Baiting is a form of social engineering that relies on the greed or curiosity of the victim. It’s similar to phishing attacks in many ways. However, what makes it different from other forms of social engineering is the promise of a good or service by hackers to entice the victim. For instance, a baiter often offers free movie or music download, in exchange of login credentials of a particular site. Moreover, baiting is not only restricted to online schemes. Rather, an attacker may use physical media for exploiting a victim.

**How is Baiting Carried Out?**

Baiting can take many forms including online techniques of downloading files or through physical devices such as a flash drive. Let’s consider a scenario of USB drive. With a USB drive that is infected with malware, cyber criminals may physically go to a lobby of a targeted company, co-working spaces, public restrooms or coffee bars and leave a USB device branded with a corporate sticker or logo. They will then wait for a curious individual or employee to pick it up and insert it into their computer system.

Once it’s installed, the victim can see files with names such as “Profit and Loss Projection” or “Confidential”. The filenames are designed to prompt the employee to download the files, which in turn delivers a trojan horse to their computer and spreads it across their entire internal network. From here onwards, the hacker can conduct the next stage of attack such as a watering hole or a spear phishing attack.

In an online scenario, the similar methods are used to prey on the greed or curiosity of the victim. A lucky draw ticket winner email perhaps, or availing the opportunity to watch the next Marvel movie premier. Many malicious sites with tempting download links lurk in the cyberspaces and wait for unsuspecting fans to download them.

**Securing Yourself Against Baiting**

Cybercriminals know well how to play with our emotions and fears. If you receive that email that is too tempting to be true, don’t act hastily. Stay calm and think of the possibilities and consequences. The strongest defense is to educate yourself and strive to create a strong security culture within your surroundings, whether it’s office or home. As an organization, conduct regular social engineering awareness and training sessions, and likewise carry out social engineering assessments either with specialized staff or by getting help of professional cyber security services.

To find out how Aardwolf Security can help you, get in touch with us today!