Issue 21 | Volume 2 | June 2016

ADDRESSING THE NEEDS AND SECURING THE FUTURE

Helping secure your world

Security Solutions

Editor's Note

June officially marks the midway point for 2016. In the Caribbean region, persons have many concerns about their personal and national security. There have been an unprecedented number of serious crimes, murders, assaults, and missing persons throughout the region. Due to this persons have adopted various methods of protecting life and property from the forces of evil. This quarter, our newsletter will look into various methods of securing one's self.

One "old school" method of protecting your life and property from the criminal elements is to get a "bad dog". This method has been proven and tested throughout the generations. Dogs give a sense of security and they are willing give the ultimate sacrifice to save yours and your family life. This is because dogs are not humans; they react based on instinct which can be both a positive and a negative. In article one, which is written by our very own Brian Ramsey, Regional Development Director, discusses how to safely have protection dogs and also have infants. Article two keeps on the topic of pets and discusses the different hazards they can face within your very own home.

Security at home and work is important but what about your third place. Some person's third place might be the gym, campus or their favorite coffee shop but for most people their third place is church. Do you know if your safe haven is secure, and if it is, how secured is it? Article three discusses church video surveillance as a mechanism in making your church less venerable to thieves. Continuations of security solutions are presented in the articles titled Changeable Padlock Code and Smart Home Solutions in articles four and five.

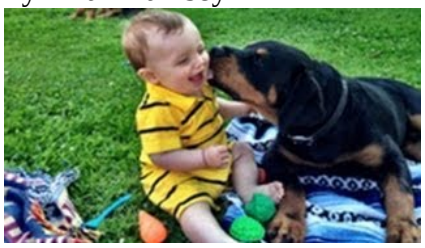
"According to the latest figures, approximately one in every 16 online hotel bookings is a fake. Six percent of travelers ended up booking on phony hotel websites that looked like the real thing". This is a telling quote from the sixth article which speaks to fraudulent activities which take place online frequently. This article is timely as we approach the July – August vacation period, as most people might be planning their family vacation, so this article teaches you what to look for when booking your hotel accommodation.

We do hope you find these articles and the safety methods helpful in some manner and we at **Amalgamated Security Services Limited** will continue to fulfill our commitment to provide quality service for all customers.

Regards
ASSL Marketing Team

Family Dogs and Infants

By Brian Ramsey



Recently there was a newspaper article that told of a 5 month old baby being killed by the family dog in central Trinidad. To some persons this would appear to be a highly unusual incident and many would blame the dog saying that it has become vicious or “turned” on its owners. While this killing of a human by a dog is not an every month occurrence it is also not unusual or unheard of.

The first epidemiological study of dog-bite fatalities in the United States was conducted by an epidemiologist with the Centers for Disease Control and Prevention in 1977. The study reported that all but one of the cases involved male dogs. Most incidents involved victims who were smaller or weaker than the dog. Thus, children under 5 years old accounted for the majority of victims.

A study conducted at the University of Texas Southwestern Medical School identified fatal dog bites during the period 1966–1980. They identified 74 incidents from newspapers and the medical literature. They found that the most (23) fatalities occurred in infants under 1 year old, and in most cases the dog was owned by the victim's family.

The group, Wilderness & Environmental Medicine conducted a study that covered the period 1979–2005. This 27-year study looked at cases in which the cause of death was dog bites. During those 27 years, the study found 504 deaths due to dog bites. The majority of victims (55.6%) were less than 10 years old.

Each of these studies shows that the killing of children by a dog and indeed one that is a family dog is not an unheard of occurrence. If we examine what has been reported about the incident it provides some clues about why it may have occurred and ultimately what individuals should know about having dogs for protection especially with young children.

The newspaper articles have said that the dog was a cross breed of a Rottweiler and a German Shepherd. They also state that the family had the dog for about one year and the baby was approximately 5 months old. Thus it is clear that the baby came into the family after they had already had the dog. In seeking to understand further about why this incident may have occurred we also need to look at the traits of the two breeds that were cross bred to produce this dog.

