- EDITOR'S COMMENTS ... 1
- ATM Crime..... 2
- Effectively erasing files..3
- Someone broke in…....4
- Security Penetration Testing…..5
- Change the glass in the Windows...6
- YouTube Scams and tricks…7
- Benefits of Gate Automation….9
- Patio Locks…….10

ISSUE 7 | VOLUME 1 | March 2012

Security Solutions

ADDRESSING THE NEEDS AND SECURING THE FUTURE.

Helping secure your world

Bank ATM are increasingly how most people interface with their Bank and obtain their cash. As a result of that cash, criminals are always looking for how to relieve individuals of that cash. It seems as though when the public becomes aware of one method the criminals move to another method. So our first article looks at **Atm Crime**.

Technology constantly marches on and so individuals are regularly upgrading their computers. Unfortunately we increasingly keep much of our personal information and all of our company's information on computers. Therefore when it is time to change computers one has to be sure that the information has really been removed. The second article gives advice on **Effectively Erasing Files.**

No one wants it to happen and hopefully readers of this magazine take steps to prevent it from happening however sometimes it does happen. Our third article on **Someone broke in, Now what**, looks at what to do on discovering a breakin.

One only knows how good your computer defenses are when they have been tested. We have therefore included the article, **Security Penetration Testing**.

Our fifth article introduces you to **Changing the Glass in your Windows for Better Security**.

YouTube is one of the most heavily used Internet sites. Because of that traffic there are con artists who prey on YouTube visitors. Our sixth article gives some tips on **How to avoid YouTube Tricks and Scams**.

Our seventh article gives information on the **Benefits of Gate Automation**.

Our final article, **Patio Door Locks Not Enough,** identifies why homeowners make a mistake when it comes to securing their home by relying on the patio door locks that come equipped on standard sliding glass doors.

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

ATM Crime

By Brian Ramsey

During November 2011 a man was robbed at an ATM in San Fernando Trinidad by a couple who were waiting outside the ATM. The male robber held the victim's arm while the female robber grabbed the envelope with the money which the victim had withdrawn from the ATM. This robbery is not particularly unusual as these types of incidents occur at intervals in Trinidad. It is however a good example of how easily these types of robberies can occur because of a lack of care on the part of victims.

Almost all ATM vestibules are enclosed with clear glass allowing persons outside to see into the ATM enclosure and at night are lighted to also allow vision into the vestibule. This is intended to allow police and other persons passing by to see into the ATM and so serve as a deterrent to someone entering the enclosure and robbing persons while they are at the ATM or hiding in the enclosure to wait for victims. Unfortunately it allows criminals to also see persons who are withdrawing money from the ATM.

At the same time having a clear glass vestibule allows persons at the ATM to see who is outside before they exit the ATM. Individuals using an ATM should always check the area outside the ATM before they exit the enclosure. In this particular case the victim was lulled into a false sense of security because he saw a man and woman together. The presence of the woman, most likely, dispelled any thoughts that these might have been criminals and this was an error of judgment on the part of the victim. Women are now involved in criminal activities either as decoys or as active participants. Persons exiting an ATM should rapidly walk away from the ATM being alert to and where possible avoiding persons outside the ATM.

The second act displaying a lack of care by the victim was that the individual had the envelope, containing the money, in his hand when he walked out of the ATM. This made it easy for the woman to take the envelope away from him. When obtaining cash from an ATM, persons should immediately place the money in their pocket or purse before exiting the ATM.

By now most persons would be aware of the technique where thieves cause the victim's ATM card to become stuck in the ATM and then they pretend to be helping the victim by having him re-enter his PIN number into the ATM while they surreptitiously memorize the PIN. When this does not cause the card to function or be released from the ATM (as the thieves know it will not) and the victim leaves the ATM, the thieves return to the ATM and remove the card, now having a valid ATM card and the associated PIN number.

All Banks have made strenuous efforts to protect against this type of crime by regularly warning customers not to share their PIN with anyone.

