Fraud Bulletin
February 2017

devon audit partnership

Purpose of this Bulletin

When reading this bulletin, employees should consider the following questions: “Could it happen to me?” and “Will the internal procedures in operation under my control stop this type of fraud being successful?”

All officers should consider whether there is fraud taking place and how this can be stopped.

How do we guard against fraud and corruption?

The annual internal audit plan has been developed to help the Council assess and take action to minimise the risks it faces.

Fraud & Corruption is one section of the audit plan and testing is undertaken on specific areas of identified risks.

However, it is the responsibility of managers to operate internal systems to ensure:

- An adequate separation of duties
- Proper authorisation procedures
- Independent monitoring and checking of data and documentation

What do we mean by fraud and corruption?

Fraud - The intentional distortion of financial statements and accounting records and/ or misappropriation of assets involving deception.

Corruption - The offering, giving, soliciting or acceptance of an inducement or reward that may influence the actions taken by the audited body, its members or officers.

Frauds come in all shapes and sizes. Many are successful as a result of the breakdown in internal control procedures in operation within the organisation. Another reason is that people do not believe it will happen to them.

Fraud Prevention Strategy’s

The Anti-Fraud and Corruption polices of our clients can be found on their respective websites.

Contact Us - Our intention is to produce this bulletin twice a year at least. We would be grateful for any information that you may have that could be included in these bulletins or for any feedback you may have on its content. For more information please contact us.

Fraud Bulletin
February 2017

devon audit partnership

Using three random words

The latest Government statistics show that only 35% of people in the UK are following Government's latest advice to use strong passwords made up of three random words.

According to the newly formed National Cyber Security Centre (NCSC), a part of GCHQ, one the most important actions people can take to protect themselves from cybercrime is by having a strong password.

Cybercrime is a growing issue, according to figures from the Office of National Statistics an estimated 2 million cybercrime offences were committed in 2015 and it cost the UK £11 billion last year.

A weak password can allow hackers to use email to gain access to all your personal accounts, leaving you vulnerable to identity theft or fraud.

The Government's cyber security campaign, Cyber Aware, is urging people and businesses across the UK to #ThinkRandom when it comes to creating strong passwords.

Using three random words to create a strong password, is the latest advice the NCSC. Numbers and symbols can still be used if needed, however, using three random words is the key to creating a strong password. You should change your password if you think it's been compromised.

A spokesperson from the National Cyber Security Centre said, "Our research shows that the best way to make a password memorable and strong is to use three random words. It doesn't matter what inspires you - from watching sport to going out for a bite to eat, thinking random is the best way to keep yourself secure online. Your most important accounts are your email, social media and online banking accounts, so it's important to use strong, separate passwords for each of these".

The statistics commissioned by Government using Ipsos MORI also show that 27% of people say they have shared their passwords. Cyber Aware is also reminding people to keep their passwords secret.

Supplier Fraud/Impersonation

The National Fraud Intelligence Bureau (NFIB) has noted a continuing issue regarding Universities being impersonated to enable fraudsters to obtain goods on a credit basis.

The supply business is initially contacted via email by the fraudster purporting to be from a University requesting a quote for goods. The fraudster will ask for the items to be provided on a 30 day credit basis. If this is approved the order is made and items are subsequently delivered to serviced offices and warehouses, not connected with and, often not located anywhere near the particular University. The items are then moved on and no payment is received.
Suspects will use email address domains very similar to that of a legitimate University address just adding a digit, or an 'm' instead of 'nn'. In addition, any mobile telephone numbers given are likely to be virtual numbers - VOIP (often starting with 070) and therefore hard to trace.

Fraud Bulletin
February 2017

Although this particular Modus Operandi has been used on various types of suppliers, recent reports reviewed by the NFIB indicate that the fraudsters are currently targeting medical suppliers and the specialised goods which they provide.

PROTECTION / PREVENTION ADVICE

- Don't be afraid to question when you receive a request for supplies from a University. If in doubt request clarification from an alternatively sourced email address or phone number.
- Check the email address against that of one that has been established as legitimate, such as one taken from the University website.
- Don't be afraid to question when the delivery address appears to have no correlation with the location of the University.
- If in doubt, check telephone numbers or email domains with open source websites such as www.telecom-tariffs.co.uk/codelook.htm or www.checkdomain.com

5 Million People Had To Cancel Their Bank Cards Last Year Due To Fraud

According to The Times, approximately five million people had to cancel their bank cards last year because of a cyber-attack, identity theft or card cloning. Leaving an average loss of £475.

