- Editors' Note……..1
- Anti Theft Deterrence for Enterprise Laptops……2
- Are you a victim of Hacked Email…..3
- Effective and Automated Key Management Solutions……..5
- How Security Fence is Determined…….6
- Invisible Beam Entry alerts can boost Small Business……7
- What to do if you think your employees are selling company secrets……9
- Protect your privacy on your iPhone…….10
- Tips on how to hide your valuables inside your home……11

Issue 9 | Volume 1 | March 2014

Security Solutions

ADDRESSING THE NEEDS AND SECURING THE FUTURE

Helping secure your world

Editor's Note

Dear Readers,

As we begin a New Year, Amalgamated Security Services Limited would like to wish each and every reader a blessed, safe and prosperous 2014. We ended 2013 with a publication of the ASSL newsletter after a gap in issues which was due to us restructuring our systems. As promised, we are keeping our schedule with quarterly publication of articles that are geared towards your safety and general security awareness.

In this issue we explore topical subject matters such as, Anti theft deterrence for enterprise laptops. This topic was chosen because statistics have shown that Laptop computers and mobile devices are easier to lose due to carelessness and/or theft. This article outlines what organizations should do in order to protect their valuable software. If you ever wondered what you should do if you are ever a victim of hacked email then article number two is a must read, it outlines how someone may have been hacked and how to tell if you are in fact hacked. The previous two topics inspired the third and very relevant article which deals with how to protect you privacy on your iPhone.

Effective and automated key management as well as determining a security fence can all seem overwhelming, however one needs to understand that security is one of the areas of increasing importance, as the world gets virtually smaller and more tightly connected. Articles four and five collectively show the benefits of additional security.

Recent business trends have revealed that the issue of invisible beam entry alerts may seem out of reach for a small business but in fact understanding this can help boost activity. More and more experts are revealing that security and protecting asset are serious issues faced by management. Furthermore, article number seven indicates that many persons may not know how to handle a situation where employees are selling company secret, this article explains this directly in a step by step method. The final article speaks to safety within your residence, by giving tips on how to hide valuables within the home.

We hope you find these articles and the safety measures outlined helpful in some manner. It is our goal that this newsletter will help build your awareness with respect to property protection and a positive impact on your personal protection.

Regards
ASSL Marketing Team

Anti-Theft Deterrence for Enterprise Laptops

By Daniel Gail

Laptop computers and mobile devices are easier to lose to carelessness and/or theft than you may realize. According to some estimates, a laptop gets stolen about once every 50 seconds. Some of the more common locations for theft include: schools, residences, cars, and airports. If your organization allows employees to take laptops, mobile devices, or USB drives off site, your data is at risk. Even if it doesn't, your employees may be storing enterprise data on personal devices or accessing the network from their home laptops and PCs. While you'll need to address any unclear data policies your organization may have, you'll also want to consider implementing an anti-theft deterrence solution across the enterprise. Hard drive encryption software can play an important role in ensuring that should an enterprise laptop get lost or stolen, its hard drive won't reveal its secrets.

What is Hard Drive Encryption Software?

Hard drive encryption software is used to encrypt the contents of a hard disk. Unless a user enters the correct "key" to "unlock" the disk, the data cannot be read. Even with sophisticated data recovery tools, the data would appear as sheer gibberish because it's encrypted. By installing hard drive encryption software on a laptop, you can thwart laptop thieves. While you'll have to replace a stolen laptop, you can rest assured that your data is safe from prying eyes.

Laptop Theft Deterrents

Of course, it's best if a laptop is not stolen in the first place. With that in mind, it's smart to use hard drive encryption software in conjunction with other anti-theft deterrents.

Visual deterrents - Identification tags and locks put thieves on alert that you're not an easy target. If your laptop is hot pink with large "property of" stickers on it, it certainly won't be as easy for a thief to slip away with it unnoticed as it would be for a thief to do with a generic looking laptop. Laptop locks make it even more difficult as the lock itself must be dealt with.

