## Common Telephone Scams

- **HMRC** – victims are told they owe money to HMRC for outstanding tax. They may even be told there is a warrant out for their arrest. This scam creates a sense of urgency & panics victims into paying up.

- **Courier scams** – Fraudsters will often pose as police officers. Victims are told there is a problem with their bank / card & their assistance is needed in an undercover investigation & they need to withdraw money from the bank / hand over their card & PIN.

- **Microsoft / BT** – victims are told there is a problem with their computer / internet & they have viruses / be cut off. Again, this scam panics victims. The fraudster then asks for remote access to the victim's computer to show the victim the 'errors'. Whilst they have remote access, they then try to access the victim's online banking & transfer the victim's money to themselves.

- **Amazon** – victims are told they've been charged for an Amazon Prime subscription & they can cancel the transaction by pressing 1. When victims do this, they're connected to criminals posing as Amazon customer services who remotely access their computer & steal personal & financial details & access the victims online banking.

## How to protect yourself

- HMRC will contact you by letter, **NEVER** a call. **NO** legitimate debt can be paid in gift vouchers – **HANG UP!**

- Don't trust your Caller ID. Fraudsters use a technique called 'spoofing', which allows them to 'hide' behind an authentic number, making a call appear genuine. They often use banks telephone numbers.

- **HANG UP** & call the organisation on a genuine number, ensuring the line is fully disconnected. If possible, use a different phone. **NEVER** call back on the number given to you on the call.

- The Police & Banks will **NEVER** call you & ask you for card / bank details, PINs, or to withdraw cash. You will never be asked to assist in an undercover investigation into the bank. They will never send someone to your home to collect cash / goods - **HANG UP!**

- Microsoft / BT would **NEVER** call you in this way. **NEVER** allow remote access to your computer or other devices. **HANG UP!**

- **NEVER** agree to download software called 'Team Viewer' off the back of a cold call.

NOTTINGHAMSHIRE POLICE
PROUD TO SERVE

**For more fraud tips & scam alerts, follow:**

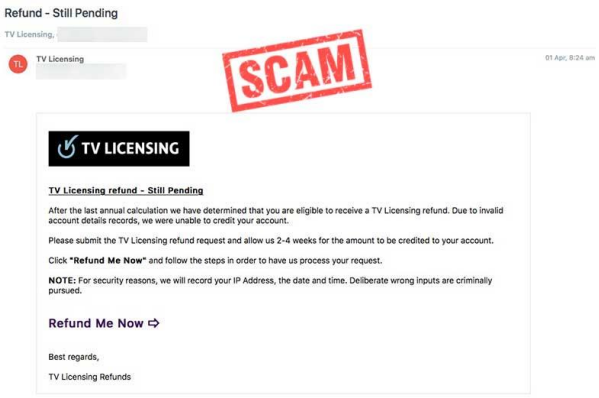
**@NottsFraudCops**

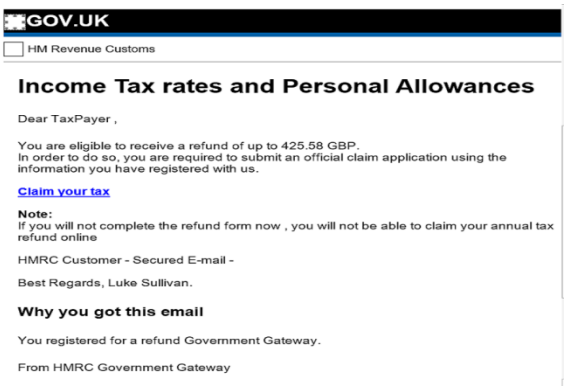
**@NottsPolice**

**Nottinghamshire Police**

## Common Phishing Emails

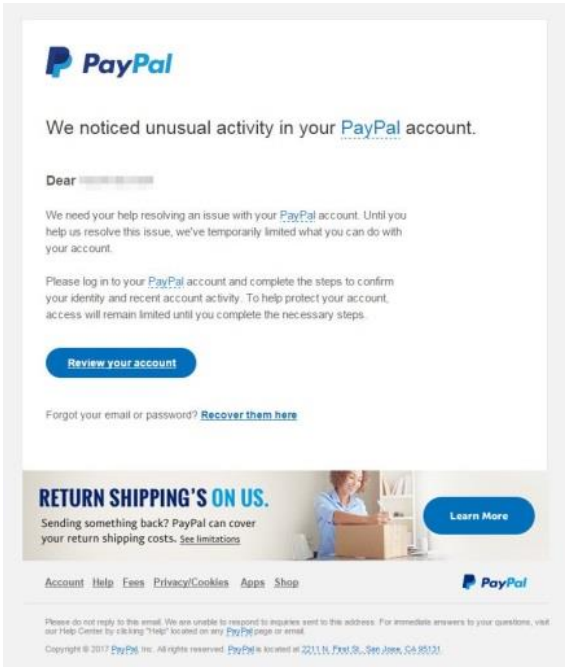
- **TV Licencing** – Emails stating your payment is due, or you're due a refund.
- **PayPal** – Emails stating there is unusual activity on your account
- **Amazon** – Emails stating there is a problem processing an order & to click the link to confirm log in details.
- **Sextortion** – Emails that claim to have accessed victim's devices following viewing pornographic websites.
- **HRMC** – Emails stating you're due a tax rebate.




## How to protect yourself

- **NEVER** click on any links or attachments. Even 'unsubscribe' links can be malicious. Verify the email via a trusted source, such as logging into your Amazon / PayPal Apps directly to check any messages.
- 
- Use your spam filter. If you detect a phishing email, mark it as spam and **DELETE**.
- The email address in the 'from' field is not guaranteed to actually be from that email address. Like telephone numbers, fraudsters can easily spoof email addresses to appear genuine.
- Watch out for spe11ing oR grAmMar ErR0Rs L1Ke tHis in the subject field. This is an attempt to get around your spam filters.




NOTTINGHAMSHIRE POLICE
PROUD TO SERVE

tell2 protect many
TAKE FIVE
TO STOP FRAUD™