Issue 11 | Volume 1 | September 2014

Security Solutions

ADDRESSING THE NEEDS AND SECURING THE FUTURE

Helping secure your world

Editor's Note

September is a month of reflection, a month where most persons remember all the promises made and tasks outlined at the beginning of the year which are yet to be accomplished before the year draws to a close. Some of these tasks may possibly be work oriented, or a project that is yet to be untaken at home. As always, Amalgamated Security has carefully selected articles which will help guide you in the direction of achieving some of your goals.

The first article, which is written by Paul Alleyne Ph.D, Manager of Amalgamated Security's Electronic Security and Integrated Systems Department, outlines the benefits of hiring a security company that will provide a monitored alarm service for your home or business while giving some pointers on what to look for when selecting your security alarm provider. The components of this article may have been a major undertaking on your 2014 "to do list". In article number two we see that most of the time as a manager, one is often asked to provide information security, however your training does not always provide the required background. In performance reviews, information security also might be a Key Performance Indicator for some managers which is yet to be achieved, so in light of the aforementioned, this article provides a short list of steps that mangers can take to help fulfill this facet of their supervisory role.

In keeping within the working environment, many have seen recently more and more Plants face the risk of machine theft. Managers and Plant owners are faced with the responsibility of mitigating against such occurrences. In order to decrease the likelihood of machine theft plant operators and managers can introduce new systems. One type of machinery that is always in the top 10 list for theft is an excavator, article number three outlines how excavators are stolen and disposed of. The knowledge obtained by reading this article can stop machinery and more specifically, excavator theft. Another item on your 2014 "to do list" which may not have been completed might be changing/updating your current locks at home. Numerous reasons may have led you to consider changing your locks, however when undertaking this project remember to select new locks which will help against Lock Bumping. Article four describes what this is and how to protect yourself, family members, your home and valuables from this simple, traditional technique.

In the last three articles we touch on an ongoing problem in today's society. In 2014 it may have been your declaration to learn more about the different type of scams out there. One important fact to remember is that scammers use various mechanisms to swindle money out of the purses of an unsuspecting victim. These include, but not limited to: your mobile telephone, an internet website and even a recently purchased used car can all land you into the claws of scammers. Articles five, six and seven respectively speak about three different types of popular scams.

These articles/safety measures were selected with our readers in mind. We know that there are many goals which are yet to be accomplished before year's end and it is ASSL sincerest hope that the measures outlined will help settle some outstanding tasks for 2014.

Regards
ASSL Marketing Team

Choosing the Right Security Alarm Provider

Written by Paul Alleyne Ph.D. – Amalgamated Security Services Limited

This article deals with the definite benefits of hiring a security company that will provide a monitored alarm service for your home or business while giving some pointers on what to look for when selecting your security alarm provider.

Statistics show that if a burglar suspects an alarm will go off when he enters your premises, he is less likely to attempt to break in.

While there are many experienced, reputable and reliable companies operating in the Caribbean there are inevitably some people who are out to take advantage of the concerned home owner. So you must be aware of the "easy money operator" and be sure that what appears to be a bargain doesn't turn out to be a costly mistake in the long run.

The percentage of homes and businesses in the Caribbean with alarm systems is rapidly growing due to efforts to combat crime, the industry efforts in increasing customers' security awareness and the affordability of the service being presented by various security providers across the region.

Individuals today are steadily becoming more willing to pay for the cost of an alarm system and the monthly monitoring charge for protection against crimes being perpetrated against their residences. To encourage individuals to acquire alarm systems some companies have been offering alarm systems on a lease rather than requiring the customer to make an outright purchase. Buying your equipment rather than leasing however could save you money in the long run. Under lease programs offered by some security companies, the customer pays a minimal installation fee but then has a three- to five-year lease payment in addition to monthly fees for monitoring services. If you buy the equipment instead, the initial investment will be higher but the equipment will belong to you, thus making it easier and more affordable to change service companies later if you have to do so.