The thieves in Trinidad have now begun to refine their technique and are importing techniques used in the US and Europe. This new technique continues to use the approach of causing the card to stick in the ATM, however the thieves are obtaining the PIN numbers planting a camera either in the ATM vestibule or in a nearby building but focused on the ATM keypad. They use the camera to record the PIN and then retrieve the card when the victim has left, thus obtaining a valid ATM card and PIN number which they can then use to obtain cash from an ATM or to make purchases.

To protect against this variation in criminal technique persons using an ATM should adopt the habit of using one hand to shield the other hand that is entering the PIN code. The shielding hand therefore blocks the code from being seen.

Criminals never rest in their quest to deprive persons of their

money and therefore individuals constantly have to adapt their protective measures.

Effectively Erasing Files

Before selling or discarding an old computer, or throwing away a CD or DVD, you naturally make sure that you've copied all of the files you need. You've probably also attempted to delete your personal files so that other people aren't able to access them. However, unless you have taken the proper steps to make sure the hard drive, CD, or DVD is erased, people may still be able to resurrect those files.

Where do deleted files go?

When you delete a file, depending on your operating system and your settings, it may be transferred to your trash or recycle bin. This "holding area" essentially protects you from yourself -- if you accidentally delete a file, you can easily restore it. However, you may have experienced the panic that results from emptying the trash bin prematurely or having a file seem to disappear on its own. The good news is that even though it may be difficult to locate, the file is probably still somewhere on your machine. The bad news is that even though you think you've deleted a file, an attacker or other unauthorized person may be able to retrieve it.

What are the risks?

Think of the information you have saved on your computer. Is there banking or credit card account information? Tax returns? Passwords? Medical or other personal data? Personal photos? Sensitive corporate information? How much would someone be able to find out about you or your company by looking through your computer files?

Depending on what kind of information an attacker can find, he or she may be able to use it maliciously. You may become a victim of identity theft. Another possibility is that the information could be used in a social engineering attack. Attackers may use information they find about you or an organization you're affiliated with to appear to be legitimate and gain access to sensitive data.

Can you erase files by reformatting?

Reformatting your hard drive, CD, or DVD may superficially delete the files, but the information is still buried somewhere. Unless those areas of the disk are effectively overwritten with new content, it is still possible that knowledgeable attackers may be able to access the information.

How can you be sure that your information is completely erased?

Some people use extreme measures to make sure their information is destroyed, but these measures can be dangerous and may not be completely successful. Your best option is to investigate software programs and hardware devices that claim to erase your hard drive, CD, or DVD. Even so, these programs and devices have varying levels of effectiveness. When choosing a software program to perform this task, look for the following characteristics:

- "Secure Erase" is performed -- Secure Erase is a standard in modern hard drives. If you select a program that runs the Secure Erase command, it will erase data by overwriting all areas of the hard drive, even areas that are not being used.
- Data is written multiple times -- It is important to make sure that not only is the information erased, but new data is written over it. By adding multiple layers of data, the program makes it difficult for an attacker to "peel away" the new layer. Three to seven passes is fairly standard and should be sufficient.
- Random data is used -- Using random data instead of easily identifiable patterns makes it harder for attackers to determine the

pattern and discover the original information underneath.

- Zeros are used in the final layer -- Regardless of how many times the program overwrites the data, look for programs that use all zeros in the last layer. This adds an additional level of security.

While many of these programs assume that you want to erase an entire disk, there are programs that give you the option to erase and overwrite individual files.

An effective way to ruin a CD or DVD is to wrap it in a paper towel and shatter it. However, there are also hardware devices that erase CDs or DVDs by destroying their surface. Some of these devices actually shred the media itself, while others puncture the writable surface with a pattern of holes. Many paper shredders will also shred CDs and DVDs. If you decide to use one of these devices, compare the various features and prices to determine which option best suits your needs.

Reprinted from Security Today, 9th February 2012

Someone Broke In, Now What?

