



- ▶ EDITOR'S COMMENTS.... 1
- ▶ BEYOND THE COMBINATION LOCK..... 2
- ▶ ACCESS CONTROL TAKES TO THE WEB ..... 5
- ▶ HANDS UP..... 7
- ▶ TIPS TO KEEP YOUR TEEN SAFE ON MYSPACE ..... 8

○ ISSUE 1 | ○ VOLUME 3 | ○ April 2007

# Security Solutions

ADDRESSING THE NEEDS AND SECURING THE FUTURE.

## Helping secure your world

An electronics revolution has overtaken the world. In every sphere of life electronic devices are in use helping to make tasks easier. The security field is no exception and electronic security devices are proliferating with the promise of enhanced protection and audit trails to provide records of activities. This growth of electronics is being combined with the use of the Internet to allow management of remote sites.

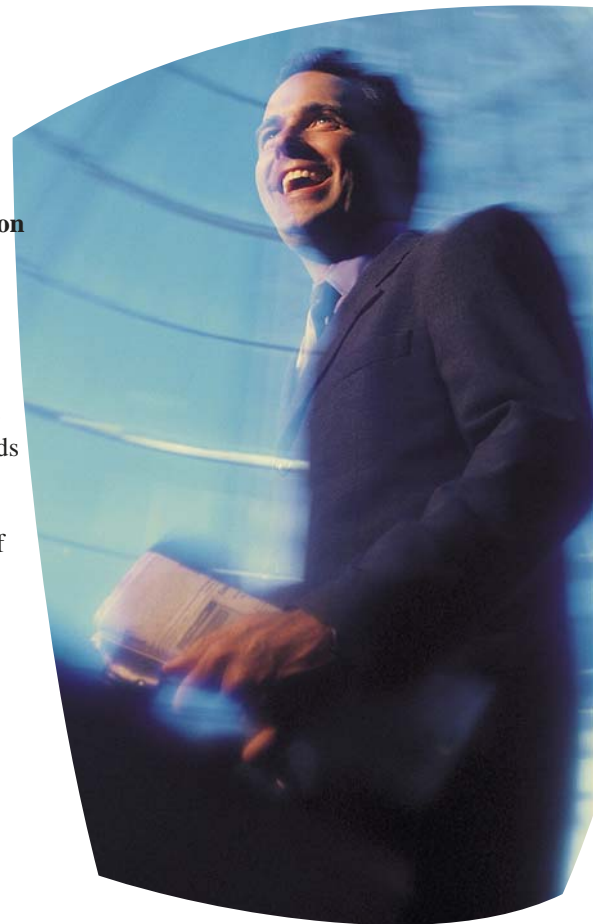
Even the area of cash handling has benefited from the electronics revolution. Accordingly in this the third issue of **SECURITY SOLUTIONS**, we provide an article that points the way **Beyond the Combination Lock**. The possibilities of using the Internet for access control are addressed in the article, **Access Control takes to the Web**.

While the Internet has increased our ability to communicate and MySpace and other social networking web sites have experience explosive growth, there are dangers on the Net particularly for those who are less suspicious. The

article **Tips to keep your Teens safe on MySpace** provides advice on the safe use of social networking web sites.

If any additional persons in your organisation would like to receive this email newsletter, just send an email to [newsletter@assl.com](mailto:newsletter@assl.com) with the words "Subscribe Newsletter" in the subject line and the email address, name and organisation in the body. To opt out of the mailing list send an email with the words "Unsubscribe Newsletter".

Brian Ramsey  
Editor



# Beyond the Combination Lock

By:  
DICK MOE



Electronic safe locking technology provides a simple solution to complex loss prevention problems.

Using electronics to control access is standard practice for most loss prevention professionals. But while many of us are familiar with access control systems for doors, there is another critical security niche that has been revolutionized by electronics: access control for cash containers.

Loss prevention managers have begun to use electronic safe locking systems to provide simple solutions to complex loss prevention problems.

Traditional safe locks have inherent weaknesses. Electronic safe locks have become popular, in part, because of problems with traditional combination locks, the most apparent of which is operation. With traditional safe locks, users are forced to memorize a specific pattern and a random combination; they must also be precise in their operation, stopping on each number exactly. If any of these processes are not followed with

precision, users are forced to start the entire operation over again. This can be a difficult process to teach and a frustrating operation for many people, particularly if under duress during a robbery.

