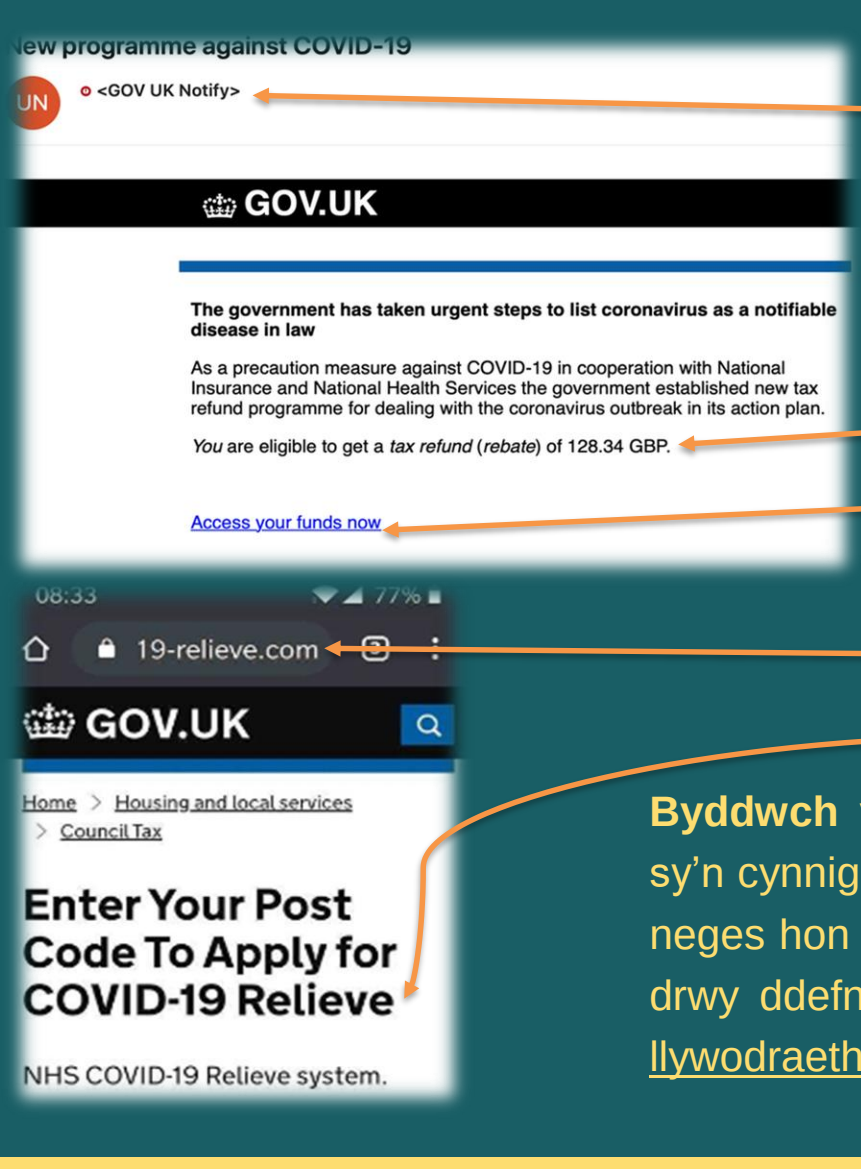
RHYBUDD I FUSNESAU AM SGAMIAU

Cyngor Sir Gâr Carmarthenshire County Council

Safonau Masnach Trading Standards

SGAMIAU O RAN AD-DALIADAU'R LLYWODRAETH

Mae'n bosibl bydd troseddwyr yn cysylltu â chi dros y ffôn, ar e-bost, neges destun neu drwy'r post yn gofyn am wybodaeth ariannol am eich busnes.



