FRAUD MATTERS

Audit Services April 2020

Covid-19 Frauds

There has been a significant increase in the number of frauds being perpetrated with Covid-19 themes. Reports are being made by organizations and individuals, some of whom have suffered financial losses. The main types of fraud include phishing, bank mandate fraud and online scams. Other frequently reported scams include:

- Suspect impersonating the government and notifying the victim they are due a payment;
- Suspect asking for a donation to tackle COVID-19, normally via email;
- Callers purporting to be from the victim's bank, saying their account was compromised. Victim advised to open a new account/transfer money immediately;
- Suspect persuades victim to make an advanced payment for a rental property. The suspect uses the outbreak as the reason for the victim being unable to view the property;
- Suspect uses COVID-19 as a hook for offering employment. Victim is persuaded to pay an advance fee for vetting/qualifications to get them the job which ultimately does not exist.

Source: *NFIB*

Working at Home

There has been a sharp increase in the number of people working from home. If you are making video calls from home remember to consider the following:

- Think about the location, what can be seen in the background?
- Who may be listening? Do you have Alexa, Siri or Google Assistant listening in the background? These devices are **ALWAYS** listening and regularly pass recordings back to their hosts, even if only to check they are working. Be mindful who might be listening — turn your smart speaker off if you are involved in sensitive or confidential conversations and make sure your conversations cannot be overheard;

If you have work related documentation at home ensure that it is properly safeguarded and access to it is restricted. Any person identifiable information must be held securely and confidentiality respected.

"Coronavirus-related frauds increased by 400% in March"

- Action Fraud 2020

Inside

- Spotting potential fraud
- Examples of fraud attempts
- Bank mandate advice
- Avoiding phishing scams
- Computer Software Service Fraud
- Courier fraud
- Office 365 fraud

Bank Mandate Fraud

A report has been made of a fraudster purporting to be a senior council officer sending several emails to payroll officers within a Local Authority to request changes to their bank account details (see image below). The request contained grammatical and punctuation errors and unusual terms such as 'direct deposit details' and took a very informal tone with HR/payroll representatives with whom they had previously had no contact. The fraudster was also unaware of the payroll deadline or payment date. The original e-mail was sent from a virginmedia.com address; however the fraudster later attempted to overwrite the address to make it appear as if it was sent from a genuine "gov.uk" account. Unfortunately a salary payment was released before the fraud was detected.

Source: *NAFN*

It has been reported that with more employees working at home, it may be easier for fraudsters to impersonate senior officers, with seemingly valid reasons why they cannot be contacted, and request a change in direct debit or standing order payments. Staff should be extra vigilante and scrutinise requests for:

- Urgent payments due to cash flow problems;
- Changes to bank account details; and
- Contact from third parties requesting changes to bank details and claiming to act on behalf of colleagues incapacitated by the virus.

Source: *City of London Police*

Protect yourself — If a request is received to pay money into a new bank account, contact the supplier directly using established contact details, to verify and corroborate the payment request. Monitor bank statements regularly for any unusual activity.

If you have made a payment inform the bank as soon as possible, to help prevent any further losses.

Online Scams

The majority of reports relate to **online shopping scams** where people have ordered protective face masks, hand sanitizer and other cleaning products that have never arrived.

Other online frauds include **ticket fraud**, **romance fraud**, **charity fraud** and **lender loan fraud**.

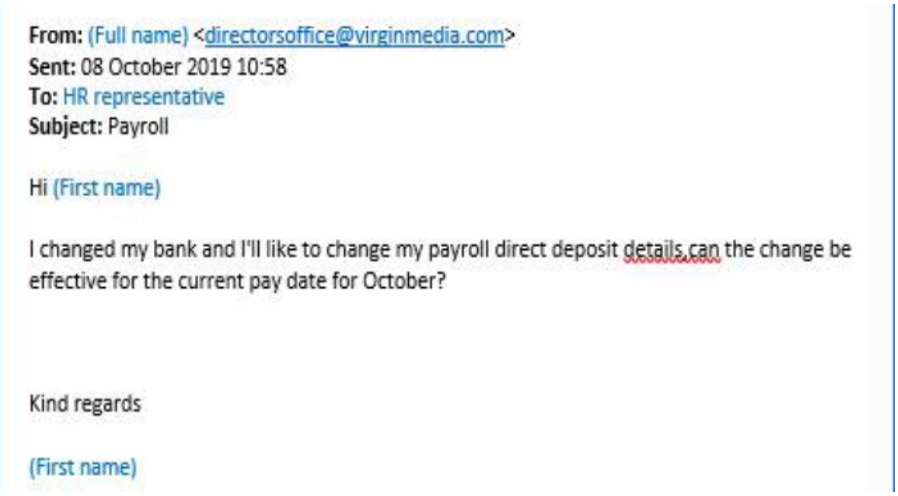
Action Fraud, NFIB.