Traditional safe locks pose service problems as well. The technology for traditional mechanical safe locks was developed during the Civil War era. At that time, the design provided security and reliability. But in today's fast-paced world, with the need to open a container multiple times each day and to change combinations on a regular basis, the owner of a traditional safe lock is forced to rely on outside technicians for maintenance and support.

The final problem with traditional safe locks is that all they do is lock the safe. They are unable to provide management controls, to report opening and closing, or to assist the user or owner of the safe in any way.

Electronic safe locks offer distinct advantages. The first step to determining whether you need an electronic safe lock, and if so, what level of lock your application requires, is to evaluate the lock's components. Most electronic safe locks incorporate numerous features, and all of them provide advantages that are lacking in traditional mechanical safe locks.

Electronic safe locks generally fall into three categories: \* At the low end, electronic safe locks provide only basic features such as PIN access and user-changeable PINs

In the middle of the market, there are locks that offer multiple-user capabilities, programmable time delays and electronic key access.

\* At the high end, locks include time lock, time windows, multiple door control and audit trail capabilities.

Advanced electronic safe locks use both PIN entry keypads and state-of-the-art electronic "keys" that can store and transmit electronic data. These locks eliminate the tedious chore of opening a safe by allowing the operator to use a PIN on a keypad and an electronic key

to gain quick and easy access to the container.

Combining electronic keys with PIN entry also increases security. With a PIN only, an authorized user could share a PIN with an unauthorized user and claim their number was "spied" without their knowledge. With key-only access, a key could be loaned to an unauthorized user and the key holder could claim the key had been lost or stolen. By using dual verification devices, authorized users become legally liable if both their key and PIN are used to access the safe.

Electronic safe locks with dual verification devices provide unprecedented levels of control and security, including: \* Audit trail. Electronic safe locks are actually microprocessor-based access control systems. Many of these locks are capable of providing a detailed and lengthy audit trail record of all transactions. Audit trails can be viewed on local LED display panels, printed on a local serial printer, or downloaded from the lock and printed on a remote printer attached to a PC.

\* Electronic time delay. Even the most basic electronic safe locks usually include a time-delay period or feature the ability to program a time-delay period. This eliminates the need for separate time-delay devices to be installed on the safe.

\* Time lock/time window. Many of the new electronic safe locks also provide time lock and time window capabilities, which allow the lock to be programmed to allow specific users access at specific times. This prevents authorized users from accessing the safe during restricted access periods. The access rights to these locks can be customized to suit the needs of most operations. Time locks allow all authorized users to access the safe only during specific hours. Time windows allow access rights to be programmed for different users at different times.

\* Door-open alarms and auto-detent. Electronic safe locks that feature door-open alarms can be coupled with auto-detent systems to increase security. If

the safe door is left open for a specified amount of time, a local alarm sounds indicating that the door needs to be closed. When the safe door is closed, the auto-detent system automatically throws the bolts, securing the safe.

Electronic safe locks mitigate risks associated with the human factor. The "human factor" often increases security risk. Electronic safe locks mitigate the human factor in safe operations by replacing many formerly required procedures and policies. Following are loss prevention problems posed by the human factor and solutions provided by electronic lock technology.

**Problem 1.** Employees often ignore cash-handling policies. Although every retail business operates a little differently, most that handle cash are confronted with similar control and protection problems. To effectively deal with these problems, many loss prevention managers have implemented a variety of cash-handling procedures, which typically form a system of checks and balances to help reduce loss. The problem with these policies is that they are often forgotten or ignored in real world, day-to-day operations. An electronic safe locking system can simplify and in many cases eliminate the need for such policies by providing real tools that solve the security problems at hand.

**Case in point:** Jewelry store finds that "day lock" offers little or no security. During a recent spot check, the regional loss prevention manager of a national chain of mall-based jewelry stores was surprised to find that one of the under-counter inventory safes was unlocked. The store manager reported that the safe had not been open in three days - or so she thought. Finally, after doing an inventory of the contents, they found nothing was missing, but realized the safe had been left in "day lock" since the last time it was used.

Day lock is typically used to allow quick access to the interior of a safe during working hours. Unfortunately, the use of day lock substantially increases the potential for internal theft because of the ready access to the safe's interior. Day lock procedures require

employees to spin the dial and lock the safe before leaving each night. All too often these requirements are ignored or forgotten.

