Mobile Access Misconceptions

One of the most significant access control advancements in recent years is mobile access, that is using a mobile phone in place of a physical access card. Companies implementing mobile access are finding it easier to manage and more cost effective than traditional forms of access control. Users love the convenience and administrators appreciate the security and privacy features that protect the organization and personal information.

Mobile access control has been a win for the industry with more companies implementing the technology into their current security infrastructure. However, some companies and individuals are skeptical about mobile access technology.

WHITE PAPER

Why? Perhaps they don't understand the technology, how it works, or the potential benefits it can bring to the organization. There is also a belief that if a user loses their mobile phone or it is stolen, that the phone can be used to access the company's buildings. They may also be concerned about the security of the user's personal information.

We will explain in the following whitepaper why this should not be a major worry. Simply, mobile access technology works to make your life easier by offering industry leading security protection with an easy to manage and more sustainable system.

In this whitepaper we have divided the content into three sections to address common myths about mobile access. We will begin our discussion by explaining what mobile access is, and its advantages over traditional lock and key systems or RFID cards.

We will then explain what happens to the information residing on your mobile phone should it be lost or stolen and how the technology protects the information so your phone functions cannot be accessed or hacked. Mobile access has also proved to be beneficial beyond only accessing doors to buildings but is also assuming a role as a multi-function tool for comprehensive security management.

The following information will detail how today's credible mobile access suppliers will develop a solution that protects your company's secure information and employee's personal data. Counterfeiters will not be able to access the secure data and use the mobile phone as a weapon against you or your company.

The information in the whitepaper will also reduce your fear about the power drain on your mobile phone when you are using it. Today's mobile access technology uses very little power and mobile phone battery drain is a fear no longer relevant with today's technology.

Mobile access functionality is here and should be embraced as an additional asset in your company's current security management system. As we have stated it is easy to manage, affordable, and provides multiple functions. It will put your company at the forefront of leading-edge technology and provide multiple benefits. Please allow us to break down a few myths about mobile access in the following pages.

Chapter 1: Stolen Phone

One of the most recent, and relevant, advancements within access control was the introduction of mobile access functionality, a feature that piggybacks on the general mobility trend to enhance the user experience with physical access control. Let's go back to the basics and discuss what this technology is and how it works.

WHAT IS MOBILE ACCESS AND HOW DOES IT WORK?

Mobile access allows your employees to enter physical and digital places by using a mobile device as an access control credential. The smartphone or wearable device contains a digital copy of a valid physical access control card, and in the case of HID Global, both the physical and the digital cards are protected by extremely secure encryption that blocks any cloning attempt.

How does it work? It uses the NFC or BLE capabilities of the device to communicate with a reader, using (in the case of HID Global) Seos® technology to securely authenticate the credential (i.e., the identity). The system then allows access to the physical or digital place, thing, or system, based on the rules defined by its administrators.

As mobile access adoption has grown and physical security started mixing with consumer electronics (smartphones and wearables), new issues began to appear, mostly for the end-users of the technology (your employees).

This chapter will address some concerns that potential users in emerging markets have expressed regarding the use of mobile access and how — as a security manager — you can approach them by providing accurate information.

In this section, specifically, I hope to diminish some of the misunderstandings people may have if their smartphone is lost or stolen and ease the anxiety that comes with suddenly finding yourself without control of the information on your mobile phone.

COMPARING MOBILE ACCESS TO TRADITIONAL LOCKING SYSTEM AND RFID CREDENTIALS

For most people, their mobile phone is their daily lifeline to their jobs, family, and personal information. Regardless of the reason, when a situation arises that separates a person from their phone or device, there is an immediate concern about the personal information on the device. And naturally, if an access credential is loaded to the device the concern extends to the potential for someone unauthorized to use the mobile access system to which it is associated.

In today's business world, many global companies have chosen smartphones as the access tool of choice versus brass keys or RFID card credentials to provide secure and highly convenient access to company locations.

