READ BOLDED MATERIAL

Attacks on Wallet Software: **The client can either go for the online wallet services or he can choose to have wallet application downloaded in his node**. Generally, the online wallets are more vulnerable to the attacks and thus need to be encrypted and backed off-line.

*Example: going to unsafe links or downloading things that have not been properly scanned to remove or warn from malicious software.*

Timejacking Attacks: The attacker announces the inaccurate timestamp while connecting to a node for a transaction. **The serious consequences of this are double-spending and wastage of computational resources during mining process.**

*Example: ?????????*

‘>50%’ Attack: Is when any colluding user or group of user acquires more than 50% of the computing power in mining process **This user or group can then be able to exclude, modify, and self-reverse transactions and prevent some or all ‘mining’ of valid blocks for their benefit**

*Example: In May of 2018, Bitcoin Gold, at the time the 26th-largest cryptocurrency, suffered a 51% attack where the attackers were able to double-spend for several days, eventually stealing more than $18 million worth of Bitcoin Gold.*

Double Spending: Attacker successfully makes more than one transaction using single coin resulting into invalidating the ‘honest’ transaction. **By varying the timestamp, the fraud transaction can be made as a real one.**

*Example: ???????*

Selfish Mining: **honest miners spend their cycles on blocks that eventually will not be part of the blockchain and they are forced by selfish miners to do so.** Allows a pool of sufficient size to obtain revenue larger than its ratio of mining power

*Example: Not adding a block to a chain for selfish actions and that ending up making other people look for one block when it has already been found*