NOTICE FRAUD

December 2018

With Christmas just around the corner, everything tends to get hectic. With so much Christmas cheer around, it's easy to forget about the darker side of Christmas. In this edition we have provided some practical advice to help protect you and stay alert during the festivities.

'Tis the season to be phishing

We have all heard or seen the emails from the Nigerian bank managers looking to share the estate of a recently deceased prince that you happen to be remotely related to. You may have received an email about a suspicious transaction on your PayPal account that requires you to press a specific link to log in and reset your password, or the numerous giveaways on Facebook.

This is known as phishing – it's a common method used by fraudsters to trick you into handing over personal or sensitive information using legitimate looking emails and websites.

Fraudsters may take advantage and send emails offering festive deals or discounts. These will be designed to entice you to click on the link, download an attachment, or enter your personal details. They may also target your work emails to gain access your organisation's data. Email addresses can be amended to make it look like they have come from someone within your organisation.

What can you do?

- Think before you click. Don't open attachments or click on links in emails you are not expecting.
- Look out for any grammatical errors or spelling mistakes.
- Log onto a website via a trusted search engine rather than clicking on links provided in an email.
- Be wary of requests that ask you to deviate from a usual process, or where there is apparent urgency.

It's worth nothing that fraudsters use text messages to obtain personal information. This is known as smishing - it works much the same way as phishing but instead of an email the fraudsters use text messages.

Don't be embarrassed to report a scam. Fraudsters are cunning and clever; there is no shame in being deceived. By reporting, you will make it more difficult for them to deceive others.

It's not the gift under the tree

We associate Christmas with exchanging gifts and hospitality between friends, colleagues and family. It can also extend to suppliers or organisations we do business with. It is therefore important to consider any gifts or hospitality, or offers of such, to ensure that it does not comprise your personal or professional integrity.

Think about the context in which the offer has been made, and the effect on your position. For example, is the gift/hospitality likely, or could it be seen as likely, to influence you? The onus is on you to make sure that the acceptance of a gift/hospitality will not be misconstrued. Below are some questions you should consider:

Genuine: is this offer made for reasons of genuine appreciation for something that I have done, without any encouragement from me?

Independent: if I accept this would a reasonable bystander be confident that I could be independent in doing my job?

Free: could I always feel free of any obligation to do something in return for the donor?

Transparent: would I be comfortable if the gift was transparent to my organisation, its service users and the public?

Remind yourself and your staff of your organisations gifts and hospitality policy.

Checking all the way…

Authorised signatories are a key defence in preventing false claims for payment. With all the fun that Christmas brings, it's easy to get distracted and not be as thorough as you would normally be. Fraudsters are likely to take advantage of this.

To reduce the risk of fraud in this area here are a few tips:

- verify that the goods / services / resources have been received. Check the details of the payee. Does this match the details of the supplier?
- ensure claims are signed by the applicant, with their name clearly printed;
- cross through errors with a single line and initial the change alongside the applicant. Cross through empty boxes on the claim/form; and
- return forms to the claimant that do not meet these criteria.

It's cold outside

We all love to do some online shopping, after all it has enabled us to have the ability to do our Christmas shopping without even leaving our home and facing the pressure of busy shops! But we must remain aware of the dangers of shopping online. Our top tips to staying safe whilst online shopping:

- only use trusted websites with secure payment facilities - never click on unsolicited emails;
- be suspicious of all 'too good to be true' offers and deals;
- do not use public WiFi networks to purchase items or transfer money; and
- regularly check your bank balance so that you can spot usual or fraudulent transactions quickly.

Wishing you a merry Christmas

Animated Christmas e-cards are amusing. We have all seen our friends and family aminated into singing elf's or dancing reindeers in our inboxes. Most can be harmless, but some could contain malware (malicious software), or a virus.

If you have received an e-card and you don't know who it came from – delete it. If you are thinking of sending a card, use a company you trust.

Reporting concerns

It is easy to report fraud, bribery or corruption affecting the NHS. Contact your Local Counter Fraud Specialist (LCFS) directly or call the national anonymous, 24-hour reporting line on 0800 028 4060 (powered by Crimestoppers). You can also report online, completely confidentially via https://cfa.nhs.uk/reportfraud.

It is the LCFS' role to take every allegation of fraud or bribery seriously and to provide anonymity and confidentiality for anyone who reports a concern. It is recommended that you refer to your organisation's policy on fraud when reporting allegations for further information on how you are protected.

When making a referral please provide as much information as possible, for example:

- the name of the person who you believe has committed a fraud;
- when and where the fraud has taken place;
- how long the fraud has been going on; and
- any details to substantiate your suspicion.

Remain vigilant during this festive period.

Spot it. Report it. Together we stop it.