

## Physical Security: The 4 Hot Trends

Physical security. In the financial services industry, especially, it has strong ties to logical security and protecting critical information assets.

In this overview, we will explore some of the key physical security trends from industry experts.

### 1. Fortifying the Branch

Unlike the trend of 10 years ago, institutions have come to understand the benefits and liabilities of openness. The open branch is going away in major cities, and bullet resistant glass above the teller line is coming back. The move away from open has a lot to do with what the tellers will be doing. If it is a transaction-based teller, to process deposits or withdrawals, the bullet resistant glass may be the way to go. The open branch approach helps when tellers are used to cross-sell other products.

### 2. Physical/Logical Convergence

Convergence of the physical and logical security within financial institutions is something that has been happening actively for the last five years. Though much work has been done in individual institutions, it remains ill-defined. The convergence is designed to provide two basic benefits: better level of security performance and lower price, lowering risk and improving an institution's abilities to prevent events. The ongoing trend of convergence isn't just in the national and regional institutions, but has reached down to the community bank level. The point where physical security has moved toward the IP backbone is here.

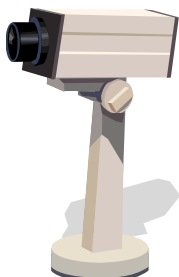
### 3. Increased Outsourcing

While many of the physical alarm systems at institutions have traditionally been connected to central reporting stations and law enforcement, institutions are also now increasingly looking toward outsourcing other portions of their security operations to offer cost efficiencies, including turning over some of the day to day monitoring and security operation jobs. Other services institutions are outsourcing include video management services. Remote video monitoring allows the institution the ability to have 24-7 coverage without the headcount of additional security personnel.

### 4. The Need for Greater Internal Controls

One area that needs more attention from both logical and physical security: the internal threat. The biggest losses are being seen through network attacks – internal or external. If a branch has been in existence for a long time, it should be examined and possibly upgraded to the newer technologies.

Source: [www.bankinfosecurity.com](http://www.bankinfosecurity.com)  
*Physical Security: The 4 Hot Trends*  
*Is it Time to Put Some Glass between You and Your Customers?*  
 August 24, 2009 - Linda McGlasson, Managing Editor



## SafeCatch: How to Deter Bank Robberies

"Don't be a hero."

For years, this is how banking institutions have responded to robberies - with an attitude of compliance.

But in Seattle, the local division of the FBI has turned this attitude on its heels with SafeCatch, a program designed to train bank employees to spot and deter potential robberies before they even occur.

Larry Carr, with the Seattle Division of the FBI, developed the SafeCatch concept in 2006 in response to an increase in robberies and a decrease in the quality of robber recognition. The concept is founded on three key principles:

- 1.) Staff vigilance and safe "friendly" action
- 2.) Clear suspect recognition
- 3.) Effective post-incident follow up



While the cost of implementing SafeCatch is surprisingly low compared to other security measures, it is proving to be highly effective. The FBI has trained staff at over 250 branches. These institutions are already seeing results. Anecdotally, through video surveillance, and based on the latest FBI statistics, SafeCatch robbery suppression is already proving highly effective. One of the reasons this program is being embraced by savvy institutions is that it delivers more than just enhanced security at a modest cost. It also can deliver a significantly heightened level of customer development, cross selling, share-of-wallet, and net-advocacy scores. Each customer entering a branch is addressed creating a customer-centric environment and providing opportunities for development. This same centrality causes staff to address unknown visitors in a friendly and non-threatening way. The same "Hi, my name is John Smith and I'm the manager. How can I be of help to you?" works with both a potential robber and new customers as well.

The success of the program has been further enhanced by the development of SafeCatch Architecture, developed to provide the retail environment required to fully support SafeCatch objectives while maximizing the productivity of each customer visit.

Together, SafeCatch and SafeCatch Architecture are proving to reduce robberies, increase apprehension of criminals and improving customer development and ROI at a very low cost.

Source: [www.bankinfosecurity.com](http://www.bankinfosecurity.com)  
*SafeCatch: How to Deter Bank Robberies*  
 Interview with FBI Special Agent Larry Carr  
 September 2, 2009 - Tom Field, Editorial Director

Source: [www.wikipedia.com](http://www.wikipedia.com)

## The Art of Creating Strong Passwords

By Michael Scalisi, IT Manager, Alameda, California

When it comes to password strength, educating users is just as important as enforcing policies.

While security has never been more important than it is today, the fastest way for an IT professional to become the most despised person in the company is to start enforcing a strong password policy.

A policy perceived as overbearing may cause people to write down their passwords on a sticky note near their computers, circumventing its very purpose. Your policy will be ineffective if your users don't know how to create strong passwords that are easy to remember.

Left to their own devices, people will choose passwords that are simple for them to remember. They'll use their spouse's name, their dog's name, their favorite sports team or a recent vacation spot.



Sometimes while working on a user's computer, I'll need to log on as that person after a reboot. Unfortunately, he's wandered off, not wanting to hover over the IT guy. I generally prefer not to know other people's passwords, so I usually don't ask. In this situation, I sometimes take a

guess. I've been right a surprising number of times, and sometimes with people who are very powerful. It's easy. I simply glance around their offices and note what their obsessions are.

Clearly, password policies are needed.

By using the following tips, people will be able to create easy-to-remember passwords that follow these typical requirements: at least eight characters long and with at least three of the following character types: uppercase letters, lowercase letters, numbers and special characters.

- *Substitute numbers for letters and vice versa. (o instead of 0, 4 instead of A, 1 instead of L, E instead of 3)*
- *Substitute words for numbers (one, two, three ...)*
- *Combine both of the above (One, thr33, f1ve)*
- *Use capitalization in random places (bLue, happY)*
- *Use special characters ( !@#%\$^&\*(){}[] ) to punctuate and separate words*
- *Create passwords out of words, numbers or phrases you'll remember*
- *Misspell words*

Using these tips, you can create memorable passwords that will be nearly impossible to guess. Here are some examples of converting memorable information into a complex password.