Protect yourself — if you're purchasing goods or services from a company or person you don't know and trust, carry out some research first, ask friends and family for advice before making a purchase.

Payments — avoid paying by bank transfer as this method offers little protection. Instead, use a credit card or payment service such as PayPal.

If you have already made a payment inform you bank as soon as possible to help prevent further losses.

Fraudulent email requesting changes to bank details:



From: (Full name) <directorsoffice@virginmedia.com>
Sent: 08 October 2019 10:58
To: HR representative
Subject: Payroll

Hi (First name)

I changed my bank and I'll like to change my payroll direct deposit details can the change be effective for the current pay date for October?

Kind regards

(First name)

Free school meals scam:

Mandate fraud — the cost

According to data obtained from the UK's national fraud and cyber-crime reporting centre, businesses reported **3,577** mandate frauds in 2018/19 with total losses of **£99,283,213** - an increase of 28% from the previous year. The average amount lost by each business was **£27,756**, a 24% increase from 2017/18.

Source: *www.accountancyage.com*

A more sophisticated bank mandate fraud attempt:

Dear Partner,

Good day, We are currently working on our bank reconciliation auditing for **DECEMBER, JANUARY, FEBRUARY & MARCH** respectively in reviewing the company's invoice outstanding balance(s) with all our esteem partners around the global world, Following the Covid-19 virus pandemic outbreak and the government decision stay home & stay safe, Our company have decided to work from home to serve all our esteem partners across the globe better. Therefore we have few questions for your company:

1. Can you please send a drafted list of your open invoice(s) and outstanding payments according to what your record shows on your balance sheet? OR attach the invoice in (PDF).
2. How much are the outstanding balances.
3. When are the payment **DUE DATE** respectively? More so, if you have not yet paid your outstanding invoice.

Therefore kindly put a **HOLD** on the payment & **DISREGARD** the IBAN Bank details you had on the invoice to avoid error on your payment as a result of our ongoing company bank reconciliation auditing on our initial IBAN Bank details you had with you. We shall be providing you with our **NEW & UPDATED IBAN** bank details for any of your current payment due to be further paid.

We apologize for any inconvenience at this time, Kindly bear with us. We hope to have a pleasant and more productive business with your esteem company this 2020! We wish you a good health during this Corona-Virus (COVID-19) pandemic outbreak. Stay Healthy & Stay Safe.

Your immediate response would be highly appreciated.

Greetings!!

Examples of recent smishing attacks:

Phishing

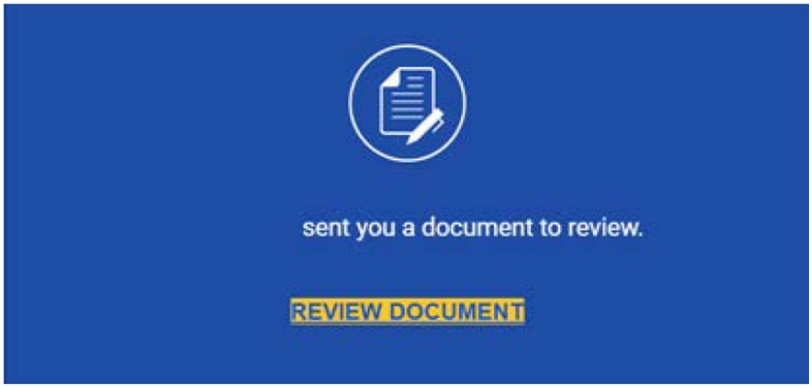
Concerns were raised as far back as February 2020 that criminals were exploiting the Coronavirus online. Since then there has been a significant increase in the number of phishing attacks/scams. On 16 February, the World Health Organization (WHO) warned of fraudulent emails sent by criminals posing as the WHO. This followed a warning from the US Federal Trade Commission about scammers spreading phishing 'clickbait' via email and social media, as well as creating fraudulent websites to sell fake antiviral equipment.

