In this essay I will look the psychological aspects of security and address the following questions: Why are phishing attacks effecctive enought to be widespread practice? Why social engineering works on people? Why many people have hard time using password in secure way? Why it is so easy to spread malware? Also I will use psychology theory like cognitive-, behavioral- and social psychology on this essay.

Secure attack means attacks to the human psychology. For example in hybrid warfare operations,like this week there were drone attacks on airports in Denmark. Some suspect were connected to Russia, even its not sure. Tactics are desinged to create fear and uncertainty. These operations aim to remind people that anyone could be a threat and that society cannot fully protect them. Fear and confusion are powerful psychological tools.

First question phishing attacks effective enougt to be widespread practice. The internet is so globalization and overloaded with information. People are searching information so hurry. People working online may act carelessly, paying little attention to detail. Criminals exploit this sloppiness through deceptive emails or websites, tricking people into sensitive information. From a psychological perspective, phishing works because it preys on our limited attention. Our tendency to trust familiar patterns and our habit of making fast, automatic decisions.

Why social engineering works on people? Social engineering operates at near of technology, psychology, and even military strategy. It works because humans are inherently social animals: we depend on each other. Society norms and values are important us. We also respond strongly to rewards and punishmenets. Social engineering takes advantage of these traits by using persuasion, authority, fear, or urgency to push people into actions they wouldn't otherwise take. Examples include fake news, targeted advertising, or manipulative messages designed to influence behavior.

As technology becomes more secure against purely technical attacks, manipulating people—the "weakest link"—becomes increasingly attractive. Security engineering must therefore incorporate an understanding of human psychology: our needs, fears, and social dependencies.

From an evolutionary perspective, humans are motivated by basic needs such as food and safety, as well as by the drive to avoid danger. We also respond to rewards and punishments and care deeply about our social standing. All these elements can be exploited in social engineering attacks, making them highly effective.

Why many people have hard time using password in secure way? Passwords are a key point where usability, applied psychology, and security meet. The history of passwords since the mid-1900s has been shaped by both economic and technological factors. Cybercriminals have long exploited weaknesses in password systems, and even today many authentication systems remain heavily dependent on centralized technologies, such as Microsoft platforms and email-based recovery mechanisms.

From a psychological perspective, there are several reasons why people find it difficult to use secure passwords. They have difficult to choice password. It could be something that people have easily to remember. It can't be too long. If its too long or complex users might have difficulty to entering it correctly. Second issue is that users cant remember their or they have difficult to remember it. Third problem is that password is naivy or too simply, so it's too easy to find. This is what Anderson sayd about that topic.

Last question is why it is so easy to spread malware? Malware is effective because it exploits both technical weaknesses and human behavior. Insecure or poorly maintained websites provide easy entry points, and many popular sites have at times been compromised. As Ross Anderson notes, a quarter to a third of websites, when weighted by traffic, attempt to trick users in some way.

Many users ignore security warnings or fail to recognize suspicious activity. People often delay installing updates or patches, leaving devices exposed. Malware often hides behind tempting content—such as free downloads, entertainment, or urgent messages—that trigger impulsive clicks. These factors mean that malware can spread fast through social networks, email attachments, or infected websites, taking advantage of both technological flaws and predictable human behavior.

Notes:

Ross Anderson Security Engineering 3 edition 2020)