



▶ EDITOR'S COMMENTS ... 1

▶ USB Safety Alert 2



▶ Committing Crime to Get Ahead..... 3

▶ How to Select the Right Lockers for your Workplace .....4



4 Tips to Using Unbreakable Mirrors.....5

How to choose the right locks for your doors...6

How to protect your valuables from a Safecracker .....7

ISSUE 7 | VOLUME 1 | June 2011

# Security Solutions

ADDRESSING THE NEEDS AND SECURING THE FUTURE.

## Helping secure your world

Thumb Drives or Flash Drives are now increasingly commonplace and many persons use them regularly without any deep thoughts regarding their use. There are however security issues related to the use of these drives. Our first article on **USB Safety Alert** identifies some of the security issues related to these devices.

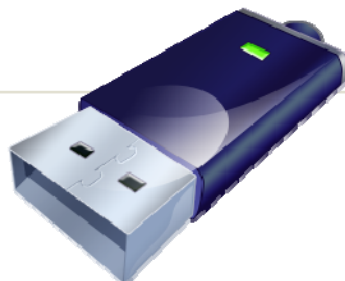
Some people are willing to go to extreme lengths to get a hike up the career ladder, even resorting to corporate espionage to get ahead in business. So our second article on **Committing Crime to Get Ahead** looks at the issue of corporate espionage.

Providing employees with storage lockers to store their personal stuff, gives them peace of mind so that they can work better. So our third article looks at **Selecting Lockers for**

### the Workplace.

Using security mirrors allows managers to monitor the environment discreetly. The fourth article gives **4 Tips to Using Unbreakable Mirrors.**

Every homeowner recognizes that locks are important for security. The problem for most individuals is that they do not know what to look for in a lock. Our fifth article therefore addresses **How to choose the right locks for your doors.**



Most people know that it is important to protect their valuables. But why is it important to understand how a burglar cracks a safe? It's really important if you want to protect your valuables because the more you know about safecracking the easier it will be to protect them. Our final article therefore talks about **How to Protect your Valuables from a Safecracker.**

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

Brian Ramsey  
Editor

# USB Safety Alert

While many people think of computer security as an Internet access issue, USB safety and scams relating to these popular "thumb drives" should not be overlooked. Those rectangular USB ports on PCs have become an essential part of everyday computing. We connect all manner of devices with them to store and transfer data, from hard drives to digital cameras.

But the USB storage devices, also sometimes known as "flash drives" or, in Europe, "pen drives," pose a particular security threat because of their easy portability and increasing capacity. They're used to steal information, install malware on PCs and even for conning people into buying them when they're next to useless.



And, as usual, the ingenuity of crooks pulling fast ones knows no boundaries.

For instance, the New York Times reported recently that employees of a company found a number of USB drives bearing the firm's logo scattered around its parking lot. Curiosity being what it is, several employees

picked them up, took them into the office and plugged them into their PCs to see what was on them. They found what appeared to be a document but when they clicked on the icon, it installed malware that was intended to steal confidential information directly from the company's computer network.

## USB Safety and Autorun

It's not a giant leap to imagine some home users might do the same thing and infect their own machines with malware. In fact, you wouldn't necessarily have to do anything more than plug the device into your machine for it to become infected.

That's because many Windows-based PCs are set to "autorun" when a disc or drive is newly connected to their machine. As soon as you insert the drive, a small program runs, scanning the drive to see what's on it. If that program has been doctored, it may also invisibly install malware.

Fortunately, you can do something about this.

Windows 7 does not allow autorun on USBs but it will permit CDs and DVD to do so. You can switch these off too, if you want, via Control Panel > All Control Panel Items > AutoPlay. Microsoft has also begun to update earlier versions of Windows to similarly restrict autorun. At the time of this writing, this was being offered as an optional update, with Microsoft promising to make it automatic -- eventually.

The technical details are beyond the scope of this article, but you can find out more about it from Internet security firm F-Secure here:

[http://clicks.aweber.com/y/ct/?l=EPyWa&m=1g\\_RHva9GtWfo&b=4zj\\_v4vhkLFgUe5Eovl2xw](http://clicks.aweber.com/y/ct/?l=EPyWa&m=1g_RHva9GtWfo&b=4zj_v4vhkLFgUe5Eovl2xw)

The site also offers a link to a Microsoft page that explains how to totally disable the autorun feature.