**Solution:** PIN entry access increases security by eliminating the need for day lock. Even the most basic electronic safe locks offer the convenience of allowing the user to enter a PIN on a keypad to gain access to a safe. This ease of use provides far more than just convenience; PIN entry access increases security. By making it simple for employees to use the locking system, there is no longer a need to leave the safe unsecured in a day lock condition. Easy access also promotes regular use of the safe, reducing the chance that employees will be tempted to overstock a cash drawer to save time later. With easy PIN entry access, a door-open alarm, and a self-locking auto-detent system, a safe is more likely to be closed and fully locked at all times and therefore is more secure.

**Problem 2.** Employees try to save money the wrong way. To maximize efficiency, many companies have implemented compensation programs that encourage store personnel to cut costs and save money whenever possible. While this is a sound fiscal management policy, most front-line personnel are not equipped to assess the risks associated with eliminating security processes.

**Case in point:** Fast-food chain finds managers reluctant to change safe combinations. One fast-food chain found that when it started compensating managers based on store profitability, the managers were tempted to cut costs by eliminating what they perceived as "non-essential" expenses. Despite a specific security policy about safe combination changes when user turnover occurred, some managers ignored the policy and did not make timely combination changes to save money and increase their bonus.

By leaving the safe combinations unchanged, the store managers significantly increased the risk of loss. Most loss prevention experts agree that the longer a combination is in use, the more likely it is that unauthorized users

will learn the combination and gain access to the safe. In addition to the increased risk of internal loss, burglary risk is significantly magnified.

**Solution:** Electronic safe locks provide individual changeable PIN access codes. Possibly the most significant reason electronic safe locks have become so popular is the user-changeable access code feature. By allowing users to quickly and easily change individual access codes, store personnel can maintain security policies while not impacting store profitability. Often, the cost savings associated with user-changeable access codes can justify the capital investment of an electronic safe lock within the first year of operation.

**Problem 3.** When losses occur, no one is accountable. It goes against the grain of most loss prevention professionals to allow criminals to go about their business without detection or punishment. It is even more frustrating when you know who is stealing and yet it is impossible to record and prosecute the crime. It is an unfortunate reality that many mysterious losses must be written off without the slightest chance of recovery.



**Case in point:** An auto-parts chain concedes that investigating small losses is futile. The loss prevention director of a regional chain of auto-parts stores reported that they don't even bother to investigate "mysterious" losses of \$100 or less out of their safes. He reports that the cost of an investigation is far more than the loss and that unless the losses are recurring, it is not even feasible to pursue an investigation.

He also notes that when losses mount or become recurring, the resulting investigations often lead to suspects, but many times an audit trail cannot be

obtained that will make the suspect criminally accountable for the loss. The problem can be further exacerbated if the investigation focuses on an innocent party and wrongful-termination lawsuits ensue.

**Solution:** Dual-user features and audit trails make individuals accountable. It is traditional in the banking industry to install two individual safe locks on a vault. This arrangement requires that two individual users be present every time the vault is opened, significantly reducing the chance of loss from one dishonest employee. But it is often impractical to use two individual safe locks on a small cash container, so many electronic safe locks have a dual-user feature programmed into the electronics. A dual-user lock requires that two separate codes be entered to access the lock. This feature is particularly effective in controlling access to larger cash amounts such as those stored in drop containers.

A more effective way to increase employee accountability is to use an electronic safe lock that maintains an audit trail record. While locks capable of providing an audit trail are usually slightly more expensive, the information they provide can significantly reduce the cost of investigations and prosecutions.

Some electronic safe locks, such as those manufactured by NKL and the Vindicator locks manufactured by Mas-Hamilton, allow users to view audit trail information on an LED panel as well as download or print the information. This record of activity can tell who accessed the lock and when, as well as when the safe was closed and locked. These locks can also report on other events such as attempted accesses, combination changes and open-door alarms. The loss prevention benefits of an audit trail system go far beyond a record of events. Many loss prevention managers have reported a significant reduction in mysterious losses just because safe users know the lock will record and report their activity.

**Problem 4.** Robbery exposes personnel to extreme risks. **Case in point:** The worst part of robbery risk is the

potential of unacceptable and costly loss of human life. In fact, Department of Labor statistics show that armed robbery is one of the leading causes of workplace deaths. By reducing the chance of robbery, you can increase workplace safety and reduce the potential costs and trauma associated with workplace violence.