One of the factors that should be taken into consideration when making the seemingly "right" decision to equip your premised with an alarm system is the creditability and proven track record of the security company which you choose to engage. The security market is being flooded with security alarm providers whose claim to fame is the ability to provide you with superior service at a low price. Typical working class citizens tend to lean towards these providers based on the perception of being able to save a dollar. However, before making a decision purely based on the lowest cost factor, I would suggest you carefully consider the track record of the company that is offering to install the alarm system. When an emergency occurs that is the wrong time to find out that the alarm system was not properly installed or did not provide complete coverage and so failed to detect an intruder.

Apart from the ability of the contracted security company to competently install your system and ensure that it works properly in the event of an attempted intrusion, one of your other concerns should be whether the individuals employed by this company can

be trusted in your homes amongst your loved ones and valuable possessions. Remember that whoever you allow into your home could potentially use any knowledge gained there to your disadvantage and so the biggest threat to your home and the security of your loved ones' may be the people who you have chosen and entrusted to provide you with the service of protection.

It is a fact that in today's society, it is important to protect your loved ones and assets from criminal activities and to have the added peace of mind of knowing that when you are away from your home either at work or on vacation or away from your business that there is a company who you can trust and rely on, watching your back.

I would like to suggest some simple guidelines when choosing your provider to ensure that you get the maximum value for your money and Total Protection for your family:

Your security company of choice should:

- Be recognized as a reputable Private Security Company
- Have been established in the Electronic Security and Alarm Monitoring business for several years
- Be certified by a board such as IQ (Installation Quality) which gives consumers a way to identify alarm companies that are committed to providing high-quality security and life safety systems.
- Employee a team of certified alarm technicians and not be dependent on sub-contractors
- Have alternative first response service available
- Have full insurance coverage meeting industry standards
- Include a Backup power supply as part of the alarm system
- Take the time to sit down and understand your needs and lifestyle and then designs a system to suit you

In addition to the above guidelines you should also narrow your choices by getting recommendations from friends or neighbors, an insurance agent or business/trade association. When you have narrowed your choices to 3 or 4 companies, arrange an appointment with each company when all members of your household will be present. Be sure to ask for the name of the person who will be calling on you, and verify his or her identification upon arrival. When the representative from the company comes to your premises ask about all the features of the alarm system and then have them do an inspection, and then prepare a written quotation for you plus provide references. Carefully study each quotation that you receive and also have them provide the written contract covering the monitoring service so that you know exactly what you are getting.

Conclusion

Security firms provide a highly sensitive service for a relatively low cost. Select a well-established company with a record of successful operation behind it. The failure rate among companies entering the security field is high and you don't want to be left with a system that requires service with no one to provide the servicing.

About the Author

Dr. Paul Alleyne is the Head of Electronic Security & Integrated Systems at Amalgamated Security Services Limited (www.assl.com). He has over 15 years experience in electrical & electronic systems design and implementation and holds a Ph.D. in Electrical Engineering. He also holds a B.Sc. in Electrical & Electronics Engineering & a Masters of Engineering in Engineering Management. Amalgamated Security is the parent company of Alternative Security Services St. Lucia

Limited and operates in Grenada, Barbados, Guyana, St Lucia and Trinidad and Tobago.

http://www.freedigitalphotos.net/images/woman-using-security-system-photo-p251913

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

What Can a Manager Do to Provide Information Assurance?

By [http://ezinearticles.com/?expert=William_G._Perry,_Ph.D.]William G. Perry, Ph.D.

Managers, generally, are specialists in fields other than computers. Most organizational leaders have expertise that falls in zones like finance, marketing, sales or some other business area. Rarely are the managers experts in computer security and if they were, they wouldn't have time to solve security related problems. The managers would be too busy fulfilling leadership roles.
We know managers are ultimately responsible for protecting information assets but lack the skills and knowledge to build a security infrastructure. So what is a manager to do about information security?

Shown below is a short list of steps that mangers can take to help fulfill their supervisory role for information security.

1. Obtain and maintain a high level of situational awareness of what the organization is doing or has done to provide for information security, the protection of information assets and backup plans for business continuity.