The American Kennel Club describes the Rottweiler as calm, confident and courageous dogs with a self-assured aloofness that does not lend itself to immediate and indiscriminate friendships. They respond quietly and with a wait-and-see attitude to influences in their environment. It has an inherent desire to protect home and family, making them especially suited as a companion, guardian and general all-purpose dog. Another description says Rottweilers love their owners and may behave in a clownish manner toward family and friends, but they are also protective of their territory and do not welcome strangers until properly introduced.

German Shepherd dogs have been described as courageous, keen, alert and fearless. They are cheerful, obedient and eager to learn, while also tranquil, confident, serious and clever. German Shepherds love to be close to their families, but can be wary of strangers. This breed needs his people and should not be left isolated for long periods of time.

We thus have two breeds that love to be around the family, but are aloof to and wary of strangers, while at the same time protective of their territory.

Having owned both breeds the writer can attest to the accuracy of these descriptions. The dog in this incident was cross bred between the two breeds and so it is likely that wariness of strangers was genetically heightened in this dog.

If we now take all the previous information and approach this situation not from human thinking but from the mind of a dog we will see that some dogs, especially these two breeds, willingly accept a new addition to the family and may even become protective of this new addition possibly viewing the child as a new puppy. Other dogs of these two breeds however can view this newborn infant as a threat to their position in the family hierarchy. They become jealous and resent the intrusion of this child which is now vying for the attention of the masters. These are dogs that love to be around people and to receive attention from their owners and now they find themselves in the situation where they are receiving less attention and this stranger, which their genetic traits make them wary of, is receiving some of the attention that they formerly received. As a result a dog with this type of breeding reacts negatively and that can be by either seeking to dominate this new addition by biting and making the infant understand that "you are subordinate to me" or in severe cases biting to kill with the intention of getting rid of this intruder and so regain their position in the hierarchy.

How therefore should dog owners deal with the situation where they are expecting a baby and have a dog that has been "like their baby". Some persons take the approach of giving the dog additional attention in the weeks leading up to the baby's arrival because they know that once the baby comes they will have less time to spend with the dog. This approach however can be a fatal mistake because now the dog begins to expect even more attention. Instead experts advise the opposite and say to reduce the attention given to the dog prior to the baby's arrival so that when the baby comes to the home the dog does not perceive the baby as the cause of the reduced attention. Even with that approach however dog owners should exercise care in the interaction between the dog and their infant and always be present and paying attention until many months after when you are sure that the dog has bonded with the child.

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

Protect your pet from these everyday poisons and hazards in your home

By Jessica Hunter on December 8, 2012

Your pet is special to you. After all, who else loves you unconditionally, is always glad to see you, and doesn't judge you? You can't always depend on people to treat you like this, but your pet does. It's up to you to treat your pet well and watch out for his safety. Learn these common items, poisons and hazards and keep your pet safe.

Rodent poison

If you occasionally get rats or mice, be extremely careful about where you place the rat poison. Rodent poison is the leading cause of poisoning among pets.

Insect poisons

Believe it or not, over the counter flea and tick sprays are poisonous to pets. Prescription flea and tick medications are much safer.

Human medication

You not only need to keep your medications out of the reach of children but also your pets. Keep all medicines in a high cabinet that your pet can't reach. Pain relief (including aspirin, acetaminophen, and ibuprofen), vitamins, diet pills, anti-depressants, cold medicine, cancer medications are all poisonous to animals. Be sure and pick up any medicine you accidentally drop on the floor.

Human food

We love them so we think our pets will love them too. Unfortunately, many of the foods we love are harmful to our pets. Some of these include chocolate, citrus, raisins, grapes, and avocados.

Household plants

They may look pretty, but to your pet dogs and cats, these are poisonous: schefflera, azalea, rhododendron, dieffenbachia, mistletoe, philodendron, and kalanchoe.

Household cleaners

Everyday household cleaners are deadly to animals. Keep them locked away.

Small objects

Small objects cause choking hazards to your pets just like they do to small children. Watch for small parts from toys, string, yarn, dental floss, and rubber bands.

Fumes

Fumes that we don't notice can cause real danger to some of our pets. The fumes released from self-cleaning ovens and non-stick pans when in use are deadly to birds. Also never use aerosol sprays around birds. Having a pet is a responsibility. One of the responsibilities is to keep them safe. All pets deserve to have a safe, poison-free, and hazard-free home. Use this list of poisons and hazards to go through your home and make it a safe environment for your pet.