Many companies are using mobile access installed on smartphones to give their employees access to their workplace or parking facilities. Companies have realized that mobile access offers them secure system management, simplicity, and financial benefits versus brass keys or RFID cards.

Brass keys issued to the entire workforce are not a cost-effective way to manage building access because a lost key means potentially re-keying the whole building (a very costly and complicated process!). Besides, the continuous monitoring and issuing of keys for individuals can be a security management nightmare.

RFID cards offer an advantage over brass keys but still have multiple challenges as the single-source access system for your building. Lost access cards can, and should, be rendered inoperable by having access rights deleted in the system and a new card quickly issued to the individual.

However, a lost RFID card may not be recognized as lost or stolen until the owner needs to use the card to access a building. It may take days for the card owner to realize their RFID card is not in their possession.

This is not true when a person loses their smartphone because the panic is nearly always immediate!

As mentioned earlier, because the mobile phone is a critical piece of everyone's daily life, a missing phone quickly causes significant concern. However, it is important to establish that a lost or stolen phone does not automatically allow unauthorized individuals to use the mobile access system inside of that phone or to access company or personal information.

WHAT ACTUALLY HAPPENS TO THE MOBILE ACCESS IF A MOBILE PHONE IS STOLEN OR LOST?

It's proven through industry research that people are much more diligent about protecting their mobile phone at all times versus an RFID card or brass key. Think for a moment how someone uses a mobile phone and how it is never very far from the owner at any moment of the day. If the mobile phone is missing, most people know it quickly.

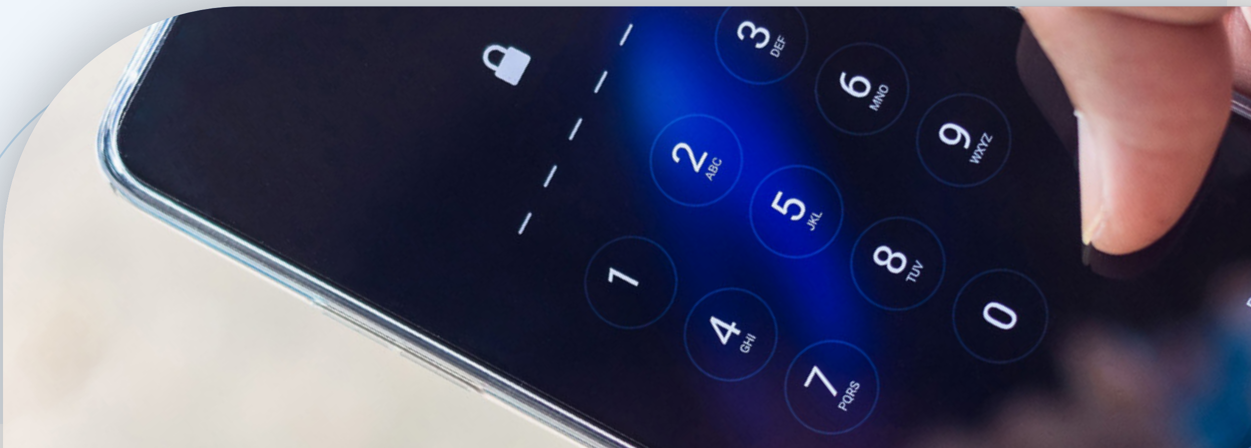
When a person realizes that their mobile phone has been stolen or lost. What do they do? First of all, there is no need to panic as the mobile access and personal information is not accessible to the person who may now possess the phone.

The owner may be concerned that an unauthorized person can now use their phone to access their company's buildings. The first thing to do is contact the system administrator, who will immediately suspend the mobile access credential.

Additionally, most users protect their phones with passwords, PINs, or biometrics that can protect the credential on the phone from being used by a thief or opportunist. Even with BYOD (Bring Your Own Device) phones, the administrator can control whether a mobile credential can be used when the phone is locked or unlocked.