Software deterrents - As mentioned earlier, hard drive encryption software is a must. While designed to protect data after a theft, some hard drive encryption software can prevent someone from hacking into your computer when it's unattended. For example, SecureDoc Enterprise Server uses Intel Anti-Theft Technology-enabled software to detect suspicious behaviors such as excessive login attempts. Imagine locking your laptop to a table at a local business center and stepping away for a few moments. If someone thinks they can crack your password by trying the names of your kids and then sneak a peek at your data while you're gone, they'd be wrong thanks to this feature (and your much more secure password strategy).

Laptops are easily lost or stolen, making it important for every laptop that leaves your organization to be protected with hard drive encryption software. Consider a robust solution such as SecureDoc Enterprise server to more fully manage laptop and mobile device security across the entire enterprise.

Daniel is an exceptional author in the technology world, having written articles on Examiner, TechCrunch and Mashable. He enjoys sharing his knowledge on computer and network security with resources coming from companies such as WinMagic, Microsoft, and the Computer Security Institute.

Article Source: http://EzineArticles.com/?expert=Daniel_Gail

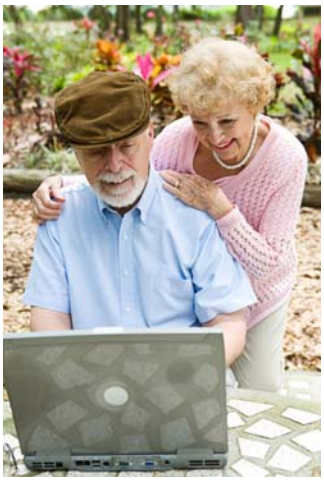
You can learn more about this service by visiting our website: Amalgamated Security Electronic and Integrated Systems website

Are You a Victim of Hacked Email?

More and more these days, we're hearing reports about hacked email accounts -- in which individuals' accounts are hijacked by crooks and used to spam their victims' contacts. Some members of our own team have been getting these types of messages, which appear to come from people they know. Often they contain a link that leads either to a sales site or, worse, a malware download. Or they may be one of those spoof distress emails claiming the supposed sender is in trouble and needs money. For more on this type of scam see:

http://www.scambusters.org/distressscam.html

So how can you tell if your email account has been hacked and what can you do about it?



The Federal Trade Commission (FTC) has recently issued guidance, which has been posted on the government's OnGuardOnline website. http://www.onguardonline.gov Here's what they want you to know, with some additional information from the Scambusters team:

How to Tell If You've Been Hacked

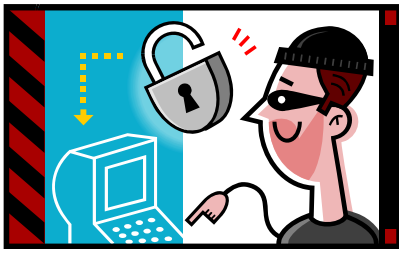
Usually, the first clue you get that someone is using your email address is when you get emails from your contacts about messages they say they've received from you and which you know for sure you didn't send. You might also check your "Sent" folder if you use an online email account and see messages there that you didn't send. Similarly, you may find your Facebook or other social network account has posts that you didn't write. You may not even be able to sign in to your social media or email accounts.

It's also possible, says the FTC, that people may be receiving emails that seem to come from you when your account hasn't been hacked at all. In that case, the crooks are spoofing your email address -- using their tech skills to "overlay" their real address with yours.

But even then, you'll still want to take action to put things right.

How Did You Get Hacked?

There are several ways crooks can get hold of your email account info but the simplest way is that you gave it to them. They already know your email address. It'll be on hundreds or thousands of messages you sent out (including those on jokes you circulated or someone sent to you) or on other sites where you have accounts.



In fact, it's not hard to guess your address if, like most people, you use your first and last name followed by the mail service provider -- like JohnDoe@somemailservice.com. Now, all they have to do is guess your password, which, depending on how wary you are, could take just seconds.

Or they may get hold of it from company computers where you have an account, which they have previously also hacked. If you use the same password on multiple accounts, you're in big trouble. See these Scambusters issues for more about passwords.

http://www.scambusters.org/passwordsecurity.html

http://www.scambusters.org/computerpasswords.html

Alternatively, you may have inadvertently installed malware on your PC, perhaps from the very same trick that's now being passed on to your contacts -- you clicked on a link you thought was sent to you by someone you know. The malware then goes through your PC, collects your password details, raids your contacts list and begins the whole process again.