Church Video Surveillance

By Dorothy Lumski | Submitted On April 23, 2016

Places of worship naturally place emphasis on creating an open and welcoming environment. Unfortunately, this can sometimes lead a church to neglect its security needs; which leaves them vulnerable to acts of vandalism or theft. A properly installed video surveillance system in a church can help to create a safe and secure environment for congregations and the people they serve.

BENEFITS

Easy Installation: The introduction of High Definition IP Cameras makes the installation of security cameras easier than ever before. Unlike older analog CCTV systems, which involve coaxial cable and power tools, HDIP systems simply require that the IP cameras be mounted in their designated locations and attached to Cat5e cables. These IP cameras can easily be moved around if the church's security requirements change over time.

Prevent Theft and Vandalism in Parking Lot: Mounting outdoor cameras as part of the video surveillance system, can deter possible car vandals or thieves.

High Resolution Images: Implementing an HDIP system for the church video surveillance system will help provide high quality resolution and make it easy to monitor the house of worship clearly and distinctly.

Check Footage Anytime from Anywhere: Network Video Recorders (NVR) make it possible to broadcast your church's security footage securely over the internet.

Remote Broadcasting: Elderly or sick members of the congregation, who can't make it to services, can take advantage of the broadcasting capability over the internet.

RISKS of VIDEO SURVEILLANCE in CHURCH ENVIRONMENTS

1. Vandalism: Vandals try to vandalize cameras in order to obscure their identity before committing a crime.
2. Outages: Power surges or outages may cause a disruption in the video surveillance system or even damage it.
3. Outdoor Damages: Storms, wind gusts, rain and other outdoor hazards can damage your security system and prevent it from recording.

CONFIGURATION of CCTV SYSTEM in HOUSES of WORSHIP

Churches, Synagogues, Mosques and other worship environments vary widely in size, congregation and services. Consider each of the following factors when setting up a video surveillance system in a church.

What are the most important security issues?

- Size of the building: one large room vs. several rooms vs. multiple buildings with classrooms, offices, and library
- Prevalence of crime and vandalism in neighborhood
- Involvement of the neighborhood with congregation
- Parties, youth events or weddings hosted in building
- Facilities leased out for the use of other events (i.e., Alcoholics Anonymous)

SURVEILLANCE SYSTEM SET-UP

- Place cameras in open areas such as lobbies, offices, libraries, classrooms and cafeterias
- If broadcasting services over the internet is desired, place a fixed camera directed at the pulpit
- Cameras placed in parking lots can help reduce theft and vandalism to cars during services and events
- During special events, install security cameras prominently to reduce theft and prevent problems from arising
- Outdoor cameras monitoring the building's perimeter can help reduce theft and vandalism of landscape equipment and other outdoor features.

DL Consultants, LLC
http://www.VigilanceandSecurity.com

Article Source:
http://EzineArticles.com/expert/Dorothy_Lumski/32707

Changeable Padlock Codes

By George Uliano | Submitted On February 29, 2016

The term "Changeable Padlock Codes" can mean a few different things. For this article I will define this as anything that changes the lock or key codes of the padlock. There are multiple ways that can accomplish this, let's take a look at them.

1. The removal of the lock cylinder and installation of a new one.
2. Removing the current lock cylinder and rekeying it then re-installing it.
3. Change the current lock code by turning a key as in the CobraMatic.
4. Removing the cylinder as in the SFIC padlocks.

Let's take a look at these one at a time. In example one CobraLock has two padlocks that are built to have their lock cylinders change very easily. The Cobra Universal Puck padlock uses standard vending locks that are easily changed. The Cobra Flex padlock uses the standard 7/8" cam lock that is easily changed. This is a very unique and patented process.

In the second example you would remove the cylinder then rekey it and cut new keys. To rekey a lock cylinder the combination pins are changed to the new lock code and the keys are cut to match. This method can be done many times. These can also be "keyed" to match another lock code that the user might be using. It should be noted that many padlocks cannot have their lock cylinder removed, therefore they are not rekeyable.

