

STAY SAFE FROM FRAUD & SCAMS

22:34



BANK CALLING...
...OR IS IT?

PROTECT YOUR
BANK ACCOUNT
& YOUR MONEY

WARNING



ISLE OF MAN BANK

LLOYDS BANK



NatWest

BARCLAYS

HSBC

iomb
ISLE OF MAN BANKERS ASSOCIATION

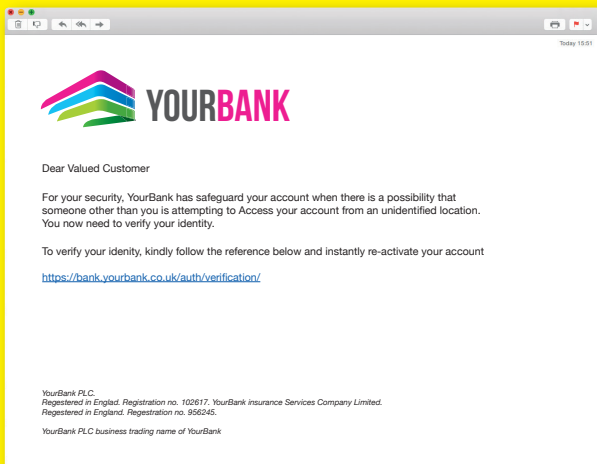
DON'T GET CAUGHT

HELPING YOU STAY SAFE

THERE ARE A NUMBER OF DIFFERENT TECHNIQUES USED BY FRAUDSTERS TO TRICK YOU INTO GIVING AWAY YOUR PRIVATE INFORMATION AND GAIN ACCESS TO YOUR BANK ACCOUNT TO SCAM YOU OUT OF YOUR MONEY.

IMPORTANT

YOUR BANK WILL **NEVER** SEND YOU A LINK ASKING YOU TO ENTER YOUR INTERNET BANKING OR CARD DETAILS



DON'T GET CAU

STAY SAFE FROM SCAMS

WHO'S CALLING YOU?

Fraudsters can use technology to show a different number on the caller ID section of your phone to trick you into believing they are calling from the bank. If you do not know the person calling you, hang up immediately and call the bank using the number from the internet or yellow pages. If you can, use a different telephone to make the call. When a fraudster contacts you by phone, this is sometimes referred to as 'Vishing'.



SCAM EMAIL

THINK! Your bank will never email you to ask you to click on a link to their Internet Banking log on page or to a page that asks for your security or personal details. Clicking on this link could lead you to a fraudulent website aiming to steal your data. Be aware of the following when looking at emails received:

- The 'From' address on an email can be faked by criminals, it can look like it is from the bank even when it is not
- Pay close attention to the 'To' address, has the email been sent directly to you?
- Scam emails will often indicate urgent action needs to be taken, be careful of emails that appear to be time critical
- Do not trust a logo on an email, logos can be copied from a banks website and used by a fraudster to trick you
- Who is the email addressed to? Would the real bank usually address you by name?
- A scam email is sometimes referred to as a 'Phishing' email
- NEVER use a link in an unexpected or suspicious email to get to any webpage. Type the website address into your browser's search bar

RIGHT: VISIT WWW.ACTIONFRAUD.CO.UK

DON'T GET CAUGHT

COMPUTER VIRUSES

Computer viruses can also be known as worms, trojans or spyware and they are all a type of 'malicious software' (also referred to as Malware). Fraudsters can gain access to your computer if you accidentally download any of these dangerous viruses. Once downloaded the fraudster can steal your personal information or access your online banking.



Malware can be downloaded by clicking on a link contained within an email, by accessing illegal websites or by clicking on advertising banners (sometimes even advertising banners on legitimate websites can contain malware).

It is important that you never click on any links unless you are confident you know what they contain. Always keep your anti-virus protection up to date. If you have any concerns about the security of your online banking, speak to your bank about how you can keep yourself safe online.

STAY SAFE FROM SCAMS

'The Little Book of Big Scams' is a comprehensive guide on fraud prevention, explaining some of the most common scams in existence, ranging from the simple to the sophisticated, providing essential advice to reduce the chances of you being parted from your money.

The guide has been produced by the Specialist and Economic Crime Directorate of the Metropolitan Police Service in the UK. Isle of Man residents are equally at risk of the scams contained in this document as persons residing in the UK, so it is important you familiarise yourself with them.

The document can be downloaded at http://www.met.police.uk/docs/little_book_scam.pdf, or by typing Little Book of Big Scams into Google.

WHAT YOUR BANK WILL NEVER ASK YOU TO DO...

- ✘ CALL OR EMAIL TO ASK YOU FOR YOUR FULL PIN NUMBER OR ANY ONLINE BANKING PASSWORD
- ✘ SEND AN EMAIL WITH A LINK TO A PAGE WHICH ASKS YOU TO ENTER YOUR ONLINE BANKING LOGIN DETAILS
- ✘ ASK YOU TO EMAIL OR TEXT PERSONAL OR BANKING INFORMATION
- ✘ ASK YOU TO AUTHORISE THE TRANSFER OF FUNDS TO A NEW ACCOUNT OR HAND OVER CASH
- ✘ ASK YOU TO CARRY OUT A TEST TRANSACTION ONLINE
- ✘ SEND SOMEONE TO YOUR HOME TO COLLECT CASH, BANK CARDS OR ANYTHING ELSE
- ✘ PROVIDE BANKING SERVICES THROUGH ANY MOBILE APPS OTHER THAN THE BANK'S OFFICIAL APPS
- ✘ CALL TO ADVISE YOU TO BUY DIAMONDS OR LAND OR OTHER COMMODITIES

THINK YOU HAVE BEEN A VICTIM OF FRAUD?

ACT QUICKLY!

CONTACT YOUR BANK AS SOON AS POSSIBLE TO REPORT THE FRAUDULENT TRANSACTIONS.

You should also report the incident to the Isle of Man Constabulary or Crimestoppers. If you have access to the internet, you can report the fraud to [Actionfraud.org](https://www.actionfraud.org) who will in turn liaise with local law enforcement.

HERE TO HELP

You can report fraud anonymously to Crimestoppers, a Manx Charity dedicated to fighting crime across the Island.



Victim Support is a local charity who help people affected by all crime, domestic abuse and fatal road traffic collisions. They provide emotional support, practical help and information to Victims and Witnesses of crime, with the help of a fully trained team of volunteers. They also provide support for those giving evidence in Court. All services are free and available to anyone.



Telephone: 679950 - Mon to Fri 8.30am to 4.30pm
E-mail: iomvictimsupport@manx.net