CAF'S SOCIAL ENGINEERING TOP 5'S

The work you do helps make a difference to society; unfortunately it also makes you a target for criminals. A social engineer will attempt to trick you into helping them commit their crimes. Here we look at what you need to know about social engineering.

Five facts about social engineering

1 **Yes, you are at risk**
If you process money, or hold information that isn't public, then you're at risk of being socially engineered to give it up. Remember: Personal information can hold a lot of value.

2 **You might lose nothing but your reputation**
Victims of social engineering don't always suffer a loss. The criminal may want access to your information to commit further crimes. Could your reputation withstand being the source of that information?

3 **The human is the weakest target**
Technical attacks require a high degree of expertise and are difficult to execute. People on the other hand can be manipulated much easier.

4 **Social engineering can be subtle**
The best social engineers are able to walk away with the information they want without their target ever realising that something's wrong.

5 **Social engineering is more than just "ishing"**
Terms like Phishing, Vishing and Smishing are common, but have you considered that the next person you meet could try to socially engineer you?

Five red flags for social engineering

1 **Know the motivators**
A social engineer will get you to act by creating:
A sense of urgency;
A risk of loss (financial or opportunity);
A sense of guilt for not helping; or
A fear of missing out on the latest trend.

2 **Beware the angry person**
A social engineer may act deliberately emotional in order to deter you from challenging their presence or actions.

3 **Your friend isn't your friend**
A social engineer may learn who your friends, colleagues and partners are, and impersonate them to exploit your trust in that person.

4 **Watch out for the knight in shining armour**
A social engineer may cause you to have a problem in order to reach out in order to "solve" the problem as a way of gaining access to your information.

5 **Socially engineered "under the influence"**
Sometimes you're in the mood to talk (or post online), but be cautious of saying more than you should. You could be talking to a social engineer.

Five ways to protect yourself

1 **Trust nothing until verified**
Until you have verified otherwise by an alternative method, assume that anything you are told or asked to do is an attempt to socially engineer you.

2 **Protect yourself online as you would physically**
You wouldn't leave your front door unlocked, or put your personal information on your front garden for passers by to read; so don't do it online. Employ appropriate IT security.

3 **Limit what attackers know about you**
Understand what information you make available online, and be careful about over-sharing. This will make it harder for social engineers to find material to manipulate you with.

4 **Focus on awareness and policy**
Awareness like this helps you to understand the threats you face. Policy sets out the way you should respond to a given situation to prevent you from being manipulated. Ensure you understand and follow it.

5 **Physical Security is also important**
Be careful of who you allow into your place of work, and what information you physically take out of it.

By being aware of how social engineers work, you make their job much harder. Remember to always be vigilant and alert to the possibility of social engineering.

If you suspect social engineering using the CAF name, email scamreporting@cafonline.org

CAF
Charities Aid Foundation