Kent Fraud Alert System

BOOTS CUSTOMER SURVEY PHISHING EMAIL WARNING

This week I have been contacted by several people about fake Boots emails. Criminals are sending phishing emails impersonating Boots, claiming recipients have been selected to take part in a customer satisfaction survey and are eligible to receive a free gift as a reward. Similar campaigns have recently been identified targeting UK consumers and have been used to harvest personal and financial information.



What does the email say?

The email may contain wording similar to:

- "You have been invited to participate in our Boots Customer Satisfaction Survey!"
- "A Special Thank-You Gift"
- "Eligible participants may receive a special gift for completing the survey."
- "START THE SURVEY"

Recipients are encouraged to click a link to complete a survey and claim a reward. Victims may then be asked to provide personal information and payment card details for a small delivery charge. However, it is a scam and they are looking to steal your personal and financial data.

How to protect yourself

- Be wary of unexpected emails offering free gifts, rewards or gift cards.
- Check the sender's email address carefully. Remember, the real sender is the part after the **@** symbol.
- Never click on links or provide personal, banking or payment card information unless you are certain the email is genuine.
- If in doubt, contact the organisation directly using a trusted website or telephone number.
- Forward suspicious emails to **report@phishing.gov.uk**.

If you have been a victim of any type of scam, then contact your Bank immediately, which you can do by calling 159 and reporting to Report Fraud at Reporting cyber crime and fraud or phishing attempts or call 0300 123 2040.

Find out more by visiting our website at Advice about fraud | Kent Police and from the Home Office at Stop! Think Fraud - How to stay safe from scams

Kent Fraud Alert System

TAKE FIVE TO STOP FRAUD™

Cyber Security Awareness Month

Do you know how to protect your email and social media accounts?

This Cyber Security Awareness Month, join the Report Fraud webinar and learn how to:

- Secure your online accounts
- Recognise the warning signs of account compromise
- Protect your personal information online

The event takes place on Thursday 29 October, between 10:00am - 11:00am and is free.

Register your place now: Cyber Security Awareness Month: Protecting your Email and Social Media Accounts

If you have been a victim of any type of scam, then contact your Bank immediately, which you can do by calling 159 and reporting to Report Fraud at Reporting cyber crime and fraud or phishing attempts or call 0300 123 2040.

Find out more by visiting our website at Advice about fraud | Kent Police and from the Home Office at Stop! Think Fraud - How to stay safe from scams





Kent Police

Report a non-urgent crime online **www.kent.police.uk/report**
Talk to us on LiveChat – available 24/7 **www.kent.police.uk/contact**
In an emergency, if crime is in progress or life is in danger call **999**
If you have a hearing or speech impairment, use our textphone service **18000**.
Or text us on 999 if you've pre-registered with the emergency SMS service.
www.kent.police.uk

Kent Fraud Alert System

FRAUD FORECAST: CHRISTMAS DELIVERY SCAMS

As Christmas approaches, millions of people across the UK will be ordering gifts online. Criminals know that households expect to receive parcels during this period and will exploit this by sending convincing text messages and emails claiming to be from delivery companies.



Typically, these messages claim that a parcel could not be delivered, that a delivery fee is outstanding, or that delivery details need updating. Victims are directed to a fake website designed to steal personal and financial information.

What The Message Might Say?

Fraudsters commonly impersonate well-known delivery companies and may send messages such as:

- *"Your parcel could not be delivered. Please pay £1.45 to arrange redelivery."*
- *"Your package is waiting for dispatch. Confirm your details using the link below."*
- *"Your delivery has been suspended due to an address issue."*



The small payment requested can make the scam appear genuine, but the real objective is often to obtain bank card details or personal information.

How To Protect Yourself

- Track parcels using the retailer's official website or app.
- Contact the delivery company directly if you are unsure.
- Be suspicious of unexpected requests for payment.
- Check for spelling mistakes or unusual web addresses.
- Never click links in unexpected texts or emails.
- Never provide banking details through a link received in a message.