Source: *NSCS*

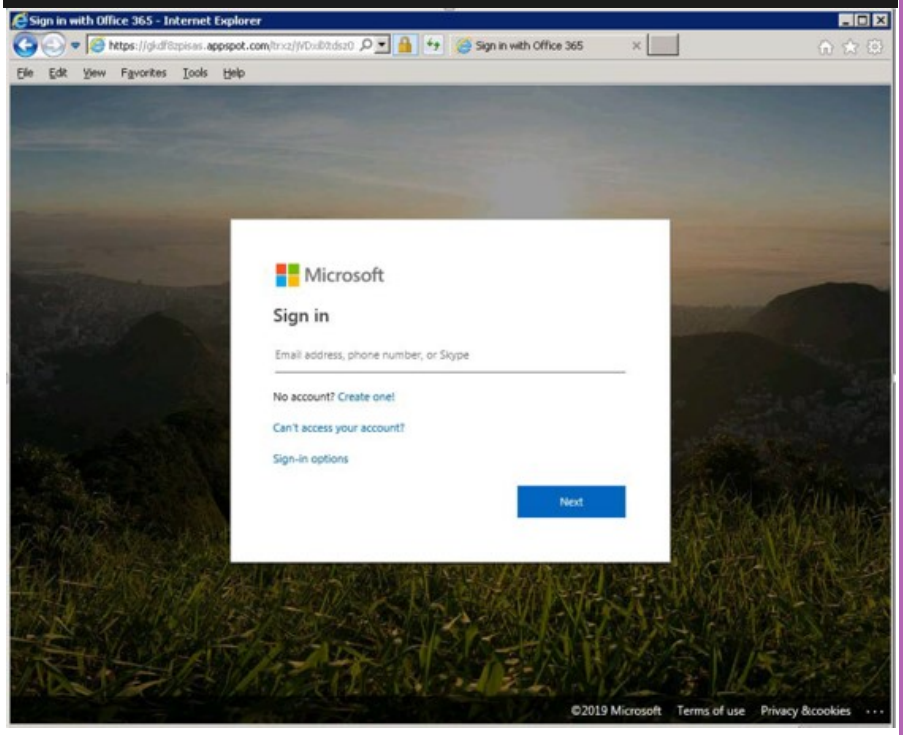
Office 365 Fraud

NAFN has reported a phishing attack from a suspected Nigerian Fraud Ring. Emails have been sent to Council officials that appear to be legitimate - but on closer inspection there are some slight anomalies, e.g. "solicltor" instead of "solicitor". The email links to a website which links to a replica of a Microsoft Login page and is used to harvest names and passwords in order to attempt various frauds.

Email link:



Fake Office 365 screen:



Source: *NAFN*

Covid-19 Phishing

By the beginning of April 2020 over 2,000 reports of phishing with Covid-19 themes had been reported to Action Fraud with total losses of **£1.5m.**

Source: *NFIB*

COVID-19 Attacks

A new COVID-19 themed phishing campaign is distributing the HawkEye malware in RTF documents. This campaign has targeted multiple organisations in the healthcare sector, and claims to provide information for treating the virus or curing it altogether. Phishing emails purporting to be from PayPal are being sent out with Covid-19 related subject lines. The email states that due to new updates, the users account has been limited and provides a link to a site for users to complete their details.

Source: *EMSOU*

Government Smishing

The Government has only sent one text message to the public regarding new rules about staying at home to prevent the spread of COVID-19. Any others claiming to be from UK Government are false. Criminals are able to use spoofing technology to send texts and emails impersonating organisations that you know and trust. Anyone who receives an unexpected text or email asking for personal or financial details should not click on the links or attachments, and do not respond to any messages that ask for your personal or financial details.

Government Smishing

GOV.UK

The government has taken urgent steps to list coronavirus as a notifiable disease in law

As a precaution measure against COVID-19 in cooperation with National Insurance and National Health Services the government established new tax refund programme for dealing with the coronavirus outbreak in its action plan.

