Bradford Care Association

STAY FRAUD FREE THIS CHRISTMAS!!

It’s the most wonderful time of the year – for fraudsters. And it’s not your mince pies they’re after. Here are our 12 tips to help you and your services stay safe this season.

And remember, the Better Security, Better Care programme can help you to check your data and cyber security arrangements by using the Data Security and Protection Toolkit.

- Brief your staff: Make sure your staff know that cyber attacks are a real risk – especially at Christmas. Help them to recognise a basic attack and how to avoid them. Share this article, and check out our information on training.
- Check your continuity plans: Ensure staff know how to manage an information **breach**Also known as a data breach. A security incident where sensitive and personal information is copied, transmitted, viewed, or stolen. See also: Cyber Security Guidance. **More** or cyber incident, especially when staff numbers may be down. You can use our template Continuity Plan for Data and Cyber Security.
- Lock up on leave: If you’re going on leave, tidy up paper records so only staff who should see them can access them. Log off your work systems and close down your devices.
- Prepare for working from home: Be ready to have some staff working from home due to self-isolation or bad weather. That should include how to manage secure communication and access to records. See National Cyber Security Centre guidance.
- Challenge tech support offers: Got a message claiming your computer is at risk and asking you to download special software or call a helpline? Tech support scams use scare tactics to trick you into unnecessary services to fix problems that don’t exist. Don’t click or call. Check your organisation’s official tech support.

- Watch out for WhatsApp: It’s a quick and easy way to contact colleagues. But make sure the message you receive makes sense. If in doubt, call the person who allegedly sent it.
- Beware of emails bearing gifts: If you’ve been sent an e-gift or e-card via a link and don’t recognise the email sender, it’s probably spam. Search online for the e-card or e-gift company name plus the word ‘scam’. If it’s allegedly from someone you know, check if they have sent you something. Check out our information on email scams.
- Dodge delivery scams: Got a text or email saying there is a package for you and asking for a payment to release it, or for details like date of birth or bank account? Don’t engage and don’t click on any links. Only interact with the delivery company via their official **app**(Application) – A software program that you can download for your computer, tablet, or mobile phone. Can also refer to a program or tool that can be used within a website although these are commonly known as a WebApp or Website, which have the adv **More**, or by finding their website yourself.
- Don’t fall for unbelievable offers: If it looks too good to be true, it probably is. Scam websites use low prices to lure bargain-hungry shoppers to quickly sell fake, counterfeit or non-existent items, and capture your personal details.
- Stay safe on social: Don’t be lured into giving away passwords or sensitive data on your social media channels. They are not private spaces and criminals may be able to guess your passwords and personal details from information that you share.
- Report cyber attacks: If you are attacked, report it to Action Fraud either via their website or by calling 0300 123 2040. Find out more about what to do.
- Get expert support: Our Better Security, Better Care programme can help you to improve your data and cyber security arrangements by using the DSPT. It’s free – and that isn’t a scam! Maybe use that Christmas to New Year period to complete your DSPT.

Thank You for all your hard work! Merry Christmas and Happy New Year!