



▶ EDITOR'S COMMENTS....1

▶ Detecting shoplifting
2

▶ Block History
Sniffing..... 3

▶ Having a deadbolt
lock.....5

Employee Theft....6

Choose a fire protection
system...7

How to prevent home
invasion.....9



○ ISSUE
7

○ VOLUME
1

○ September
2011

Security Solutions

ADDRESSING THE NEEDS AND
SECURING THE FUTURE.

Helping secure your world

Shoplifting is a worldwide problem that affects every type of business that has goods on display for customers to browse and examine. Every year, billions of dollars are lost around the world to shoplifting. As a result our first article is on **Detecting Shoplifting** and focuses on methods for detecting shoplifters.

No one really likes having others see what they have been looking at on the Internet. Yet many persons, without knowing it, have been allowing others to see their Internet history. So our second article on **How to block Internet History Sniffing**.

In an age that is caught up with the marvels of technology some traditional basic security devices still have great usefulness. One of these devices is a deadbolt lock, so our third article looks at **Why it is a**

good idea to have a deadbolt lock.

Having an employee steal from a company leaves every manager with a sickening feeling and worse with the financial loss. The fourth article gives methods **To prevent Employee Theft**.

Shouts of Fire, Fire, leaves everyone who hears it with a feeling of dread. Fires can wipe out a lifetime of hard work. Our fifth article therefore addresses **What you need to know when choosing a fire protection system**.

Home invasion type robberies have spread around the world and are a terrifying ordeal for any family. Our final article therefore talks about **How to Prevent Home Invasions**.

Is there anyone who you think would benefit from receiving this magazine? Just send their name and email address to newsletter@assl.com and we would be happy to add them to our mailing list.

Brian Ramsey
Editor



All about Detecting Shoplifters

By Ricardo La Borde, CPP –
Amalgamated Security Services

Every year, billions of dollars are lost around the world to shoplifting and it has been estimated that retailers lose an average of 1.7% of their annual sales to shoplifters. The problem affects every type of business that has goods on display for customers to browse and examine. In this article we present some tips and reminders to help you maintain the edge on Potential Shoplifters. This article focuses on understanding the methods used by shoplifters as part of retail business owner's loss prevention strategy against shoplifting.



Who Shoplifts

Shoplifters appear in any possible form, any age, sex or size, but for the purpose of this article we can break them down into four types, (Professional, amateur, drug users, and thrill seekers). Statistics show that the amateur is by far the largest in number.

Amateurs come from every economic group and represent every level of education. Their thefts are generally impulsive, although a significant number of them find some kind of economic or more often emotional satisfaction in their action, and as the frequency of theft by a particular individual increases they become virtually indistinguishable from the professionals. The rest of the amateurs have no particular pattern of theft and may only steal once or, at most a handful of times.

Professional shoplifters can wreak havoc on retailers all over the world. Their methods are well planned and practical and most times they work in groups or with a partner. One author described it as “The professional approaches shoplifting just as a dancer studies dance or a ballplayer plays ball.” They appear to be ordinary shoppers in every way; after all, fitting in to their environment plays a critical role in the success of their operation. The really clever ones actually purchase items from the retailer they single out.

Detecting the Shoplifter

Professional shoplifters will not be deterred by normal means, nor would they be discouraged by measures that would discourage the great bulk of amateurs from stealing. In today's world you need a combination of effective electronic surveillance equipment working together with well-trained security personnel or store detectives to have the best chance at apprehending them. Other than being familiar with the routine and operations of your outlet, the floor staff, store managers and surveillance team must make it their business to understand and learn the different patterns that shoppers use, for instance;

- A secretary on lunch hour, or any other person who shops to kill time.
- The energetic early morning customer with a specific mission in mind.
- The after work rush hour
- Understanding the difference in the pace of customers in the 10:00 am Crowd from that of the 4:30 pm crowd
- Shoppers who are hurry to get home.