**Solution:** Convenience stores reduce robbery risk by reducing cash on hand. The regional loss prevention director of a convenience store chain reported that the risk of robbery could be greatly reduced by keeping the amount of cash available on hand to a minimum. He added that it was critical to publicize this information with window and in-store signs.

In addition to these changes, the chain started replacing their old safes with new containers. The new safes featured electronic safe locks with an electronic time delay and a duress alarm system tied into their alarm provider's central station.

Time delays have proven to be quite effective in discouraging armed robberies. If the robber is given a small amount of money from a register, he or she will usually flee, unwilling to wait for a time delay on the safe to count down. The time delay offered by electronic safe locks is precise, and some models even display the countdown on an LED panel, further proving to the robber that the safe will not open until the delay period has expired.

In addition to time delays, some electronic safe locks feature an alarm

interface that allows the user to open the safe and at the same time send a duress signal through the alarm system to a central station. By integrating the safe lock into the alarm system, the manager can comply with the robber's demands, increasing life safety, and also signal authorities, reducing the risk of loss (see Illustration 2).

**Problem 5.** The budget does not allow for an electronic safe lock upgrade. A significant part of any security manager's job is to maintain the balance between equipment and personnel investments versus real returns in cost savings and reduced loss. In some cases, as a loss prevention professional, it is as difficult to "manage" upper management as it is to do the job for which you were hired.

**Case in point:** The loss prevention director of a national restaurant chain was confronted with selling an electronic safe lock upgrade to upper management.

**Solution:** After careful analysis of operations, some hidden costs were discovered that could be significantly reduced by installing a sophisticated electronic safe lock on a multiple-compartment container.

The restaurant had been using a two-compartment container that featured a drop slot for employee deposits. The drop container had a dual-key locking system. The store manager had one key; the armored car service maintained the other. As the servers cashed out each day, they recorded their totals on a drop log and deposited an envelope into the safe with their receipts. Each day when the armored car arrived, the compartment was opened, and the manager would reconcile the drop log with the number of envelopes in a tightly compressed time frame that resulted in periodic errors and losses. The armored car service would then deliver the deposits to the bank. The bank would reconcile the envelopes, charging \$1-\$1.50 a piece, and then complete the transaction. With 10-15 envelopes a day, bank charges were almost \$7,500 per year per store. Reduction of the number of bank

charges resulted in the safe more than paying for itself in less than a year.

The loss prevention director determined that if the store managers reconciled the banking before the armored car pickup, there would be fewer errors, less confusion and significant banking cost savings. However, he also recognized that allowing their managers unrestricted access to the drop compartment would increase the risk of robbery and internal theft.

The solution was an electronic safe lock that controlled multiple doors on the container and featured a time-lock system. The time lock allowed the managers to access the compartment with a 10-minute delay to reconcile the deposit during a two-hour window before the armored car pickup. When the armored car driver arrived, consecutive presentation of the manager's electronic key and the driver's electronic key provided immediate access to the drop container. The result was quick removal of the consolidated deposit and the driver's expedient departure.

The compartment was open a limited amount of time each day prior to opening for business, but the result was an almost 95 percent savings in bank costs. Upper management was presented with a plan for new safes with electronic safe locks that would pay for itself in real cost savings in about six months to a year.



Another way to reduce the cost of upgrading to electronic safe locks is to retrofit the locks onto existing safes. Most electronic safe locks use the same footprint as mechanical locks and can

be easily retrofitted to replace dial-type locks. Retrofitting can usually be done on-site.

The electronic lock revolution is here. Electronic safe locks are revolutionizing many of the processes that businesses have traditionally used to manage cash containers. The features these systems provide allow managers to control costs, reduce loss and reduce the threat of robbery by automating many loss prevention procedures. Training staff to follow policies and to properly service and maintain the equipment are two of the most difficult challenges faced by management. But if properly implemented, an electronic safe locking system will secure cash containers and eliminate many of the headaches associated with managing the flow of money through retail locations.

Reprinted from:  
**Access Control & Security  
Systems**  
July 1998

## Access Control Takes to the Web

Web-enabled systems find their niche in the right facilities

By [Chris Wetzel](#)

Just as the Internet has changed the way we shop, entertain and inform ourselves, it has transformed the manner in which we protect and secure our buildings, critical facilities and infrastructure. With the Internet, security directors and corporate and government executives can view and control video surveillance systems from almost anywhere in the world. The same is true for access control systems.