2. Show an active interest in information security and let those you supervise know you are familiar with their responsibilities. Those who work for you will get the following message: Information security is important to my manager.

3. Set a good example. The manager must engage in following security best practices. Otherwise the employees will quickly get the message that information security isn't important.

4. The manager should identify the key metrics for information security in his or her department and monitor each one. Subordinates will quickly determine that their boss places a high value on protecting key information assets.

5. Inform your subordinates of security incidents or recent security breaches that have happened in your company or in industry. Supply those who report to you with examples of what could go wrong and the consequences of failing to put a high value on security.

6. Orient your employees to any existing organizational information security plan. Make sure that each person is aware of his or her responsibility.

7. Be supportive of information security awareness training for your employees. If the information technology department is without such a plan, ask them to help you create one.

8. Volunteer to lead the effort to help your company create an information assurance plan if your company is without one.

9. Ask your employees if they perceive of any way that security can be enhanced.
10. Part of a manager's job is to anticipate potential problems and consider possible actions that can mitigate negative surprises. Educate yourself. Conduct an information threat and vulnerability assessment.

Speak with people in your company who are responsible for information security and ask them for any suggestions that they might make to help improve your department or organization's security.
Mangers work in an asymmetric threat environment. Attacks against information assets can come from just about anywhere. Being alert and developing a culture of secure information practices among employees is highly recommended. Building support throughout your organization to protect important information assets is essential. The manager is in the unique position to do so.

Download our FREE ebook, "How to Secure Your Computer". Just access the web site (no registration) at http://www.computer-security-glossary.org and click on the "FREE eBook" link.

Dr. William Perry also publishes the Computer Security Glossary.
Dr. Perry is an information security specialist with significant experience as a university professor, author and service provider to various federal agencies including the Office of the Director of National Intelligence, the Department of Defense and the Federal Bureau of Investigation.
Article Source: [http://EzineArticles.com/?What-Can-a-Manager-Do-to-Provide-Information-Assurance?&id=8608137] What Can a Manager Do to Provide Information Assurance?

http://www.freedigitalphotos.net/images/Computing_g368-Business_People_Working_Together_p45797.html

http://www.freedigitalphotos.net/images/Business_People_g201-Business_People_In_The_Meeting_p40850.html

Excavator Security: How Equipment Is Stolen and Disposed Of

By [http://ezinearticles.com/?expert=Ben_Halliday]Ben Halliday

How exactly does one steal a vehicle which weighs several tons, is yellow and has a big scoop attached to it? It might seem like a bizarre idea to steal a digger, or an excavator to give it its proper name, but the theft of excavator equipment is a huge market. Theft is commonplace and this is as a result of the low level of excavator security that is present. There is also a lack of awareness about the problem and a neglect of the problems which, when combined, means that this is a huge problem.

However, one of the biggest reasons why excavator security is so undermined is because a lot of equipment is controlled by a universal key. Most plant fitters hold a set of these and they give access to a huge number of vehicles, meaning equipment can be started up and removed from a site. Plant thieves will often be part of a criminal network which shares information about sites with poor excavator security, allowing them to pounce on specified targets. After the equipment has been stolen, it will often be driven for a few hours before being left in an area where the equipment is visible for 24 hours. This is so that the thief can work out whether or not the excavator has a tracking device on it. Excavator security systems have made it significantly harder for thieves to get away with thefts, and as a result, they have to leave the equipment for a day or two to see whether it is recovered. GPS tracking devices mean that the equipment is traceable to an area of two metres squared.

However, if the equipment does not have GPS tracking, then the owner is in trouble. After leaving the equipment for 24 or 48 hours, the thief will recover the equipment before taking it to a holding depot where they are based. This is likely to be out of sight, with a single road access and with security measures along this road. This means that the thief can tell if the Police show up and make a getaway on foot. When the thief has the equipment, they will decide whether to simply sell the excavator on as it is, or to try and either alter the vehicle identity or clone the identity of another piece of equipment. Removing registration plates and erasing the vehicle identity number is the simplest thing to do, before selling it at a very cheap price to someone who would probably know the item is stolen. Some criminals will get false registration plates and create a new identity number to put on top of the old one, however, or give it the identity of an existing piece of machinery located somewhere else around the country. The vehicle is now ready to be sold.