The paper reported that online fraud is so prevalent that people are starting to avoid the internet to make payments. Linked article - The Times

Consumers Avoid Firms That Have Suffered Data Breaches

A study of over 3,000 adults from the UK, France and Germany has identified that 50% of all consumers wouldn't share data with or buy products from firms that have suffered a data breach.

The study undertaken by F5 Network also revealed that 61% of UK respondents thought firms aren't doing enough to protect themselves from attack. Linked articles - Infosecurity Magazine

PayPal Using Artificial Intelligence to Combat Fraud

PayPal is ahead of many big banks in using Artificial Intelligence (AI) to combat fraud. The company uses a home-grown artificial intelligence engine built with open-source tools to detect suspicious activity and separate false alarms from true fraud.

The system works in conjunction with human detectives who train themselves to think like fraudsters and like law-abiding citizens as they examine real-life cases that have triggered fraud alerts. They develop scenarios for good and bad user behaviour that they then feed into the artificial intelligence program to put this human intelligence into production. Linked article - American Banker

Fraud Bulletin
February 2017

devon audit partnership

CallJam Malware

A newly identified mobile malware named as “CallJam” repeatedly calls premium rate numbers once installed, racking up huge bills for the victim. The malware presents itself as a downloadable game in the official Google Play Store.

The unique threat of this malware is that the downloadable game it hides behind is rated four-stars on the Google Play Store, encouraging people to download it. It is believed that as many as 500,000 people have downloaded the malicious app since it was first uploaded to the Google Play Store back in May 2016.

Phishing Email Alert

There is a phishing email currently in circulation that claims to be from the City of London Police. The departments that it claims to represent include the ‘Fraud Intelligence Unit’ and the ‘National Fraud Intelligence Bureau’. The email is titled ‘compensation fund’ and has a letter attachment that claims to be offering financial compensation to victims of fraud. The letter uses the City of London Police logo.

The letter states that in order for compensation to be arranged, the receiver of the email should reply disclosing personal information. It states that HSBC and the South African Reserve Bank have been chosen to handle the compensation claims. All of these claims are false.

The email and letter are fraudulent and should not be replied to.

Protect Yourself

- Opening attachments or clicking links contained within emails from unknown sources could result in your device being infected with malware or a virus.
- The City of London Police and the National Fraud Intelligence Bureau will never email you asking for you to disclose personal information.
- If you believe you have become a victim of this fraudulent email get your device checked by a professional and make a report to Action Fraud, the UK’s national fraud and cyber crime reporting centre: http://www.actionfraud.police.uk

Don't Be a Money Mule

Students are being recruited, sometimes unwittingly, as “mules” by criminals to transfer illegally obtained money between different bank accounts.

What is a money mule?
A money mule is someone who is recruited by those needing to launder money obtained illegally. Criminals advertise fake jobs in newspapers and on the internet in a number of ways, usually offering opportunities to make money quickly, in order to lure potential money mule recruits. These include:

- Social media posts
- Copying genuine company's websites to create impression of legitimacy
- Sending mass emails offering employment
- Targeting individuals that have posted their CVs on employment websites

Students are particularly susceptible to adverts of this nature. For someone in full-time education, the opportunity for making money quickly can understandably be an attractive one. The mule will accept money into their bank account, before following further instructions on what to do with the funds. Instructions could include transferring the money into a separate specified account or withdrawing the cash and forwarding it on via money transfer service companies like Western Union or MoneyGram. The mule is generally paid a small percentage of the funds as they pass through their account.

Money Laundering is a criminal offence which can lead to prosecution and a custodial sentence. Furthermore, it can lead to the mule being unable to obtain credit in the UK and prevented from holding a bank account.

Protect Yourself

- Be aware that the offence of money laundering carries a maximum prison sentence, in the UK, of 14 years.
- Never give the details of your bank account to anyone that you do not trust.
- No legitimate company will ever ask you to use your own bank account to transfer their money. Don't accept any job offers that ask you to do this.
- Be wary of unsolicited emails or social media posts promising ways of earning easy money. If it seems too good to be true, it probably is.
- Don't be afraid to question the legitimacy of any businesses that make you a job offer, especially if the recruitment procedure strays from the conventional.

Companies House Malware

Fraudsters are sending out malware infected emails claiming to be from Companies House in the hope that businesses will download the attachment.

Another scam email has emerged which impersonates Companies House, an executive agency responsible for the registrar of companies in the UK.

The emails all seem to originate from domains closely resembling Companies House, including: @companieshouse.me.uk;@companies-house.me.uk;@companieshouses.com; @companieshouses.co.uk. All of these domains have been set up by fraudsters.