Using Web-enabled or Web-hosted applications, authorized system users can add or delete cards and change access control and alarm schedules—all from remote locations.

Web-enabled and Web-hosted access control systems can offer you tremendous advantages in the

right circumstances. However, as with any technology, this technology may not be the best choice for every situation. I asked several of the country's leading systems integrators to share their opinions and experiences, and those of their customers, in dealing with these systems.

### What Is Web-Enabled Access Control?

First, a couple of definitions are in order. In the Access Control Trends & Technology supplement published with Security Technology & Design's June 2006 issue, Christie Walters wrote a backgrounder on the different types of Web services available for access control. In this article we'll focus on two of the categories Ms. Walters discussed: Web-enabled and Web-hosted applications.

Web-enabled applications use on-site software and a server that can be remotely accessed with a Web browser and password. The user, or the security department, is responsible for maintenance, software updates and security upgrades. In some cases, adding the software—which controls the system's functions—to the controller eliminates the need for a separate server. Remote system control is available through dial-up or network configurations such as a LAN/WAN or VPN. Another option available to corporations is the use of multiprotocol label switching (MPLS) networks. MPLS gives network operators a great deal of flexibility to divert and route traffic around link failures, congestion and bottlenecks. MPLS networks are private and lend a known and comfortable network design model for corporate implementation.

The choices among Web-enabled systems are becoming more plentiful as manufacturers rush to capture their share of the market. Some of the systems my colleagues and I have installed recently include the NetBox from S2 Security, the Access Easy Controller from Bosch Security Systems and Integral Technologies' Intelli-M.

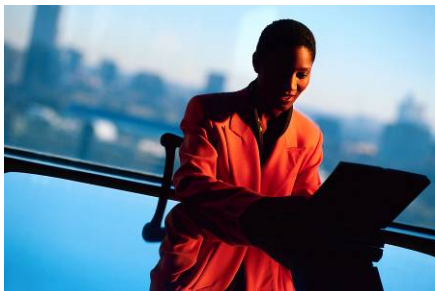
In the Web-hosted model, an application service provider

(ASP)—usually a systems integrator or equipment manufacturer—hosts the server, software and user databases in its own data center. The ASP also provides system redundancy in case of equipment failure. Authorized security staff and executives can access the system via a browser and password. This type of service requires no use of your corporate bandwidth and no network configuration between multiple sites.

### **The Fit for Small- to Mid-Size Facilities**

Many of the integrators I spoke with agreed that Web-enabled and Web-hosted access control systems seem best suited to small- to medium-sized companies with a need for some level of security—traditional intrusion security integrating access control for a few doors.

Potential problems may occur as more people are authorized to remotely view the system reports or are permitted to add a door or delete a person's access card—all of which is likely as a system is expanded to cover 25, 50, 100 or even more sites. The administration of the system database is best left in the hands of a few knowledgeable professionals within the corporation. Also, implementing changes over a handful of Web-enabled boxes is relatively easy, but can become a major challenge in larger numbers.



Multi-tenant facilities may provide one of the more ideal situations for a Web-enabled access control system. Such a system can be partitioned to give the building manager control over common areas such as lobbies, elevator banks, parking garages and cafeterias. At the same time, the

building tenants can use the Web to control access to their own spaces.

According to Jim Coleman, president of Atlanta-based Operational Security Systems, these systems offer several advantages to the end user. "Out of the box, these Web-enabled systems are pretty easy to get going," he said. "There is no need for patches or the need to worry about viruses or software updates. The simplicity may entice more people to use these systems."

But Bill Savage, president of Security Control Systems, warned that simplicity could have a downside for a system user who is relatively new to access control. "Just because you have a simple potential for a product, that doesn't mean that every application is going to be simple to execute," Savage said. "People that have a history of buying because products are simple and inexpensive get involved and then cannot execute the full range of applications. And that generally turns into disaster."

### **What About Enterprises?**

Web-enabled access systems can also appeal to the enterprise user under the right set of circumstances. A corporation with widely dispersed locations may not want to be dependent upon a large head-end system with a single, centralized control center or security operations center. Corporate executives also may give a high degree of independence to remote site managers and expect them to handle the day-to-day administration of the access system. A Web-enabled system still allows the headquarters-based security director to keep tabs on outlying operations or take control of the system if necessary.