By revoking the access credential even if the person has an unlocked phone, the suspended credential will not be recognized as valid by the access control solution. The suspension of the mobile access credential on the mobile phone is immediate and much faster than managing an RFID card or brass key.

Once the person replaces the lost smartphone with a new smartphone, the mobile access app can easily be downloaded and the company's system administrator can immediately re-issue a credential.



And though a mobile phone may not be with you for accessing a building, in many cases, companies install a backup solution for employees to gain building access. Regardless of the credential solution, the back-up system may include a complementary credential (an RFID card, master key, or admin password) or even a physical person, such as a security guard.

Another common strategy and one that aligns nicely with mobile access is the use of a Personal Identity Number (PIN). The PIN can be used as an additional alternative solution to access the building. So, if a mobile phone is lost, stolen or the phone battery dies, company employees can use the alternate method, if authorized, to access. The mobile phone is really no different from a key or an RFID card in this respect.

Though users are generally passionate about maintaining the charge in their devices, this type of back-up solution is definitely something to consider. I also recommend that companies adopt a strategy of requiring phones to be unlocked for mobile access to work. This reduces convenience, as the app must be opened for it to work, but it increases security. The decision will be governed by the risk of unauthorized access balanced against the likelihood of phones being lost or stolen.

It's important to emphasize that companies and individuals should generally have a backup procedure for accessing the building, for example with traditional mechanical lock and key, keypad (PIN) or RFID card. This is good practice regardless of the primary method of access control.

LOSING THE SMARTPHONE ISN'T THE END OF MOBILE ACCESS

As you read earlier, losing the smartphone or having it stolen does not mean the user won't be able to access a company building or control the information on the smartphone.

If the company and employees follow a few simple rules for managing mobile access on the smartphones, the pain of losing the smartphone will be minimized. Users won't be giving the "bad guys" full access to their company's buildings or their personal information contained in the smartphone.

Installing a mobile access system that balances security, privacy, and convenience, while offering important options and choices such as multi-factor authentication and enterprise-wide credential rules are vital to maintaining a mobile access control system that remains secure, easy to manage and that is sustainable.

In our next chapter, we will talk about the operational procedures mobile access companies install to ensure that an individual's private information is totally protected and eliminate concerns about protecting personal information on the smartphone.

Chapter 2: Personal Data

In the previous section, we shared information about the benefits of mobile access control, i.e. using your smartphone to open doors and compared this to traditional access control methods. We also detailed the steps an individual and organization can take to restore their access when a smartphone is lost or stolen.

In this chapter, we'll focus on discussing how access control suppliers securely deliver mobile access applications to smartphones. Allowing secure access to company facilities while maintaining the privacy of the owner's personal information.

Before we begin, let's summarize some of the key points from the last section.

Smartphones have become the preferred choice for secure access control substituting for traditional brass keys and RFID credentials to provide employees with access to company buildings.

Mobile access offers significant benefits over traditional access tools because it's easy to adjust and it will typically cost less to manage.

Mobile access gives employees permission to enter physical and digital places by using their smartphone as an approved credential. The mobile phone uses Near Field Communications (NFC) or Bluetooth of Low Energy Consumption (BLE) capabilities to authenticate permission for the owner to use the access control system.

When an employee's smartphone is lost or stolen, the affected employee can contact the company's system administrator to immediately revoke the employee's access control credential protecting unauthorized access to company properties.

It's recommended companies install two-step authentication to ensure all smartphones with mobile access cannot be used by unauthorized people. For example, requiring a Personal identification number (PIN) be used before the mobile access application is available.

IS PERSONAL INFORMATION AT RISK WHEN USING MOBILE ACCESS?

Previously we talked about what you need to do if your smartphone is lost or stolen. Now let's discuss how companies like HID Global provide a secure mobile access application for your phone.

Companies concerned about the vulnerability of their mobile access system may be concerned about mobile credentials being used in the event a smartphone is lost or stolen. An important mitigation for this risk is to use an enterprise-wide policy that requires users to unlock their device and open the app before the credential can be used. For most devices this means the user will need to use a PIN or biometric to open the phone, thereby much reducing the chance that an unauthorized person is using the device.

