DERBYSHIRE AUDIT SERVICES

INFORMATION SECURITY & FRAUD AWARENESS

COVID – 19

Background

With more restrictions being put in place to manage the coronavirus outbreak leading to an increase in agile working and absence from work due to sickness, it is important that the Council is not exposed to unnecessary risk of fraud.

Over the next few weeks and months, there is likely be an increased risk in a number of key areas including:-

- cyber-attacks against the Council's network infrastructure;
- scams and phishing attacks by attempting to exploit staff who are still getting to grips with new ways of working;
- potential for data breaches as staff will be communicating and working differently;
- opportunities to commit fraud and theft.

This briefing highlights some fraud risks that may emerge or increase in the near future, and all colleagues are encouraged to be aware of these risks and report any concerns promptly to Audit Services.

Working from Home

When working from home staff should continue to comply with the Council's information security and governance requirements and use Council equipment to carry out your work. Do not send Council data to personal email addresses to allow you to work on personal IT equipment.

Where you may be carrying your laptop or files on your walk home, to the car or on public transport please take steps to travel safely and maintain the security of any information and data. Advice is provided at: https://staff.derbyshire.gov.uk/your-wellbeing/coronavirus/working-from-home/working-from-home-temporarily-health-safety-and-wellbeing-advice.aspx

Fraud Risks Areas

Supplier Fraud

It has been noted that during the early months of 2020 several new websites have been created selling supplies forecast to be in high demand as coronavirus became prevalent.

If regular suppliers do not have items available please be wary of placing orders with previously unknown businesses as there may be a risk that they will not deliver goods as promised. Further advice can be obtained from Procurement staff.

Fraudsters will try and take advantage of concerns surrounding coronavirus. Please be aware of individuals trying to sell products with fabricated claims. Amazon has been reported as removing listings for over one million products falsely claiming to treat or cure coronavirus.

The "Executive Director/Senior Management" Scam

A well-known scam involves a person impersonating an Executive Director or other member of Senior Management by phone or email requesting that an urgent payment is made. The employee contacted makes a payment as required, which is later found to be to a fraudster's bank account.

Coronavirus disruption could present the opportunity for a fraudster to try to exploit staff covering colleagues' positions, or 'acting up' in order to request a payment. Please be aware that should you be requested to process an unexpected, urgent payment you should ensure that you verify the authenticity of the request before actioning it. Wherever possible our normal, robust payment processes must be maintained.

Ordering and Approval of Invoices

During periods of staff absence efforts should be made to maintain segregation of duty over key controls. You must not share passwords to allow colleagues to approve transactions on your behalf. Sharing passwords can expose the Council to an increased risk of fraud and theft.

To prepare for potential absences from work, please review individuals authorised to place and approve orders, and ensure there is adequate cover in the event of the absence of key members of staff.

You should continue to raise all orders for goods and services using the OrderPoint system. If you are experiencing any difficulties getting your shopping carts approved you should, in the first instance, check the shopping cart to see who is able to approve it and then contact them direct. Information on how to do this is being circulated by the OrderPoint Team to all shoppers. If you need further support please email sap.OrderPoint@derbyshire.gov.uk and one of the Team will get back to you as soon as they are able.

Bank Mandate Fraud

The National Anti-Fraud Network has reminded Council staff to be extra vigilant, particularly concerning bank mandate fraud. Scrutinise requests for:

- urgent payment due to cash flow problems,
- changes to bank account details,
- contact from third parties requesting changes to bank details and claiming to act on behalf of employees incapacitated by the virus.

Home working, different methods of communication and potential absence of team members during this period bring additional risks to all organisations. However with robust procedures, effective authorisation processes and frequent, scheduled communications we can protect the Council from fraudsters.

Theft

Shortages of supplies in supermarkets increases the risk of theft of Council stocks of certain items such as handwash, hand gel and toilet rolls. If you are responsible for the use of, and storage of such supplies please consider this risk and ensure proportionate security is in place.

Corporate Debit Cards

Council debit cards are issued for use by the named card holder, sharing of cards is not permitted. Sharing of debit cards can result in unauthorised transactions and a lack of accountability in the event of misuse.

In order to ensure business continuity please review current debit card holders and business requirements.

Requests for Charitable Donations (personal risk)

Please be aware that fraudsters have even been identified seeking donations to support coronavirus victims. Donations can be made to well-known charities which provide support in this area.

Phishing (Scam Email/Phone Calls)

Fraudsters have been identified emailing individuals, particularly in the healthcare sector, using the coronavirus outbreak to trick them to hand over personal data. One such example involved distribution of a link to a COVID-19 e-learning package which then required the user to log in to a fake look-a-like Outlook 365 sign-in page, allowing the fraudster to steal usernames and passwords.

Other known phishing attacks try to steal bank log-in or HMRC/GOV.UK sign-in information by encouraging the recipient to visit fake websites. It would not be surprising to see new versions of these older scams being updated to include a coronavirus narrative.

Reports have recently been identified where scammers rang individuals claiming to be from their bank to arrange loan and credit card payment holidays, and seeking to obtain bank account details.

The BBC has published an article which outlines some of the methods and tactics which hackers are employing to scare or coerce individuals to part with money and disclose personal information.
https://www.bbc.co.uk/news/technology-51838468

Please remember to check that callers and website addresses are genuine and, if in doubt, seek advice from IT staff or contact the caller or sender of the email by phone. You should use a separate known or published number to verify their authenticity. Please do not click on emails or embedded links if you have any doubts of its legitimacy. A guide to assist in identifying a suspicious or phishing email can be found at https://www.ncsc.gov.uk/guidance/suspicious-email-actions

Unfortunately fraudsters and thieves will take any opportunity to take advantage of a situation which may benefit them, particularly where changes to established systems may be considered. Controls are put in place to protect the Council, its staff and the public money which it spends. Please be vigilant and report any suspicious activity to Audit Services and your line manager.