What to Do If You've Been Hacked

You should take five key actions if you believe your email account has been hacked:

* First, check for and get rid of any malware on your PC. Update and run your Internet security software for this. If nothing is found, visit the software company's website or search the Internet for more malware-scanning tools from reputable companies.

If you haven't found any malware, download the free scanner from www.malwarebytes.org. Although this is NOT a substitute for full-blown Internet security (as the company will tell you), it does have a good reputation for tracking down and removing installed malware that other tools miss.

* Second, change you passwords. Again, check out our earlier reports on how to create strong passwords. And follow the two golden rules: Don't use the same password for different sites, and change all of your passwords regularly. Use a password manager.

* Third, check with your email provider or social networking site for guidance on restoring or resetting your account. You may find, for example, that the crooks have already changed your password and you can't log on to your own account. You'll find links from most of the big providers here:

http://www.staysafeonline.org/stay-safe-online/keep-a-clean-machine/hacked-accounts

* Next, check your account settings. Says the FTC: "Once you're back in your account, make sure your signature and 'away' message don't contain unfamiliar links, and that messages aren't being forwarded to someone else's address. On your social networking service, look for changes to the account since you last logged in -- say, a new 'friend'."

* Finally, make sure you tell all your contacts about what has happened, as soon as possible. If you email them, use the "bcc" address field so all their details remain hidden to the others.

How to Avoid Being Hacked

It would be better, of course, if you didn't get hacked in the first place. You can reduce the risks by following our password guidance and keeping your passwords secret; using a difficult to identify address or at least adding numbers to your address name and keeping your security software up to date. For more information on this FTC guidance, visit:

http://www.onguardonline.gov/articles/0376-hacked-email

Before we sign off, there's just time to alert you to another useful set of guidelines from the OnGuardOnline site. This explains how to stay safe and avoid being hacked or spied on when you're using public wi-fi spots.

Check it out here:

http://www.onguardonline.gov/articles/0014-tips-using-public-wi-fi-networks

Put both sets of guidelines together and you've got a great basic formula for protecting yourself from hacked email and other hijacking tricks.

That's all for today -- we'll see you next week.

- Please Check Out These Offers - They Keep Scambusters Free -

Amalgamated Security Services offer a full range of security service solutions which are inclusive of the following:

Response Services
Alarm Monitoring
Guarding Services
Electronic Service
Courier Services
Assess Controls
Data Services
Cash Services
Investigations

Effective and Automated Key Management Solutions

By Alexis Campbell

Managing big facilities and taking full control of the secure zones is a difficult task. An effective way of managing the security, protecting the staff, valuables and assets is necessary for all organizations. It may be a hospital, a financial institute or an educational institute, but everyone wants to take full control of their buildings. Many systems have been tried and tested since the industrial revolution. However, with the advancement in technology and computer based systems, key control has emerged as a fool-proof, effective and affordable key management solution.

Necessity of Key Management Systems

In any organization or a company, there are many rooms, zones and departments that require limited access. This is because of the sensitive and confidential information and other valuables stored in these rooms. Any individual walking in without any restriction to these rooms could pose a severe threat to the company. Therefore, it is necessary to protect these zones and departments with efficient key control systems.

How Key Control Systems Work?

A basic system would include standard locks on restricted access doors. The keys are then attached to unique RFID key tabs and are used to provide access to authorized personnel only. The keys themselves can be stored in a restricted access locker, which requires a code to access a specific key. The system also logs every key transaction, tracking who had what key, and when it was returned. The RFID key tags also transmit to the system each use, and can transmit a warning if the key accidentally leaves the facility. There are many more products and features that include electronic lockers, key location systems, and key exit systems as well as security perimeter tracking.

Electronic asset lockers
Assets and other valuables are locked in electronic lockers that are strong; metal coated and come with access-controlled compartments. Many businesses and corporations install these machines for protecting their assets and enhance their security systems. The features of these lockers make them a popular choice to many entrepreneurs. A control terminal with multiple authentication options, RFID data transfer and LED identification makes it a fool-proof security option.

