Scripto MK.1

“When a hacker is faced with a secure system they have two choices. They have to either attack the system, or they can use the people working with the system to get around it. This second method is called social engineering and can be used in a number of ways from Nigerian princes to someone rushing in to work at the last second and forgetting their ID. In this video we’re going to talk about some of the most popular social engineering attacks as well as how to prevent them.

The most common type of cyber attack is one most of us have experienced. It’s called phishing and its usual form is an email that’s supposed to contain exciting or important information. When the target opens it however, it usually holds a link which can install malware or a request for personal information the attacker can then use. This method is called phishing with a P.H. instead of an F and tends to involve the attacker sending out thousands of emails to unsuspecting targets and hoping that one of them will actually take the bait. The problem is that people know about scam emails and for the most part know not to click on suspicious emails, this has led to a new more malicious attack called spear phishing. It gets its name from the fact that while normal phishing is like casting out a net and hoping to catch anything, spear phishing is targeted at a single or a few people. The attacker will carefully plan the attack researching what the target is most likely to believe and then spring the trap posing as a higher up in the organization or a trusted source. Whatever the method the result is the same, malware or identity theft. The easiest way to prevent yourself from falling prey to this kind of attack is skepticism. Never follow any link given over email and think twice before opening emails from suspicious sources.

Another less common attack is baiting. In this attack the hacker uses physical data storage like usbs or cd-roms to deliver malware inadvertently. The methods of delivery vary from droping a bunch of usbs on the road near a target to using company logos or titles andgiving them away as free gifts or software updates. The result however is that as soon as they are inserted they go to work installing viruses which get around the firewall. This method uses greed and curiosity to gain access and grant it to the attacker. Prevention of baiting comes mainly from recognizing it. Employees must be trained to understand what they should do with data storage containers given to them freely.

For all of these attacks there is one easy solution. Stay vigilant when on the internet or dealing with technology, because you never know who might be trying to get in.