u3a Beacon

BEACON *NEWS*

Edition: 46

September 2025

In this edition:

- Purpose of newsletter
- Message from National Support Lead
- Further Information
  - ⇒ Beacon User Statistics
  - ⇒ Beacon Hints and Tips
  - ⇒ Cyber Crime -Top Tips
- Beacon Team

The purpose of this bi-monthly newsletter is to provide useful information to our Beacon Users.

Message from Beacon National Support and Development Lead

Hi all, I am pleased to announce that we now have more than 650 u3as on Beacon. All of them supported by our extensive help and support team. We have recently had an issue with Beacon, in that u3as using the online joining feature of Beacon and claiming Gift Aid found that the processing of Gift Aid was incorrect.

It seems this problem was introduced with the implementation of BT1890 - Remove "Continue with Payment" screen on 7th January 2025. The change resulted in Gift Aid being processed regardless of whether or not the member elected to **gift aid**.

All u3as affected have been notified and the Beacon Team are working with those affected to rectify the situation.

Continued on next page

Message from Beacon National Support and Development Lead (continued)

We now have our new four person Software Testing team in place. This will reduce the chance of this happening again.

Pam Young is now in post as Beacon Training coordinator and has sent out a request to administrators and others for Beacon users with a role in their u3a to sign up for a course. These replies should be sent to Pam via the following email address: admin@beacon.u3a.org.uk.

Please continue to enjoy using Beacon and we will continue to enjoy improving the user experience.

Frank Bailey

FURTHER INFORMATION

Beacon User Statistics

As of the 4th September 2025, the number of live sites and their members, are shown below.

u3as / Networks / Regions	Number
u3as using Beacon	652
Members in these u3as	311,787
Networks / Regions using Beacon	16
u3as (10) / Networks / Regions (6) preparing to migrate to Beacon	16
u3as using Demo24/25 (Demonstration site) to investigate joining Beacon	43

John Alexander

Training and Documentation Lead

John Hopkins

Support and Migration Lead

Beacon Hints and Tips

Getting Help on Beacon

We still get users sending questions on Beacon to the Trust. Many are covered in the Beacon User Guide, so this is the easiest way to obtain an answer as it is always available. We take care to update this before changes to the software so you can always read the appropriate advice.

If you have any other questions, we suggest that the quickest and best way is to send them to: info@beacon.u3a.org.uk.

This saves work for people at the Trust who pass them on to us anyway.

If it is a particularly complex problem, there is always the Help Desk accessed via the User Guide.

Sending E-mails

Please, please use the tokens when sending emails.

Two reasons:

1. Your members will feel more wanted and involved to get something addressed to Dear John or June rather than Dear Member.

2. Going via Beacon are approaching 800,000 emails sent each month. This can trigger some systems to see them as spam and dropped. Sending with Tokens, such as #FAM makes each email individual so lessens the chance of it being seen as spam.

You might want to note that Beacon does not receive emails so is very unlikely to have initiated a Phishing attack. It is worth checking with the person who is purported to have sent the email. Also, you might want to note this advice. To report a phishing email in the UK, forward it to report@phishing.gov.uk a UK Government body.

Continued on next page

Renewal both by Membership Secretary and using the Online process

I come across Membership Secretaries and Treasurers who, when someone renews membership for two people, can't easily find to whom it applies.

If you look in the PayPal ledger you will see two Membership numbers against a payment. These identify to whom this payment applies, it is the same as when a membership secretary renews two members who made a single payment. These go into the Membership or Current account depending on how it is paid and the settings in your site.

Beacon Accounts

Occasionally I see sites with Accounts names that are either the same or very similar. May I suggest that this is unwise as it increases the chance of entering a transaction into the wrong account.

I also hear the response, "I cannot delete the extra Finance account or Finance Category". If there are transactions in it, you cannot for sensible reasons.

Good News, in both cases you can still make them Inactive.

Membership Fees

I also find sites where a number of Membership Classes are set to cater for people joining at different times of the membership year.

I suggest that you do not do this as at the next renewal, each of these members will need their record individually editing to stop them renewing at the reduce part-year fee but paying this for the full year.