- Cyfeiriad e-bost nad yw'n gyferiaid e-bost y Llywodraeth
- Ymddangos yn swyddogol
- Heb ei bersonoli
- Addewid am arian
- Creu ymdeimlad ei fod yn fater brys
- Dim llofnod
- Nid yw'n wefan .gov
- Gramadeg gwael

Byddwch yn wyliadwrus o negeseuon annisgwyl brys sy'n cynnig cymorth ariannol. Ceisiwch feddwl o ble mae'r neges hon wedi dod. Gwiriwch fod y wybodaeth yn ddilys drwy ddefnyddio cysylltiadau a gwefannau swyddogol y llywodraeth. Cliciwch yma i gael rhagor o wybodaeth.

Sgamiau am anfonebau

Yn 2019, dywedodd UK Finance fod busnesau wedi colli

£82m

oherwydd sgamiau am anfonebau

- Rydych yn cael cais annisgwyl i newid manylion banc cyflenwr cyfredol.
- Rydych yn derbyn mwy o anfonebau na'r arfer neu sawl anfoneb am gynnyrch neu wasanaeth.
- Gallech hefyd dderbyn anfoneb ffug.

Meddyliwch. A oes gennych chi gyfrif gyda'r busnes hwn? Allai hwn fod yn dwyll?
Cysylltwch â'r busnes gan ddefnyddio rhif ffôn neu e-bost yr ydych wedi'i ddefnyddio o'r blaen i sicrhau bod hwn yn gais dilys. Cliciwch yma i gael rhagor o wybodaeth.

Y DECHRAU
Gall troseddwyr dreulio misoedd yn ymchwilio i fusnes er mwyn esgus bod yn Brif Weithredwr neu'n uwch- swyddog yn y busnes.

GWE-RWYDO
Anfonir ffug-negeseuon ar e-bost i weithwyr yn y sefydliad.

YR YMATEB
Mae'r gweithiwr awdurdodedig yn cael y neges ac yn ymateb ar unwaith oherwydd yr ymdeimlad o frys heb wirio'r ffynhonnell.

Y NIWED
Mae'r sgam wedi llwyddo a bellach mae'r troseddwr wedi derbyn taliad neu mae ganddo fynediad at wybodaeth bwysig am y busnes.

Y CANLYNIAD
Yn dilyn sgam llwyddiannus, gall y canlyniadau fod yn niweidiol iawn: colled ariannol, gweithdrefnau disgyblu, posibilrwydd o golli enw da, ymchwiliadau hirfaith

Sgamiau o ran Prif Swyddogion

Mae hon yn sgam soffistigedig sy'n chwarae ar awdurdod cyfarwyddwyr busnesau ac uwch-reolwyr. Y gost gyfartalog i Brif Weithredwyr o ganlyniad i sgam tebyg yw

£35k

Dilynwch y gweithdrefnau mewnol a **gwiriwch y cais yn bersonol** os yn bosibl, neu dros y ffôn– cofiwch ddefnyddio rhif dilys yn hytrach na'r rhif ar y cais. Cliciwch yma i gael rhagor o wybodaeth.

Sgamiau am gymorth technoleg

Wrth i ragor o bobl weithio o bell ac wrth i systemau TG fod o dan bwysau, gallai troseddwyr esgus bod yn fusnes adnabyddus a chynnig atgyweirio dyfeisiau.

- **Byddwch yn amheus** o alwyr digroeso sy'n honni eu bod yn ffonio o ganolfan fusnes neu'ch adran TG ac sy'n cynnig unrhyw fath o gymorth technegol.
- Ni fydd busnes go iawn yn cysylltu â chi heb rybudd a gofyn am wybodaeth ariannol, cyfrineiriau na manylion mewngofnodi.
- Peidiwch byth â rhoi caniatâd i rywun gael mynediad o bell i'ch cyfrifiadur na gosod meddalwedd arno yn dilyn galwad digroeso. Cliciwch yma i gael rhagor o wybodaeth.

