IT / Cyber Security/Fraud

All staff are reminded to stay vigilant to *phishing, smishing* and *vishing* attacks from cyber criminals who are becoming increasingly more sophisticated. Examples include; giving advice about Corona Virus, asking for payments, from clicking on links in emails and asking for personal information which could be or from callers.

Phishing, Smishing and Vishing Fraudsters may contact their victims by various means and, as such, it is important to stay vigilant to all methods to ensure you can protect yourself, your family and the organisation. It has been widely reported that whilst most crimes have reduced during the COVID-19 crisis, fraud has increased significantly.

All methods seek to gain financial or personal details from their victims, such as bank details, credit card, or other login information, or download malicious content such as malware to their device. Usually, fraudsters will impersonate an official body, such as Government agency or utility provider, with the aim of gaining the victim's trust.

Three common methods are as follows, with some recent examples of each scam:

Phishing Scams are where fraudsters send emails and/or create bogus web pages, which encourage the recipient to click on a link or download an attachment.

Smishing Scams are where fraudsters seek to obtain financial or personal details of their victim by SMS text messages. As with phishing, they usually encourage clicking on a link.

Vishing Scams are where fraudsters seek to obtain financial or personal details of their victim by telephone.

Action(s) to take: Spotting a phishing, smishing or vishing attempt is becoming increasingly difficult, and many scams will even trick experts utilising what are known as 'social engineering' techniques. However, there are some common signs to look out for:

- **Authority** - Is the sender claiming to be from someone official (such as your bank, doctor, a solicitor, government department)? Criminals often impersonate a source you're more likely to trust in order to trick you into doing what they want.
- **Urgency** - Are you pressured with a limited time to respond (such as 24 hours or immediately)? Criminals often threaten you with fines or other negative consequences.
- **Emotion** - Does the message make you panic, fearful, hopeful or curious? Criminals often use threatening language, make false claims of support, or tease you into wanting to find out more.
- **Scarcity** - Is the message offering something in short supply (such as a COVID- 19 test or cure)? Fear of missing out on a good deal or opportunity can make you respond quickly. C**urrent events** - Are you expecting to receive a message like this? Criminals often exploit current news stories, big events or specific times of year (such as a global pandemic) to make their scam seem more relevant to you.
- If you are approached unexpectedly by email, text message or telephone, remember to:

  Stop - Taking a moment to think before parting with your financial or personal information could keep you safe.

  Challenge - Could it be fake? It's ok to reject, refuse or ignore any requests. Only criminals will try to rush or panic you. An official organisation will not try to stop you contacting the organisation directly through known contact details.

  Protect - Contact your bank immediately if you think you've fallen victim to a scam.

If you do receive a suspicious phone call or email, please contact the IT Service Desk right away on **0151 – 676 5678**.

All employees are responsible for:

- Using the personally provided removable media devices only by agreement of the Trust IT department who in turn have to be satisfied that the device is encrypted to a secure standard and represents no risk or threat to data integrity & confidentiality and that there is a legitimate business reason for the transportation of this data by this mechanism.
- Ensuring desktop PCs that have been taken off site and used in staff homes during the pandemic are not encrypted and staff must ensure that these devices are stored securely in their homes and no **Person Identifiable** or **Sensitive Information** is stored on any local drives.
- Ensuring personal responsibility and security for any Trust provided removable media device in his/her care - Remember to press CTRL-ALT-DEL or the Windows & L Key to lock your PC or laptop when not in use.
- Returning all removable digital media devices to the IT Department when no longer required and any PCs, Monitors, Keyboard and Mouse with all cables back to the Department when no longer required.
- Ensuring that they comply with the requirements of this policy and use technology devices appropriately.
- Ensuring the appropriate use and security of any information and IT equipment they use in accordance with their duties, e.g. computers, laptops, internet, removable devices, etc.
- Ensuring that patient consultations are conducted using Trust approved software.

Staff must not:

- Disable Trust virus protection software on Trust equipment;
- Download or load unauthorised software onto Trust equipment;
- Save Personal Identifiable Data (PID) or Business Critical Information (BCI) data directly to the local disk or desk top, (e.g. C:\ Drive), of a computer, laptop or device;
- Install or connect any unauthorised hardware on any Trust device;
- Connect mobile devices to unsecured public Wi-Fi networks;
- Use Trust provided portable devices for personal use;
- Use Trust provided portable devices for the processing, storage or transfer of person identifiable data without sufficient encryption in place;
- Use Trust portable devices for bulk transfer of data off site without authorisation;
- Use personal portable devices of any kind to connect to the Trust's network infrastructure, apart from trust guest Wi-Fi;
- Use Trust provided portable devices as a permanent or indefinite storage mechanism; data must be transferred, as soon as possible to a secure networked drive and removed without hesitation from any trust provided portable device;
- Use Trust provided portable devices for any type of a commercial or profit- making naure, or for any other form of personal financial gain; or any use that conflicts with an employee's obligations to their employer; or any use considered to be against the organisation's rules, regulations, policies and procedures in particular this policy;
- Allow any unauthorised persons to access or use the portable device provided.

Any staff member who removes information or equipment from Trust premises is responsible for ensuring the safe transport and storage of all Trust equipment to ensure that items:

- must not be stored in places where a thief can easily steal them;
- must not be left in a vehicle overnight;
- must not be left visible in a vehicle when travelling between locations;
- must not be left unattended in a public place;
- must not be placed in locations where they could easily be forgotten, e.g. overhead racks, taxi boots, train stations, exhibition halls etc.;
- must be password protected;
- must be transported in a secure, clean environment.