After this, it is commonplace for the equipment to be shipped overseas and sold. Sometimes the criminal(s) will recruit a haulage company to transport the item or they will do it themselves. Ports have hundreds of plant vehicles passing through their gates everyday so it is very difficult to trace equipment which is stolen.

Once the vehicle is overseas it will be almost impossible to recover. As a result it is crucial that sites do more to improve their security. By fitting equipment with excavator security systems, you can significantly increase the chances that equipment is recovered within a day or two of it being stolen. On top of this, users must try to improve site security and register all equipment with a database. It is difficult to tackle excavator theft but by shying away from it, those in the industry are breeding a culture of theft.

Ben works for [http://www.plantsecurity.co.uk/excavator-tracking/]Plant Security. The company is a specialist provider of security tracking and telematics products designed specifically to meet the needs of the construction industry.

Article Source: [http://EzineArticles.com/?Excavator-Security:-How-Equipment-Is-Stolen-and-Disposed-Of&id=8475712]

Excavator Security: How Equipment Is Stolen and Disposed Of http://www.freedigitalphotos.net/images/big-excavator-photo-p168299

If you are interested in learning more about our vehicle tracking software click the attached link:

http://gis.assl.com/our-services/inteltrack-service

How to Protect Your Home Against Lock Bumping

By Shalini Mittal | Submitted On July 26, 2014

With security systems in place and doors properly locked, you often believe that your home is impervious to robbers. However, thieves take advantage of the loopholes you are most likely to ignore. Simple, traditional techniques such as lock bumping can give a robber easy access into your home.

What is lock bumping?

Lock bumping is one of the many lock-picking techniques. It is a method used by locksmiths to open locked doors

with no key and is equally popular with dacoits as a technique to break into homes. In this technique, a specially filed down key is inserted into the cylinder lock. The ridge is cut to a maximum depth of nine on a key making machine and hence, the bump key is also known as the 999 key.

After this, it is gently bumped or struck with another object that is usually a screwdriver or mallet. The force used to bump the key jars the pins and pushes them to the sheer line. If this is accomplished successfully, the lock turns and the door opens. Thus, there is no sign of forced entry or the need to damage property which could alarm homeowners or passersby. To add, it takes only a few minutes to complete and does not make any loud noise.

As per the statistics provided by professional locksmiths, a large number of burglars use the lock bumping process. There were three main reasons noted for it. Most homes continue to use cylinder locks to secure their homes and cylinder locks are the most vulnerable to the so-called bumping process. A key used to bump a lock is easily available and can be ordered over the internet. Also, the procedure does not require any special skill. Hence, it is important to consider how vulnerable your home is to lock bumping when evaluating the security needs of your home or office.

Protecting Your Home against Lock Bumping

It is necessary to shield your home against lock bumping. It includes installing stronger locks as well as beefing up other security measures. A few measures have been listed below.

1. If possible, change all the old cylinder locks around your house. Locksmiths have started manufacturing locks that are both resistant to bumping and picking. It is quite difficult to get a bump key for these models.
2. If the project of changing locks it too expensive for the moment, you can consider modifying the existing locks by asking a professional locksmith to add more pins. Rekeying locks makes it difficult to pick and bump locks.
3. Locks today have an option to install a protector over the cylinder. This metal guard protects the cylinder and requires magnetized keys to open it. Since the key cannot be duplicated, there are no chances of bumping a lock.
4. Install a home security system to monitor indoor and outdoor areas. The home security system alerts home owners when a door has been opened by tampering the lock.

You can make it more difficult for burglars to break into your home by adding chain latches to exterior doors.

Click Here to know more about Locksmith Corpus Christi TX.

