JAN-WILLEM BULLÉE

SOCIAL ENGINEERING: FROM THOUGHTS TO AWARENESS

Would you give your keys to a stranger? Probably not. However, Jan-Willem Bullée's research has shown that, in an office environment, 59% of participants did exactly that. He tells us why, here.

PSYCHOLOGICAL MANIPULATION

Most people underestimate the degree to which they will engage in insecure behaviour, something that criminals exploit through 'social engineering'. Our vulnerability to these kind of attacks is exploited by offenders who use psychological manipulation to make us assist them. These kind of attacks are successful since we use heuristics (i.e., rules of thumb) in our decision making. These mental shortcuts work well in most circumstances. However, when a heuristic fails, a cognitive bias occurs. A cognitive bias is mistaken thinking due to errors in reasoning or evaluation. There are several ways in which this tendency can be exploited to influence people to make it hard for them to say no. One tactic is reciprocity, whereby receiving a gift can make someone feel indebted and more likely to give something in return. A common example of this is when restaurants give customers a mint when presenting the bill, a gift which can result in bigger tips.

THREE ATTACKS

In my research, we performed three type of attacks in a controlled environment. During the first attack employees were called by an unknown and untrusted 'offender' who persuaded them to download and install some software. In this attack, the offender induced reciprocity by warning the victim about their PC being in danger. During the second attack, offenders visited employees in their offices and asked them to hand over their electronic office key. In the third attack, phishing emails were sent to office employees in an attempt to convince them to share network credentials.

NOBODY THINKS THEY WOULD FALL FOR THIS

As an outsider, it seems obvious that such social engineering schemes are scams. It is hard to believe that someone would fall for them. A survey among academic researchers in The Netherlands confirms this. In the survey, no-one reported that they would install the software from a cold call and only 3% reported that they would hand over their office key to a stranger. My experiments suggest otherwise. In total, 40% of the employees installed the software and 59% of the employees handed over their office key to a stranger.

TRAINING

On a positive note, there is hope. I divided those who participated in the first two attacks into groups. One group received information showing them how to recognise potential scams. This group performed better than a group which received no training, at both the installation of software (17% vs. 40%) and handing over office keys (37% vs. 59%). However, this improvement disappeared when the length of time between the information campaign and the attacks was increased.

