Some say that people are the biggest risk of cyber security.

Select five terms from ISO/IEC Standard 27000 Section 3 Terms and Definitions and write a 300-word [**blog post**](https://www.my-course.co.uk/mod/oublog/view.php?id=701741) on how people can be managed to overcome cyber security attacks from the inside.

No system is secure from attacks or hacking. Every system is vulnerable to outside attacks, no matter what. Even air gaped computers are vulnerable to outside attacks by inserting a USB drive from an unknown origin. Allegedly that is how the Iranian nuclear attack was performed (Saunokonoko, *How stuxnet worm took out Iranian nuclear facility in 2010* 2021). Today anyone can buy the Hack5 USB Rubber Ducky (Hak5, *USB rubber ducky*). This USB can be programmed to perform any number of tasks, from keylogging to executing scripts to grabbing images, videos, browser history, credit card information or erasing an entire computer content. All it takes is to drop this USB on the floor or someone's bag and for someone to pick it up and plug it into a computer. There is no need for an internet connection to perform these attacks. This kind of tool is widely available, and anyone can purchase it and use it, making IT administrators' life much harder. The only thing IT administrators can do is completely block the ability to insert USB drives into a system.

Once an IT administrator understands that no system is secure, even air-grabbed ones, then they can start working towards securing systems and software.

Another issue is how to secure a network that is not connected to the internet. There are a few approaches.

1. Hide wifi SSID from the public. However, anyone with enough experience can easily find wifi SSIDs using a wifi analyzer (Acrylic WiFi, 2022).
2. Only allow specific devices to connect to a network if their MAC address matches the router MAC address whitelist. However, even that is easy to get around using MAC address cloning. (CABLE MATTERS, 2020).
3. Monitor the network at all times and keep a log of all network activities from connected devices, even trusted ones.

Combining all these techniques gets the network closer to being secure, but even then, it is still vulnerable to attacks and hacks.

References:

*ISO/IEC 27000:2018(EN) - international organization for standardization*. ISO. Available at: https://www.iso.org/obp/ui/#!iso:std:73906:en (Accessed: December 11, 2022).

Saunokonoko, M. (2021) *How stuxnet worm took out Iranian nuclear facility in 2010*, *Natanz cyberattack: How Stuxnet worm took out Iranian nuclear facility in 2010*. 9News. Available at: https://www.9news.com.au/world/how-stuxnet-cyberattack-took-out-natanz-nuclear-facility-in-iran/37694f90-c2e1-454c-9597-e7de8f54e495 (Accessed: December 11, 2022).

Hak5 (2022) *USB rubber ducky*, *Hak5*. Hack5. Available at: https://shop.hak5.org/products/usb-rubber-ducky (Accessed: December 11, 2022).

Research, T. (2022) *Discover the hidden SSID of a WIFI network with these simple steps*, *Acrylic WiFi*. Acrylic WiFi.com. Available at: https://www.acrylicwifi.com/en/blog/hidden-ssid-wifi-how-to-know-name-of-network-without-ssid/ (Accessed: December 11, 2022).

*What is mac address cloning?* (2020) *Cable Matters Blog*. CABLE MATTERS . Available at: https://www.cablematters.com/Blog/Networking/what-is-mac-address-cloning#:~:text=Login%20using%20your%20admin%20details,IP%20address%20and%20admin%20details. (Accessed: December 11, 2022).