Key location system.
This system enables setting up of multiple security zones that make tracking and locating missing keys possible. If somebody tries to take a key out of the premises or out of the authorized area, a real-time alert system sends messages to a smart phone or a computer. In addition, automatic detection and data transfer of key tags makes it an efficient key management alternative.

Key exit system.
Securing exit systems play a significant role in safeguarding the premises itself. This system prevents security breach and theft from a facility. If an employee of an organization forgets a key in his pocket, an audible alarm sounds. Moreover, this system enables automatic key tracking at multiple zones with the help of real time alerts.

Key Tracer is an expert in offering high performance based key management systems including key control systems, electronic lockers, RFID asset security systems, Key location system and much more in Port Coquitlam, BC.

Article Source:
http://EzineArticles.com/?expert=Alexis_Campbell

If you are interested in learning more about our access control systems visit our website at:

Amalgamated Security Electronic and Integrated Systems website

How Fence Security Is Determined

By Ador Talukdar

Security is one of the areas of increasing importance, as the world gets virtually smaller and more tightly connected. There appears to be parallel need to feel more secure. It is not only information that moves much faster, but people can follow the flow of information, and may move equally as fast. Security extends not only to the safeguarding of information, but also to physical assets that include property and persons.

Fence security is one of the important measures that is used effectively for protection of assets that include businesses, homes, government institutions, and factories. In fact most stationery complexes will benefit from the use of fence security.

Because many of the circumstances and situations where protection is needed, can and do vary, customization of fence security solutions will be required. They will depend on a very large part, on the assets to be protected, and how the solution is designed and deployed. The solution should be designed as an effective two-way solution that keeps unauthorized personnel from

gaining illegal entry while restricting unauthorized exits.

A few pertinent questions should be answered to assist in developing the most suitable fence security solution. It may be best to develop a detailed plan that will address some of the major issues.

The first issue is to define what is being protected. Protecting people will be handled differently from property. Larger property will also be handled in a different way, than properties of smaller sizes. The physical composition of the property will also determine the elements that can be included in the fence security solution. There may be some areas of the property that deserve special attention, while others can be considered to be of less importance.

If you are concerned about keeping intruders from entering your property, it can be good idea to emulate the thoughts and actions of the intruders. You should be thoroughly familiar with all areas, and discover even those areas that appear to be hidden or disguised. In much the same manner that investigators emulate the activity of perpetrators, to decipher their methodologies, you can try to think like an intruder, to determine the attack mode, and apply preventative measures.

Depending on the level of security needed, you may opt to use an electric fence, which can be made of a variety of wires, than include high-tensile wire or even barbed wire. In many regions, this use of electrified barbed wire is prohibited, and can be replaced by wire of stainless, with fine rope-like webbing, that is still able to conduct electricity.

Where protection and visibility is required, some care must be exercised with the use of electrified fences, that need proper insulation. If possible, direct contact with vegetation should be avoided, and the fencing material must be securely attached to the posts with porcelain or plastic insulators. The height of the fence is also determined by the purpose for which the fence is installed, and there may be some restrictions that limit the height of the fence.

A popular type of fencing that provides a high level of security, while it does not obscure visibility is the steel palisade fencing, that is highly resistant to damages and is extremely difficult or near impossible to climb.

The fence security solution that is chosen, can be customized to suit your requirements. Some careful consideration, and a closer look at some important details will determine if the fence security solution is appropriate. For more information click here.

Article Source: http://EzineArticles.com/?expert=Ador_Talukdar

Invisible Beam Entry Alerts Can Boost Small Businesses

By Gen Wright

When it comes to being a success in the retail market today, small stores have to work smarter and harder. This means that small businesses need to get value in everything that they do but they also need to provide the consumer with an excellent experience from the moment that they engage with the business. At times it can seem as though these two goals stand at opposite ends of the spectrum but there are ways that small businesses can provide themselves with the best chance of meeting all of their goals.

