



**HEDDLU
GOGLEDD CYMRU
NORTH WALES
POLICE**

Response Date: 23/02/2024

2024/169 - Phishing

In response to your recent request for information regarding;

The number of people who have reported being a victim of phishing scams for the years 2019, 2020, 2021, 2022 and 2023.

How many of these reports how many are related to phishing scam links pretending to be "Royal Mail"? Of these cases can I have a breakdown of the outcome and/or current stage of investigation?

We have carried a keyword search on "phish" and "email scam":

Calendar Year	HO Description	Status	Summary
2019	Cheque, Plastic Card and Online Bank Accounts (not PSP)	UU undetected	IP reporting that he has received and email scam from BT. £15,000.00 has gone from his bank account, and another bank has frozen it stopping £600 from being transferred.
2019	Cheque, Plastic Card and Online Bank Accounts (not PSP)	Police - formal action not in the public interest	Bank Account details available on request. Within our detailed IT logs we have found a fake website set up in relation to the phishing attack which has an email address
2019	Computer Hacking - Social media and email	Victim not support/withdrawn support - Named suspect identified	Report on behalf of Money Supermarket, which suffered unauthorized access off the back of a phish via LinkedIn, from a known contact. The employee compromised is responsible for managing the commercial relationships with global energy suppliers. The suspect, having gained access, has used the account to send false invoices to these suppliers.
2020	Computer Hacking (Extortion)	UU undetected	Victim reporting that he has received an email from unknown suspect demanding £2000 or they will distribute compromising photos and videos of him to his contacts. No monies have been paid. Phishing attempt.
2020	Computer Hacking (Extortion)	UU undetected	Inft reporting a scam phishing email asking for details she deleted email straight away.

2020	Send false message by public electronic communication network to cause annoyance inconvenience or anxiety recordable	Not a crime (NCRS compliant)	UNKNOWN OFFENDER HAS SENT THE IP A PHISHING EMAIL IN AN ATTEMPT TO FRAUDULENTLY OBTAIN MONEY FROM THE IP.
2021	Computer Hacking - Social media and email	Victim declines/unable to identify offender - Suspect not identified	THE VICTIM HAS REPORTED THAT HER WHATSAPP HAS CREATED A PHISHING TEXT WITH A WEB LINK TO HER FAMILY.
2021	Other Fraud (Not covered elsewhere)	UU undetected	IP REPORTS RESPONDING TO A PHISHING EMAIL AND HAS SUBSEQUENTLY LOST A LARGE SUM OF MONEY.
2021	Computer Hacking - Social media and email	UU undetected	IP has been subject to a computer mis-use offence where by his cloud based e-mail and contacts have been hacked and used for Phishing by an unknown source.
2021	Other Fraud (Not covered elsewhere)	UU undetected	IP has been subject to a phishing scam, which has resulted in him purchasing Amazon vouchers to the value of £200.00. He has released that it was a potential scam before revealing any vouchers numbers and has managed to gain a full refund.
2021	Cheque, Plastic Card and Online Bank Accounts (not PSP)	UU undetected	IP REPORTING THAT A PHISHING EMAIL HAS BEEN SENT TO HIS WIFES PAYPAL ACCOUNT STATING HE HAS JUST ORDERD AN IPAD FOR £399. NO MONIES TAKEN AS WOULD NOT ACCEPT. ADDRESS PROVIDED WAS IN NORTH WALES AND IS LINKED TO SIMILAR INCIDENTS. CREATED AS AN ATTEMPT
2021	Online shopping and Auctions	UU undetected	Victim has received a phishing email purporting to be Freemans regarding the purchase of an Ipad. The email request the victim to confirm payment. Victim has cancelled the order.
2023	non crime occurrence	Not a crime (NCRS compliant)	Have stats classed as non crime as IP appears to be reporting having received a phishing text, no actual fraud has taken place.
2023	Computer Hacking - Social media and email	UU undetected	Email phishing attack
2023	ASB PERSONAL	Not a crime (NCRS compliant)	IP reporting having received a world wide phishing scam stating if he does not respond to the email then the send would post a video of him,

THIS INFORMATION HAS BEEN PROVIDED IN RESPONSE TO A REQUEST
UNDER THE FREEDOM OF INFORMATION ACT 2000, AND IS CORRECT AS AT 22/02/2024