By Stephanie G Ross

Imagine coming home and finding that your door is wide open or your window has been smashed in and you don't know what to do or what happened. It is a terrifying feeling when you come home and realize your home has been broken in. Home break-ins sadly are quite common and although nothing may have been stolen, but it still can leave you feeling very uneasy and unsure of what to do. However, there are some things that you will want to make sure are taken care of after something like this happens.

The first thing you want to do is call your local authorities. You will want to avoid going into your house if it is possible. If there is anyone or any pets still in the house try to get them out to prevent them from any injury.

For the pets, if they do not come to you right away, don't go looking for them since you don't know who may be waiting for you in the house. You need to stay close till the police get there, but if you can, stay inside a neighbor's house or a locked car if you have too. Whatever you do, do not disturb the crime scene, this means do not do a walkthrough of the house to see if anything was taken, don't touch anything, don't even close doors or windows that may still be open.

When the police get there, try to remember everything you can about when you got home and what you saw. Try to stay calm, yes you may be nervous, jittery, upset, and angry, but you need to stay calm and keep a clear head so you can help give the police the most accurate information that you can. They will probably do a walk through and may ask you to go with them to see if anything has been taken. After they have done their initial walkthrough, they may collect evidence if they feel it will be helpful in an investigation if there is one. They will also ask you to fill out forms to document what has been stolen or damaged and what the estimated cost of your loss may be.

The next step will be to talk to your insurance company. Have a copy of the police report to give to your insurance company for their records, also show them the list of items that were stolen or damaged. If you happen to have photos of those items, give them and the police a copy of the photos too. The list and photos will help both the police and

your insurance company to find any stolen items.

Of course, going back to living a normal life may seem difficult right after something like a burglary or home break in, but eventually, things will go back to normal. However, you may want to invest in a good security system and new locks. This will at least help you move your life forward by giving you a little peace of mind. You may also want to do a sweep of your home to check for any loose windows and doors, or fix the windows and doors that may not have locks or are easily pushed in.

About this Author

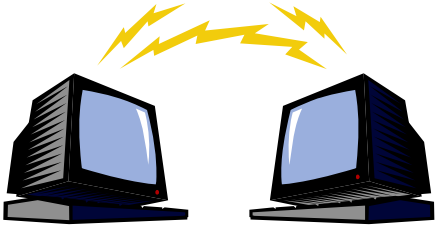
Home Insurance Quotes

Insurance Policy for Theft

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

Security Penetration Testing: What Goes on in a Penetration Test?

By Andrew Leith



Security penetration testing is an essential part of any organisation's information security provision. However many security controls you implement for your data, you will never know for sure how effective they are until you actively test them by commissioning security penetration testing (also known as "pen testing").

In the course of security penetration testing, the tester will probe your organisation's computer and network defences, and will then attempt to breach them (with your permission), but without causing the damage that a malicious hacker might cause. The results are explained in a report which also includes recommendations for actions to correct any security loopholes in your systems.

In order to get the best out of the test results, it is important to be aware of the general pattern taken by a penetration test. This also makes it possible to check that your provider is following the correct methodology. The main stages are as follows:

* Foot-printing: Public sources of information are used to gather information about your organisation's Internet presence.

* Scanning: Standard tools are used to map your network in a non-intrusive way, determining the number of computers and the network configuration.

* Enumeration: This stage involves attempting active connections to your systems in order to discover information (such as valid account names) that might be exploited by hackers. This stage and the two preceding stages are all legal: the further stages would not be legal without your organisation's written permission.

* Gaining access: This is the point where security penetration testing comes into its own, as the test demonstrates whether or not a hacker would be able to gain access to your network.

* Increasing access rights: Having gained access, the pen tester now seeks to increase his/her access rights to the highest level possible, in order to find out whether your network is vulnerable to this kind of "exploit". A hacker who succeeds in gaining high-level access would be able to wreak considerable damage on the systems.

* Pilfering and theft of data: Moving into an even more active mode, the security penetration

testing procedure now covers the attempted theft of information.

