Logical Thoughts

FINANCIAL FRAUD AND SCAMS

At Logical, we believe there is a difference between a “fraud” and a “scam”.

It is our view that a fraud is a breach of confidence, whilst scam is more of a trick.

The prevalence of financial fraud has been on the increase in recent years. It appears it will only worsen as we look into the future because the perpetrators are becoming more sophisticated in their attempts to steal money.

Recent research indicates that almost half of the victims of financial fraud are aged 55 years or over, often called Edler Financial Abuse. The victims are not necessarily very wealthy, and often victims and perpetrators are within the same age bracket. The sad reality is this activity comes not from some distant stranger, but someone close to the victim. It may be a relative, or it could be an otherwise caring neighbour. Unfortunately, there are too many cases of family members and close friends defrauding their elderly relatives / friends. Examples include people taking advantage of relatives grieving the loss of a spouse, exerting undue influence and people suffering from cognitive impairments, which are fertile ground for would be fraudsters. This is usually coupled with an absence of proper professional financial planning and / or legal advice.

Powers of Attorney can be abused, and funds can be withdrawn and used for other than their proper purpose. Or it may be simple theft. The motivation may be inheritance impatience or involve emotional blackmail and include a failure to provide proper care. Sometimes it comprises intimidation and threats. Or it can be a loan guarantor situation gone wrong.

On the other hand, scams are usually online, via a phone call or text and come from an imposter of one kind or another. Mostly, they can be detected, however, even those of us with a keen sense of smell can still fall victim to a major loss. Be aware that criminals work a numbers game, and they are constantly honing their skills in an attempt to trap us.

The banks and other corporates are putting hundreds of millions of dollars into strengthening their systems and their ways of doing business, but most often the error resides with the account-holder. The systems, including two-factor authentication, usually work as designed, however, oftentimes the account-holder has simply been tricked into authorising a transaction they soon deeply regret. The funds move to another Australian bank account, usually an account that has been established with false identification, and then the funds are quickly whisked offshore, never to be recovered. As well as a financial knock, it is mentally debilitating to learn that some anonymous criminal has run off with substantial cash.

Unsecured emails can be the equivalent of leaving your front door wide open and asking the perpetrators to assist them load the truck with all your personal information.

Logical tries hard to be vigilant with fraudsters and the scammers. With respect to fraud, we use our professional processes and experience to determine whether our client’s best interests are being met.

One practical change we have made to combat scams is when sending confidential & private documents as attachments via email, we use passwords to secure them, so they aren’t readily openable attachments.

There are many ways in which you can control these risks, and here are some of our favourites:

- Protect your passwords and personal information. Don't make them easy to guess and don't share them, especially with someone you don't know;
- Establish 2 (or multi) factor authentications where possible;
- Learn to recognise "red flags" in phishing emails, including spelling & grammar mistakes, coming from an unknown sender, coming from a sender purporting to be a government department or authority, urgent (or sometimes threatening) language and instructions to click on links;
- Be very wary of publicly available Wi-Fi. Logging on to a public Wi-Fi network is one of the easiest ways for cyber criminals to hack into your systems;
- Protect your computer with up-to-date anti-virus software and fire walls;
- Check your bank account and statements regularly;
- Keep your transfer limits low. Only raise them when you are sure and do it temporarily;
- If you feel a phone call sounds in any way suspicious, quickly hang up;
- Always use secure websites when shopping online;
- Let us (& your family & your bank) know before you travel overseas;
- Don't send money or personal information to people from unusual locations;
- Avoid swiping your credit or debit card when making purchases – insert or tap it instead.

The Australian Competition & Consumer Commission's ScamWatch website has a wealth of reliable information, tips and traps, see here: ScamWatch.