# Important Announcement: Beacon CRM Data Breach

On Monday 3 August, Include.org was informed about a **cyber-security incident** affecting Beacon, the charity database that we use to hold data, in which unauthorised **access may have been gained to information** held on this database. Unfortunately, this poses a risk to everyone at Include.org.

At this stage, there is **no evidence that any Include.org data has been published** or misused, but Beacon believes copies of some encrypted customer databases were likely downloaded. As we cannot identify what, if any, information has specifically been used, we wanted to get the message out to our general community.

We understand that this will be worrying for those involved, and we are very sorry that this has happened. Protecting your data is very important to us. **We are working hard to establish the facts as quickly as possible** and we will be in touch with everyone affected as soon as we know more.

If you are concerned or have any questions in the meantime, please get in touch with us via info@include.org.

## Frequently Asked Questions

### What information does Include.org hold?

**We don't hold bank or card details in Beacon**. Beacon has stated that there is no evidence that any bank or card details have been compromised.

The records we hold in Beacon are:

- Name
- Address
- Contact details (only used with consent)
- Record of donations or payments made to Include.org
- Any communications sent to you
- Information you have provided to us in connection with our services

## What actions is Include.org taking?

While we do not know what, if any of our supporter data, has been accessed, we have reported the incident to the ICO and Charity Commission. **We have immediately taken all precautionary measures as soon as we were made aware of the incident.** We will continue to monitor the situation closely, and will share any further information with you which becomes available.

## What actions is Beacon taking?

**Beacon has engaged external cyber security specialists;** their investigations are ongoing and they are continuing to update customers. They have reported the incident to the Information Commissioner's Office and contacted the authorities via Report Fraud.

You can get a more comprehensive update on their website Incident Guidance

## What should I do?

Please be alert to any communications which appear suspicious.

There is a risk that someone could make a very plausible approach to you by email or phone, appearing to be from us or from another charity.

- **Be cautious** with any unexpected emails, phone calls, messages or postal correspondence which mentions Include.org or your support. It's a good idea to remain cautious in general, not just for this specific example. Please see Action Fraud's resources for protecting yourself here.

- **Do not click links**, open attachments or share any personal information if you are unsure.

- **Check with us directly** if anything feels unusual or suspicious, or you just want to be sure. If you have any concerns at all about whether a communication is genuine, please call our main number - 07918 470190 or email info@include.org.

## What happens next?

We would like to sincerely apologise for any worry or concern this incident has caused. We are committed to keeping you informed, and if we identify any further information that may affect you, we will provide an update as soon as possible.