One of the biggest problems that small businesses have is ensuring that everything gets done. Many stores would love

to have an employee in the back of the store sorting merchandise and taking care of the administrative duties while another employee was available in the front of the store to provide a service for any clients. The problem comes with the fact that not every firm has the budget for two employees and there is therefore a need for the employee to remain at the front of the store at all times.

This means that administrative tasks do not get completed or the store owner has to ask the employee to undertake overtime to ensure that all of the tasks are taken care of. Some employees will be delighted at the additional pay, which may not be of benefit to the firm, but some will be annoyed at having to work extra hours. This is where having a reliable door system in place that will inform an employee if a customer is present is good for business.

An Invisible Beam Entry Alert enables employees to be more flexible

With an Invisible Beam Entry Alert or a motion focused system in place at the front door of the store, an employee can work and then be notified whenever some enters via a chime or even through hearing the sound connected through an intercom in the back office. This provides the firm with the benefit of an employee undertaking activities in the back office while ensuring that all customers receive a warm welcome and will have an employee greet them.

With respect to customer service, the fact that an employee will make their way from the back of the store to the front of the store on the arrival of a customer is a high level of customer service. The customer will feel honored and privileged that their appearance in the store has been greeted with an employee stopping what they were doing to come and serve them. With respect to developing a positive feeling between the client and the firm, this is an impressive way to start.

Another great thing about this style of solution is that invisible beam entry alert and entry alert motion sensor can be found for a wide range of prices. There are simple yet effective systems available and these can be attached to doors with the minimum of fuss. There are also more technologically advanced systems available at a higher price which will offer advantages such as not using wires or being able to linked to intercoms but no matter the budget of a business, there will be an opportunity to welcome every customer, no matter where employees are being utilised.

For more information on how your business can benefit in the long run from Invisible Beam Entry Alert or entry alert motion sensor please visit our website at http://www.doorentryalerts.com

Article Source: http://EzineArticles.com/?expert=Gen_Wright

Amalgamated Security Services offer a full range of security service solutions which are inclusive of the following:

Response Services
Alarm Monitoring
Guarding Services
Electronic Service
Courier Services
Assess Controls
Data Services
Cash Services
Investigations

What to Do If You Think Your Employees Are Selling Company Secrets

By Lori Ann

Having a business these days is hard enough without having to suspect your employees are selling company secrets to your competitors. This is an unscrupulous thing to do, but it is becoming more and more prevalent.

It is something that is hard to detect unless you know what you are doing. Sometimes you can ask an employee if they are doing it but unless you have evidence, they are going to deny it until they are blue in the face.

Also, if you ask someone and they really aren't spying on you, then you will lose their trust forever and if you continue to treat them differently, they are likely to take legal action against you. That is why you should always have evidence before you confront someone.

There are many ways that you can get evidence on someone. Some ways are better than others and some may not be entirely legal in a court of law so you have to be careful on the steps that you take when you are trying to compile the evidence.

Inform the employees

If you are going to do any of the things below, you have to inform the employees that they are under surveillance. You can do this as soon as they sign their contract, or if it is further down the line, you can put up signs that indicate they are on camera at all times and their work might be monitored.

This works as a prevention method because they are less likely to sell their allegiances to another company. Also, this keeps you in line with the law because in some countries you are not allowed to film people without their consent.

You can also look at it as a character assessment when you first hire them. If they refuse to sign the waiver, then it might be the case that they would be up to something untrustworthy later on. If they sign, then you know that you can trust them.

Keep an eye on their computer

As an employer, you have every right to access an employee's computer and see what they are up to. You can do this under the guise that you are checking up on the performance levels, or you can just be up front and say that you are monitoring because they work with sensitive information.

A lot companies have trackers on their computers and you will be informed when an employee does a certain thing or keys in certain information. You are well within your rights to do this, especially if you have your employees sign the data protection act when they start to work with you.

Surveillance

You should have cameras in operation at your place of work. This is for your protection and for your employee's protection as well. The cameras probably work in conjunction with a

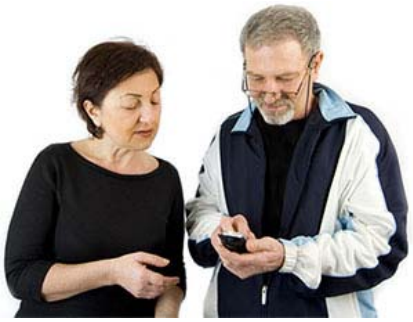
security team to make sure that no one breaks into the premises or tries to injure the employees.