Based on our experience, however, these systems may not be ideal for a Fortune 500 company doing business globally, although some are using this model to provide access control to multiple remote office locations.

"I think they are going to have to get a few systems of substance under their belts and know how they work and what their limitations are before we can roll these Web-based systems out on a large-scale basis to the big corporations," said Coleman. "Database synchronization and scalability issues will have to be overcome." Also, Web-enabled systems based on thin clients currently are not as robust in feature offerings as the more traditional client-server systems. But Coleman said that feature gap could narrow as technology develops.

### **Security Concerns**

Another issue that users should keep in mind concerning Web-enabled and Web-hosted systems is security. Because these systems put sensitive data on the network, they require diligent network security and rights management. Without this, outside hackers could maliciously attack an access system to gain entry into a critical operations area, or employees could give themselves access to restricted areas or mask alarms to hide transgressions.

Appropriate security measures can help guard a Web-enabled system against attack. "These systems can be as secure as you make them," said Steve Morefield, president of Firstline Security. "If you enable the appropriate safeguards and know how to implement them, you can make these systems as safe as any other Internet-based system."

### **Considering the ASP Model**

The integrators I spoke with said their customers have not yet been attracted in large numbers to the ASP—or Web-hosted access control—model. As mentioned above, this service does not tie up corporate bandwidth or require an IT team on staff, but the cost savings of it is offset by recurring monthly fees. Savage commented that he's seeing operational costs driving some users away from the hosted model.

Morefield has also seen a shift away from ASPs by some of his major office building customers.

While the systems work in providing service to individual tenants, the cost is being passed along to the leaseholders. "The ASP solution may work fine when rents are going up and companies are paying whatever it takes to move into a property that they like," he said. "But in today's economy, the idea of not keeping an eye on expenses is gone."

Without a doubt, the Web-enabled and Web-hosted access control systems have opened new markets, bringing customers into the market for the first time. And these systems have a place in providing better security in the right situations. But before making the jump, remember that proper product selection is critical. The best way to make that choice is to count on the expertise of a systems integrator with experience in this area of security.

Reprinted from:  
Security Technology & Design  
Feb 2007

## Hands Up

By Tom Barry ·

### Security technology protecting banks has taken big steps

IN most old Western movies as well as new ones, like the remake of "Ocean's Eleven," bank robbers are usually successful. That Hollywood success rate has changed in the real world.

In the movies, outlaws simply go to the home of a bank president take their family hostage while the outlaw's sidekick opens the safe. The bandits get away successfully stealing the loot.

Time locks, which are still in use today, are designed to easily and successfully thwart this type of crime. The technology limits the time of which a bank vault can remain open. Modern, electronic time lock technology allows users to program intricate time lock schedules.

Today, three out of four bank robbers are caught within 18 months of their crime, according to Steven Kodak, an FBI special agent and spokesman.



### Handy Technology

FBI and local law enforcement efforts are aided by financial institutions using current technological advancements, including enhanced surveillance cameras, state-of-the-art recording units, professional prevention equipment, along with specialized training and practices by bank employees.

"Incorporating biometrics is the latest evolution in banking security with safe deposit boxes," said Brian Costley, a 36-year veteran employee and certified Master safe technician at Sargent and Greenleaf, a manufacturer of locking technology and a Stanley Security Solutions company.

Sargent and Greenleaf recently introduced the TouchVault™ Biometric Safe Deposit System. It is designed to decrease intensive labor costs by providing unescorted access and control, eliminating the current use of keys, which remains predominant throughout the industry.

"Fingerprints employ one of the highest levels of authentication since they cannot be lost, stolen or shared," Costley said. "And this respective system provides pertinent information in recording a comprehensive audit trail, which is provided by the reporting software."

Bank customers are provided a unique PIN and register their own fingerprint in

the system when signing up for a safe deposit box.

"Our technology uses an 'active capacitive' sensor technology in our biometric pad," Costley said. "This active capacitive technology reacts to the presence of live skin and creates a mathematical template of a finger based upon the ridges and valleys found in the human finger. To boost security, this template is stored and encrypted to prevent possible reconstruction of the fingerprint."