* Covering one's tracks: A skilled pen tester will attempt to cover his/her tracks so that the attack remains undetected, in order to demonstrate that this is possible, since a stealth attack is the most dangerous kind.

* Creating a back door: A further refinement is to create a "back door" that will make it easier to access your systems in the future. If the penetration tester finds that this is possible, it will certainly be highlighted in the report as a major weakness of your systems.

* Denial of service: Finally, the tester may seek to discover whether a "denial of service" attack is possible, whereby resources become unavailable to legitimate users.

It is important to note that the more active phases of testing may disrupt the normal operation of networks, leading to a certain amount of denial of service. For this reason, some organisations prefer the rel=nofollow [http://www.commissum.com/security-testing/penetration-testing/]security penetration testing to stop short of those stages. Each pen testing project should be covered by a specific contract setting out exactly what will or will not be attempted. In general, penetration testing should be carried out at regular intervals, and certainly after major changes to the computer network. Used correctly, pen tests can be an indispensable aid to your organisation's information security management system.

About the Author

Andrew Leith is a security consultant at Commissum, a specialist information security consultancy in Edinburgh, Scotland, UK (see www.commissum.com).

Reprinted from ezinearticles.com

Change the Glass in Your Windows for Better Security

By John C Cherry

Breaking windows has never been a popular MO for burglars; however, these days, criminals who want to get into your house will do whatever it takes, including smashing windows. Typically, they didn't break windows because it's a very noisy process, so they focused on trying to pry windows open instead. Sometimes, though, burglars would stick a piece of duct tape to the window pane, smash it, and carefully pull the tape and the pieces away to reveal a hole. If you have done everything else to make your home more secure, including installing a security system, one of the last layers of protection you can install is to change the glass in your windows to a material that is less likely to be broken.

Wire Glass

This is a glass window that has wire mesh embedded in it. These windows will break just as easily as traditional windows but the mesh will keep the majority of pieces in place, and makes it much harder to find an opening. This kind of glass is usually seen in businesses, but it would work well for garage and basement windows.

Tempered Glass

This kind of glass is stronger than typical glass; however, it can still be broken if a strong force is used. This is often seen in storefront windows of commercial businesses. A fist is probably not going to break tempered glass, but a hammer, tire iron or other blunt force most likely would.

Plastic Glazing

This kind of window is essentially plastic and is extremely resistant to force that

would easily smash typical glass windows. There are two basic kinds of plastic glazing windows, which are acrylic (Plexiglass) and polycarbonate (Lexan). Acrylic windows will not break if a rock hits it, but it would break if hit by a hammer or tire iron. Polycarbonate, on the other hand, will not break at all. It is very expensive, but it will not give in to heat, hammers, flames, picks, axes or extreme cold. The downside to plastic windows is that they are easily scratched and they can become discolored in the sunlight.

Laminated Glass

This kind of glass is found in vehicle windows and is made by sandwiching a plastic sheet between two layers of glass. When hit, the glass will break, but the plastic will keep it from falling out of the frame. This is the most secure kind of glass, but it is also much more expensive. Because of its special installation needs, you will have to hire an expert to install laminated glass panes for you.

Once you have your home security system installed and you have secured your doors and windows with locks, the next step is to upgrade your window panes by changing out the ordinary glass to one of the above options. It might seem like overkill, but when it comes to the safety of your family, you can't go too far.

About this Author

John is a shrewd consumer who writes about personal finance, home technology and home security topics like: San Francisco security system reviews and home security.

Reprinted from Ezinearticles.com

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

Your Guide to YouTube Scams and Tricks

<>~<><><><>~<><><><>~<><><>
~<><><><>~<><><><>~<><><><>

The online video site YouTube is one of the most successful and heavily used areas of the Internet, with over 3 billion videos viewed every day and uploads equivalent to 240,000 feature films every week.

Sadly, that popularity also makes it a lucrative target from crime, ranging from scams and account hijackings to illegal use of the YouTube name and abusive videos and comments.

