TACTICS USED BY SCAMMERS

SMISHING	An attempt to gain personal information through the use of text message
MALWARE	Software which is specifically designed to disrupt or damage a computer system
CYBER CRIME	A type of crime that is committed using information technologies such as a computer and a network
SOCIAL ENGINEERING	A method of manipulating people to reveal personal information about themselves
VISHING	An attempt to gain personal information over the phone
PHISHING	An attempt to gain personal information through the use of email communications

IF YOU ARE TARGETED IN ANY OF THE WAYS OUTLINED IN THIS HANDOUT, PLEASE REPORT IT TO ACTION FRAUD ON

0300 123 2040

FOR CONSUMER ADVICE OR TO LOG A COMPLAINT PLEASE CONTACT

CITIZENS ADVICE CONSUMER HELPLINE ON

03454 04 05 06

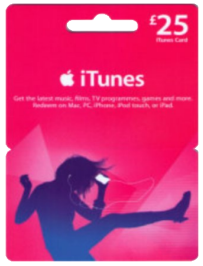
IF YOU WOULD LIKE TO BOOK A WORKSHOP FOR YOUR SERVICE USERS OR ARRANGE TRAINING FOR YOU AND YOUR TEAM, PLEASE E-MAIL

SAFER@WYJS.ORG.UK.

SCAMS EDITION

SAFER
Scams And Frauds Education for Residents

Are you buying discounted iTunes voucher codes?



Ever wondered where these voucher codes come from? Scammers contact vulnerable and elderly people **pretending to be from HMRC or the Police** and threaten them with prosecution or arrest for an outstanding balance/ fine. As our older family members may not be familiar with what iTunes vouchers are, they agree to purchase them, return home and provide the scammers with the code to clear the outstanding balance. The codes are then sold online to unsuspecting buyers who don't realise the true cost of these discounts. These so called 'Fines' can run into the £1000's!

"I know what you've been watching? I've been filming you…."

E-mails like this are very common. Scammers claim to have installed malware on your computer/ device which has filmed your activity and also claim to have gained access to your webcam to film you! These types of e-mails will even contain a password that you have previously used and claim to have monitored your activity when accessing adult sites.

Scammers use tactics like this to make you nervous so you react quickly and within e-mails like this they will even threaten to release the footage to your family and friends list. This is known as **SEXTORTION!** They will request you pay via **BITCOIN** to avoid the footage being shared.

Your password contained within that e-mail will be an old password likely to have been obtained from a data breach elsewhere and you are likely to get this email whether you have accessed adult websites…. or not!

Report the message as SPAM & **DO NOT** click the links!

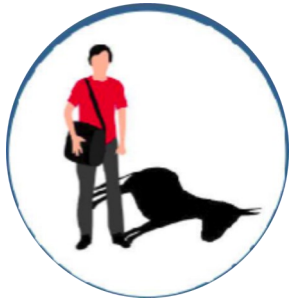
NATIONAL LOTTERY FUNDED

BIG LOTTERY FUND

West Yorkshire Trading Standards

It$@Sc4M

“Fancy making some quick cash?”



If you ever get a message like this, don’t ignore it, REPORT IT!! This is **MONEY LAUNDERING!** Criminals target people with the incentive of making hundreds and sometimes thousands of pounds by allowing use of their bank account to deposit money.

Remember there is no such thing as FREE MONEY!

Once the authorities have tracked you down, its likely the criminals will disappear leaving you to take full responsibility.

These criminals work worldwide, conceal their whereabouts and make it difficult for authorities to find them.

There’s no such thing as FREE MONEY!

How secure are your online shopping transactions?

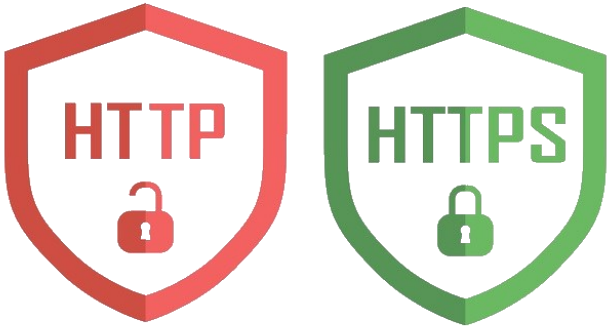
Do you regularly shop online?

How safe are the websites you use?

Always look for the padlock in the address bar and make sure the URL has **https:** at the beginning.

HTTPS stands for **H**yper**T**ext **T**ransfer **P**rotocol **S**ecure.

If the **S** for **SECURE** is missing, avoid using the website and **DO NOT** add your personal information or bank details to make a payment.



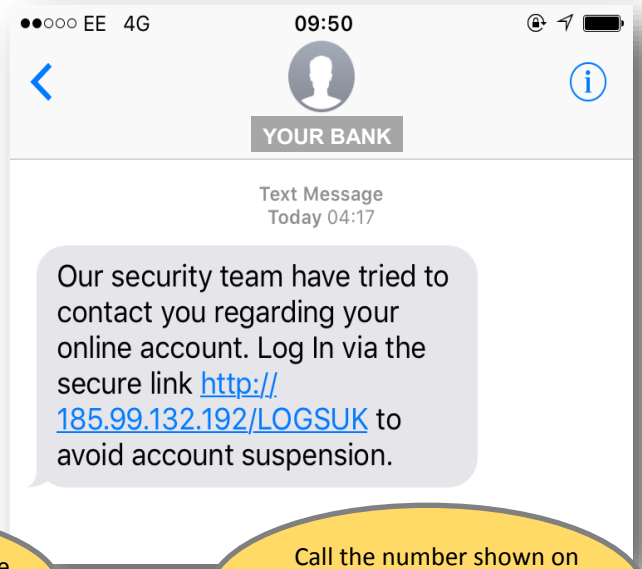
Beware of the spoof text!

Is the text message really from your bank?

Scammers have a way of ensuring their text messages fall in to the same communication channels as your bank!

STOP, THINK, BLOCK!

If you are suspicious of the text message follow these steps:



Don’t click the links or call the number in the text message

Call the number shown on your bank statement or the reverse of your bank card.

Delete bank texts from your phone when they have been read.

“Hi I’m from your internet provider, is your broadband or laptop running slowly?”

If your internet is running slowly, visit your service providers’ website to check for service issues in your areas.

If your laptop is running slowly take it to a reputable repairer who can check it for viruses/ hardware problems.

DON’T allow the caller to remotely access your device to repair the issue!

Scammers use this tactic to gain access to your device, scan it for sensitive information and even encourage you to log in to your online banking to check “It hasn’t been compromised” all the while watching you enter your details.