Once we become familiar with these patterns, then we must learn how to spot a potential shoplifter. As some of us may be aware, shoplifting is conducted in every imaginable way; Robert J. Fisher once wrote “the ingenuity of the shoplifter is legendary”, I myself have been surprised on at least one occasion by the ingenuity of shoplifters. Although the great majority of thefts are simple and direct, involving nothing more sophisticated than putting the stolen items into a handbag or a

pocket, we must be cognizant that there are certain methods that are beyond the simple taking of merchandise if we are to be successful in protecting our commodities.

Some of the shoplifting methods include:-

1. Using large baggy clothes like bloomers or pantyhose that can be fitted like shopping bags
2. Slitting pockets in coats or jackets, or hiding merchandise inside a jacket or upper sleeve.
3. Wearing stolen clothes under the thief's own clothing.
4. Hiding items in Purses or umbrellas.
5. Placing small items in the palm of the hand
6. Using shopping bags, sometimes even using the store's own bag.
7. Hiding items within other packaged items, for instance, placing jewelry into soap, toothpaste or cotton boxes.
8. Wearing the item in plain view and walking out with large items.
9. Snatch and Run - Grabbing Items placed close to the door and running out of the store.
10. Cages - these are specially designed to be worn by women to make them appear pregnant.
11. Hiding items in books, newspaper and magazines.
- 12 A technique usually used by females is where an item is held in place by the thighs under a skirt or dress.
13. Using baby prams or strollers to hide the items in.
14. Uses a baggy jacket to hide items under

Learning the methods used by shoplifters is one of the keys to reducing this theft problem.

Understanding the methods enables store personnel to determine who the potential shoplifter is and so focus their attention on that particular individual which would increase the chances of detecting the individual before they are able to leave with the goods thus reducing the possible loss.

There are several anti-shoplifting options available to retailers which include Closed Circuit Television, Uniformed Guards, Electronic Article Surveillance, Close Customer Service, Exit Inspections, No Package Inside policy and In Swinging Doors. When these anti-shoplifting options are combined with knowledge of shoplifting methods the deterring and apprehending of shoplifters is increased.

About the Author

Mr. Ricardo La Borde is a Certified Protection Professional with over 25 years in the Caribbean security field. He is the Chief Firearms and Courier Officer for Amalgamated Security Services Limited. Amalgamated Security through its consulting arm provides consulting services on security protection.

Update Your Browser to Block History Sniffing

History sniffing. It's as sneaky and creepy as it sounds.

And despite improvements to web browsers -- the programs we use to surf the Internet -- this dubious tactic for tracking the sites we visit remains a threat to hundreds of thousands of people who haven't upgraded browsers to the newer versions.



Towards the end of 2010, a new report showed how dozens of sites were checking visitors' surfing history by exploiting a browser feature most of us know well.

A visit you make to any site is "remembered" by your browser so the next time the site name shows up in a search you make or on another website, it's colored purple instead of blue. That way, you instantly know you've been there before.

But this handy feature, which has been around almost as long as the Internet, means your previous Internet activity potentially could be "read" by

simply looking for the color purple in your browser's records.

There's one limitation: A spy program can't just "ask" your browser for a list of purple addresses.

It has to ask: Has this person ever visited such-and-such website? In other words, it must name the websites whose name-color it wants to check.

That's not as big a problem as it sounds though because history sniffing spies are usually interested in your interaction with a narrow range of other sites and the programs they use are capable of asking for a check on 20,000 names a second!

Here's an example. You visit a site selling jeans. As soon as you arrive, the site checks for "purple" names of all its competitors on your computer to see if you visited them.

Maybe it also checks for names of sites popular with male or female surfers and scores of other special interest sites, which help create a picture of you, your gender, age range, fashion taste, whether you're an impulsive or cautious shopper and what your likely budget is.

All in less than a second.

It can then present you with a specially-made page that will appeal to you, with jeans that match your spending profile. It can even adjust prices to make sure it beats competitors.