YouTube, which is owned by Internet giant Google, has lots of security checks in place and offers guidance on things like phishing and hijacks, but the sheer scale of the operation makes it virtually impossible for the organization to monitor videos and comments as they're posted.

So, for example, as we disclosed a few months back in our report on Ponzi schemes, the Better Business Bureau claims there are at least 23,000 YouTube videos promoting fraudulent investment schemes.

http://clicks.aweber.com/y/ct/?l=EPyWa&m=J79dnn2PqGtWfo&b=2vn8.aLaziA0pItKNa9yJQ

Let's take a look at the most common types of YouTube scams and other "red flags," and what you can do to prevent them catching you out.

Phony Products

From pyramid schemes to claims you can run your car on water -- you'll find them all on YouTube.

The problem is that promoting an idea or product via video somehow gives the claims extra credibility.

We're more inclined to believe what we see, especially if the video is disguised to look like a TV news bulletin or an interview with a supposed happy customer.

One current investment scam to be aware of is a video presentation inviting viewers to get in ahead of initial public offerings (IPOs) of new technology stocks.

The Financial Industry Regulatory Authority (FINRA) has more details here: http://clicks.aweber.com/y/ct/?l=EPyWa&m=J79dnn2PqGtWfo&b=gdIwZNT6qshTK1siZ90Yww

Link Click Tricks

There are all sorts of ways crooks use the YouTube name to lure victims into giving away personal details or downloading malware.

For example, they send you an email with a link supposedly to a YouTube video.

Instead you're taken to a page that looks exactly like the real thing but you're asked to sign on, thus enabling the scammer to hijack your account.

In one common case, you're asked to provide your cellphone number before you can view, and you're then charged via your phone bill, either for a one-off viewing or some sort of recurring service.

Other link click tricks they use include emails claiming to be from YouTube itself and inviting you to get in touch (via a link) because your video has been removed or because it's the most popular item on YouTube.

Alternatively, you may get a message saying your version of the Adobe Flash video application needs to be updated before you watch. When you click the "update and install" link, a virus is actually installed on your PC.

Another frequent virus trick is to send victims an email or post a message on their Facebook page claiming a revealing video of them has been posted on YouTube.

Again, you're taken to a spoof YouTube page that uploads malware.

Typosquatting

We wrote about typosquatting in an earlier report.

http://clicks.aweber.com/y/ct/?l=EPyWa&m=J79dnn2PqGtWfo&b=L6VKpDXjBgxa7qOtVJoADg

Tricksters set up websites with very similar names to genuine sites. They just change one letter, or swap the letters around, to take advantage of users mistyping the sitename (a mistake commonly referred to as a "typo").

Depending on where you end up, you may be the victim of a scam or just bombarded with advertisements.

A well-known typosquatting address (we're not giving it out!)takes you to a page that looks similar to YouTube, but it doesn't use the name and thus stays within the law.

You're asked to complete a "survey," which involves giving personal details including your cellphone number. Again,you'll find a charge on your phone bill.

Phony Comments

One of the key elements of the YouTube service is the ability for subscribers to leave comments on videos.

This is used for a range of tricks involving bogus postings.

For example, a phony product video of the sort mentioned above may also have favorable comments from fake customers.

In other cases, posters use the comment facility to promote their own products or include malware links.

Abuse and Pranks

Some YouTube videos contain nasty scenes, unsuitable for most adults, let alone children.

In other cases, individuals post abusive and offensive comments, peppered with foul language.

In the meanwhile, unsavory characters prowl the YouTube listings looking for videos that have innocently been uploaded by children or teens (of themselves).

We don't need to tell you what these nasty people are up to. Just make sure your kids are aware of the risk.

And a word of warning to parents of tweens and younger kids: one Scambusters team member was shocked to discover that the #1 result when searching for a certain cable all-cartoon channel was an adult film with an expletive laden description of the "cartoon." Sometimes even innocent searches can return
some nasty results. Be aware.

Sometimes, of course, people produce videos that pretend to be of genuine events but are really spoofs.