Of course, if you have up-to-date Internet security software, this should also detect any attempt to install malware. But not always... if you plug in the USB drive before you switch on your PC, a virus or spyware program could begin running before your malware protection kicks in. And if anyone gives you a USB drive (or you find one!), have your autorun disabled and scan it for viruses before using it.

## How Keyloggers Threaten USB Safety

A more blatant use of USB drives to steal information comes in the shape of key-loggers -- malware programs that record every key press on a computer. Computers in public and shared-use locations like libraries and colleges are especially vulnerable.

In a recent incident in the UK, a keylogging USB drive was found plugged into the back of a PC in a public library. If it hadn't been spotted by an assistant who was checking the machine's connections, it would have collected all those keystrokes for the crook who, presumably,

would have come along later and removed it.

The two key USB safety lessons here are: first, to do a quick visual check for thumb drives in any shared PC you use; and second, don't key confidential information into "public" PCs.

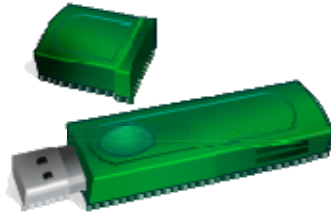
Even if you don't see a connected USB drive, the machine may still have a key-logger installed.

### USB Drive Scams

As the data we use and store on our PCs grows, so too does our hunger for higher-capacity storage devices, including USB flash drives.

Crooks, mainly based in China, Hong Kong and India, have used the opportunity this creates for a scam by creating knock-off designs of well-known drives, chiefly the highly-reputable Kingston brand, and lying about their supposed capacity.

These phony devices sometimes do work but have nowhere near the capacity claimed on the label. Devices with claimed capacities of 32, 64 and even 128 gigabytes are being sold online, when they really only hold 4 or 8 gig. Buyers can't necessarily tell because the scammers hack the devices so that they show the wrong, higher capacity even when you check this on your PC. You don't find out until you run out of space far earlier than you thought you would.



The giveaway on this USB scam is usually the price -- a third or a quarter of what the genuine item would cost. Time to repeat our favorite warning: "If it looks too good to be true, it probably is." This scam is the subject of a lot of debate on eBay forums, so check that site out for more information on what to look for and how to protect your interests.

Go to [http://clicks.aweber.com/y/ct/?l=EPyWa&m=1g\\_RHva9GtWfo&b=NzVGH7P691h9CF\\_IO8rNA](http://clicks.aweber.com/y/ct/?l=EPyWa&m=1g_RHva9GtWfo&b=NzVGH7P691h9CF_IO8rNA), click on the "Search" button and enter in "USB drives."

Let's face it, USB drives are a boon -- especially as we so often move data between PCs, both in the home and between home and work.

They're light and easy to use and transport. But that's also their weakness -- it makes them vulnerable and potentially expensive.

So, be cautious rather than curious with others' drives, be wary when using shared machines, and don't fall for those cheap "high capacity" drives. Those are our simple rules for USB safety first!

Article Reprinted from Internet Scambusters Newsletter

# Committing Crime To Get Ahead In Business

By Nicola Brown

Some people are willing to go to extreme lengths to get a hike up the career ladder, even resorting to corporate espionage to get ahead in business.

The conviction of Gary Min, a DuPont employee found guilty of stealing intellectual property worth \$400m is one of the most memorable examples of recent years.

Between August and December 2005 Min, who was a research chemist at the Chemical giant accessed 16,706 confidential technical documents and over 22,000 scientific abstracts on the company's electronic data library (EDL). Min, who had been employed by Dupont for 10 years intended to give the files to Victrex, a rival company with whom he had been in discussions about a new job.

When Min informed DuPont that he would soon be leaving the company unusually high data-access rates on his account were noticed, arousing suspicion. Since most of the documents accessed were unrelated to his specific job role the investigators were pretty certain of his guilt and indeed Min pleaded guilty to the charges.

Disgruntled or bribed employees accessing, copying and transferring data to a competitor

is one of the most obvious forms of commercial espionage. The other form is attacks from outside the organisation, typically using technology to break firewalls and 'hack in' to steal company secrets. A recent report from McAfee has revealed that cyber criminals have found that stealing confidential company information, such as legal documents or technical information, and selling them to competitors or foreign governments is such a lucrative business that it is now the preferred method of raising revenue in the criminal community.