The third method must have a very special lock cylinder already installed. This lock cylinder is known under a number of trade names such as Cobramatic, ChangeMatic, and Gematic to name a few. These locks already have eight lock code changes built in. There is a special key the "Change Key" that allows the user to change the lock code to one of eight different codes. Once changed a new key must be used.

The forth method is a padlock that comes with an SFIC (small format interchangeable core). These lock cylinders are very popular and heavily used in door hardware. Padlocks are also made to accommodate the SFIC cylinder. To remove the lock core you simply use a change key that is specially cut to remove the lock core. You use the same type of key to insert the new lock core. With this type of padlock it is possible to have a padlock or door unlock with the same key.

These are the most popular types of changeable padlock codes.George Uliano is a security professional with years of law enforcement and security experience. He earned a Bachelors Degree in Criminal Justice and Business graduating with honors. George holds three U.S. patents on different locking principles. This combination gives George and His Company Locking Systems International Inc the unique ability to provide its customers with the correct security at an affordable price.

For additional information or to purchase Locks go to http://www.lsidepot.com

Article Source: http://EzineArticles.com/expert/George_Uliano/1500014

If you are interested visit our website at: http://esis.assl.com/alarms-electronic-products/cctv-systems

Home - What Your Thermostat Knows

By Jen Martinson | Submitted On April 08, 2016

New technologies that allow users to control important home devices, such as appliances and security systems, from their phones also give creative hackers plenty of opportunity to hijack and glean information from these "smart" devices. It sounds like the plot of a science fiction movie (and in fact, it has been) but these devices have surprisingly few security features and can give over a shocking amount of information and control to those who might wish to do their users harm.

Good-guy hackers have proven again and again that they can hack into smart devices. Not only are they playfully scaring users by becoming digital poltergeists, but on a more serious note, they have found that they could orchestrate break-ins and harvest valuable personal data.

One security company investigated smart home thermostats and found that they were, in fact, hackable. The hackers found that they could peek into users' web history, the times when they were and were not home, and other crucial information that you wouldn't want a hacker to know.

A thermostat-based security breach is unlikely since the hacker would have to have to physically enter the building and hook up to the thermostat with a USB cable-unless you bought it secondhand.

However, that doesn't mean that there aren't other dangers when all your most important items can connect to WiFi. This trend of internet-connected appliances, known as the Internet of Things, gives hackers multiple routes into your personal life, and they've definitely made use of that ability.

Hackers can already breach camera systems, smart TVs and baby monitors. It may not seem like much of a threat, but it has led to nude images of innocent people being leaked online. Smart meters in Spain have fallen victim to electricity blackouts and billing fraud. One woman found that she had the ability to control all the utilities in the houses of eight strangers, opening them up to poltergeist-like activity and break-ins. Luckily, she decided to alert the company and the device owners to the security problems instead.

Many of these vulnerabilities are impossible to fix because they were built right into the device when developers and engineers neglected to think about cyber security. That means that without altering the router they use to connect to the internet, they are completely unprotected from hackers.

So what are the security experts at these companies doing? The creators who make these smart devices are only taking into account the accusations of data harvesting and surveillance they might face. Right now, companies avoid the accusation that they are collecting personal data via devices by using only server-side privacy measures to protect users. It's well-meaning, but incomplete. It leaves the device itself totally open to tampering.

Some will argue that smart device security is unnecessary, since smart homes are unlikely targets for hackers compared to large databases of personal information, but that doesn't mean hackers aren't going to try to succeed. As addressed above, they already have. The devices may not hold large stores of information like the more common targets of bank or hospital databases, but they are a prime target for hackers or stalkers who want to infiltrate the home and life of a particular person. Celebrities and public figures will be particularly vulnerable, and the danger will only increase further once smart home devices become more mainstream.

However, there is another, more present danger. Smart devices will help hackers become more successful at hacking other targets. A common tactic of hackers is to add malicious code to a website that will invite itself into your device and invisibly enslave it to work for a "botnet," which is a connected network of devices all working to hack something else. Internet of Things devices would be a perfect target, since they're seldom disconnected from the internet and their security is rarely considered.

