large image of a police officer in a yellow and blue uniform standing next to a police car. Overlaid on this image are two buttons: a green "Sign In" button and an orange "Register" button. Below the image, there is a grey box with the text "Welcome to Neighbourhood Link" and a dark blue box with the text "For emergencies call 999. For non-emergencies report online email or call 101." The Windows taskbar is visible at the bottom of the screen, showing the search bar and various application icons.



# More advice ....?



**The Silver Line**

helpline for older people

**0800 4 70 80 90**

Welcome

What We Do

Who We Are

Get Involved

Contact Us

Donate now

## Our helpline



The Silver Line Helpline is the only **national, free and confidential** phone line dedicated to older people which is **open every day and night of the year**

# 0800 4 70 80 90

Our specially-trained helpline team:

- Offer **information, friendship and advice**
- **Link callers to local groups and services**
- Offer **regular friendship calls**
- **Protect and support** older people who are suffering abuse and neglect

You can call us **at anytime and from anywhere in the UK**

There is no questions too big, no problem too small and no need to be alone.



# Useful Websites

## General advice on Cyber Security for Business & Public :

Cyber Aware [www.cyberaware.gov.uk](http://www.cyberaware.gov.uk)

## Online safety on all areas for everyone :

GetSafeOnline [www.getsafeonline.org](http://www.getsafeonline.org)

## CEOP online safety for under 18s, parents and schools :

ThinkUknow [www.thinkuknow.co.uk](http://www.thinkuknow.co.uk)

## Online safety for under 18s, parents and schools :

UK Safer Internet Centre [www.saferinternet.org.uk](http://www.saferinternet.org.uk)

Know the Net [www.knowthenet.org.uk](http://www.knowthenet.org.uk)

NSPCC [www.nspcc.org.uk/](http://www.nspcc.org.uk/)

**\*\* NetAware App \*\***

National Online Safety [www.nationalonlinesafety.com](http://www.nationalonlinesafety.com)

Take Five <https://takefive-stopfraud.org.uk/>

Action Fraud [www.actionfraud.police.uk](http://www.actionfraud.police.uk)

## Check to see if your email has been breached

Have you been pwned? [www.haveibeenpwned.com](http://www.haveibeenpwned.com)



# What can we do for each other?

- Please **#Tell2** in the real world!
- Contact me if you have any questions and share my details with any groups that would be interested in running an awareness session
- If you use Twitter or Facebook, follow us and help spread our cyber security messages
- Help us spread the key messages to family, friends, neighbours and the public at any opportunity :o)



# If you need further advice or guidance

Cyber Protect Officer - Samantha HANCOCK  
(Force HQ)

101 extn 330 7916 or 07814 226278

[samantha.hancock@leicestershire.pnn.police.uk](mailto:samantha.hancock@leicestershire.pnn.police.uk)



@EMCyberSecure

Follow us!



Leicestershire Police  
Cyber Aware