PHISHING AND INSIDER FRAUD

Phishing

The practice of Fishing is the removal of a creature from its habitat which does not wish to be removed.

The practice of Phishing in many ways is not dissimilar, and is the removal of information from an individual who does not wish to provide the information which has been removed.

Other than the similar sounding name, there is a world of difference between the two, and this article looks at the fraudulent activity of Phishing, the means by which the victim can then be persuaded to give up information and the consequences which then are likely to take place.

Many of us will be familiar with the letters which would arrive from some high ranking individual, usually in a foreign country who as a result of a substantial profit on a contract, or some other unexpected gain, had very substantial funds locked up, which could only be released if the bank account of the person who had received the letter, would allow their account to be used, for a substantial percentage to enable the funds to be transferred, then to be paid to the foreign individual.

Of course, there were no funds, and the whole purpose of the letter was to gain access to the likely victim's bank account from which funds would then be extracted.

As information technology has become much more part of daily lives, the fraudster now uses that technology to fool a potential victim that for what appears to be a wholly legitimate reason they should disclose some personal detail to the author of the email which has arrived in their Inbox.

What the fraudster wants is information from the victim – a username, a password or bank details.

The message can come by email, SMS or on a social network, but by whatever means it is to extract information known only to the victim.

The message can appear to come from a company or even from a Government Department, whereby the email is made to look entirely official.

However, it is possible to spot a phishing email and the following are examples which provide a clue that the message is not genuine.

1. A website address which looks similar to the organisation from which it purports to come, but on inspection there is a subtle difference in the address from the genuine organisation.
2. Poor English or mis-spelling in the text of the message.
3. A difficulty with a payment or that an account will be blocked unless some action is taken.
4. A suggestion that a service will be discontinued or is being amended and the victim has to verify certain details.
5. Your password is about to expire.
6. The account will be blocked unless personal information is provided.

A further variation is known as "Spear Phishing" which is more of a direct attack where the fraudster has gathered information about an individual, and uses that information to make the victim believe that the email has come from a source that the victim can trust.

Moving away from the written word, the use of the voice to obtain information is now known as "Vishing". One popular method is for the victim to be called up by their bank with the caller posing as the Bank's Fraud Department, and advising that suspicious activity has been detected on the account and possibly asking for verification of passwords or account numbers. The victim is told that to satisfy themselves that the call is genuine, they should call the Bank's fraud department and may be given a phone number. Even if no phone number is given, and the victim does call their Bank, modern technology may simply transfer the call to the fraudster.

A search of the Internet will provide many websites providing examples of phishing and ways to detect and recognise a phishing attack.

There are some basic rules to follow that should help to protect personal details.

1. Never provide personal details either by email or on the telephone, whatever the reason.
2. If there is a suggestion to call back a number after a call requesting information, use a different phone line to make the call if possible.
3. Look very carefully at the address of the email and if possible, find an email from the same source and check if there is a minor difference in the email requesting information.
4. Read the email and check for poor grammar or spelling mistakes.

While phishing generally strikes at individuals or corporates, the public sector is not immune from fraudulent activity. While there may very well be attempts of organised crime to attack public funds, there is also a considerable danger from those working in the public sector.

Public Sector Insider Fraud

Insider Fraud takes many guises and can be just as impactful in the Public Sector as it is in the private sector. The National Crime Agency estimate c£40 billion of public funds being lost through insider fraud annually with money that could otherwise be used to help those in need, improve our schools, NHS and other public services.

Data breaches tend to grab headlines, which in many cases are due to unintentional human error. However whilst the unintended fraud losses can be reduced by improvements in internal controls, training and oversight spending, intentional fraud is much more difficult to identify and indeed prosecute offenders in the absence of evidence of intent.

As Accountants, we are trained to act with integrity and report on fraud when discovered in our work, however not all those who could do this are bound to do so, and indeed will have ethical dilemmas in doing so (e.g. a perpetrator is in their line management, and they are in a household

that relies on a single income). The below case study is based on a real-life fraud in the UK public sector and has been designed to help identify red flags as you read through. How many will you find? What controls are not in place that should be? What lessons could be learned to prevent re-occurrence?

A County Council serves a population of c2.2million citizens and provides the usual range of services; schools, housing, environmental health etc. In other words, it is a typical council which could indeed be your local council. The Council operates from across four core corporate sites and the payments function is centrally located, consisting of a team of 12 FTE staff reporting through the Financial Controller to the Finance Director. The payments function operate strict segregation of duties from other departments in the council and their role is process based on the paperwork presented/ they do not perform any other activities, including trend analysis.

Over the course of 12 months £128,000 was transferred to the personal accounts of fictitious Foster Care workers, and then to accounts in the name of a council worker. The fictitious payments were only discovered 6 months later following budget reviews resulting from a value for money exercise.

The council worker was convicted of fraud two years later and sentenced to a four year custodial sentence.