Please look here in the User Guide: 8.7 Membership Set-up

If you scroll down the article, it covers how to do this under Assigning Varying Membership Fees.

Continued on next page

Beacon Hints and Tips (continued)

If you use this, then at renewal time, the member is automatically expected to pay the full fee for year 2 and no work is required from your Membership Secretary. Please this is one of the hardest roles so anything that can be done to help reduce the workload, especially at the busy renewal period, will be much welcomed by them.

An email that appears to come from a previous Group Leader

There is a detailed explanation in the User Guide of why this happens and how to stop it.

Here is a link: 6.1.5 Email tips, duplicates and sender issues

If you scroll down the article to the section **Beacon Emails appear to be sent by the wrong person** you will find how to stop this.

I am planning on including these and previous Hints and Tips in a section in the User Guide.

John Alexander

Training and Documentation Lead

Cyber Crime -Top Tips

The following details are copied from a leaflet distributed by an area's Cyber Protect Officer which provides some very helpful information about Cyber Crime, thought this would be useful to share with other u3a members.

1. **PASSWORDS / 2FA / 2SV**. Use Strong Passwords. Consider using - **ThreeR@ndOmWord$**. Your password MUST contain at least 12 characters. Don't use the same password for all your accounts. The strongest should be for your primary email account and this password should not be used for anything else. Where possible activate 2 Factor Authentication (2FA) / Two-Step verification (2SV). This generally involves sending a text to your mobile phone to double-check that it is you carrying out a particular transaction. If you have difficulties remembering lots of passwords, consider using an on-line 'password manager'. There are various free and paid for password managers available.

2. **UPDATES and APPS**. Always take operating systems and software updates as soon as possible. Turn on your Anti-Virus / Firewall and keep them updated. Don't use old operating systems that are no longer supported. These are particularly vulnerable to attacks. Only download Apps from accredited Apps stores.

3. **BACK-UPS.** Regularly back-up your important data onto a removable hard drive (or USB stick or SD Card, if more practical). Consider keeping your back-ups off-site, in a fireproof /waterproof safe.

4. **PHISHING / SOCIAL ENGINEERING.** Never assume incoming emails are genuine. Even if you recognise the email address because email accounts can be *'hacked'*. Never believe voice calls and text messages are genuine, even if you recognise the phone number. Phone numbers can be 'Spoofed' (falsified). ALWAYS CONFIRM using the contact information you have obtained from your own records or from publicly available sources.

Continued on next page

Cyber Crime -Top Tips (continued)

Remember – Criminals will PHISH to obtain information from you. **DON'T GIVE OUT ANY SENSITIVE INFORMATION TO INCOMING CALLERS.** Send all email PHISHING attempts to report@phishing.gov.uk and send fake text messages onto 7726 (Spam). Call 159 to quickly be directed to your banks Fraud Team.

5. **PRIVACY SETTINGS**. Regularly check the privacy settings on your Social Media accounts and be careful what you post on social media. Do you really want everyone to know your house is empty when you are away on holiday?

6. **WI-FI**. Be cautious when using public Wi-Fi and don't pass sensitive information, passwords, or bank account details over public Wi-Fi.

7. **SECURING YOUR DEVICES.** Ensure all your devices including your mobile phone(s) are password or PIN protected - Keep them 'locked' when not in use. Use Fingerprint or facial recognition if available. Only grant remote access to your device (computer / mobile phone / tablet), to someone you personally know and thoroughly trust. Never grant remote access to any incoming telephone callers. Try and avoid using publicly available USB re-charging points. These can be interfered with to compromise the security of your device (Juice Jacking). It is generally safer to charge devices from a standard electricity point or your own portable powerpack.

8. **CREDIT CARDS**. For added protection, please use a credit card for all your on-line transactions.

9. **QR CODES.** Carefully check QR codes before scanning them. Do they look genuine? Have they been tampered with? Can you do the transaction without using the QR code? Avoid Scanning from unknown / untrusted sources.