Whichever method is used what is certain is that they are equally as damaging to a business. Years of research, development, planning and spending can be lost through weak information security practice, unethical employees or criminal acts.

Organisation can fight back against industrial espionage. Regular reviews and updates to information security policies, practices and procedures is a good start. But to really see off external threats from spies and hackers it is essential to call in the experts. TSCM (technical surveillance counter measures) professionals are experts in spotting and securing weaknesses in your technical security and identifying whether any bugs or listening devices are currently in operation.

TSCM, also known as bug sweeping or counter surveillance, is the process of electronically and physically inspecting offices, buildings, vehicles, telephone

systems and cabling for the presence of eavesdropping devices. In addition, computers and word-processors can be examined for possible sources of data leaks and intrusive surveillance software. Providing a safe and secure environment in which to do business.

QCC Interscan offer a range of professional [TSCM services](#) designed to remove the threat from covert surveillance and ensure a safe and secure business environment.

**Reprinted from Ezine Articles**

## How To Select The Right Lockers For Your Workplace

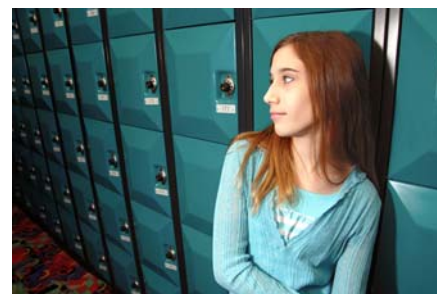
By [Wilde Ferguson Green](#)

Selecting the right lockers for your office is of utmost concern when you consider the frequent thefts that occur in any workplace. When you provide employees with storage lockers to store their personal stuff, you are actually giving them peace of mind so that they can work better. Such lockers are capable of storing items like handbags, laptops and cell phones and they can be locked by their owners to keep them well-protected. Once all valuables are tucked away in safe lockers, employees are more

at ease to perform their tasks efficiently.



School lockers are what come to our mind when we think of lockers, but these are traditionally large and cumbersome. Today, lockers for offices appear far more chic and sophisticated. They are more secure and some can be opened only with authorized fingerprints. Being equipped with greater security features, these lockers are likely to be far more costly.



Ideally, you should opt for combination locks for securing your lockers so that you do not

have to face the predicament of keys getting misplaced.

For office use, lockers can be purchased in different colors and materials so that they match with the rest of the office furniture. For instance, metal lockers with laminated coating to prevent rusting are preferable in manufacturing plants because these are sturdy and long-lasting. Locks installed here must be tamper-resistant.

Points to consider when selecting the Right Lockers for your Workplace:

\*The brand you buy must score high in security features. You need to research and gather information on the fire ratings of lockers to make sure there is no fire hazard.

\*The lockers you purchase must match the safety standards specified for the materials and the installation methods for these lockers.

\*You must buy from stores that have dealers in your location and they should be able to cater to your needs in the shortest possible time, particularly, if you face any problems regarding installation or post-installation.

\*To ensure that the lockers you buy fit conveniently into locker rooms and designated spaces that you have assigned for their installation, you need to buy lockers in different sizes and dimensions.

\*Find out in detail about the guarantees offered by product manufacturers.

\*Preferably opt for a tamper-proof locker to prevent anyone from breaking in.

You can browse through many websites dealing in lockers to get data on prices of diverse types of lockers before making the final choice. You can download all locker designs and obtain an evaluation from the respective security manager and amenities supervisor to decide on the type that is best suited for your business needs.

It is even possible to acquire lockers for specialized needs like lockers for garment hanging, for storing health and safety equipment, for saving work-space and for storing personal belongings. There are also other kinds like lockers meant especially for wet areas, for safely storing laptops and charging them if needed and those meant for food factories.

Lockers are a must have in today's workplace to enable employees to store their belongings in neatly organized designated areas without cluttering the office space. Because of their numerous advantages, storage lockers have slowly come to be accepted as part of the office décor.

Check out <http://www.csstorage.co.uk> to know more about storage [lockers](#) that you can install in offices. This company offers different types of lockers. They provide attractive rates and their experienced and amiable staff offer their services whenever you call them.