This type of access control enforcement feature can, and should, be used for Bring Your Own Device (BYOD) employees if there's a higher degree of security is required. It works hand-in-hand with corporate policies to provide a consistent experience and to manage risk. Employees bringing their own phones into the workplace must embrace the same rules of protection.

Companies requiring the enterprise enforcement feature ensure the mobile access system for the company is better protected by greatly limiting the unauthorized use of employee's phones.

We understand there may be reluctance by an employee to install a corporate app on their phone. This can be because they fear that the company will be monitoring them, and they wish to protect their privacy. For example, some employees may ask why "location services" need to be enabled on the mobile app. They must understand that this is to allow easy acquisition of the Bluetooth signal so that the best phone performance can be achieved.

We should note that, as many of you may know, Apple offers a unique feature for its iPhone customers. If an individual owns an iPhone, there is a feature that allows owners to use their device to locate their phone if it is lost or stolen.

One component of this feature is the ability to remotely wipe app data, which when activated will delete the mobile access credential. This works even if the phone is off, or appears to be dead.

At all times, world-class access control suppliers are doing their very best to protect your company's access control system and your personal information.

Credible suppliers providing mobile access apps are very sensitive to protecting all personal information that is stored in their platform. Make sure your chosen supplier has a publicly available Privacy Policy. These types of policy detail what limited information is collected and why, and how it is protected and/or anonymized.

Look for compliance with regional security policies and legislation. For example, in Europe, the General Data Protection Regulation (GDPR) is a very powerful and important piece of legislation that covers the right to individual privacy for all citizens.

Mobile access companies must commit to being focused and transparent about the information that is collected on behalf of the individual. They proactively let their customers know what data they collect and what data they do not collect.

These companies can be trusted resources for companies to partner with in developing a mobile access control policy and mitigating mobile access issues when they happen.

WHAT ARE THE BENEFITS OF A MOBILE ACCESS PARTNERSHIP?

Ultimately, the individual phone owner has a responsibility to protect both company access and personal information on the smartphone. Once a smartphone is lost or stolen, the individual owner is accountable for notifying the company's system administrator that the phone is missing. This is true for brass keys and traditional access control cards, fobs, or tokens.

The administrator, using the tools in their systems will prevent unauthorized access to the company buildings and systems while protecting personal and company data.

Mobile access providers must also share the load; ensuring the mobile access platform enables workflows and policies to support the customer and all of their mobile access users.

You can rely on global access control suppliers to be at your side to protect company access and your employee's personal data. They are your partners to help you resolve any access control system challenges. This relationship of a collaborative strategy works for everyone.

Chapter 3: Reduced Performance

In the past chapter, we shared information about the benefits of partnering with a reliable mobile access control systems provider to protect your company's buildings, employees and assets. These benefits are numerous and include:

- State-of-the-art technology with experts available to customize the system to meet your requirements.
- Compliance with international individual privacy legislation like the General Data Protection Regulation (GDPR) in Europe that protects individuals' personal information.
- A wide range of features to suit the needs of your organization, such as the Enterprise Policy Enforcement setting that can enforce two-step authentication providing flexible security design based on specific operational risks.

This section will address common misconceptions regarding the impact of the mobile access control system apps on mobile phone performance and battery life. Individuals who utilize an app installed on their mobile phones to interface with their workplace physical access control system, have two primary concerns. First, that this activity will require high levels of their mobile phone's memory or CPU that will negatively affect performance, and second, that their battery consumption may be significantly affected.

Let me address these concerns in two parts. First, let's talk about how the mobile app affects performance on your mobile phone. Second, I'll discuss the effect that mobile access has on a smartphone's battery life.

HOW DO MOBILE ACCESS CONTROL SYSTEM APPS AFFECT THE PERFORMANCE OF MY MOBILE PHONE?

