Name of theory
Nudge theory, also known as nudging

Key reference
(Thaler & Sunstein, 2008; 2021)

Description
Nudge theory, or nudging, refers to designing the available choices in such a way that preferred options are more likely to be chosen, a method called choice architecture. There are several basic nudging techniques.

Defaulting
Defaulting is deciding which option is chosen if people do not actively choose a specific option. The reason defaulting is successful is that people experience inertia and that defaulting sets an implicit norm for what is considered the most appropriate behaviour or choice.

Opt-in and opt-out
Opting in or out is a specific case of defaulting where people need to manually sign up for a service (opting in) or are automatically signed up to that service (opting out). Simple examples include whether people are automatically enrolled in pension schemes, need to register to vote, or whether they are automatically listed as an organ donor or not. The effectiveness of opting-out systems lies in the inertia experienced by people, as is the case in defaulting. However, opt-outs are seen as ethically more difficult since they make use of people's inertia to nudge them towards accepting a situation that they might not have chosen themselves. One option to, partially, mitigate this ethical issue is to make the opting-out process as easy and transparent as possible.

Social proof
Social proof is the technique of informing people of the behaviour of others (usually peers), to steer them in the same direction. People who are told that "80% of your co-workers also chose X", are more likely to also choose this option, as they believe that their co-workers will have chosen this option for a reason, and that it would be rational to follow their behaviour.

Decoy effect
In the decoy effect, a specific unenticing option, the decoy, is added to a set of choices to make other options look more favourable. For example, when presenting people with a cheap and an expensive option, the expensive option can be presented as more favourable by adding a decoy option that is nearly as expensive but offers a much lower reward. In that situation, people are more likely to only compare the decoy and the expensive option, with the latter being perceived as more attractive.

Application within the field of cybersecurity
Nudging is used in cybersecurity to both enhance and hinder cyber secure behaviour. In terms of enhancing, software designers can decide to eliminate unwanted options, or to set defaults so that people are more likely to behave in a secure fashion. For instance, a software designer or system administrator can set two-factor authentication (where a user needs to confirm their identity beyond a username and password with a code sent to a mobile phone for

example) as the default in the organisation, thereby nudging people to adopt this practice. Nudging is also used to encourage the use of stronger passwords, and to nudge people towards better privacy settings. However, software developers have also used nudging to hinder personal security and privacy, by purposefully making it difficult to choose the secure and private options in for example cookie settings menus. In those instances, the "accept all cookies" button is usually large and flashy, while the "reject all cookies" button is often small or even completely missing. These methods to purposefully hinder of cybersecurity are colloquially called "dark patterns".

Annotated bibliography

Cho et al (2019). Cho et al. investigated how people could be nudged towards more stringent privacy settings in a mock-up of a social media platform. They offered five options for sharing future posts in two orders: "Only Me", "Close Friends", "Friends", "Friends of Friends", and "Everyone", or the reverse. The first option of the five was considered the default (So either Only Me, or Everyone), and they tested whether people chose different privacy options as a result. They found that people are more likely to stick to the default, and that if they do make a change, this change stays close to the default.

Peer et al (2020). Peer et al. investigated how people could be nudged towards the use of stronger passwords. They used a variety of nudges such as a password meter (a visual indicator of how strong a password is) and social proof, where they explain whether this password is stronger/weaker than X% of their peers. The authors found that nudges could be successfully used to improve the creation of strong passwords.

Thaler & Sunstein (2008; 2021) This book covers the basics of nudge theory, with the 2021 version being an updated 'final' edition of the book. The authors provide many examples of how nudging can help society, as well as discussing ethical issues and other related themes.

van Steen & De Busser (2021). This report contains a rapid literature review of nudging research in the area of cybersecurity. The authors cover some of the basic nudging principles, as well as providing an overview of various behaviours influenced using these techniques. One of the main findings is that password creation and privacy settings are particularly well investigated behaviours in the field of cybersecurity.

References

Cho, H., Roh, S., & Park, B. (2019). Of promoting networking and protecting privacy: effects of defaults and regulatory focus on social media users' preference settings. Computers in Human Behavior, 101, 1-13.

Peer, E., Egelman, S., Harbach, M., Malkin, N., Mathur, A., & Frik, A. (2020). Nudge me right: Personalizing online security nudges to people's decision-making styles. Computers in Human Behavior, 109, 106347.

Thaler R.H., Sunstein C.R. *Nudge.* Penguin Group; 2008.

van Steen, T., & De Busser, E. (2021). *Security by behavioural design: A rapid review*, The Hague, The Netherlands. https://www.ncsc.nl/binaries/ncsc/documenten/rapporten/2021/september/14/security-by-behavioural-design-een-korte-samenvatting/Security+by+Behavioural+Design+%28Leiden+University%29.pdf