Continued on next page

Cyber Crime -Top Tips (continued)

10. **INCOMING MESSAGES.** Be wary of ALL incoming messages, including voice calls, SMS text messages, emails and social media messages, even from people you may know or email addresses you recognise. Remember accounts can be hacked and emails, social media addresses and phone numbers can be 'Spoofed' (falsified). Both voice calls and videos from individuals know personally can be 'DEEP FAKED'. Don't rely on caller ID display. If you are concerned about an incoming call, hang up, call the caller back using another phone and the phone number YOU have obtained yourself from your own trusted sources. Never Assume, Never Believe, ALWAYS CONFIRM. Be particularly cautious of any requests you may get to change the details of a regular outgoing payment or to create a new payment.

11. **Never share your passwords.** Organisations including financial institutions, HMRC, the DVLA, the NHS, other Government bodies, and the Police will never ask for YOUR PIN, YOUR Passwords, YOUR personal / financial details. NEVER-EVER share those details. Any requests you get, claiming to come from such organisations, WILL BE A SCAM!

12. **Don't Rush.** Question Everything / Seek Advice / Never Assume, Never Believe, ALWAYS CONFIRM. Go to Have I Been Pwned: Check if your email has been compromised in a data breach to see if your email has been involved in a data-breach.

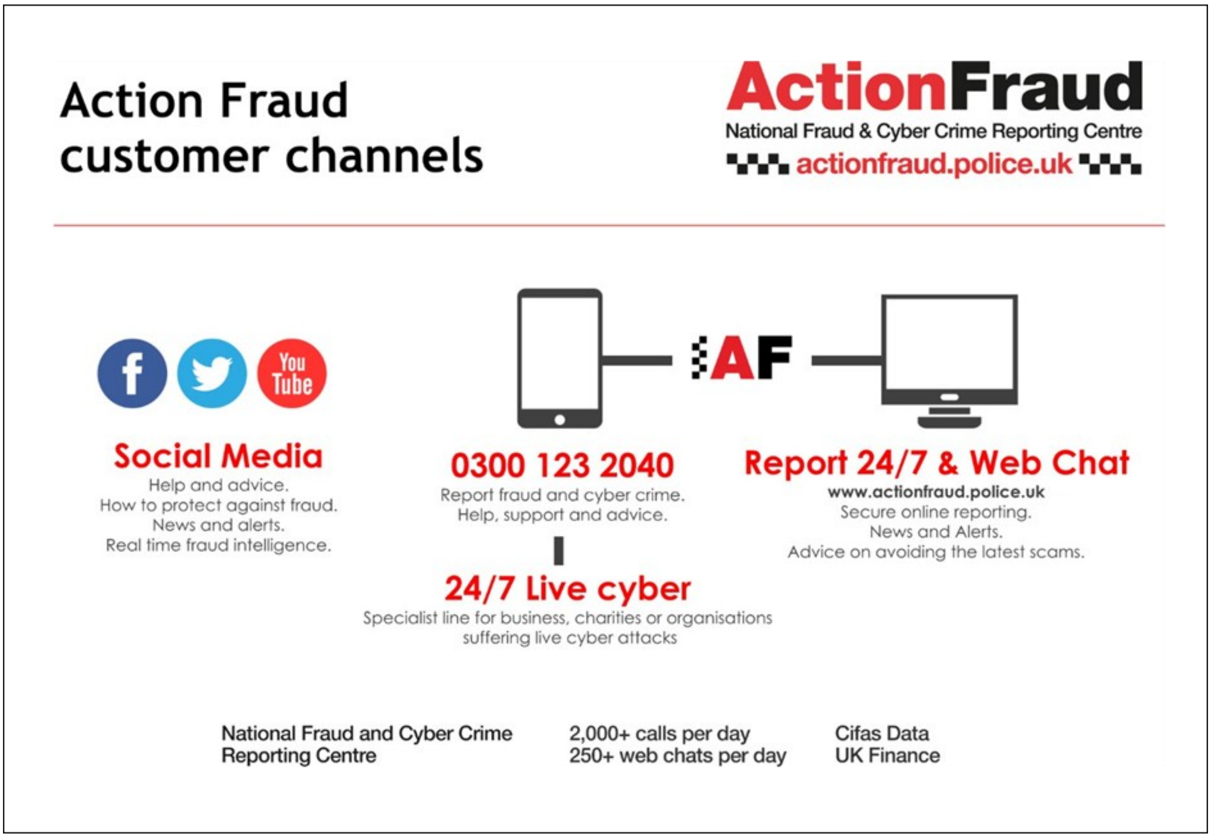
Please see the next page on how to:

- Report Cyber Crime
- Contact the Fraud Department of your bank

Continued on next page

Cyber Crime –Top Tips (continued)

Reporting Cyber Crime



Action Fraud customer channels

ActionFraud
National Fraud & Cyber Crime Reporting Centre
actionfraud.police.uk

Social Media
Help and advice.
How to protect against fraud.
News and alerts.
Real time fraud intelligence.

0300 123 2040
Report fraud and cyber crime.
Help, support and advice.

24/7 Live cyber
Specialist line for business, charities or organisations suffering live cyber attacks

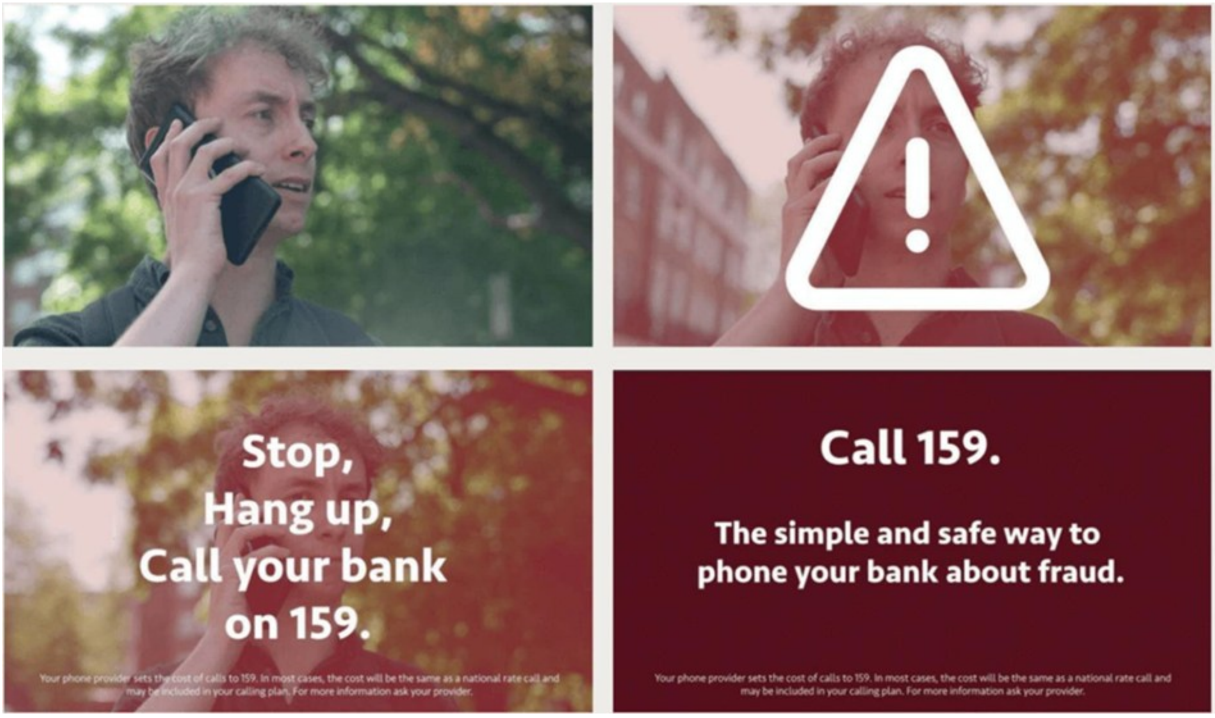
Report 24/7 & Web Chat
www.actionfraud.police.uk
Secure online reporting.
News and Alerts.
Advice on avoiding the latest scams.