YouTube is full of these and they are mostly harmless -- provided you realize at the outset that they're not real.

However, a group of young pranksters were recently arrested for faking an attack in a parking lot, which they were recording for a YouTube video!

What You Can Do About YouTube Nasties

We've only just exposed the tip of an iceberg when it comes to potential YouTube related scams.

The organization itself posts numerous warnings on its site. The best starting point to learn more about how to protect yourself is the YouTube Safety Center at http://clicks.aweber.com/y/ct/?l=EPyWa&m=J79dnn2PqGtWfo&b=uCa1W2zXhS3h56mufgfFxg

Beyond that, the key to staying safe is to follow these five
rules:

1. Be wary about clicking on links to YouTube videos. If you do click, check the address bar carefully when you arrive to ensure that it contains "YouTube.com." If it contains another word before that -- like "Anotherword-YouTube.com" -- it's not YouTube.

2. Even if you key in the address

yourself, check that you spelled it properly.

3. Be skeptical about the videos you watch and never take action purely on a recommendation you see either in a video or comments. Always take further advice.

Similarly, be skeptical about videos that seem to portray something sensational. It may just be a clever spoof.

4. Be aware yourself and warn your children about the public nature of any videos you or they post.

It is possible to post videos for private sharing only. The option presents itself when you upload.

5. Be prepared to be shocked -- and, again, warn your kids appropriately.

If you see a video or comment you find offensive, report it to YouTube. You can also click the "flag as inappropriate" icon located just below the video, to the right.

The advent of YouTube has turned us into a nation of amateur filmmakers, and it's a great way of sharing experiences and ideas both with friends and the public generally.

But YouTube works best only if it's used responsibly, viewed cautiously and considered skeptically.

Reprinted from Internet Scambusters

4 Benefits of Gate Automation and Access Control

By Charl F Mijnhardt

As members of the human race, the desire - or, to be more accurate, the *need* - to protect what is ours, is inborn. Thousands of years of evolution have ensured that we will fight tooth and nail so that no harm will to come to us, our loved ones, or our possessions. Whenever we are in danger, those little evolutionary alarms go off and our bodies offer us two choices: either run away or stand and fight. This is what psychologists call the *fight or flight* response.

But modern technology provides us with a third alternative: *prevent.* What if we didn't have to stand and fight but didn't exactly have to turn tail and run, either? We can efficiently protect what is ours by simply making good use of the tools that the Cyber Age has given to us.

Gate motors have been around for the last two decades or so and, much like us, they have also evolved to be quick-thinking, robust machines that are able to relentlessly guard our homes and offices like unflinching sentinels. They also act as faithful servants, opening and closing our entrance gates without so much as a word of objection - it's what they were built to do.

The benefits offered by gate motors are manifold, and we will now look at some of them. We'll also discuss a very close relative of gate automation, namely access control.

1. Safer

The obvious detriment to one's lumbar region aside, getting out of your vehicle to open a gate can be extremely hazardous from a personal safety perspective. We've all heard of people getting hijacked or attacked while opening their gates. Having a gate motor installed may not eliminate this possibility entirely, but it will certainly reduce the likelihood. Some modern gate motors have adjustable speed settings, meaning that you can have your gate open and close rapidly and thus reduce the time that the gate is open and also the time that you are stationary in your vehicle. There are also some particularly advanced operators with innovative features such as beam automatic closing, whereby the gate closes the moment that the safety beams have been cleared.

2. Convenient

Why go through all the effort of stopping your car, getting out,

and then straining your poor, long-suffering back just so that you can get into your own property? It is certainly much more convenient to simply press a button and let your gate motor do the rest. Gate motors also offer you considerable freedom when it comes to the manner in which you will activate it, since you can connect anything from a remote receiver to an intercom and use that as a triggering device. There are even GSM-modules that allow you to trigger your gate using your mobile phone. It doesn't get more convenient than that, especially in an age where our phones have become extensions of our arms.

