

**In the know**  
**Surrey and Sussex**

**ActionFraud**  
National Fraud & Cyber Crime Reporting Centre  
0300 123 2040



Scam Warning - Fake Tv Licensing Emails

---

## SCAM WARNING

Fake TV Licensing emails

Dear subscriber,

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 that are designed to steal their personal and financial information. Since April 2018, Action Fraud has received over 900 crime reports with victim losses totalling more than £830,000.

### How you can protect yourself:

- 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, even if someone knows your basic details (such as your name or address). Remember, criminals can spoof phone numbers and email addresses to appear as companies you know and trust, such as TV Licensing.
- 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. Use a reputable service provider and follow 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](https://www.actionfraud.police.uk), or by calling 0300 123 2040.

PLAIN TEXT:

Dear subscriber,

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 that are designed to steal their personal and financial information. Since April 2018, Action Fraud has received over 900 crime reports with victim losses totalling more than £830,000.

#### **How you can protect yourself:**

- 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, even if someone knows your basic details (such as your name or address). Remember, criminals can spoof phone numbers and email addresses to appear as companies you know and trust, such as TV Licensing.
- 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:**

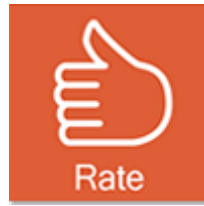
- Let your bank know as soon as possible and monitor your bank statements regularly for any unusual activity.
- If you suspect your identity may have been stolen you can check your credit file quickly and easily online. Use a reputable service provider and follow up on any unexpected or suspicious results.
- If you have been a victim of fraud or cyber crime, report it to Action Fraud at [actionfraud.police.uk](https://www.actionfraud.police.uk), or by calling 0300 123 2040.

#### ***Message Sent By***

Action Fraud (Action Fraud, Administrator, National)

---

To reply or forward this email please use the buttons below or these links: [Reply](#), [Rate](#), [Forward / Share](#).



To login to your account, [click here](#), To report a fault, [click here](#)



You are receiving this message because you are registered On In The Know - Surrey and Sussex. Various organisations are licenced To send messages via this system, we call these organisations "Information Providers".

Please note that this message was sent by Action Fraud (NFIB) and that Action Fraud (NFIB) does not necessarily represent the views of In The Know - Surrey and Sussex or other Information Providers who may send you messages via this system.

You can instantly review the messages you receive and configure which Information Providers can see your information by clicking [here](#), or you can [unsubscribe](#) completely, (you can also review our terms and conditions and Privacy Policy from these links).

This e-mail communication makes use of a "Clear Image" (gif) to track results of the e-mail campaign. If you wish to turn off this tracking for future e-mails, you can do so by not downloading the images in the e-mail itself.