**Security and Password**

**Introduction**

Security is the state of being free from danger or threat. There are 3 main types of security in computing:

**1. Physical Security:** Using physical barriers to prevent unauthorized access to data (like locking the door of the server room).  
**2. Software Security:** Fixing flaws in your application that could grant attackers unwanted levels of access to your systems.  
**3. Network Security:** Security of networked services (websites, [databases](https://lms.clarusway.com/mod/lesson/view.php?id=995" \o "Databases), etc).

The computer is like a castle with walls, inside and outside are very different. The bad guy cannot just access the bytes outside the computer but inside the computer at will. The bad guy needs to work at it.

A couple of bad guy strategies:

* obtain a password allowing access
* trick the computer into running bad guy code

| **https://docs.google.com/uc?id=11EtqcaHoaZSZdleIMbyyXeoTQkyA5RBZ** |
| --- |
| *Bad guy will want to access your castle from open doors (network)* |

**Access Control**

Access Control is a framework for controlling who has access to what resources on a system. There are many ways to implement Access Control, but the three basic principles of Access Control are **Identification**, **Authentication**, and **Authorization**.

* **Identification:** Who is this person?
* **Authentication:** Is this the person who he claims to be?
* **Authorization:** Is this person allowed to perform this action?

**Passwords**

Passwords are the de facto form of Authentication for computers, but they aren’t a perfect solution. Passwords are hard to remember and surprisingly easy for computers to guess.

There are some problems for passwords:

* People use same passwords for different accounts,
* People use simple passwords that are easy to guess,
* Passwords are hard to remember.

Solutions to these problems:

* Using a password manager,
* Changing passwords regularly,
* Using multi-step authentication.