3. Versatile

Yes, gate motors do open and close gates, but there are several models on the market that do so much more than that. Some models provide onboard timers, allowing you to set automatic activations or to bar certain inputs from working at set times, while others can be interfaced with third party alarm systems and infrared beams so that you're notified when would-be criminals are loitering in front of your gate. It's easy to see how a device that once had a singular purpose has now become a compact electronic defence force.

4. Total control

As I mentioned in the introduction to this article, we'll also take a brief look at access control. Now, access control is rather a broad term and can refer to any number of devices including keypads, proximity card readers, GSM-modules, traffic barriers and of course gate motors. The wonderful thing about access control is that it affords you total control over who enters (or leaves) a property. Some variants, particularly proximity tag readers, can be interfaced with computers and allow the user to upload transaction logs, edit functionality remotely, selectively add and delete users, etc. This does its bit for convenience as well as security.

Innovation in the field has also ensured that no matter what your automation requirement - whether you have a swing or sliding gate, light or extremely heavy, whether you require automation for your home or business - there is bound to be a gate motor and/or access control system out there for you. So don't wait: Automate!

Charl Mijnhardt is the copywriter for Centurion Systems, a leading South African gate automation and access control company specialising in:
•Sliding gate motors
•Swing gate motors
•Garage door operators
•Intercom systems
•Proximity access control systems
•Traffic barriers and accessories
•Keypad access control and
•GSM devices

Reprinted from ezinearticles.com

Existing Patio Door Locks May Not Be Enough To Protect Your Home

By Aady Mircal

Many homeowners make an all too common mistake when it comes to securing their home: Relying on the patio door locks that come equipped on standard sliding glass doors. While many people feel that their sliding doors are secure enough, it is mostly due to the fact that many of them are not aware of the fact that patio doors may be one of the easiest points of entry for an intruder.

Sliding Doors Are Secured By Latches, Not Locks

Among the many reasons that burglars favor sliding glass doors as their point of entry is the fact that the mechanisms that is holding them shut is not actually a lock. Rather, the pins that are holding the slider in place are simple latches. These small pins are responsible for stopping a very large door from being forced open, and unfortunately, they do not always live up to their expectations.

Pins that have been made with substandard craftsmanship or installed by an amateur can often become loose and fall out of their position. This greatly weakens the security, even if nothing seems amiss upon quick inspection.

Sliders Can Be Easily Lifted Off Of Their Tracks

Homeowners who fail to perform regular maintenance on their sliders face bigger problems than the occasional slider becoming stuck. Rollers that are in poor condition or are improperly fitted are the easiest doors for intruders to open, although their means may be much different than expected.
Sliders that are fitted with inadequate rollers can very easily be lifted from their tracks, even from the outside of the home. While some people may assume that placing a dowel into the tracks will prevent unwanted predators from entering their residence, it will only deter them from sliding the door open.

Special Patio Door Locks Should Be Used To Secure Sliders

Rather than relying on cheap and sometimes ineffective blocking devices, homeowners should consider having patio door locks installed on all of their sliding doors. There are many different types of patio door locks that can be installed as a DIY project or by a residential locksmith.
One way to secure your slider is to install track blockers that can be screwed into the tracks, which prevent sliders from being forced open horizontally. Foot operated patio locks work the same way, and they only require the push of a foot to engage and release the locking mechanism.
To prevent doors from being lifted off of their tracks, choose a lock that contains a pin that is inserted through both the slider and the frame. These locks are commonly placed at the top of the frame, which works well for some families due to the fact that they are out of the reach of small children.
Keyed patio door locks are also a great option for securing this otherwise vulnerable entryway. Keyed patio door locks allow the homeowner to gain access from the outside, which is not standard for most sliders. Having this type of lock may require the work of a residential locksmith, due to the more complex installation requirements.

About the Author
As South Florida's premiere residential locksmith Accredited Lock and Hardware has 20 years of experience in installing high-security, custom patio door locks. For information regarding home security, contact Accredited Lock and Hardware at (954) 467-8606.

Reprinted from Ezine Articles.com-

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