5 cost of living scams to watch out for right now

Submitted by: Key Loans & Mortgages Limited t/a KIS Finance
Friday, 24 June 2022

With energy bills, fuel prices, and the cost of food all rising at a seemingly unstoppable rate, scammers have been cashing in.

They're using the cost of living crisis to their advantage as they prey on those who are most vulnerable. Being caught out by one of these scams could be hugely damaging to those who are already struggling financially.

Holly Andrews, Managing Director at KIS Finance (https://www.kisbridgingloans.co.uk/) and personal finance expert talks about five scams that consumers need to be aware of right now.

Fake energy bills

The chaos surrounding energy bills and price caps has made easy work for scammers as they try to trick people into paying for energy bills that don't exist.

According to Action Fraud, the first quarter of 2022 has seen a 10% increase (year on year) in scam reports that mention energy suppliers such as British Gas, EDF, Eon, and Scottish Power. January alone saw a 27% increase is these scams when compared to January 2021.

Scammers are posing as well-known energy providers, like British Gas and EDF, telling victims that they have an overdue energy bill that needs to be paid immediately otherwise their energy will be cut off. They're using rising prices to their advantage as they trick people into thinking they haven't paid the correct amount.

The links provided within phishing emails take the victims to a malicious website where they are prompted to enter their personal details and pay the bill.

How to avoid this scam:

If you receive an email and you are concerned that you haven't paid your energy bill correctly, then make sure you ignore any link in the email and go directly to your energy provider through your search engine. Logging in to your account or giving them a call will confirm whether you have any overdue bills.

Shopping vouchers and discounts

Shoppers are always on the hunt for discounts, but the cost of living crisis has seen some of the poorest families having to choose between heating their homes and buying food. Unfortunately, heartless scammers

have seen this as a big opportunity to target those who are most vulnerable.

These scams often come through phishing emails as scammers offer victims a chance to get discount vouchers or refunds on your shopping for well-known supermarkets. The links take you to a survey which asks for personal information and your bank details so you can receive your shopping refund or be sent supermarket discount codes and vouchers.

Recently, scammers have been crafting emails that appear to have come from supermarket giant Tesco and offering £500 gift cards. They lead you to a website which asks for your personal information and PayPal log in details.

The refund and/or vouchers will never materialise but the scammers will use your information to steal money and sometimes even sell on to other criminals who will use your details to try and con you further.

How to avoid this scam:

Phishing emails are one of the most common types of scam and thousands, if not millions, are sent out every day. You should never click on a link that you have received via email or text unless you know the sender and it's something that are you specifically expecting.

If you see a discount or voucher offer for a well-known supermarket, note it down and ask in the supermarket next time you go. They will be able to give you the details if it's a genuine offer.

Fake jobs

Scammers have been capitalising on people who are looking for extra ways to earn money. They pose as marketing companies and post adverts online which promote easy ways to earn money in your spare time. This could be jobs as simple as taking surveys, liking posts, or watching videos online.

While there are genuine companies who provide money earning opportunities for these sorts of jobs, these scam companies will ask you to pay a deposit to be assigned tasks. They will claim that you will make that money back plus hundreds of pounds more within just a matter of days or weeks.

Sometimes the scammers will ask you to download an app to work from; one of which was made to look exactly like the Pinterest app. After making several deposits and completing the assigned tasks, users have been unable to log back in to the app to withdraw earnings, meaning the deposits are also being stolen.

How to avoid this scam:

Stay away from any job offer that requires you to pay them money first. Genuine companies would never ask

someone to do this. You should also be wary of any jobs that promise huge returns for very little effort. There are genuine companies that offer payment for things like taking surveys and watching videos, but the return is small so you need to build it up for a long time. Make sure you do your research of different companies first and check genuine reviews websites to find other people's experiences.

Lottery scams

With bills mounting, fuel costs increasing, and day to day living just simply getting more expensive, many of us dream of a windfall to make all our financial worries melt away. Again, scammers are using this to their advantage.

The scammers contact you via email, message, or phone call to say that you've won a lottery or prize draw. They will tell you that you need to pay a small fee to them in order to verify your bank details before you can receive your prize. Obviously the prize never comes and the scammers steal your money and information.

How to avoid this scam:

It's impossible to win a prize draw or lottery that you haven't entered, so make sure you don't get carried away by the excitement of thinking that you have won.
You should also only ever enter lotteries and prize draws through well-known legitimate organisations like The National Lottery or The Postcode Lottery.

Investment scams

Investment scams are an ongoing, year-round danger, however they seem to have been particularly rife over the last few months.

Fake investment opportunities are posted via social media adverts or sent out to victims in emails. Cryptocurrencies are a common topic as scammers can promote high returns in a short amount of time, which cryptos make more believable than something like stocks, shares, or gold.

Victims are urged to make an investment with their company but the returns never come and the scammers will disappear with the money and never make contact again. They may also use your details to steal more money plus sell your information to other scammers.

How to avoid this scam:

Never invest money with a company that you haven't thoroughly researched and certainly not one that's promoting their services through unsolicited emails.

If you're contacted by a company and you are interested in making an investment, you can check the FCA Register to find out whether they're authorised and regulated.

You can also check the FCA's Warning List for companies that are known as being suspicious. If you invest money with a firm that isn't authorised and regulated by the FCA then you won't be protected under the Financial Services Compensation Scheme or the Financial Ombudsman Service if things go wrong.

- ENDS –

Notes to journalists/editors:

Comments provided by Managing Director at KIS Finance (https://www.kisbridgingloans.co.uk/), Holly Andrews. If you would like to use these comments then a link back to KIS Finance is required to credit the source.

KIS Finance fraud guides - https://www.kisbridgingloans.co.uk/guide-to-fraud-prevention/

About KIS Finance:

KIS Finance are an independent finance broker specialising in bridging finance, development finance, commercial mortgages, equity release, and secured loans. Their team of advisors have considerable experience across multiple different areas of the finance sector, as well as insurance and compliance. KIS Finance are also very invested as a company in fraud awareness and prevention and keeping their clients safe from financial fraud and scams.