The Art of Hacking Humans: Intro to Social Engineering

Piggy-backing

Piggy-backing is also known as tailgating. In piggy-backing, an attacker gains unauthorized access to a restricted area by shadowing an authorized personnel, giving the impression that they are together. For example, an intruder could go to a building with access restricted to only authorized people and tail one of them, making security personnel who control entry think he is with such a person giving him hassle-free access. The attacker can also pretend to be an authorized personnel, like an employee, making it appear that he has forgotten his access card or the card is malfunctioning leading an authorized personnel to offer assistance and let him into the restricted area. Another strain, Chapman (2009) quoted Colin Greenless as saying just hold two cups of coffee and wait for someone to help you open the door. That is to say an attacker can give the impression his hands are full, leading someone to help with gain entry. Once a malicious attacker gains access through piggy-backing, he can steal data, install malware, or even drop a bait to entice an unsuspecting victim to install malware.

Piggy-backing takes advantage of human gullibility to deceive personnel into giving access. It also takes advantage of people's willingness to help a distressed fellow human. There is also an element of fear, a fear of offending or embarrassing someone – a security personnel may be afraid of offending/embarrassing an employee who is probably higher in rank to them; an authorized personnel may feel not helping someone who is apparently another personnel in distress may be offending or embarrassing the person, might even feel awkward asking questions.

Piggy-backing can be tackled by use of methods to authorize access like identity badges, access cards, PIN codes, biometrics, dead man doors, and so on. But most importantly, security operatives and employees should be trained and enlightened about techniques used by malicious attackers like piggy-backing. The security personnel and employees should be made to understand and appreciate why they should not shy away from following laid down procedures for allowing physical access, and should ask questions, make enquiries before authorizing access to situations that are out of the ordinary (like an employee who has lost access card or has a malfunctioning card for example).

References:

Chapman, S. (2009) *Consultant Uses Social Skills to trick Corporate Security* [Online]. Available from: https://www.cio.com/article/2428266/infrastructure/consultant-uses-social-skills-to-trick-corporate-security.html (Accessed: 27 October, 2017).