How to Avoid History Sniffing

That may or may not be a bad thing, but the point is that users don't even know it happened -- that they're effectively being spied on via this history sniffing.

Hardly surprising then that these antics recently led to the launch of a class action suit against one online company, alleging invasion of privacy.

Worse, the technique can be used for much more dubious purposes like providing you with links that target your interests, increasing the chance you'll click on them, but which really link to malware and phishing sites.

Most popular web browsers have now been changed to block history sniffing. Apple's Safari and Google Chrome were reportedly first. But Firefox and Internet Explorer eventually followed suit, though Firefox pointed out that it's possible to switch off the color feature from within some earlier versions of their browser.

But how is the average user supposed to know all this and, equally, how to make any settings change required to switch it off?

And how are they supposed to know about the need to upgrade? Although, for instance, Google Chrome automatically upgrades, others generally don't.

Instead, they bombard users with messages that a new version is available, but many users get

stuck in their ways and often are reluctant to upgrade for fear they'll lose bookmarks and settings (even though they probably won't).

The result is that hundreds of thousands of users, possibly even more, haven't upgraded to the more secure versions.

Action: There are two things you need to do here.

First, make sure you are using the latest version of your browser.

How you do this depends on the browser. Rather than us going into detail here, if you don't know how, just do a search with the words "How do I check my version of" followed by the name of the browser.

Second, in addition to blocking history sniffing, most recent browser versions also have tightened up on other aspects of security and privacy.

Take the opportunity to get to know your browser by reading the help files or visiting its website.

Most PC attacks come via the Internet, so it's just plain common sense to know how to use your browser to protect yourself.

Another Privacy Issue

Although it's not strictly history sniffing, the whole question of websites storing information about your visits to their pages remains a controversial issue for

the security minded.

As many subscribers know, this is most commonly done via storage of "cookies" -- small bits of data that "remember" your identity and other stuff on your computer.

You can learn more about cookies at the website of our friend Leo Notenboom.

<http://clicks.aweber.com/y/ct/?l=EPyWa&m=JaaSbrH1gGtWfo&b=GKAfi0plQL1ichIJbx2UJw>

What you may not realize is that a very common PC program -- Adobe Flash Player -- can collect cookies that may be stored on other computers rather than your own PC.

You might be surprised to learn what records it already has and how its clients can use that data. It even has a setting that could let someone switch your webcam on or off (with your permission).

Fortunately, to be fair to Adobe, they make it fairly easy to see this information and alter your privacy settings -- provided you know where to look!

From your own computer, here's where to go if you have Flash installed (and you probably do):

<http://clicks.aweber.com/y/ct/?l=EPyWa&m=JaaSbrH1gGtWfo&b=0BV.1txhmCsS17WvIxoJKQ>

Then, you need to check out every tab on the settings panel. There's an explanation of what each one does.

If you want, you can delete all the records it currently has and forbid it from collecting details again (or allowing your camera to be switched on).

There's no doubt that Internet privacy will continue to hit the headlines and that whatever protections are put in place, someone will find a way to get around them or abuse them.

When it comes to issues like tracking and history sniffing, getting to know your browser and how to use privacy controls is the key weapon of self-defense.

Article Reprinted from Internet Scambusters Newsletter

Is It a Good Idea to Have a Deadbolt Lock

By [Venard Frater](#)

You may be wondering is it a good idea to have a deadbolt lock. After all, you already may own a doorknob that locks, on your front door. Normal doorknob locks provide some security, but nowhere near the security of a dead bolt mechanism.

When you install a new door knob on your front door, you may notice something. They tend to last few years, and then they wear out. This is because the

mechanism is constantly turned and being used, all the time. On the other hand, a dead bolt locking mechanism is only used when you are securing the door. It does not receive the wear and tear of standard doorknobs.

Dead bolt locks are made to be stronger than doorknobs. In most cases, they are designed with security in mind. They will last longer than doorknobs, because they usually contain heavier grade hardware. This makes them a very good security investment.