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

Reprinted from Ezinearticles.com

If you are interested in learning more about our access systems visit our website at: http://esis.assl.com/alarms-electronic-products

One Ring Phone Scam Cashes in on Curiosity

It goes by several different names -- the missed calls scam, the one ring scam, the ring and run scam, and the dial-and-disconnect scam -- but the aim is always the same: to steal 20 or more dollars from you.

Your cell phone rings once then stops and you're left with a sense of curiosity that will only be satisfied by finding out who phoned you by calling them back. That's what the crooks know and that's why they use this trick.

You won't recognize the number or even the area code, which is often something like 268, which is used for the Caribbean island of Antigua. Other Caribbean codes you might see include 242, 246, 264, 284, 345, 441, 473, 649, 664, 758, 767, 784, 809, 829, 849, 868, 876 and 869.

You may have family or friends living in or visiting the Caribbean region and may think it's a genuine call. But, almost certainly, that one ring is a clue to the fact that it's a scam.

Alternatively, the caller may wait for you to answer and then respond with a muffled voice you can't understand or other distressing sounds that leave you puzzled and worried.

And, in a third variation, if you use voicemail, the scammer may leave a message, claiming to be from the police or, say, a hospital, claiming there's been an emergency and asking you to call back.

Whichever route they use, if your curiosity does get the better of you so that you decide to call back, you'll be making an international premium line call with a basic fee of around $20, plus a billing charge of between $9 and $20 a minute. And it may take a couple of minutes or more before you realize something's not right, and hang up. In the meantime, you'll be greeted with a "please hold" message followed by a music recording or perhaps an advertisement.

If you don't know about this trick, you won't know just how costly that call back was until your phone bill arrives.

Phone and law enforcement officials say victims' numbers are dialed randomly by computers operated by scammers who work from various parts of the Caribbean.

7 Key Actions

So, what can you do to minimize the risk from this scam? Here are 7 key actions:

1. If the phone only rings once and you don't recognize the number, don't call back.

2. Be aware of and wary about the area code numbers we listed above. They look like they're from the US but they're not. Some smartphones and carriers actually provide the location of the number on-screen.

3. Set up and use voicemail on your cell phone service. If a call is genuine, a serious caller will usually leave a message. However, as we indicated above, beware of scammers leaving phony alert messages asking you to call back. You may have to use your judgment on this. If you don't know anyone in the relevant area code region and haven't visited it, don't call back. The scammer won't say which region he's calling from. He'll probably want you to think he's in the US, so check that code carefully against the list we've provided. Also, ask yourself how the

supposed caller would have your number.

4. If you do think you should make the call, check the number through online directories first. They will tell you where the phone number is registered.

5. Always check your phone bill carefully for unexpected and unusual charges. If you get stung by the one ring scam, try to resolve the bill with your cell phone carrier.

6. Also, ask your carrier about whether numbers from particular areas can be blocked.

7. If you've lost money and can't get it back from your phone service provider, consider filing a complaint with either the Federal Trade Commission (see https://www.ftccomplaintassistant.gov/#crnt&panel1-1) or the Federal Communications Commission (https://www.fcc.gov/complaints).

The one ring scam is just the latest in a number of tricks that crooks use to try to fool you into making calls on premium-charge lines.

We reported on this many years ago, in one of our earliest issues.
http://www.scambusters.org/ScamBusters8.html

Sad to see that it's still around in a new guise. So, just remember this simple rule: One ring, one scam!

Reprinted from Internet Scambusters

http://www.freedigitalphotos.net/images/agree-terms.php?id=100254916

http://www.freedigitalphotos.net/images/agree-terms.php?id=100121182

Stolen Goods Online: 8 Red Flag Warning Signs

You might have seen news reports a few weeks ago about Federal authorities charging three people in connection with the sale of more than $7 million of stolen goods on eBay. The scale of the alleged crime might have been surprising -- it was said to have run for 10 years and netted around $4 million -- but there's certainly nothing unusual about the sale of stolen items online.

