MONTHLY GATESHEAD HEALTH STAFF ADVICE BULLETIN

ISSUE 16: HOW TO PROTECT YOURSELF FROM CURRENT SCAMS WHEN ONLINE AND ON YOUR MOBILE

Once again, scams are on the rise – there are a seemingly never-ending supply of callous and manipulative methods being used by scammers to target not just the most vulnerable people in society, but also those of us who think we will never get caught out, but inevitably are.

In this months update, we're looking at scams that come through mobile phones and other online sources – what are they, how do they work, and what can you do to avoid them

WHATSAPP SCAMS ON YOUR MOBILE

WhatsApp Account Takeover Scam

Scammers are attempting to take over WhatsApp accounts so that they can carry out other frauds by accessing victim's account contacts by sending seemingly normal messages, at the same time as trying to log into the new target account. This generates a WhatsApp six-digit code which the target receives as a message. The scammer then asks the target to send the code to them as they 'sent it by accident'. Once they have the code they can lock the user out and begin the process again!

You can read about the WhatsApp account takeover fraud on Action fraud website

WhatsApp 'Friend/Loved One in Need' Scam

Scammers are sending messages to mobiles, regularly on WhatsApp. They pretend to be a friend or relative claiming to have lost or broken their phone. The scammers will supply bank details and ask for money because of an terrible incident - relying on the goodwill of close relatives and then taking their money.

What can you do?

- Follow the Stop, Think, Call method. Take time before you respond, think whether the request makes sense, and then verify who it is by calling them directly.
- Never share your account's activation code (that's the 6 digit code you receive via SMS)
- Set up two-step verification on WhatsApp to give an extra layer of protection to your account: Tap Settings > Account >Two-step verification > Enable
- You can report spam messages or block a sender within WhatsApp

ONLINE SHOPPING SCAMS

Shopping online has become a normal part of everyday life, but with this increased popularity we have seen an increase in scams too. There are dozens of different scams out there, but these are two of the most frequent.

Online Purchase Scams

Scammers can purchase pretend or misleading adverts in an attempt to lure people in through unmissable deals, normally advertising low prices for high value items. So whether it is someone selling you an 'X-Box' and sending only the box, or a beautiful piece of clothing being advertised but turning up far from the quality item you expected, you have been scammed!

Fake Websites

Scammers have become incredibly adept at creating websites that look like the real thing and thus fool you into either paying for items that won't arrive or divulging your personal or security information, allowing them to use that data on other accounts with your name.

What You Can Do?

- Only buy from websites that have 'https' preceding the website address - this means the site is a secure connection. If you are still unsure, you can also contact the retailer directly and check you have the correct web address, but get the number from another source – not from the website you think is suspect!
- Checking customer reviews on websites such as Trustpilot will give you an idea if a retailer is trustworthy and reputable.
- There may be other warning signs to determine if a website is fake such as spelling and grammatical mistakes, in addition to a lack of contact details.
- Create strong passwords for sites when providing card details or signing up to an account. Using different passwords for each of your online accounts will prevent scammers getting into your other online accounts if there is a data breach.
- If you think you have been a victim of online shopping fraud, contact your bank immediately and see if they can stop the transaction.
- Sometimes the hidden costs aren't revealed till the checkout, make sure you're happy, don't feel pressurised, and do shop around.
- Pause before you pay. Always know the term and conditions, know what you're signing up for, and know how to unsubscribe.

Remember the golden rule - If an offer seems too good to be true it probably is!

The Governments New Online Rip-off Tip-off Campaign

The Government has a new online form as part of the Online Rip-off Tip-off campaign which allows people to report unfair online sales tactics. There is also more information about some common sales tactics that people might want to report on the campaign webpage. These tactics include: hidden charges, pressure selling, subscription traps, and fake reviews.

You can find the The Online Rip-off Tip-off form, and other information on the campaign on GOV.UK

ENERGY SCAMS

And finally, we have a selection of new energy-related scams. The UK's energy crisis has left millions of households struggling to pay their energy bills. Unfortunately, this has prompted scammers to broaden the types of scams used to make people part with their cash.

Fake Refunds

Scammers pose as energy suppliers, stating you are entitled to a refund. Often a link will be supplied which asks you to enter your bank details in order to get your money.

Fake Discount Offers/Coupons

Significant discounts on gas or electricity rates are advertised by scammers. People sign up to the service only to discover that the rates are false, and there are no actual savings. Similarly, scammers may offer discount coupons which require an upfront cost. After you have paid, the scammers walk away with the money and no discount is applied.

Deceptive Marketing Practices

Like the methods used above, people may be enticed by misleading promotions/advertising that imply saving on energy bills. After signing the associated contracts, scammers may change the terms without warning or hide important information in the fine print.

Price Comparison Phone Scams

Fraudsters are calling people pretending to be from popular price comparison websites, they give details of special offers that are available to a limited number of customers. Pressure will be put on the person to switch immediately to secure the deal.

Energy Saving Equipment

Devices marketed as 'energy saving' have been on sale through websites such as eBay and Amazon. Previously known as Motex, these devices have been rebranded under the name of Voltex. There is no evidence that they save money, and none of these passed the Which? basic safety test.

What You Can Do

- Check your energy suppliers contact details from their website directly. If you want to confirm they have contacted you, ring them directly from their website info.
- Your energy supplier will never ask for your bank details, as it should already have these.
- Be wary of claims made by companies marketing 'energy saving devices'. Look for the CE/UKCA mark to ensure it meets safety standards. If you have purchased a dangerous/useless device using a credit or debit card, you may be eligible for a refund using chargeback or Section 75 of the Consumer Credit Act.
- If you receive a cold call, never hand over any personal details and refuse to engage in conversation. Companies such as price comparison websites will not call you endless you've requested a call back.
- If unsure never click on any link but go to the website via your own search.

WE'RE HERE TO HELP IF YOU'VE BEEN SCAMMED

Your Citizens Advice Gateshead team are here to help if you have any worries about being scammed. Email qestaffswa@citizensadvicegateshead.org.uk or call 0191 490 4231 and we'll be back in touch with you within 1 working day Monday to Friday.

If you have been scammed and require emotional support you can find a number of organisations on our website who you can talk to.

You can check on our website if it is possible to get your money back after a scam. We offer advice on PayPal, bank transfers, Direct Debit, and gift cards/vouchers.

You can report it to Action Fraud either online or by calling 0300 123 2040 so they can monitor reports of fraud and act quickly to stop it.