A dead bolt locking mechanism is very difficult to pick or jimmy, compared to a standard doorknob locking mechanism. The only way that a dead bolt can be opened, is to move the cylinder. On the other hand, doorknob locks can often be bypassed with something as simple as a credit card. This is because the mechanism does not need to be turned, to open the door. All you need to do, is move the latch inward, and the door opens without turning the knob.

Another area that a dead bolt assembly is more secure than a doorknob, is on doors with windows. It is not hard to defeat the security of a door with

windows, if there is only a door knob keeping you out. All you need to do is break out the window, and reach inside. Once your hand is inside, you can unlock the doorknob by simply twisting it, or turning the locking mechanism.



If you own a door with windows, you can easily invest in a double cylinder dead bolt assembly. With this kind of mechanism, you must use a key to open it from the inside, as well as the outside. If someone breaks a window, they still cannot get the door open, as they need to possess a key to get in.

A standard front door with a doorknob assembly is not hard for someone to kick in, and gain entry to a residence. However, you can invest in a deadbolt assembly and a metal plate that fits over the door jamb. This makes kicking in a door, much harder. The best thing to do, is utilize both kinds of locks. You can have them both use the same key for convenience, and be more secure.

Summary

Is it a good idea to have a deadbolt lock? The answer to

that question should be yes, because they are much more secure than a standard doorknob. They are harder to pick or defeat than doorknob locks, and even if someone breaks the window, they cannot open a double cylinder deadbolt mechanism, without a key. However, the best thing to have is both locks that take the same key.

My name is Venard Frater owner of NF ONLINE MARKETING selling top of line fireproof safes and locks.

<http://www.fireproofsafesplus.com>

Reprinted from Ezine Articles

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

Guarding Your Agency Against Employee Theft

By [AnMarie Bozick](#)

There is no feeling worse than when you find out that an employee has stolen from you. After hiring, paying and

mentoring an employee, finding out that they've betrayed your trust is not only emotionally upsetting but can be financially draining as well. However, employee theft isn't just about stealing cash and office supplies. It also can involve the theft of client files, prospect lists, proprietary planning information and so forth. This type of employee theft can be much more detrimental to your agency than just having someone with sticky fingers.



There are ways to guard your insurance agency against employee theft without making your employees feel guilty before proven innocent.

1. Secure access to all software programs: Comparative Raters, customer relationship management databases and all other agency management system software should be accessible only by utilizing user-specific passwords. You should assign different passwords for each system to ensure that the right employees have access to only those systems that are appropriate for their job duties.

2. Use a software product that stores your client data on the vendor's servers: This decreases the ability of employees to make a quick backup of the agency computer. Watch for employees using thumb drives, floppy disks and CDs to make sure they aren't trying to copy data onto them.

3. Lock employees out of certain areas of the system: You can configure many software systems, like your agency management system, to allow limited access to employees. Strategically doing so can ensure that employees are not able to run reports that generate lists of client and prospect data.

4. Prevent remote or after hours access to the system: It's impossible to monitor what employees are doing when they have after hours or offsite access to computer systems. Restrict the number of employees who have access to the systems remotely or when the office is closed.

5. Change employee passwords immediately after discharging them: Once you let an employee go, you should immediately change their password so that they cannot gain entry into the office, and the system, again.

6. Sign non-compete agreements: According to the Trading Secrets blog by attorneys Seyfarth and Shaw, not every state will uphold a non-compete agreement, but that doesn't mean you shouldn't have one. Have an attorney look at your non-compete to make sure it's going to be upheld, and ask them to explain any circumstances in which it wouldn't—don't just print a

template off from the web and expect it to be enforceable.

Using these methods will help you comply with many privacy requirements while also guarding your office against theft.

Whether working to protect yourself from employee or non-employee theft, you'll be implementing consistent policies that keep your office, and your clients, safe.

AnMarie Bozick, CIC is the [Comparative Rating](#) Product Manager for Insurance Technologies Corporation (ITC). ITC is a leading provider of automation solutions for the insurance industry.