STOPIO

Os byddwch yn derbyn cais i wneud taliad brys, newid manylion banc cyflenwr neu ddarparu gwybodaeth ariannol, arhoswch am eiliad a meddyliwch.

HERIO

Allai hwn fod yn ffug?
Yn y lle cyntaf dylech wirio'r holl fanylion o ran y taliadau a'r cyflenwr gyda'r busnes ar rif ffôn cydnabyddedig neu wyneb yn wyneb

DIOGELU

Cysylltwch â'ch banc busnes ar unwaith os ydych o'r farn eich bod wedi cael eich twyllo a rhowch wybod i Safonau Masnach ar 01267 234567

Cliciwch yma i gofrestru a chael gwybodaeth am y Tîm Sgamiau Safonau Masnach Cenedlaethol - Busnesau yn erbyn Sgamiau

STOP

If you receive a request to make an urgent payment, change supplier bank details or provide financial information, take a moment to **stop and think**.

TAKE FIVE TO STOP FRAUD™

HM Government

UK FINANCE

takefive-stopfraud.org.uk

BUSINESS SCAM WARNING

Cyngor Sir Gâr Carmarthenshire County Council

Safonau Masnach Trading Standards

GOVERNMENT REFUND SCAMS

You may be contacted by phone, email, text message or post by criminals seeking your business financial information

- Non government email address
- Designed to look official
- Not personalised
- Promise of reward
- Creating a sense of urgency
- No sign off
- Not .gov website
- Poor grammar

Be cautious of unexpected urgent communications offering financial assistance. Think about where this message has come from. Check that the information is genuine by using official government websites and contacts. Click here to find out more.

Invoice/mandate scams

In 2019, UK Finance reported that businesses had lost over

£82m

to invoice/mandate fraud.

- ❑ You receive a request out of the blue to change the bank details of an existing supplier.
- ❑ You receive more frequent than usual or duplicate invoices for a product or service.
- ❑ You could also be contacted and supplied a false invoice that is under your authority limit.

Think about it. Do you have an account with this business? Could this be fraudulent?
Contact the business using a phone number or an email that you have used before to ensure that it is a genuine request. Click here to find out more.

THE START
Criminals can spend months researching a business in order to impersonate a CEO or senior figure within the business.

THE PHISH
Spoofed emails are sent to employees in the organisation

THE RESPONSE
Employee with authority receives the communication and acts on the sense of emergency without questioning the source

THE DAMAGE
The scam has been successful and the criminal now has received a payment or has access to important business information

THE RESULT
Following a successful scam, the results can be damaging: Financial loss, Disciplinary procedures, Potential loss of reputation, Time consuming investigations

CEO scams

This is a sophisticated scam that plays on the authority of business directors and senior managers. The average loss to a CEO scam is

£35k

Follow internal procedures and **check the request** in person if possible, or by phone – make sure to use a verified number rather than the one in the request. Click here to find out more.

Tech support scams

With more people working remotely and IT systems under pressure, criminals may impersonate a well known business and offer to repair devices.

- **Be suspicious** of cold callers claiming to be from a major business or your businesses IT department offering any form of technical support
- A genuine business would never contact you out of the blue and ask for financial information, passwords or login details
- Never install any software, or grant remote access to your computer as the result of a cold call. Click here to find out more.

STOP

If you receive a request to make an urgent payment, change supplier bank details or provide financial information, take a moment to stop and think

CHALLENGE

Could it be fake?
Verify all payments and supplier details directly with the business on a known phone number or in person first

PROTECT

Contact your business bank immediately if you think you've been scammed and report it to Trading Standards on 01267 234567

Click here to sign up & learn more from the National Trading Standards Businesses Against Scams team

STOP

If you receive a request to make an urgent payment, change supplier bank details or provide financial information, take a moment to **stop and think**.

TAKE FIVE TO STOP FRAUD

HM Government

UK FINANCE

takefive-stopfraud.org.uk