



Suffolk Against Fraud

A Police & Trading Standards Partnership



Hosepipe Ban Smishing

Residents are being warned to be vigilant following reports of scam text messages, emails and phone calls claiming to be from water suppliers.

Fraudsters are sending convincing messages that appear genuine, often using official logos and professional wording. The messages may claim:

- There is now a hosepipe ban. Click here to see if your area is affected."
- "You are eligible for a free water-saving kit. Click here to request it."
- "Your water bill is changing due to restrictions. Please update your payment details."



The links contained within these messages direct victims to cloned websites designed to look like legitimate water company websites. These sites are used to steal personal information, login credentials and financial details.

Advice is to use your app to contact your water supplier and check there for any messages regarding changes and forward any texts to 7726.

Fake RingGo Parking Payment Text Messages

Drivers are being warned about fraudulent text messages circulating that claim to be from **RingGo**.

The messages typically state that you have an **"outstanding parking payment"** or an **"unpaid parking session"** and urge you to click a link to make a payment or update your details. These texts are **not genuine** and are designed to steal your login credentials, personal information and financial details.

Signs the Message May Be a Scam:

Check the sender

RingGo will never send text messages from a generic or personal email address, such as Gmail, Yahoo or other unofficial accounts.

Inspect the link carefully

Fraudulent messages often contain links that look legitimate at first glance. Always check the web address carefully. Fake links will not direct you to RingGo's official website.

Be wary of unusual requests

Scam messages may ask you to reply with a letter such as "Y" or instruct you to copy and paste a link into your web browser to activate it. RingGo will never ask you to do this.



Report crime online – suffolk.police.uk/report

To get in touch directly with the SAF team - saf@suffolk.gov.uk

To report fraud or suspected scams to Report Fraud - www.reportfraud.police.uk

To report fraud or suspected scams to Citizens Advice -

www.citizensadvice.org.uk/consumer/scams/reporting-a-scam/

In an emergency, always call **999**



Suffolk Against Fraud

A Police & Trading Standards Partnership



Be wary of unusual requests

Scam messages may ask you to reply with a letter such as "Y" or instruct you to copy and paste a link into your web browser to activate it. RingGo will never ask you to do this.



How to Stay Safe

- Do not click on links contained within unexpected text messages.
- Never provide personal, banking or payment information through a link sent via text.
- If you are unsure whether a parking payment is outstanding, check directly through official channels:
 - Open your RingGo app.
 - Visit the official My RingGo website by typing the address into your browser yourself.
 - Log in to your account.
 - Check your **Receipts** or **Parking History**.

If your parking session is recorded there as paid, your account remains secure.

If you believe you have been a victim to fraud, contact your bank immediately and report the incident to Report Fraud at www.reportfraud.police.uk or by calling **0300 123 2040**.



Suffolk
Against
Fraud



Report crime online – suffolk.police.uk/report

To get in touch directly with the SAF team - saf@suffolk.gov.uk

To report fraud or suspected scams to Report Fraud - www.reportfraud.police.uk

To report fraud or suspected scams to Citizens Advice -

www.citizensadvice.org.uk/consumer/scams/reporting-a-scam/

In an emergency, always call **999**