Reprinted from Ezine Articles

What You Need To Know When Choosing A Fire Protection System For Your Business

By [Steve Mike Levy](#)

A fire suppression system is a major consideration for any business. Although no one wants to think of the worst-case scenario, not being prepared in the event of a fire can leave your business devastated. A fire suppression system is a vital part of protecting the business from potential disaster.



Depending on the nature of your business, having a fire protection system might be a legal requirement. One such consideration is whether the public will have access to the business or not. This is in the best interest of public safety and often precludes the business from actually opening. Other considerations would be whether you would be working with hazardous chemicals or other materials that could be considered to be particularly flammable. Protecting your business from fire should include the protection of any data that is collected and stored for the purpose of conducting business. You might be able to rebuild the shop, but without the vital data, you're going to be at an extreme disadvantage when it comes to getting back on your feet. All of these factors will determine which type of fire suppression system that you ultimately decide on.

Fire suppression systems use either water or the combination of various chemicals to automatically deploy and put out the fire. Here are some of the most commonly used fire protection systems:

Water - This is the most commonly used fire suppression system where people might be involved in the event of a fire. Obviously harmless to humans, you will typically see these sprinklers when entering public spaces where people are likely to be. Another consideration is that these types of systems are not portable and not movable to a new location if necessary.

Gas - These fire protection systems don't put the fire out by smothering it with chemicals or some other agent. They work to suppress the fire by depriving it of oxygen or inhibiting chemical processes needed for it to burn. For this reason, it's obvious that this would not be the ideal solution for areas where a human presence is likely. This method is used quite often in computer rooms or data centers where water or fire suppressive chemicals could damage the computer systems, hence compromising vital data. This requires that the room be sealed and a warning system be in place in the event of deployment. This way, anyone in the room has ample time to escape before the system deploys.

Aerosol - This is the latest technology in the area of fire suppression. These fire protection systems release a fine mist or fog that settles and suppresses ignition of the fire. Considered non-toxic and safe, the material used is easily cleaned with a light dusting after deployment and does not appear to have any adverse affects to the surfaces that it settles on.

Most efficient fire protection systems involve the use of more

than one of these technologies to provide ample protection to all areas of the business. Utilizing just one may leave other vital areas of the business unprotected. This is why having a fire suppression system that is customizable is key in getting complete coverage.

As an example, you could use a gas fire protection system in your computer room and a water based system in your offices. This way you have adequate protection for both areas. Each business is unique and the combination you choose is going to be determined by your individual situation. Additionally, cost is another factor when implementing a fire protection system. Typically water based systems are more expensive and cost greater amounts for installation.

Post fire clean up is something few consider. The fire may be suppressed, but the time to clean up and get things back up and running may take longer than you thought. The sooner you can get things back to normal, the less revenue you're going to lose. Make sure you inquire about any residue left by the fire protection system and any damage that the system itself could cause.



Another thing you might want to factor in is the cost benefit on your insurance. You might want to contact your insurance company beforehand and find out what if any benefits they can provide based on the system you choose. Some systems might have a cost offset that makes them more affordable than you previously thought which could mean that you can get more extensive fire protection coverage.

A good resource for information is your local fire department. They are familiar with the structures in their coverage area and should be able to make recommendations based on their experience and what they've seen work effectively. When you consider that they are in the business of putting out fires, they should know which systems fail as opposed to which configurations consistently work in minimizing damage during a fire. Additionally, they are also familiar with current fire codes and what's legally required. This way you'll have the information before you spend money only to be told that it's not adequate requiring further cost or delay in opening your business.

In addition to your local fire department, the city or county where your business resides should be able to provide you with any additional codes or ordinances that you need to be aware of. Laws and rules are there for a reason and rather than trying to find ways around them it's best to get the information straight from the source and install your fire protection system accordingly.