Remember

If you are expecting a parcel, always go directly to the delivery company's website rather than using links received in messages.

Fraudsters know Christmas is coming. Stay cautious and keep your money safe.

If you have been a victim of any type of scam, then contact your Bank immediately, which you can do by calling 159 and reporting to Report Fraud at Reporting cyber crime and fraud or phishing attempts or call 0300 123 2040. Find out more by visiting our website at Advice about fraud | Kent Police and from the Home Office at Stop! Think Fraud - How to stay safe from scams

Kent Fraud Alert System

BUDGET, BENEFIT AND GOVERNMENT SUPPORT SCAMS

Whenever there is significant national discussion about government spending, taxation, benefits or financial support, fraudsters quickly adapt their scams to exploit public uncertainty.

Many people may be unsure whether they are entitled to new payments, grants, rebates or support schemes. Criminals exploit this confusion by sending convincing messages claiming that money is waiting to be claimed.



What Could We See?

Fraudsters may send messages claiming that recipients are eligible for:

- Cost of living support.
- Energy grants.
- Council Tax rebates.
- HMRC tax refunds.
- Government assistance payments.
- Household support schemes.



These messages often contain links to fake websites designed to harvest personal and financial information. The following is examples of some of the wording used -

- *"Following the latest Budget announcement, you are eligible for financial assistance."*
- *"You have been selected for a government rebate payment."*
- *"Your support payment is waiting to be released."*

The language may appear official and may include government logos or branding.

Protect Yourself

- Check information directly through GOV.UK.
- Contact the organisation using official contact details.
- Discuss suspicious messages with trusted family members.
- Report suspicious emails to report@phishing.gov.uk.
- Never provide banking details via a link in a message.
- Never assume a message is genuine because it contains official logos.

Remember - Government departments do not randomly contact people asking for personal or banking information through text messages or emails asking you click on links.

Kent Police

Report a non-urgent crime online **www.kent.police.uk/report**
Talk to us on LiveChat – available 24/7 **www.kent.police.uk/contact**
In an emergency, if crime is in progress or life is in danger call **999**
If you have a hearing or speech impairment, use our textphone service **18000**.
Or text us on 999 if you've pre-registered with the emergency SMS service.
www.kent.police.uk

Kent Fraud Alert System

QR Code Scams (Quishing)

QR codes are now commonly used for parking payments, restaurant menus, charity donations and accessing information. Unfortunately, fraudsters are increasingly exploiting this technology to steal personal and financial information.

Known as **"quishing"**, these scams involve fake QR codes that direct victims to fraudulent websites designed to capture payment card details, banking credentials or other personal information.

How the Scam Works -

Criminals may place fake QR code stickers over genuine codes on parking machines, EV charging points, posters or public notices. Once scanned, the QR code takes the victim to a convincing website where they are asked to make a payment or provide sensitive information.

Be Alert For -

- QR codes that appear to have been stuck over another code.
- Requests for payment details when you were not expecting to make a payment.
- Website addresses that look unusual or contain spelling mistakes.
- Messages creating urgency or demanding immediate action.



How to Protect Yourself -

- Inspect QR codes for signs of tampering.
- Check the website address before entering any information.
- Use official apps where available rather than scanning public QR codes.
- If in doubt, visit the organisation's website directly.
- Never enter banking or payment details unless you are certain the website is genuine.
- Don't assume a QR code is safe simply because it is displayed in a public place.

Remember -

Scanning a QR code is no different from clicking on a link. Taking a few extra seconds to check where it leads could prevent you from becoming a victim of fraud.

Find out more by visiting our website at Advice about fraud | Kent Police and from the Home Office at Stop! Think Fraud - How to stay safe from scams

Kent Police

Report a non-urgent crime online **www.kent.police.uk/report**
Talk to us on LiveChat – available 24/7 **www.kent.police.uk/contact**
In an emergency, if crime is in progress or life is in danger call **999**
If you have a hearing or speech impairment, use our textphone service **18000**.
Or text us on 999 if you've pre-registered with the emergency SMS service.
www.kent.police.uk