The cameras should be equipped with infrared so you get a good image when the lights are out and when the premises are closed. This is because the most break ins occur when the buildings are closed and no one else is on the premises.

If you suspect that a person is selling company secrets, you should inform the police and you are well within your rights to put that worker under surveillance. This could be in the form of cameras on their desk, or having someone else keep a close eye on them as they work.

Article Source: http://EzineArticles.com/?expert=Lori_Ann

Protect Your Privacy on Your iPhone



These days more and more people are beginning to use their **smart phone** as their main tool for browsing the web, transferring documents, sharing and storing personal pictures, and managing financial accounts.

There is also an increasing use in the workplace. A smart phone can be a treasure trove of personal information and proprietary work information that can be exploited for financial or personal gain. **Sensitive data** can be found in a multitude of places on your iPhone:

- **Private emails** containing passwords to other accounts, financial account information and attachments containing sensitive information such as a tax return;
- **Work emails** containing confidential business communications, intellectual property or protected customer information;
- Should your **iPhone passcode** be bypassed or left unlocked, a thief can use apps installed on your phone to manage bank or financial accounts and other sensitive transactions; and
- **Pictures** in the iPhone camera roll may be of a private personal nature or contain scans of sensitive documents for personal or professional use.

Unfortunately, many people don't realize just how much personal information is accessible via their iPhone and don't take necessary steps to protect it. Sometimes people go beyond failing to take protective measures and actually take proactive measures to reduce the security of their iPhone.

For example, many people opt to "jailbreak" their device which entails the owner making unauthorized modifications to the operating system of the phone. These modifications allow users to download apps or perform other tasks normally not allowed by the iOS. This

can result in severely reduced security measures that come with the iOS in order to protect your personal information and ward off malware targeted at your iPhone. (**Yes, there is malware designed to attack iPhones**).

The latest iPhone has a fingerprint scanner that can be used to unlock your iPhone in lieu of entering a four digit passcode, but was successfully hacked about two days after the iPhone 5s was released.

New hacks and tricks are discovered every day by white hat hackers looking to expose iPhone's vulnerabilities so that Apple can resolve them. Many of these hacks are short lived as Apple is good at providing updates to close security loopholes when they are discovered, but they continually surface and this requires vigilance on the part of the iPhone owner to stay up to date on iOS updates. These hacks often include methods to bypass the unlock passcode to access limited capabilities of the iPhone via Siri or the control panel.

While there is no surefire way to avoid having your iPhone hacked, there are many ways to reduce your chances of unauthorized access:

- Keep your **iOS updated** and be quick to install the updates as soon as they become available;
- **Disable access to Siri and Passbook** while the phone is locked by navigating to Settings -> General -> Passcode Lock and switching Siri and Passbook to off;
- **Disable access to the Control Center** while the phone is locked by navigating to Settings -> Control Center and turning off the "Access on Lock Screen" option;
- Should you decide to use the fingerprint scan option to unlock your phone, use it in conjunction with a **four digit passcode** to increase security;
- Whenever browsing the web using free WiFi in a public place, **use a VPN service** to prevent thieves from monitoring your Internet activity; and
- **Always have your iPhone passcode lock activated** and consider using the auto-lock feature to avoid accidentally leaving your phone unlocked in a public place.

(*"Protect Your Privacy on Your iPhone"* was written by **Sam Imandoust, Esq**., CIPP, CIPA. He serves as a legal analyst for the **Identity Theft Resource Center**.)

Tips On How To Hide Your Valuables Inside Your Home

By Larry Graham

Where Do You Hide Your Valuables?

Do you have a clever place inside your home to hide your valuables? Are you definitely sure that a thief won't look there first?

If you've watched TV shows about real burglars, you'll realize that a robber will pull out all your drawers, flip over your bed mattress, and tear everything off of shelves to get to where he knows you hide your belongings. He is aware of your hidey holes because that's where HE hides his stuff.

