News

How to protect from Card Cloning

Physical Access Control Systems (PACS) continually evolve as vulnerabilities are identified.

It is no exaggeration to say most RFID cards used for access at office buildings, data centers, factories, government buildings are susceptible to card cloning or hacking. Today, card cloning devices can be obtained online for as little as $10. The battle is ongoing and is relatively cost-effective to put right.

Legacy Systems

The majority of legacy PACS installed use standard open transmission protocols such as Wiegand and MIFARE®. These cards have been in use for many years without being

managed by industry standards resulting in hundreds of different types card types being developed and in use. The proliferation of 125KHz proximity and latterly Mifare standard proximity adoption revolves around perceived convenience and low cost however these cards have little to no encryption and therefore vulnerable to attack. The following offers practical ways to update existing systems and future-proof new ones.

Two-Factor Authentication

Two-factor authentication is the combination of two out of the three possible methods (something you know, something you have, something you are). Most access control systems will couple an access card with a pin code.

Contactless Smart Card Technology

MIFARE® DESFire® EV2 allows for fast and highly secure encrypted data transmission with read/write capability. This high frequency 13.56MHz technology is ideal for access control management. In this ever-expanding universe of credential technologies, it is advisable to opt for open global standards for both air interface and cryptographic methods. MIFARE® DESFire® EV2 is the latest secure credential technology to hit the market that provides 128Bit encryption and is compliant to all 4 levels of ISO/IEC 14443A and uses

optional ISO/IEC 7816-4 commands. Put simply, these cards cannot be copied of cloned and offer the additional benefit of being used to exchange data with third party applications such as cashless vending and logical access control systems.

Mobile Access

Smartphones are becoming increasingly replacing access cards in the security industry. Mobile credentials are easy to assign, monitor, and revoke in real time. They cannot be copied or duplicated, and users are less likely to share their phone than key card. From a security and convenience standpoint, mobile access is second to none.

Talk to our experts on how to protect your business from card cloning. Email us at **michaelbyrden@vanderbiltindustries.com**.