The customer accesses the system by going to the terminal, entering their PIN and placing their finger onto the reader, where it is authenticated. The customer then pulls an encrypted, doorknob-like device from the terminal which flashes green when ready. The customer inserts the knob into their safe deposit box, rotates it and opens the box. Upon closing the box, the customer removes the knob and returns the unit to the terminal.

The system is designed to prevent a customer from opening another safe deposit box. If attempting to open another box, the knob flashes red, the audit trail is documented and access is denied.

### Delay of Game

According to the FBI, in 2005, there were 6,019 commercial bank robberies in federally insured financial institutions across the nation. An FBI spokesman said most current bank robberies involve the use of notes being given to a bank teller.

One of the key deterrents of reducing attempted bank robberies and keeping customers and employees safe is buying time. The longer it takes to access the cash through procedures, the more time is provided for security and law enforcement to respond to foil the attempt, said Costley, who is only one of nine people to hold both Master locksmith and certified Master safe technician credentials in the country.

In 2005, the FBI noted 6,525 incidents occurred at the counter. There were 384 occurrences reported in the vault/safe area and 26 events at safe deposit areas.

Current technology can effectively reduce a significant amount of robberies in the teller area by incorporating a silent alarm. A bank employee can comply with the robbery request and access funds from a secure drawer or

teller locker.

The employee can use a slightly altered access code to immediately alert bank security of a robbery in progress while simultaneously notifying local law enforcement. Another deterrent is a locking mechanism equipped with a duress feature capable of sending a silent alarm signal, Costley said.

The American Bankers Association said bank robberies across the nation have fluctuated in the past 20 years and seem to go up when the economy heads in a downward trend. The money stolen in the average bank robbery currently averages approximately \$4,600, according to the FBI.

Despite all of the ongoing technological advancements, some things have not changed. Bankers can still be conservative when it comes to investing money to incorporate the latest and greatest technology. These significant advances often come with a stout price. Purchasing decisions are typically weighed after conducting a cost-benefit analysis.

As with every industry, security and safety of customers and employees is of utmost importance. However, to some, it is surprising that some banks and other industries continue to use low-tech surveillance equipment.

Low-tech cameras still being used are unable to capture distinguishing features of pertinent suspects. In most cases, frequently used and recycled recording tapes are unable to assist professional law enforcement in identifying potential suspects. Saving a few pennies can often be proven to be foolish when it comes to investing in reliable security.

#### **Passing the Test**

In 1923, UL first tested safes for burglary resistance. The first bank safe was tested by the organization in 1925. UL began product testing in 1894, said John Drengenberg, an engineer at UL for more than 40 years, sharing that the organization's label appears 19 billion times a year on products.

Chisels, wrenches, screwdrivers, power saws, cutting torches, crowbars, abrasive cutting wheels, jackhammers and even specified amounts of nitroglycerin are just a few of the tools Underwriters Laboratories technicians use during a safe attack.

"UL's safe attacks are conducted by a team of two technicians who examine

the blueprint and attempt to create an opening large enough to withdraw valuables, activate the locking mechanism so the door opens or to cut as many bolts from the door as necessary to pry it open before the time specified and the rating requirement expires," Drengenberg said.

UL also rates safes for fire resistance protection.

Currently, some financial institutions technology incorporates biometric recognition. Many banks use high-resolution surveillance while other authentication advances are used in its main locations and branches.

The ABA noted there are currently more than 80,000 branch banks throughout the country. Many of the locations are housed in supermarkets.

Much attention and financial resources at banks is being focused to enhance security efforts relating to Internet technology. The Internet is where the largest amount of fraud exists with an ever-growing volume of transactions. Another area of increased security interest and concern are the frequently used ATMs, within the bank premises and in remote locations.

#### **About the author**

##### Tom Barry

Tom Barry is a freelance writer based in Denver.

Reprinted from:

Security Products Magazine March 2007

## **Tips to Keep Your Teens (and Yourself) Safe on MySpace and Other Social Networking Sites**

By Audri and Jim Lanford

MySpace is one of the most popular social networking websites (with well over 100 million users). It lets users interact with a network of friends, and create personal profiles and blogs that include photos, music, audios and videos, as well as text.

In fact, MySpace is a great place for teens to communicate and interact with friends who live down the

block -- or across the world. They can share photos, music, messages... just about anything. And bands have used MySpace very successfully to communicate directly with fans.