We'll start with some easy ones:

- *Friday becomes frYday!*
- *Robert becomes #robERT#*
- *867-5309 becomes 8siX753o9*

More complex passwords:

- *19 Peach Place becomes: One9peacHp!!*
- *I love Jill becomes: eYelov3Jill*
- *My dog Fritz becomes MeyedogfritZ*

While some of these examples look nearly indecipherable, you can see how they're not difficult to memorize -- as long as you know the originating word, number or phrase and the basic methodology used to create it. By educating users on how to create strong passwords, you strengthen the security of your company, and your users will benefit additionally by having safer personal experiences with online banking and social networking.

Source: <http://tech.msn.com/security/articlepcw.aspx?cp-documentid=21468386>

## Password Hackers Are Slippery To Collar

Services such as YourHackerz.com are still active and plentiful, with clever names like "piratecrackers.com" and "hackmail.net." They boast of having little trouble hacking into such Web-based e-mail systems as AOL, Yahoo, Gmail, Facebook and Hotmail, and they advertise openly.

And there doesn't appear to be much anyone can do about it.

Federal law prohibits hacking into e-mail, but without further illegal activity, it's only a misdemeanor. The FBI cannot police the Internet and is aware of these illegal services, however they have been successful in the past in identifying criminal activity and working with prosecutors to bring indictments. Users of these services should know that just because a product is marketed on the Internet doesn't mean it's legal.

Experts said there are numerous ways to steal someone's e-mail password, from simply guessing at family names or pet names to high-tech infiltration. The most common way is to send the target a link to a greeting card or something else they might specifically be interested in. When the target opens the link, software is installed on his or her computer that snatches the password the next time it's typed in and sends it to the hacker. Web-based e-mail, such as Google's gmail and Yahoo, can also be attacked through bugs in the Web browser. Another problem is that many computer users are not terribly computer savvy.

Beware of malware, such as viruses, worms and keystroke loggers. Choose the least risky communication channels. Use encryption. Use different passwords for everything. Change operating systems and carry all important data on portable disks.

## 10 Tips to Make Sure Your Firewall is Really Secure

Security studies back up this fact: It takes less than 20 minutes for an unprotected computer to be attacked once it's connected to a broadband connection. Imagine what would happen if you connected your corporate network to the Internet without a security measure in place? Digital intruders could swarm your opened ports, infect machines and even abscond with your intellectual property.

Buying a firewall is the first key step toward securing your network, but it's just as important to make sure that it's configured according to industry best practices. How you set up your firewall will make a big difference in how it performs, so it pays to learn from the experts. You can tune up your firewall and boost your security by following these 10 expert tips:

### 1. Harden Your System

'Hardening' is the practice of reducing the vulnerabilities in your hardware. Before you even install a firewall, you'll want to harden your host machine by closing any unused ports and disabling any protocols or user accounts you won't use.

### 2. Keep it Simple

### 3. Organize Your Rule Elements for Quick Evaluation

Firewalls process rules in the order you set for them, so you want to make sure that the most easily processed rules are at the top of your list.

### 4. Deny, Deny, Deny

Allow only approved traffic to flow on your network.

### 5. Monitor Outbound Traffic

Set up your firewall to filter outbound traffic, as well as incoming traffic.

### 6. Set Up a DMZ (Demilitarized Zone)

A DMZ is a small network that sits between the internal (corporate) network and the Internet and prevents outside users from getting direct access to company computers.

### 7. Configure NTP (Network Time Protocol)

NTP is the name for a protocol and a client/server program that allows you to synchronize computer clock times on a network. Synchronized time is important for implementing distributed procedures over a network and for delivering file-system updates.

### 8. Configure the Firewall as an IDS (Intrusion Detection System)

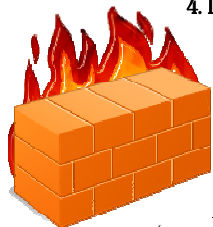
IDSs detect attacks on a network or a computer.

### 9. Test for Vulnerabilities

### 10. Log On

A firewall's log records information about the traffic flowing on your network and can be invaluable when you're trying to investigate suspicious traffic and attacks.

Source: [www.itsecurity.com](http://www.itsecurity.com)



## How to Defend Against New Botnet Attacks

Botnets are networks of computers infected with an instruction set, controlled and manipulated through software that is deliberately or unknowingly installed, directed by a malicious server or master.

Botnets may have legitimate business functions to share program processing, but most often linked to criminal actions to disseminate spam, malware or phishing schemes.

Botnets are the ultimate blended threat delivering a variety of attacks:

- *Distributed Denial of Service (DDoS) Attacks*
- *Spyware and Malware*
- *Identity Theft*
- *Adware*
- *Email Spam*
- *Phishing*

### So what can you do about it?

#### 1. Stay vigilant

Review system logs. Monitor bandwidth usage. Know who is connecting to what from your network. Know what devices are connected to your network.

#### 2. Increase user awareness training

Make sure users do not open attachments that arrive unsolicited and unexpected; do not click links in email; and think twice about any unusual links they click.

#### 3. Watch Those Ports

#### 4. Block JavaScript

#### 5. Layer Your Defenses

#### 6. Get a Security Assessment



*Are there topics that you would like to have covered in future newsletters? We are always looking for topics of interest. We welcome all suggestions! To submit a topic, subscribe, or unsubscribe to our distribution list, please email Shama Renée-McIntosh at [smcintosh@aasysgroup.com](mailto:smcintosh@aasysgroup.com).*