

Credit Card Scams

Scammers may try to make contact with you by phone, by email or by text message to initiate one or more of the following credit card scams:

A limited time interest rate reduction in return for the immediate sharing of your CC details; genuine CC issuers do not make such unsolicited calls.

Charity scams often follow closely on the news of some natural or man-made disaster and can use the names of genuine charities to seek CC donations. If you wish to help those in need, do so *via* the official charity web site.

Charges for accessing public wi-fi is often simply a means of the scammers collecting details of your CC for subsequent use by them.

Reward scams offer you discounts or upgrades on desirable goods but take you to a false web site designed just to collect your CC details.

Overpayment/overcharge scams try to persuade you that you have been overcharged for something and the refund requires your CC details.

Skimming uses special devices installed in CC payment terminals just to collect information from your CC. If a terminal looks to have been tampered with, do not use and report to the owner.

Phishing is the most widely seen CC scam and is the subject of a separate paper.

For more Police advice on Credit Card Scams, tap here.

What Is Credit Card Fraud?



Identity theft that occurs when someone steals your credit card information to make fraudulent purchases or transfer funds.

Information in this note is based on that used by Surrey Police Cyber Crime Unit; it is provided in good faith but neither the author, the Innovation and Technology Committee or Phyllis Court Club can accept any responsibility for its use. © Jeff Maynard. 2023.