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**

## 4 Tips to Using Unbreakable Mirrors Effectively

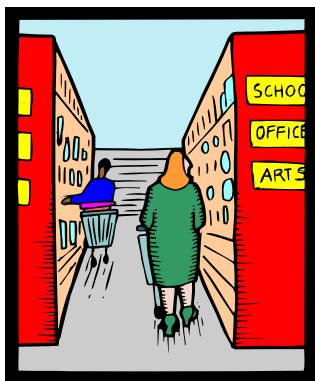
By [Jeremy K Stevens](#)

Protecting your business is extremely important to maintaining its prosperity. Without the proper systems in place it can be a full-time job, requiring you and your staff to take time away from helping customers. This can hurt your business by making people feel unwelcome in your establishment. To protect yourself without alienating your customers you should invest in unbreakable mirrors, which will allow you to monitor the environment discreetly while having your employees continue with their regular jobs. Below are some tips to help you use your mirrors effectively.

Materials - The first thing to consider when you are evaluating

whether you are using your mirrors effectively is what materials you are using. In most cases security mirrors are made of acrylic, a type of plastic that is molded to the desired shape. These mirrors provide a fairly clear picture, allowing you to keep track of movement more than tell what a customer is doing. The more expensive glass mirrors provide a much clearer picture but are easier to break. Unlike their acrylic counterparts these mirrors can be used in conjunction with cameras to allow them to see from several angles.

**Style** - There are several styles of mirrors that can be used in protecting a building. Convex mirrors are the most frequently used for security purposes as they allow you to look at several angles depending on what part of the mirror you focus on: a small convex mirror can allow an employee to scan the entire store from behind the counter if it is placed in the right position. Other, less widespread, types include the flat panel, dome, and inspection mirrors. Each of these has a very specific situation that they are adequate for, trading versatility for specialization.



**Positioning** - Where you choose to put your mirrors is extremely important. If you place them randomly you will most likely leave gaps in your viewable area, which a savvy shoplifter will make use of in a heartbeat. If you are using a convex mirror then you can safely place it at any intersection, or in any corner, to provide you with an angle on all paths from a single point. While this will provide you with the ability to see everywhere from a single location, a small convex mirror placed close to the observer can provide much of the same benefits. Thus, if you have fewer employees it behooves you to save your money by buying only one mirror, because you will only receive a marginal increase in efficiency with every mirror you add.

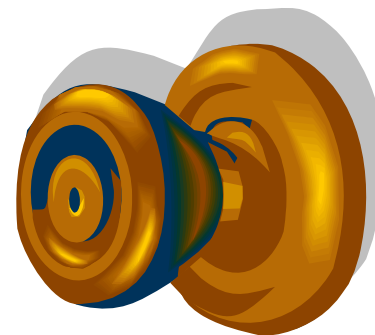
**Training** - The most important thing to consider when using mirrors for security purposes is how to train your employees. It is not difficult to learn, but if your employees do not know how to properly use a mirror then there is almost no point in having them because they will not be effective. Teaching people to watch for suspicious movements and people can help you utilize your mirrors to the fullest extent.

Whether you are looking for a [small convex mirror](#) or a set of [unbreakable mirrors](#), [security-mirrors.com](#) has a solution for all your mirror needs.

Article Source:  
[http://EzineArticles.com/?expert=Jeremy\\_K\\_Stevens](http://EzineArticles.com/?expert=Jeremy_K_Stevens)

# How to Choose the Right Locks For Your Doors

By [John R. Stewart](#)



Most burglars will try to tamper with the locks as the main point of entry into the house instead of, say, kicking the door open with brute force. After all, no burglar will want to harm himself trying to literally force entry into a well secured home when there are many other less secured ones nearby.

As such, homeowners are well-advised to look for the best locks that their money can buy. These high-quality locks must then be installed by an experienced residential locksmith to ensure maximum efficacy as the primary deterrents against unwelcome intruders. This article will deal with the things to look for when buying high-quality, theft-resistant locks for your home.

## Look for Key Control, I.E. Restricted Keys

No, this is not a form of remote control. Instead, key control

refers to the type of keys that have built-in features that prevent easy duplication without the necessary tools, techniques and technology at one's disposal. These keys can only be duplicated by their manufacturers and by licensed locksmiths rather than any experienced cat burglar and lock pick.

Yes, you may have to spend a few more dollars on key control. Keep in mind that the benefits of these type of keys more than justifies their cost.