Now, you don't have to be a teenager to obtain a MySpace account. Anybody with access to the Internet can sign up for this website.

Though most users are honest -- and many can be great Internet acquaintances -- there are enough shady users to warrant your concern as a parent, grandparent or teen.

Here are a few things that parents and teens can do to make MySpace, and any similar online meeting place, a safer environment.



#### **8 MySpace Safety Tips for Teens:**

1. Don't use your real name anywhere on the site. If you have a common first name -- Thomas, Samantha, or Chris -- use that and nothing more.

You can also pick a name that is meaningful to you without giving away personal details. For example, create a username that reflects your interest in music or writing, art or cars.

2. Fill out as little of your personal profile as possible. You don't have to tell everybody how old you are or where you live. Some people opt to give only their home state, or region in some cases, for safety reasons.

You also don't have to upload a photo of yourself. If you want to share some sort of image, you can find an avatar online that fits your personality.

A good rule of thumb is to not post

anything you don't want the whole world to know about.

3. Only let people on your "friends" list access your profile and other information. The less you reveal to strangers, the safer you'll be.

This will only work, though, if you use discretion when you add people to your friends list. If you reciprocate every friend request that you receive, you'll quickly lose control over profile access.

4. When you post a blog entry, proofread your writing a couple of times before you submit. After all, you don't want to give away too much personal information.

For example, Internet strangers don't need to know which school you attend, your kid brother's first name or where you go to church.

Also, don't post things that could embarrass you later. Even if you set your profile to "private," it could still come back to haunt you later.

5. Sometimes you'll receive comments or messages from people you don't know. If that happens, you should be careful if you decide to reply.

Dangerous people often have subtle ways of making you slip up and share the wrong information when you aren't on guard.

6. Remember that the moment you send a comment or message to somebody else, whatever you wrote is no longer in your control.

What you send to one person -- even a friend you know IRL ("in real life") -- can travel all over the Internet (and your school's hallways) without you even knowing this is happening.

If you have something to say that you don't want just anybody knowing, tell only your most trusted relatives and friends -- in person, not via the Internet, text messaging or email.

7. If another MySpace user is making you uncomfortable -- trying to send you photos that you don't want to see, or asking overly personal questions --

report that user to MySpace administrators.

Then add that user to your "ignore" list and forget all about him or her once you've contacted MySpace.

(Confronting that user won't solve anything. Some people actually feed on conflict: don't give the user the satisfaction of being sucked in.)

8. Recognize the employers often check MySpace before making job offers. So be careful about what you post on your MySpace pages.

Here are four things that parents should do:

1. Ask for access to your teen's MySpace page.

You need to decide on the rules about your access to your teen's page. If you feel you need/want access, then you should be able to hop on your computer and visit the page any time you want. If your child has "friends only" enabled, then your username should be on that list. This way, you can view your teen's page to make sure that he or she hasn't posted anything overly personal.

2. Depending on your teen's age and maturity level, you might want to restrict Internet access to times when you're around. Many parents keep the family computer in a common room so they can check on what their children are doing without having to barge into a bedroom.

3. Again, depending on your teen's age, you might want to know who is on your teen's list of friends. Some will be other teens that you already know: lassmates, teammates, youth group buddies or the like. Others will be strangers to you.

Knowing who these people are could help you keep your teen safe.

4. If your teen is supposed to meet an online-only friend in person, consider being there as well. If your teen is meeting another teen who lives in the area, they could probably still have a good time together even though boring old Mom or Dad is not too far away.

But if a predator shows up to meet with your teen and sees you there, he or she will leave as quickly as possible.

When you and your teen follow these tips -- and remember to communicate with each other every step of the way -- you'll be able to sleep well at night knowing that you're doing what you can to protect your son or daughter's virtual life.

Teaching your teen how to stay safe on MySpace (without being overly protective) is something you can -- and should -- do.

Internet ScamBusters (tm)  
The #1 Publication on Internet Fraud  
<http://www.scambusters.org>

Issue #219 February 21, 2007



**Amalgamated Security provides a full range of security services, which include:**  
Cash Services  
Electronic Security  
Access Control  
Data Storage  
Courier Services  
Guarding Services  
Alarm Monitoring  
Response Services

**If you are interested in having First Aid Training or Defensive Driving Training for your staff, contact Amalgamated Security**