In case you've been hiding your money under your mattress or in your underwear cabinet ... Yeah, so does everyone else and robbers know it. These are NOT secure places to keep your valuables. From an interview with a burglar, "I would toss everything surrounding the bed."

I'm going to give you some advice and provide you with some smart ideas for hiding valuables inside your home.

Places Burglars WILL Look For Your Hidden Valuables

Don't Hide Your Valuables Here:

- the back of the cabinet in a box
- the toilet bowl tank
- around the toilet--boxes of tampons, toilet paper rolls, potpourri
- cereal boxes
- refrigerator & freezer
- beds, pillows, between the mattresses, under the bed and inside something close to the bed

1. Start Simple With Diversion Safes

Hide Your Money in Plain Sight!

1. **The number 1 best way to hide your cash stash or jewelry is a diversion safe!** I'll bet you already know that you can buy a soda can that's not really a soda can or a can of shaving cream that's not really shaving cream or an outlet that's not really an outlet. Although most thieves know about can safes, they don't have a lot of time to go through every single can of soda or every can of shaving cream to see if it's the real deal. But be smart and don't keep a can of fruit cocktail in the bathroom or a, "can of shaving cream," in the kitchen pantry. Your bratty siblings will never find your hard-earned lawn-mowing money in one of these, just don't buy a can safe that looks like their favorite drink! These are some of the BEST places to hide jewelry or extra cash and they also make a great gift for college kids. Your average dorm thief will never suspect you have a hidden safe.
2. **Buy a jar of spices from the grocery store.** Empty and clean the jar. Use a small paint brush to completely coat the inside of the jar with glue. Fill the jar with the dumped spices and allow to sit. When dry, empty out the excess spices. Spray the inside of the jar, spices and all, with a clear-coat spray to keep them in place. Allow to dry well.
3. **Pick up an old book and simply carve out the interior**. I used glue to seal the inside. Can even use a phone book!

4. **Put your valuables in several layers of plastic bags** then hide things in hollowed out legs of patio furniture, or metal garden furniture legs, or even the hollow legs of a child's swingset, or fence post.

Hide The Diversion Safe In Plain View

Wall Safe or Electrical Outlet

I see a lot of videos by college-age kiddies showing how easy it is to hide things from their

roommate by cutting a square out the carpet in your closet or making holes in the wall. A hole in the floor or the wall isn't going to fool anyone. This little wall safe will fool thieves and you can hide quite a bit of jewelry and cash in the wall without anyone knowing.

2. Furniture With Secret Compartments, Wall Safes, and Floor Safes

Want something larger and more secure? If a diversion safe isn't big enough, go one step further and get a wall safe.

Ever since that scene in Casino with "Nicky Santoro" (Joe Pesci) pulling back the carpet in his closet and uncovering a floor safe--I've wanted one!

But keep in mind, a safe only working if no one else knows about it. Don't tell your buddies all about it the next time see them. You never know who THEY'LL tell.

The premise of, "In Cold Blood," comes to mind. The ex cons broke into the Clutter farmhouse because they were told about a safe with large amounts of cash. Truth be told, there was no safe and the entire family was murdered for nothing.

"I didn't want to harm the man. I thought he was a very nice gentleman. Soft spoken. I thought so right up to the moment I cut his throat."

Keep your mouth closed, a secret safe in your home needs to be a secret. And don't hire the cheapest sketchiest guys to install your home safe. Do it yourself and save yourself the headache.

Prestige Home Security knows that home safety and security for loved ones and property are family priorities. We are passionately committed to helping you, and they, with our Home Security solutions. Contact us today, secure your properties and love ones. Call 1-832-735-7735 or visit our website at http://www.prestigehomesecurity.com/

Article Source: http://EzineArticles.com/?expert=Larry_Graham

If you are interested in learning more about our home security systems visit our website at:

Intrusion detection systems

Amalgamated Security Services offer a full range of security service solutions which are inclusive of the following:

Response Services
Alarm Monitoring
Guarding Services
Electronic Service
Courier Services
Assess Controls
Data Services
Cash Services
Investigations