Having a reliable and professionally installed [fire suppression system](#) will give you peace of mind knowing that your business will be back on its feet quickly in the event of a fire. By making an informed choice, you'll be protecting your business, your data, your employees and your patrons. With this system in place, you'll be able to concentrate on the running of your business and not how you're going to recover should the worst-case scenario occur. Shop around and ask questions so that you know that you are making the right choice for your business and your needs.

I suggest you take the time to visit the website of Steve Mike levy at: <http://www.securitysystemsnetwork.com/index.php> and learn more about the changing world of Fire Alarm Systems.

Reprinted from Ezine Aricles

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

How to Prevent Home Invasions

By [Jose R Castillo](#)



Lets start by defining what home invasions mean. Wikipedia.org defines that: Home invasion is the act of illegally burglary or entering a private and occupied dwelling for the purpose of committing a crime (such as robbery, assault, rape, murder, kidnapping, or any violation of the law against the occupant(s)). Home invasions and break-ins are one of the most terrifying and horrific crimes, aside from homicide and murder. So, how can we prevent and reduce the chances, of us becoming victims to this crime?

About a few months ago, I was talking to a Law Enforcement Officer from the Miami-Dade County Police Department, about how crimes rates are super high! The officer and I conversed for a while about how some young teens are breaking into cars, stealing from shopping centers, and committing senseless vandalism to properties, etc. As the conversation went on the officer told me about an experience they had; the explained that a home owner's

house alarm went off and how they had to response. When they arrived to the scene, they carefully inspected the doors, windows, and the backyard to check if there was some kind of forced entrance.

There were only 2 officers at the scene, when the officers noticed nothing was wrong they knocked on the door of the resident. When no one answered they checked to see if the door was opened. Miraculously, the front door was unlocked, so the officers opened the door and yelled " Hello, is anyone here", when suddenly they hear a scuffle upstairs. Carefully they went upstairs, to find two elderly couple tied to a chair. The burglars stole most of their jewelry and belongings. Sadly the burglars are still at large. So how can we prevent this horrible crime to happen? How can we reduce the chances of becoming victims to "home invasion"? As we continue I will give you powerful tips in preventing this crime to happen to you.

Residential Security:

- Know who you are letting in your house. Ensure contractors have been requested.
- Restrict the possession of house keys; change locks if keys are lost/stolen.
- Use solid core doors with deadbolts and peepholes.
- Lock all entrances at night, including garage.
- Keep the house locked, even if you are at home.

- Do not open mail from unknown sources.
- Destroy all envelopes or other items that show your name or other personal information.
- Avoid frequent exposure on balconies and near windows.
- Keep mailbox locked, and do not place family name on mailbox.
- Install security/fire alarm system and associated security services.
- Ensure fire alarms and extinguishers are operational.
- Participate in a neighborhood watch program
- Use motion- and light-activated exterior lighting.
- Install emergency lighting.

General Security:

- Be unpredictable
- Keep a low profile; avoid publicity.
- Do not post your schedule on publicly accessible websites such as: Twitter, Facebook, etc.
- Security personal and identity related documents and information.
- Pay attention to surroundings and report

suspicious activity to local law enforcement.

With these general and specific guidelines you can prevent and reduce your chances of become victim to home invasions and other associated crimes. Always remember that you can take control of any situation. Always be alert and aware of your surroundings! I hope you find these tips useful and helpful.

Jose R. Castillo has been in the security industry for 2 years and already has experimented with many crimes as an Officer. Trained by one of Florida's upcoming security agencies, Regions Security Services, Inc., Jose learned how to deal with the violence and crimes that are taking over the United States today due to the economic crisis. A young expert in his field, Jose has done many activities for children, adults, and elders to always ensure they are alert and aware of any vulnerability. Jose R Castillo is still an employee of Regions Security Services, Inc., located in Doral, Fl. You can contact Regions Security Office at (305) 517-1266 or 1(877)505-7774 or visit their website at <http://www.regionssecurity.us>

Reprinted from Ezine Articles

Amalgamated Security has offices in Trinidad and Tobago, Barbados, St Lucia and Grenada.

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