


Collection


Users can Collect posts into a printable, sortable format. Collections are a good way to organize posts for quick reading. A Collection must be created to tag posts. [More Help](#)

| | | | |
|----------------|--|------------------------|-----------------------------|
| Thread: | Group#2 Authentication | Posted Date: | September 15, 2019 11:23 PM |
| Post: | RE: Group#2 Authentication | Status: | Published |
| Author: |  LEAH DREW | Overall Rating: | |

You did a good job of explaining authentication. I agree that biometric authentication such as palm scanning or facial recognition is a more reliable way of verifying someone's identity, but personally I feel like some of these encroach on people's privacy. If a hacker gets access to say, what someone's fingerprint looks like, it's not like that person can just change it. That information is compromised forever, and that hacker could also use it to take advantage of the security system in the future.

You're right that it's more reliable than a password or ID though. People will always find ways of getting through security systems, so we have to be adaptable and innovative to keep outsmarting them.

(Post is Read)

| | | | |
|----------------|--|------------------------|----------------------------|
| Thread: | Physical Security Methods | Posted Date: | September 14, 2019 5:08 PM |
| Post: | Physical Security Methods | Status: | Published |
| Author: |  LEAH DREW | Overall Rating: | |

Physical security is protecting hardware from physical events such as theft, usually with other physical measures like locking doors and installing security cameras. Physical security is important because it provides an extra layer of security to protect important information with. Hacking or cracking passwords requires a certain amount of technical knowledge, but almost anyone can steal or vandalize a device. Also, encrypting data or using forms of authentication are good for thwarting damage by humans, but can't protect against damage from non-human sources, such as a fire.

In an article titled "Physical Security and Why It Is Important" on SANS.org, David Hutter writes about an attack the US Department of Defense suffered in 2008. An employee carelessly left a flash drive in a place where an attacker was able to take it and infect it with a virus without the employee knowing. The next time the employee plugged the USB into a government laptop, the virus spread throughout the entire network and the attackers used it to access classified data. With better physical security, an incident like this would be much less likely to happen. As discussed in our reading, one measure they could have implemented better to reduce the chance of an attack like this is securing their equipment. Employees should also be trained so that they know to keep devices locked down to prevent them from being compromised so easily.

According to a blog post at Veristream.com titled "Six Levels of Physical Security", there are at least three layers that physical security should be implemented at. There should be security around the outer perimeter, such as a locked gate to keep intruders out. Businesses should use "natural access control," meaning a layout that guides people coming and going from the area, such as with fences

and landscaping. Doing this can deter intruders because it lowers their confidence in their ability to enter undetected. Territorial reinforcement, such as a fence or a “no trespassing” sign, can also be used to deter intruders at the outer perimeter. There should also be security at the inner perimeter of the building—alarm systems, locked doors, and access control are all examples of this. Finally, there should be security within the interior of the building, like security cameras and having a visitor management system, which can include background checks.

(Post is Read)

← OK