Fraud and Social Engineering

Fraud affects us both at work, and in our personal lives.

Understanding the tricks criminals use, and how they fool us, as well as identifying where we might be exposed to fraud, are some of the things we can do to help protect ourselves.

So this is Fraud and Social Engineering by What You Need To Know.

Broadly speaking fraud is the deliberate use of deception or dishonesty to: make a financial gain, cause someone a loss, or expose someone to a risk of loss.

Let's start by having a look at some of the ways fraud is committed.

Fraud by abuse of position is when someone is in a position of trust, and expected to look after the financial interests of another person, and they abuse that position for personal gain.

Here's an example.

Nick was a financier who used his strong reputation in the City to convince customers to invest with him. However, instead of investing their money, he used it to pay for his extravagant lifestyle.

Abuse of a position would also include things like:

selling client information to a competitor

copying software products and then selling them for personal gain, and

could even include giving special discounts to friends or relatives.

Another form of fraud involves failing to disclose information.

Helen believed her expensive watch had been stolen, she made a claim to the insurance company and later received a payment from them. Then Helen found the watch, but didn't let the insurance company know. She can't have the both watch and the money.

People often fail to disclose information when applying for things such as jobs, mortgages, and insurance policies. But when people lie on this type of application, it's called fraud by false representation.

And false representation also occurs when someone pretends to be someone they're not, which is what Harry did.

Harry used to phone people up and pretend to be 'from the bank'. He'd try to get customers' personal details, then sell these to criminals.

Other examples of fraud by false representation include: using a stolen identity to get a loan, or a stolen credit card to buy things, or pretending to be an official representative, as Harry did, when really he was just a confidence trickster, a grifter, a scammer.

Whether fraud happens in person, through the post, over the phone, or through the internet, there are a number of psychological manipulation techniques that fraudsters use to get us to do things, or divulge information, which we wouldn't normally do and this is sometimes called social engineering.

Let's have a look at some of these manipulation techniques.

One is using authority and trust

When someone speaks and carries themselves with authority, we'll often assume that they're genuine and therefore take them at their word. As a result, we do what they ask us to do, especially if they look the part. A sense of authority and trust can also be conveyed through forged letters, fake websites and bogus emails.

Another technique they use is to try and create a sense of urgency or scarcity. We also see this in advertising, when a 'fear of missing out' is exploited to get us to act quickly.

Sometimes they'll try and convince us that something is real, because everyone else is doing it, in other words there's some form of social proof, or consensus of opinion.

They do this because, when we're not sure what we should do, we tend to follow the crowd. So if we're told that everyone else has agreed to something, we're likely to assume that they can't all be wrong, and we go along with them.

Another trick is to present themselves as being likeable and familiar.

We like to help people, especially if we like them and feel that they're 'one of us' for example, by working for the same organisation.

Fraudsters will often appear to be extremely pleasant and sometimes pretend to know someone within the organisation so as to give the impression that they 'belong' there, and to get us on their side and willing to help.

Hackers use similar tricks, such as befriending a person on a social media site to get them to lower their guard and therefore take less care than usual.

And if that doesn't work, they might try using threats and intimidation. Perhaps a threat of reporting someone to their boss for not doing their job properly, or just appearing to be really angry to avoid being challenged or questioned.

Email phishing scams often use intimidating language like, 'you'll be locked out of the system', or 'unless you act now, you'll have to pay a fine', to both threaten and create a sense of urgency, so that we act quickly and without thinking.

Criminals will use any - and all - of these techniques and if you feel someone is trying to put pressure on you, or to manipulate you, it can be a good idea to verify that the person really is who they say they are.

But be careful, fraudsters are prepared for challenges like these, so make sure the person doing the verifying is genuine.

Being aware that criminals use these techniques can help alert us to scams while they're happening, but there are more things we can do.

One is identifying where you're most vulnerable, then taking steps to make these areas more secure.

At work, there are four general areas you could look at: assets, staff, customers and suppliers.

Assets can be physical such as equipment, stock and money, or things like ideas, information and client details, all of which can be sold on. An organisation's brand and reputation are also valuable assets which can be exploited or damaged by criminals.

Nearly one in five small businesses have been defrauded by a member of staff at some point, either by the person acting on their own, with a colleague, or in collusion with someone outside the business.

Criminals also pose as customers in order to commit fraud.

Perhaps by making purchases using someone else's payment card, or using the overpayment scam. Here's how it works. They overpay by cheque, then later point out the mistake and ask for a refund. The scam works if they get the refund before the cheque inevitably bounces.

Fraudsters sometimes pretend to be a known supplier and then arrange for a regular payment to be redirected into a different bank account. Or a trusted supplier might start to regularly, and intentionally, overcharge – perhaps in collusion with a member of staff.

When you look at areas of personal vulnerability consider unsolicited or unexpected phone calls, letters and visitors.

If you use the internet, think about how you do things like make purchases online, fill out forms with personal information and use social media. These are all areas fraudsters exploit.

The old sayings that if something sounds too good to be true, then it probably is, and if something doesn't feel right, then it probably isn't, are worth keeping in mind. So listen to what your instincts are telling you and if you feel that something's wrong, be especially careful.

Understanding where you're most vulnerable, and most exposed to the risk of fraud, then taking measures to protect yourself.

Being aware of the psychological manipulation techniques that fraudsters use, and paying attention to your instincts, are all steps you can take to build up your protection against fraud and social engineering.