National Fraud and Cyber Crime Reporting Centre

2,000+ calls per day
250+ web chats per day

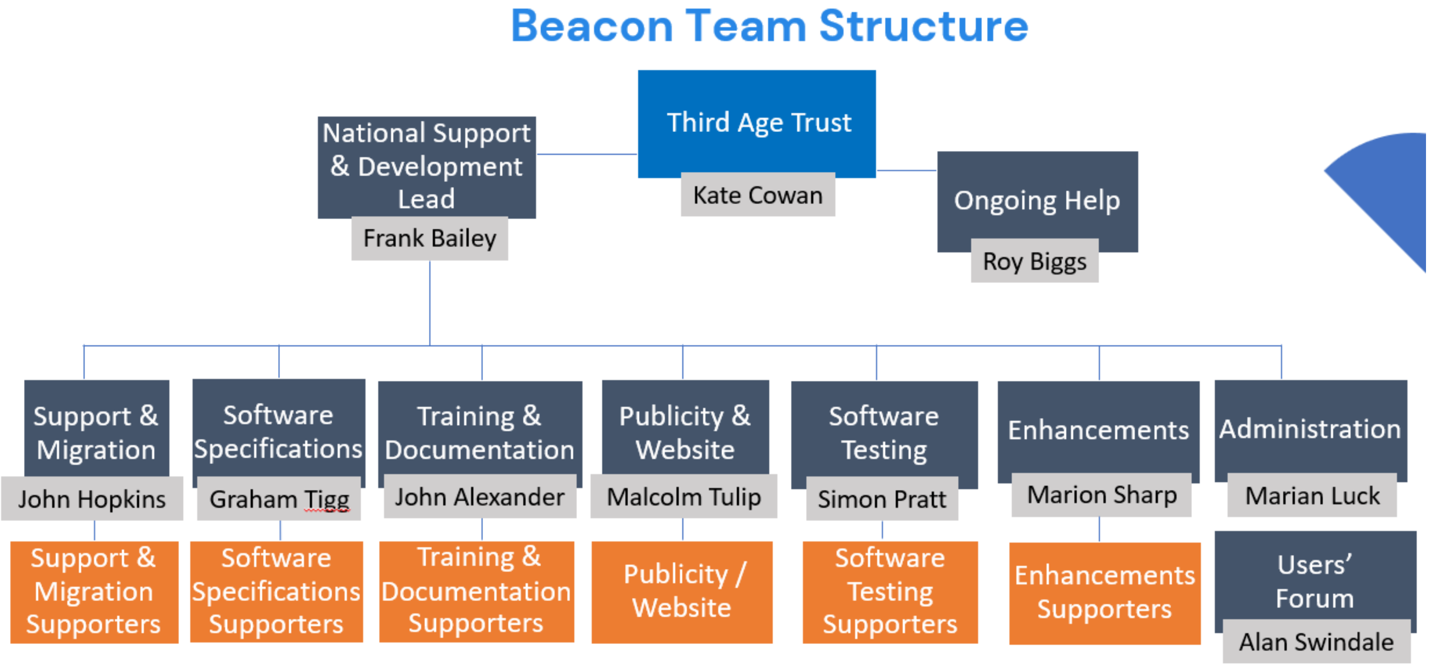
Cifas Data
UK Finance

Contact the Fraud Department of your bank – Dial 159


Stop,
Hang up,
Call your bank
on 159.
Your phone provider sets the cost of calls to 159. In most cases, the cost will be the same as a national rate call and may be included in your calling plan. For more information ask your provider.
Call 159.
The simple and safe way to phone your bank about fraud.
Your phone provider sets the cost of calls to 159. In most cases, the cost will be the same as a national rate call and may be included in your calling plan. For more information ask your provider.

BEACON TEAM

Who we are and what we do



Individuals can have multiple roles and hence be in several Supporter roles

BEACON WEBSITE

Beacon is an on line management system designed by u3as, for u3as. It provides a simple interface for managing members, groups and finances. Beacon is available to all u3as in the UK that wish to take advantage of it. More information about Beacon can be found through the link to the website.

The members of the editorial team are as follows:

Editor: Malcolm Tulip

Email: malcolm.tulip@beacon.u3a.org.uk

Proof Reader: Graham Tigg