Social Engineering – don't be manipulated

Social Engineering is the practice of manipulating people so that they give up confidential personal information such as school/work credentials and banking information.

Criminals use Social Engineering tactics because it is usually easier to exploit your natural instinct to trust rather than to try and hack your software or devices.

Security is about knowing who and what to trust. Security professionals tell us that humans are the weakest link in the security chain and this is why it is essential that you know how to recognise when you are being engineered and when not to trust what you are hearing or seeing.

So, what can a Social Engineering attack look like?

- An unexpected email, supposedly from a friend, that stirs your curiosity and/or invites you to check out a link or download.
- A plea for help, e.g. the Prince with £50 million that he will share with you in exchange for your assistance.
- Official-looking communications from your bank, school, employer or the Government. Commonly, these offer money or try and scare you with account closure or potential fines.
- Baiting scenarios such as offers that simply seem too good to be true.
- A response to a request for help that you never made which then prompts you to reply, starting a conversation with the criminals.
- Social media posts that trigger you to get involved and suck you into more detailed conversations, generating distrust or conflict.

Think you wouldn't fall for social engineering tricks?

Try TakeFive's quiz and find out!

- https://quiz.takefive-stopfraud.org.uk/

How do you make sure you don't become a victim?

- Slow down, think and take your time. Urgency and high-pressure tactics are often the hallmark of someone wanting your information for criminal purposes.
- Research the facts. Don't trust information, ratings or links without further investigation.
- Be vigilant of clicking on links without first verifying where they might take you.
- Understand the email policies of organisations such as your school, employer and bank. Know which details they will, and will never, ask you.
- Take extreme care downloading anything sent to you unless you absolutely know and trust where it came from.
- Anything that looks too good to be true usually is.

What additional ways can you protect yourself?

- Delete anything asking for personal, financial or password information.
- Ignore requests for help or offers of help. Reputable organisations will never contact you in this way unless you have asked them to.
- Ensure that all your devices are secure, with the latest versions of software, firewalls and anti-virus installed and operational.
- If it doesn't look right, the likelihood is that it's not right.

Remember that Social Engineering can happen anywhere and to anyone. Protecting yourself is as important as protecting where you work or study, your social groups, and your friends and family.

Still unsure?

If you're still unsure, or if you would like advice, contact the Service Desk – servicedesk@abdn.ac.uk or https://myit.abdn.ac.uk.