LENGTH OF SERVICE MATTERS

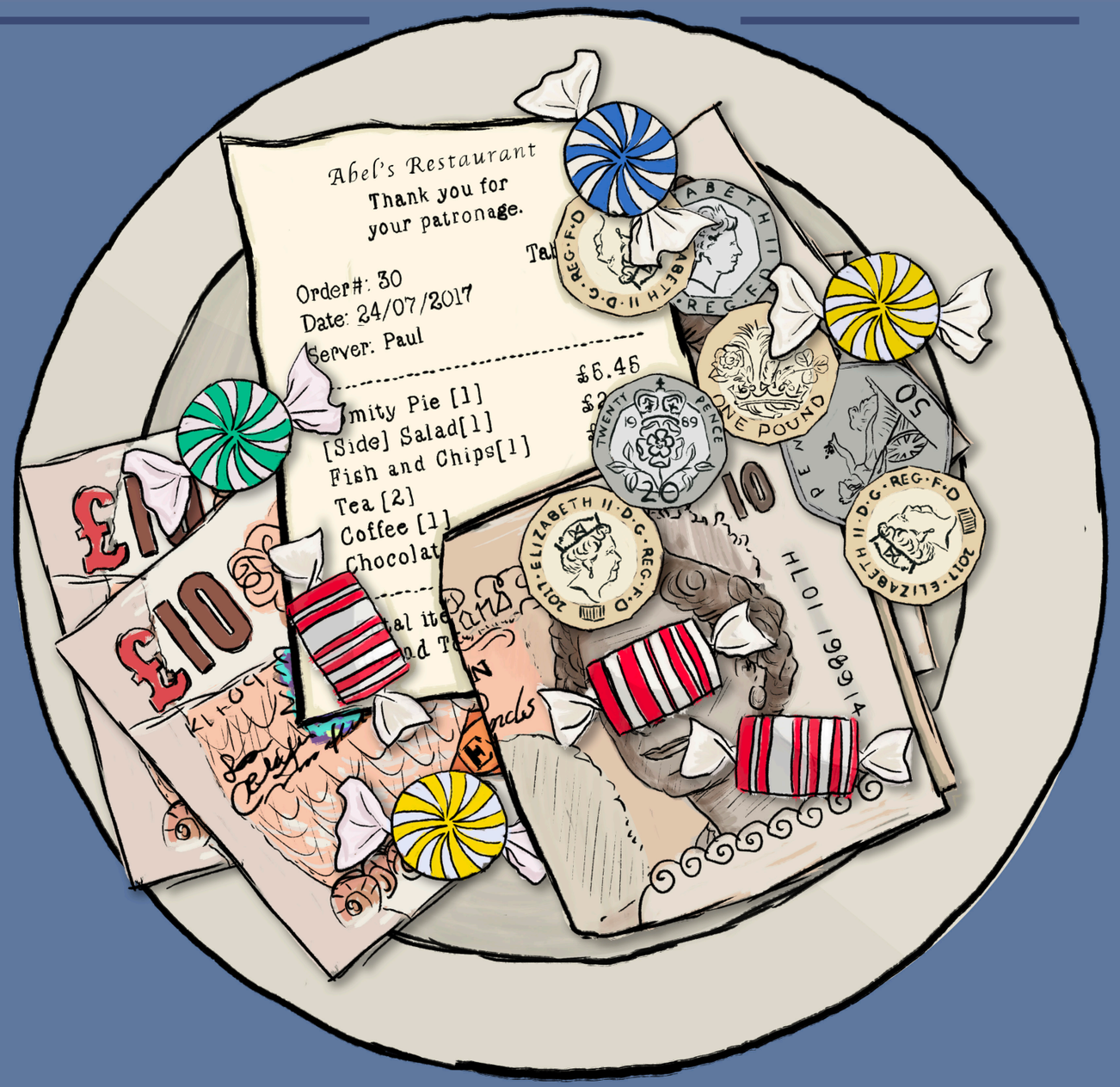
My analysis of the subjects' socio-demographic characteristics in the three experiments showed that both target gender and age did not influence the outcome. However, in the email experiment, the victim's length of service with their employer did influence the outcome and had an interaction effect with age. This suggests that young employees with only a few years of service are those most vulnerable to phishing emails.

IMPLICATIONS FOR PRACTICE

I suggest that there are some important implications arising from these results.

1) Awareness-raising about social engineering reduces the probability of falling for a scam. Training should include how to recognise the tactics people use to influence victims and how to react.

2) Awareness-raising training is only effective for a short period of time. Therefore, a single round of training is insufficient. However, merely repeating the same message over and over again is also ineffective and could even be counterproductive. The solution is likely to lie somewhere in the middle; in regular repeat training with innovative approaches and materials.



3) People tend to be overly optimistic about their level of risk. My research discovered a difference between intended and actual behaviour. If people do not see the urgency of the problem, they may not accept any training or countermeasures. One explanation for this is the optimism bias (another cognitive bias), which can run along the lines of: 'I am less likely to be targeted by an offender. If I am targeted, I am better at resisting than someone else. Therefore, this training is not relevant to me.' Tackling and reducing this optimism bias should, therefore, be a part of awareness-raising training.

4) Vulnerable groups should get special attention. I found that young, recently hired personnel are most at risk. An easy way to reduce this vulnerability is to provide awareness training during induction. As I found no effect of gender or age I would suggest that there is no need for training targeted specially for men, women, younger or older colleagues.

Jan-Willem Bullée researches information security at the University of Twente.