You are eligible to get a *tax refund* (*rebate*) of 128.34 GBP.

Access your funds now

The funds can be used to protect yourself against COVID-19(https://www.nhs.uk/conditions/coronavirus-covid-19/ precautionary measure against corona)

Online Scams

UK domain name registrar Nominet has taken down over 600 coronavirus scam sites. These websites have been selling fake vaccines, protective equipment and frauds remedies related to coronavirus. The company is filtering all coronavirus-related content in a bid to stop scams and disinformation from being spread.

Source: *EMSOU — East Midlands Special Operations Unit*

Computer Software Service Fraud

As more people work from home due to the pandemic, fraudsters have attempted to capitalise on slow networks and IT problems, and there has been a reported increase in the number of attempts to commit computer software service fraud. Staff should be wary of cold calls or unsolicited emails offering assistance with networks or devices or to fix a problem. The most common attempts being reported are:

- Receiving a phone call from 'Microsoft Tech Support' to fix your computer;
- Receiving unsolicited emails with attached security updates;
- Being asked for credit card information to 'validate your copy of Windows'; and
- Being told you have won the 'Microsoft Lottery'.

There have also been several reports of emails purporting to be from Virgin Media and BT internet IT helpdesks. Emails use the corona virus as a hook and direct the recipient to a link in order to provide their details. Be aware that computer firms do not send unsolicited emails or make unsolicited phone calls to request personal or financial information, or to fix your computer/network

Source: *East Midlands Special Operations Unit (EMSOU*)

Advice

Anyone who receives email communication along these lines should simply delete the email. Staff contacted by telephone should terminate the call by hanging up the phone.

- Never install any software, or grant remote access to your computer, from a cold caller;
- Treat unsolicited phone calls with skepticism and never give any personal information;
- Microsoft does not request credit card information to validate copies of Windows and never asks for any personally identifying information, including credit card details; and
- The 'Microsoft Lottery' does not exist.

Source: East Midlands Special Operations Unit (EMSOU)

Courier Fraud

Victims are contacted and advised that money has been taken from their account by staff at their local branch and that suspects have been arrested but the police need money for evidence. Victims are asked to co-operate in an investigation by withdrawing money, or foreign currency from a foreign exchange and handover the money to a courier. At the handover the victim is promised that the money or item will be returned or they will be reimbursed but in reality there is no further contact and the money is never seen again.

General Advice

Criminals are experts at impersonating people, organisations and the police. They spend hours researching you hoping that you will llet your guard down for just a moment.

Fraudsters may contact you by phone, email, text, on social media, or in person. They will try to trick you into parting with your money, personal information, or buying goods or services that do not exist.

If you are approached unexpectedly remember to:

Stop: If you receive a request to make an urgent payment, change supplier bank details or provide financial information take a moment to stop and think.

Challenge: Could it be fake? Verify all payments and supplier details directly with the company on a known phone number or in person first.

Protect: Contact your bank immediately if you think you've fallen victim to a scam and report it to Action Fraud.

The police, or your bank, will never ask you to withdraw money or transfer it to a different account. They will never ask you to reveal your full banking password or PIN.

Do not click on links or attachments in unexpected or suspicious texts or emails.

Confirm requests are genuine by using a known number or email address to contact organisations directly.

To keep yourself secure online, ensure you are using the latest software, apps and operating systems on your phones, tablets and laptops. Update these regularly or set your devices to automatically update so you do not have to worry about updates.

Source: *NFIB*

Reminder of Procedures

All employees who are involved in the ordering process are reminded to follow the Council's procedures which are detailed in the Financial Regulations and Standing Orders Relating to Contracts and ensure payments are only made for goods and services received. Payments should not normally be made in advance and where unsolicited goods are received the company should be requested to collect them.

Further information regarding security and working at home during the pandemic can be found on the staff website (https://staff.derbyshire.gov.uk/site-elements/documents/information-security/information-security-and-fraud-awareness-covid-19.pdf).

Contact Us

If you require advice or wish to raise concerns Audit Services can be contacted via email or Skype.

Carl Hardman
Assistant Director of Finance (Audit)

Jayne Wallhead
Audit Clerk and Business Services Assistant