### Multiple Tumblers on Deadbolts

Deadbolts also require keys to open but some deadbolts are harder to open because of the number of grooves in the key with each groove representing a pin or tumbler. The general rule is that the greater the number of tumblers, then the harder it will be for the burglar to copy, pick or bypass the lock and, hence, open the deadbolt.

Security experts recommend the deadbolts with 7 or more tumblers since the time spent on picking or bypassing the tumblers can stretch for a longer period of time than required for conventional locks. But be sure to choose the deadbolts made from extra-durable materials like brass and steel.



### Saw, Drill and Pick Resistance in Locks

Another desirable value to look for in deadbolts is saw-resistance. The lock can still be sawed through but only up to a certain point, said point being the internal anti-saw pins that spin back and forth with every movement of the saw blade. The result is that the burglar can saw for hours and yet have little progress at breaking the lock.

Then there is the anti-drill resistance in deadlocks. Basically, the manufacturer installs hardened steel chips inside the lock that tear up the bits of the drill as it tries to get through to the internal mechanism. The burglar can end up with broken drill bits with little success on the target lock itself.

Since burglars like to pick open locks as well, manufacturers have come up with some added security components such as spooled driver pins and anti-bump springs. These extra security components help protect the lock cylinder from even advanced picking techniques.

These features will mean a few dollars more on the price tag but the higher price is commensurate to the greater number of benefits. Prospective burglars will find these locks to be too difficult to break, which is good news for you and your family.

A residential locksmith can provide most if not all of the security related services that you may require now and into the future. If your home is located in the Rocklin California area then

please visit your local [Locksmith Rocklin California](#). While there check out our blog at <http://www.norcallocksmith.com/blog> and feel free to leave a question or post a response to any of the security related topics.

Article Source:  
[http://EzineArticles.com/?expert=John R. Stewart](http://EzineArticles.com/?expert=John_R._Stewart)

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

## How To Protect Your Valuables From A Safecracker

By [Wendy Moyer](#)

You've probably seen some movies where a suave and sophisticated cat burglar has broken into a mansion, found a safe, put his ear up to the tumbler, turned the dial, and opened the safe to disclose a king's ransom in jewels and cash.



This sounds very thrilling and romantic - provided you're not the victim. But cracking a safe can be a lot easier or a lot harder

than what we see on the big screen.

But why is it important to understand how a burglar cracks a safe? It's really important if you want to protect your valuables because the more you know about safecracking the easier it will be to protect them.

Most professional safecrackers don't really crack safes. However, they do know that the easiest way to get at the contents of a safe is to know all that they can about it.

So, the first thing to know is that you should buy the type of safe you need.

Different types of safes are built for different situations. For example, let's say that you're a trust attorney. If so, you will probably need to own a fire safe because they are built to withstand a lot of intense heat. So, if there's a fire in your building your clients documents - their wills, etc - should remain intact.

However, because these safes are built to protect documents if there's a fire, they usually are not built with high security in mind. Therefore, they are quite easy to break into. So, you would not want to keep other valuables in a fire safe.

Now, safes that are designed with security in mind will usually melt if there's intense heat. That's because they are made of materials such as heavy duty steel, which will prevent easy access into the safe. And, because they usually have a difficult to crack combination

lock, they are very difficult to break into.

Do you want to know the most common way that a safecracker "cracks" a safe? It's by knowing what the combination to the safe is!

It's not that they can read minds or have an "inside person" giving them the combination. It's that a lot of people who buy a safe never change the combination from what was pre-set at the factory.

They may think that the combination is unique, or that it's randomly generated. Well, they're wrong.

What many safe buyers don't know is that the combinations that the safe factories set are industry standards. And, because a safecracker's "job" is to break into safes, you can bet your bottom dollar that the professional burglar knows the different combinations that safe manufacturers use.

So, as soon as you buy a combination safe reset the factory combination. And use a meaningless string of numbers. Using your birthday or street address is just too obvious. Then keep the combination in a secure place that's not anywhere near the safe.

For example, if you have the safe in your home you may want to keep the combination in your office. Or write it out an address book under a fake name. Just make it look like a phone number.

And to find a wide variety of [Sentry](#) combination safes go to

<http://www.authoritysafes.com/entry-safes.html>

Article Source:  
[http://EzineArticles.com/?expert=Wendy\\_Moyer](http://EzineArticles.com/?expert=Wendy_Moyer)

*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**