Fraud Guidance (Appendices)

Definitions

Phishing	Phishing is a method used by fraudsters to access valuable personal details, such as usernames and passwords. These can have a monetary value to criminals. Phishing can also involve sending malicious attachments or website links in an effort to infect computers or mobile devices. Criminals send bogus communications: emails, letters, instant messages or text messages. Very often these appear to be authentic communications from legitimate organisations. Embedded links within the message can direct you to a hoax website where your login or personal details may be requested. You may also run the risk of your computer or smartphone being infected by viruses. Once your personal details have been accessed, criminals can then record this information and use it to commit fraud crimes such as identity theft and bank fraud. Phishing messages generally try to convince the recipient that they are from a trusted source. “Spear-phishing” is a technique whereby criminals use personal information to earn trust and lower the intended victim’s defences increasing the chances they may open attachments or embedded links. Criminals have stepped up their activity by targeting business users by claiming that they have specific knowledge of the business. These may be business critical issues: customer feedback, requests for information, staffing or legal notices. (Source: Action Fraud)
Smishing	Smishing is when criminals use text messages impersonating other organisations to trick people into giving away their personal and financial information or money. These scam texts often claim to be from government departments, banks or other trusted organisations, offering payments related to the coronavirus outbreak or claiming to be issuing fines. Often the messages will include a link to a fake website that is designed to trick people into giving away their financial and personal information such as bank details, passwords and credit card numbers. Criminals are also using a technique called “spoofing”, which can make a message appear in a chain of texts alongside previous genuine messages from that organisation. The banking industry continues to work closely with mobile network operators, government, and other industry stakeholders to crack down on this type of fraud. (Source: UK finance)

Vishing	The word 'vishing' is a combination of 'voice' and 'phishing.' Phishing is the practice of using deception to get you to reveal personal, sensitive, or confidential information. However, instead of using email, regular phone calls, or fake websites like phishers do, vishers use an internet telephone service (VoIP). Impersonating a person or legitimate business to scam people isn't a new thing. Vishing is simply a new twist on an old routine. In fact, vishing has been around almost as long as internet phone service. Using a combination of scare tactics and emotional manipulation, they try to trick people into giving up their information. These vishers even create fake Caller ID profiles (called 'Caller ID spoofing') which make the phone numbers seem legitimate. The goal of vishing is simple: steal your money, your identity, or both. (Source: Fraudwatchinternational)

Specific Guidance

Phishing guidance:

- check that the sender email address looks correct
- look for spelling mistakes in the email
- if there is a hyperlink within the email text be suspicious
- be wary of generic salutations (e.g. Dear colleague instead of Dear Gillian) or the lack of a salutation
- don't feel pressured by threats within the email e.g. "If you do not respond, your pension benefits will be frozen"
- ignore requests to take immediate action/urgency.

Further guidance can be found at www.actionfraud.police.uk/a-z-of-fraud/phishing.

Smishing guidance:

As above for phishing but in relation to text messages however, more specifically

- do not click on a link contained within a text
- if the text is unprompted then be wary
- ask yourself if you usually receive texts from the sender of the text, if not be suspicious.

Vishing guidance:

- Be aware of unsolicited calls
- Do not share any personal details when receiving an unsolicited call
- Be wary of promises of high returns, the offer of a free pensions review, advising you can access your pension before age 55
- Don't feel pressured into making a decision or taking any action.

Further guidance can be found at www.fca.org.uk/scamsmart or www.thepensionsregulator.gov.uk/en/pension-scams.

Examples

Phishing emails:

From: Michael Steinitz <michaelst@ekmd.huji.ac.il>
Date: 27 March 2020 at 14:51:10 GMT
To: Michael Steinitz <michaelst@ekmd.huji.ac.il>
Subject: March & April payment benefit | Covid-19 Update

During these exceptional circumstances, we would like to request the cooperation of everyone to maintain our health and safety in and outside the Institution. Please due to the latest update, all staff & Employee are expected to kindly Click PRMA and complete the required directive to be added to March and April benefit payroll directory system.

You will be omitted if you fail to comply with the directives.

Thank you,
Admin Department .

Phishing emails:

HMRC is aware of a phishing campaign telling customers they can claim a tax refund to help protect themselves from the coronavirus outbreak.

Do not reply to the email and do not open any links in the message.

The email has been issued in various formats. An example of this scam is below:

----- Forwarded message -----
From: GOV UK Notify <danielnhs@pinkcontract.com>
To: "
Sent: Friday, 6 March 2020, 08:28:50 GMT
Subject: UK Updates on COVID-19

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)

At 6.15pm on 5 March 2020, a statutory instrument was made into law that adds COVID-19 to the list of notifiable diseases and SARS-COV-2 to the list of notifiable causative agents.

From Government Gateway

This is an automatic email - please don't reply.

Fake letters:

Fake texts:

'Goodwill payment' SMS

HMRC is aware of coronavirus SMS scams telling customers they can claim a 'goodwill payment'. Do not reply to the SMS and do not open any links in the message.

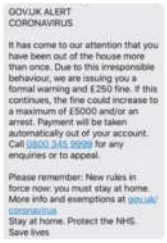
This is an example of the scam wording:

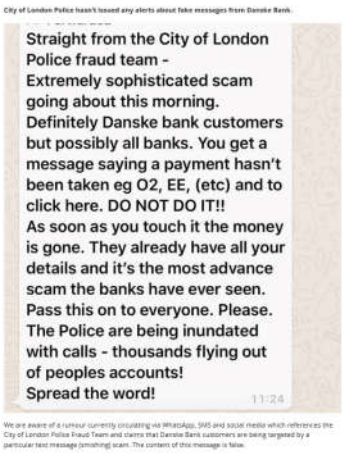
'As Part of the NHS promise to battle the COV- 19virus, HMRC has issued a payment of £258 as a goodwill payment. Follow link to apply.'.

'£250 fine' SMS

HMRC is aware of a SMS scam which states you will be fined £250 for leaving the house more than once. The message asks recipients to call an 0800 telephone number to appeal.

Do not reply to the SMS or call the phone number listed. An example of the scam is shown below:





Additional Guidance

You can obtain further information from the following agency websites on the different tactics fraudsters can take and how to protect yourself from such approaches:

Action Fraud, www.actionfraud.police.uk/a-z-of-fraud/pension-scams
Action Fraud, www.actionfraud.police.uk/individual-protection

The Pensions Regulator (TPR) leaflet, www.thepensionsregulator.gov.uk/-/media/thepensionsregulator/files/import/pdf/16423_pensions_consumer_leaflet_screen.ashx

The Money Helper website, https://www.moneyhelper.org.uk/en

Hymans Robertson Pension Scheme Administration Teams