Online shoppers find themselves victims of this crime every day and police have specially trained squads who constantly scrutinize sales sites looking for the proceeds of burglary and theft. Law enforcement organizations also have access to a national database of missing items, including their serial numbers.

So, what can you do to avoid buying something that's stolen? And if you do buy something in good faith that turns out to have been stolen, what are your options?

Red Flags
Though you can't always be certain whether an item being offered for sale online is stolen, there are a number of warning signs that should put you on your guard.

For instance:

- The price is extremely low. Check prices of similar items that have already been sold. This is easily possible on eBay by clicking on "sold listings" in the left-hand panel of the product listings page.

- There is no detail with the listing, just a plain statement of what it is. Before making an offer, contact the seller for details about condition, how long they've owned it and why they're selling.

- The description claims the item was "found." Despite the saying, finders are not keepers without first following a process that includes reporting the find to police.

- If it's a computer, tablet or smartphone, the description says the item is password locked. The seller may claim they forgot the password.

- The seller has little or no positive feedback, or their existing feedback is for a handful of very cheap items. Crooks use this cheap product feedback to build up their credibility record.

- In an online classified site the seller is from out of town and is cagey about giving you any contact information. Usually they don't want to meet, but if they do it'll be away from their home.

  From a personal safety point of view, meeting in a public place like a mall or coffee shop is actually a wiser action than going to someone's home. But request their name and home address anyway (which you might be able to confirm online) and ask them to bring some personal identification with them, like a driver's license or proof of ownership. If they make excuses, it's best not to buy.

- They also cannot provide proof of ownership, such as a receipt or product registration record. If it's a private seller, ask if they have a receipt.

- The seller asks you to pay with an untraceable money wire or a cashier's check, and will not accept credit cards or PayPal. Individually, some of these red flags may not indicate that a product has been stolen but they should put you on your guard, especially if there are multiple red flags.

If you know or suspect an item may have been stolen, don't buy it because you could be committing an offense.

What If You Buy A Stolen Item?
First, let us make an important disclaimer: Scambusters does not provide legal advice. Our reports are purely for information and we don't accept liability for any actions you take. Also, we don't have the resources to answer your questions. If you find yourself in a situation involving stolen or suspicious goods, you should get appropriate legal advice.

So, having said that...

First, if you buy a stolen item in good faith and behave honestly when you discover the theft, you are unlikely to be in trouble with the law. Behaving honestly includes reporting it to the police or confirming you have it and cooperating with them if the police contact you -- but make sure it is the police who are contacting you, not a scammer!

Second, a stolen item still belongs to the person it was stolen from, not you, and the police will almost certainly want to return it to them.

Third, you can try to get your money back.

If you bought it from someone who also didn't know it was stolen, they may refund your money when they find out. If they won't, you can try the disputes procedure on the selling site, or check if the purchase is covered by the terms of any buyer protection program they have.
If you paid by credit card, your card company might be prepared to help but company policies vary.

In all cases, the time between when you buy the item and discover it's stolen can be critical. Too long (usually more than 30 days after purchase) and they're unlikely to help. One of the most contentious issues is whether the selling site should compensate duped buyers if the money can't be recovered from the seller.

Unlikely. Think of it like this: Suppose you saw a card advertising a product for private sale on the community board in your local supermarket. If you buy it and it turns out to be stolen, should you expect the supermarket to cover your losses? We think not. So don't be surprised if, when you contact the selling site, you don't get your money back. Most online organizations do their best to try to prevent stolen items from being listed in the first place, and they work closely with police to nab suspects. But, like the grocery store, they probably won't dip into their own pockets to compensate the purchaser of a stolen product.

It truly is a case of "Buyer Beware."
Reprinted from Internet Scambusters

http://www.freedigitalphotos.net/images/Retail_and_Sales_g195-Shopping_Online_p72226.html

http://www.freedigitalphotos.net/images/money-photo-p182397

VIN Switching: Identity Theft for Autos

It's not just us humans that are identity theft targets -- it happens to autos too, only then it's called VIN switching. VIN is your unique Vehicle Identification Number, etched on labels that are supposed to be permanently fixed to the body and other parts of your car. It's the only, mostly reliable, way of being able to accurately trace a vehicle's history and help to confirm title ownership.