There's nothing wrong with using smart home technology to help users manage their homes and their lives more efficiently, but it is irresponsible of companies to leave such a gaping security flaw in their products, and their consumers deserve to be aware of the true hacking dangers of the products they're buying and bringing into their homes.About the Author: Jennifer Martinson is an internet security expert and blogger at http://securethoughts.com. She's passionate about educating people on how to keep themselves and their families safe while staying on the cutting edge of technological innovation.

Article Source: http://EzineArticles.com/expert/Jen_Martinson/2267145

To learning more about our home security systems visit our website at: Intrusion detection systems

15 Million Bogus Hotel Bookings Every Year!

How do you rate your chances of being scammed when you make a hotel booking? You probably think the likelihood is pretty remote. But it's not. According to the latest figures, something like one in every 16 online room bookings is a fake. That's right. Six percent of travelers ended up booking on phony hotel websites that looked like the real thing.

That adds up to 15 million bogus bookings every year, handing the crooks an estimated $1.3 billion -- to say nothing of the millions of credit card numbers they harvest at the same time. These fake sites can be really convincing. The website address (URL) often contains the name of the hotel and the photos are copies of pictures on the genuine website.

In other cases, the bogus sites actually pose as online travel agents, again using genuine logos and photos. And in at least one reported case, a fake site had a "contact now" button that connected victims with a fully-staffed, bogus call center.

The American Hotel & Lodging Association (AH&LA), who uncovered the scale of the fraud, say scams are only part of the problem. Almost one third of people who booked rooms via an online travel company (including legitimate ones) rather than directly with a hotel had other complaints, including getting a room that was different from the one they expected, being charged unexpected or hidden fees, being charged an extra booking fee and failing to get refunds for a cancellation.

In other cases reported by the Federal Trade Commission, travelers have arrived at hotels only to learn there's no record of their reservation, the hotel is fully booked, or they have to pay more for the only upgraded room available. "These deceptive practices harm consumers, who don't get what they want or need, suffer the loss of reservations or face additional charges and fees," the AH&LA says.

"These findings clearly show that online hotel booking scams have eroded consumer confidence among third-party vendors," said Katherine Lugar, its president and CEO.

"Consumers deserve transparency in knowing who they are booking with. That is why we have been actively

working with state and national government agencies, including the FTC, as well as consumer advocacy groups, to ensure that consumers are protected and can feel comfortable in the booking process. It's always safest to book directly with the hotel."

But, of course, that advice only makes sense if you know for sure that you really are dealing with the genuine hotel.

As the FTC says in a recent alert: "Just because a webpage looks like the official site of your favorite hotel chain doesn't necessarily mean it is. Before you reserve a room for your next out-of-town meeting or family vacation, make sure you know who's at the other end of that BOOK NOW button."

If you key in the name of a hotel on Google or another search engine, it's not safe to just assume that the first result is the hotel's official site. Some legitimate booking agencies pay for that coveted top slot -- and scam sites can turn up at the top too. And even if you manage to make a successful booking via one of these sites, you may discover, as bookers in the AH&LA survey did, that you may not get your reward points or other perks.

To stay better informed and reduce the risk of being scammed or being simply short-changed on a deal, the FTC suggests you should:

* Book directly through a hotel chain using the toll-free number or web address on your rewards card or in print ads.

* Check any booking website you use for details of additional charges hidden in the small print.

* Carry a printed copy (or an easily accessible smartphone copy) of any email confirmation you receive after making your booking.

* Before setting out on your journey, call the hotel (using a number you know to be genuine) to confirm they're expecting you.

We'd add to that: Make sure you know what's included in your room fee. Is there an additional room tax or an extra charge for Wi-Fi services, for example?

There's nothing worse than arriving at the end of a long journey only to find your hotel booking was either a fake or not what you thought you were paying for.

Save yourself the heartache by investing a little time in taking these precautions instead.

Alert of the Week: You already know about the tech support scam in which someone pretending to be from Microsoft, Dell or another tech company calls you saying they detected a problem with your PC and need to gain remote access to the machine.

But what about a similar call from the Global Privacy Support Network warning that your email account has been hacked and is sending out fraudulent messages?

Nope, that's a scam too. Although the organization is legit, the calls are not. The GPSN doesn't do that sort of thing. So if you get the call and a demand to access your PC, hang up!

Reprinted from Scambusters.org