TV Licensing / Email Scams

An ongoing TV Licensing phishing campaign first identified by the National Fraud Intelligence Bureau (NFIB) in September 2018 continues to be reported to Action Fraud in high numbers. Fraudsters are sending the public fake TV Licensing emails to steal their personal and financial information. Victims who click on the link are led to a convincing looking TV Licensing website – where fraudsters can obtain bank account details and commit identity fraud.

The increase in reporting was identified in September 2018, following publicity the same month around a security issue with the TV Licensing website. Reporting to the NFIB has increased month on month since then. Since April 2018, 926 crime reports have been made to Action Fraud, with a total loss of over £830,000. The highest single recorded loss is £50,000.

Reports made to Action Fraud identify that the current TV Licensing phishing emails are part of a larger scam where criminals call individuals claiming to be bank employees. This is how the scam works:

1. The victim receives a TV Licensing phishing email with links to a convincing-looking website that steals personal and financial details.
2. Within a week or two, victims will receive a phone call from a fraudster claiming to be from the fraud department of the victim's bank. The fraudsters are able to convince victims they are genuine banking staff by providing some of the personal details that were obtained using the fake TV Licensing emails and websites.

The fraudster states that the victim's account has been compromised, possibly by a phishing scam they may have fallen victim to recently, and states that they need to transfer their money to a new 'safe account'. The average age of a victim is 54 and that 65% of victims are female.

Unsolicited emails, texts and calls:

- Don't click on the links or attachments in suspicious emails and never respond to messages that ask for your personal or financial details.
- Don't assume a phone call or email is authentic:
- Just because someone knows your basic details (such as your name or address), it doesn't mean they are genuine.
- Remember, criminals can spoof the phone numbers and email addresses of companies you know and trust, such as TV Licensing.

Requests to transfer money:

- Your bank will never call and ask you for your PIN, full banking password, or ask you to transfer money out of your account.

What to do if you've fallen victim:

- Let your bank know as soon as possible and monitor your bank statements regularly for any unusual activity. If you suspect your identity may have been stolen you can check your credit file quickly and easily online. You should do this every few months anyway using a reputable service provider and following up on any unexpected or suspicious results. If you have been a victim of fraud or cyber crime, report it to Action Fraud at actionfraud.police.uk, or by calling 0300 123 2040.