It's totally illegal to change a VIN -- even for restorers who might be building a car from numerous different parts. That even applies to vintage motorcycles, which are often rebuilt from "cannibalized" parts. (What owners should do faced with that situation is beyond the scope of this report. You can get advice on that from your state motor vehicle department.)

More worrying is the incidence of criminal VIN switching to either disguise a vehicle's true history or to conceal the fact that the car has been stolen.

The bad news is that sometimes, VIN-switched cars have been sold by perfectly respectable dealers who were totally unaware of the crime themselves. Even worse, if you buy a car in good faith that turns out to have been stolen and VIN switched, you could end up out the total cost of the vehicle unless you can persuade a legitimate seller to give you a refund.

Compared with many other scams, VIN switching is comparatively sparse. After a recent report from Minnesota, the state's investigator for the National Insurance Crime Bureau (NICB) said he encountered about 100 cases a year. That might suggest several thousand cases a year across the United States as a whole.

That means, though, that the crime has flown below the radar of many consumer-watch groups, and victims are usually left helpless to do anything about it. However, it's definitely on the rise. A recent bust of a VIN switching ring in Florida found that more than a thousand vehicles had been stolen and "doctored" to conceal their true identity. Nor is it always possible to detect a VIN switch, with the result that a vehicle might change hands several times without any owner realizing their car is "hot."

Often, the crime only comes to light when big-time car thieves are arrested and their activities are thoroughly investigated, or when two identical VINs are recorded in different states.

According to the NICB, the most common crime is known as the Salvage Switch. A badly damaged car is bought or acquired by a crook using a false name for the title. The vehicle is then officially listed as "salvaged" and the crook uses both the title and the VIN on a similar stolen car.

Another crime, though not really a case of VIN switching, is known as Strip and Run. This is a complex scam in which crooks steal a car and strip it of just about everything that's removable.

The car is listed by police and insurers as "stolen" and therefore can't be sold by the thieves. So, they abandon what's left -- the frame, with its VIN -- somewhere it can be found. Once found by the police, it's now considered by the authorities as "recovered" and is no longer listed as "stolen." In other words, it's a legit auto, just without its parts, and can be sold. The car frame, its VIN and its title are then usually auctioned off by insurers or police, where -- you guessed it -- the crooks buy it back. Then they reinstall all the pieces they removed and suddenly they have a complete, legally owned car, which they can sell.

An even simpler technique is for car thieves to scour parking lots for similar vehicles to the ones they've stolen, read the VIN number off the dashboard plate, and then use it to fabricate a new identity for the stolen vehicles.

You can see a 2008 TV news report on this crime here (warning, this YouTube video may be preceded by an unconnected ad -- it has nothing to do with Scambusters): http://www.youtube.com/watch?v=MeZF0NST-W4

As we said, it's not always easy to detect these crimes.

Most vehicles do have a "hidden" VIN label but viewing it usually involves removing the engine, which even legitimate auto dealers are unlikely to do to check its authenticity!

All you can do is be vigilant. Here's what the National Insurance Crime Bureau (NICB) suggests:

* Look closely at the VIN plate, located on the driver's side of the dashboard, to see if it appears tampered.

* Never buy a used car without getting the vehicle's title or pink slip in person; and double check the vehicle identification number with the number listed on the title, the registration papers and the federal certification label on the driver's side door.

* Ask to see identification of the person who is selling you the car; write down his/her name, address, phone number and driver's license number for your records.

* Call the phone number given to you by the vehicle's owner. Often, scam artists will provide the phone number of a random pay phone.

NICB also has a service for law enforcement and insurers to translate VINs, which contain coded information about the vehicle make, model and engine size.

Also, of course, you should be on the alert for car deals that seem too good to be true, extremely low odometer readings, and individual sellers who seem cagey about their identity or address.

Reprinted from Internet Scambusters