Security Psychology

Phishing attacks are a common threat in the IT-field and in general. Phishing attacks gather sensitive information from the user through fake emails, fake websites etc. Most of the time these phishing emails for example are impersonating a friendly and trustable source like a known person, company etc. These phishing attacks are effective because they usually offer some kind of reward in them, and behavioural psychology suggests that human behaviour is affected by the rewards and punishment, so a human might click a phishing email if it offers some kind of price. The phishing emails can also create panic in humans and affect their behaviour that way. For example, if a phishing attack says that your password needs to be switched within 2 minutes, humans can panic and it can affect their behaviour.

Social engineering works because some people can easily be manipulated. Social engineering manipulates emotions and instincts. This appears in social psychology, where people's thoughts, feelings etc. are affected by others. an example of this would be that people are made to believe certain stereotypes, even though they are not true. This is the same in social engineering and that's why it works on people. An example of this would be a phishing attack where the attacker pretends to be the CEO of the company and sends phishing emails to a new employee. The employee is more likely to click on the phishing email because it is presented to be sent from the CEO.

Why people have a hard time remembering passwords is related to cognitive psychology. Long and complex passwords are hard to remember and that's why people tend to use shorter passwords. There are many other cognitive factors related to people having a hard time using passwords in a secure way. For example, people might have habits related to weak passwords and breaking them can seem difficult and make people think it's too hard. People also might think they have secure enough passwords, but in reality they haven't taken the time to find out what secure passwords actually are. Furthermore, reusing passwords might be connected to the fact that people can only remember certain amount of passwords and also coming up with new ones might be challenging.

PGP fails to be effective way to secure email, because the implementation of it can vary and it might be disregarded. If the key sizes used to encrypt are long enough, then it should be secure, but there are also more factors. Many attacks target the implementation rather than the PGP itself, for example HTML based emails handled by PGP have been a target of attacks. Users should make sure to handle data correctly and use the right size keys for encryption in order to make PGP more secure.

Malwares are easy to spread because new ways of spreading them are increasing and they are becoming more convincing day by day. Humans trust sources that seem reliable which furthermore increases the spreading of malware. Vulnerable softwares are also still to this day an occurring factor, which allows the spreading of malware. Zero-day attacks in softwares also are a reoccurring factor. Also poor security in hardware enables malwares to spread.