First, the installed mobile access control system apps are designed to be small, fast and efficient. They require a relatively tiny amount of memory. There is also almost no loss of mobile phone performance when the mobile app is installed. The app works in the background and has practically no impact on other phone operations.

The mobile access control system app lies dormant until the user takes the device to a reader to gain access to a space. As I've stated, this action uses minimal memory, CPU and battery power to complete.

Consider that on a typical 64 GB iPhone, the app takes up just one fiftieth of one percent (0.0002) of the phone's storage. The credential itself is even smaller, with optimized code designed for use on smartcards and other forms of electronic devices. Remember, small, fast and efficient.

As a world-class mobile access control provider, HID Global works daily with thousands of customers to open tens of thousands of doors and entries in buildings and structures across many countries. Our mobile access control system app is continuously working to satisfy the secure access requirements of our customers and is designed to be efficient to minimize the impact on phone performance and processing time.

HOW DO MOBILE ACCESS CONTROL SYSTEM APPS AFFECT THE BATTERY LIFE OF MY MOBILE PHONE?

The installed mobile access control system app is designed to be energy efficient. It does not have the power requirements that a user may experience when streaming music or recording video. The mobile access control app is designed to use as little memory and processing power as possible. It is very efficient and has minimal impact on battery life.

For example, in one series of mobile app tests, we saw as low as one quarter of one percent (0.0025) battery level consumption during a two-hour test where the phone was used to access a door once every minute.

Consequently, you can use the application hundreds of times without seeing a significant loss of battery power. Consumers do not have to worry that using mobile access control systems will drain the life of their phone battery, or affect device performance in any way.

Let's compare the efficiency of the HID mobile access control system app to that of a high-end Ferrari. We've installed a mobile access control app system that is efficient, agile and paired with a smartcard with similar characteristics. It races through the operating system with controlled efficiency to deliver super-fast results. We won't burden the mobile app system's efficiency by asking it to drive a clunky Sport Utility Vehicle (SUV). We understand that our customers like the Ferrari much better.

Takeaways

After reading our whitepaper we hope we have improved your understanding of the many benefits that can be realized when mobile access is deployed. Furthermore, we trust that any fears you may have had about the vulnerability of the information residing on a mobile phone are allayed. We would like to highlight some key takeaways from the information presented in the previous pages.

Mobile access can be easily managed, with the service working seamlessly with the access control software to provide a wide range of functionality.

Enabling PIN or biometric authentication on the phone or device, e.g. facial recognition, protects the credential on the mobile phone from thieves and other nefarious actors.

Mobile access technology uses very little battery power, nor does it require much memory or processing power. Users do not have to worry about the system draining their battery.

Quality, credible mobile access providers are viable partners to help you implement a secure mobile access system to meet the needs of your organization.

As you have read, many of the fears regarding mobile access are unfounded. Mobile access technology provides the features that protect your company's information and that of the user, and the necessary controls to manage the complexity of today's security systems. It can be integrated with existing infrastructure and provides a single system with a wide range of capability, beyond simply opening doors.

In today's complex world, with security threats waiting around every corner, mobile access simplifies system management, empowering security personnel with a powerful and flexible set of tools. Mobile access allows you to create a system that balances security, privacy protection and convenience.

It delivers tremendous versatility, making the mobile phone a credential that can be used enterprise-wide for a diverse range of access applications. As a security professional it certainly warrants a thorough review. We believe the many benefits could help almost all modern organizations. Best of all, it positions your company or institution today with leading edge technology that can evolve as you develop and grow.

HID
hidglobal.com

North America: +1 512 776 9000 | Toll Free: 1 800 237 7769
Europe, Middle East, Africa: +44 1440 714 850
Asia Pacific: +852 3160 9800 | Latin America: +52 (55) 9171-1108
For more global phone numbers click here

2021-06-10-pacs-mobile-access-misconception-wp-en PLT-06045
Part of ASSA ABLOY