Issue 22 | Volume 2 | Sept. 2016

ADDRESSING THE NEEDS AND SECURING THE FUTURE

Helping secure your world

Security Solutions

Editor's Note

2016 has thus far been a challenging year from a security perspective. This issue of personal security has been heightened due to factors such as; the global terrorism threat, identity theft and off/online scam. Because of the daily stresses of life that persons face recreational activities and the gaming industry has grown. The September 2016 issue of the Security Solutions will outline and examine some of the new and emerging trends in personal and public security.

Terrorism and its threat is not a new phenomenon in the history of mankind. The history of terrorism is as old as humans' willingness to use violence to affect politics. The Sicarii were a first century Jewish group who murdered enemies and collaborators in their campaign to oust their Roman rulers from Judea. Here we see that terrorism was used even in pre-modern times. Amalgamated Security Services Regional Director Mr. Brian Ramsey discusses terrorism in relation to Caribbean businesses in the first article. In the article a quick examination of the last 50 years reveals that there has been terrorist activity within the Caribbean region showing that we are not immune to it.

Article two is very timely. The latest trend and currently most popular game is Pokemon GO. This game is a recreation of the Pokemon television series which was created in 1997. It is nostalgic for today's adults which have resulted in its tremendous popularity. However scammers have found ways to infiltrate this as well. So our second article identifies ways to keep you safe while playing Pokemon Go. In keeping with the theme of scams our third article discusses tricks used by lottery scammers. Identity theft can be done in a number of ways, one which includes your router; in the fourth article you will discover what should be done to avoid this from happening to you.
The fifth and sixth articles highlights the different safety items you should have always have at home such as: mask and respirators; chemical cabinets; gloves; eye glasses; fire extinguishers. Important to note also are tips for improving the security of your PVC-U windows and doors.

Knowledge of these and other scams, along with the knowhow on how to protect oneself is an important life skill. We do hope that these articles are worth your while and that the information is put to good use.

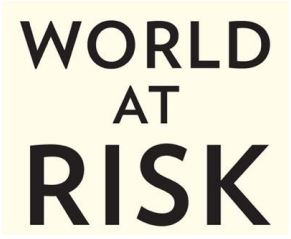
Regards
ASSL Marketing Team

Should Caribbean Businesses be Concerned about Terrorism

By Brian Ramsey – Amalgamated Security Services Limited

There is a tendency in the Caribbean to view terrorism as something that happens in other countries away from this region. Yet if one examines regional history one can clearly see that the Caribbean has not been immune from terrorist activity. A quick examination of the last 50 years reveals that there has been terrorist activity with some of these being;

- 1968, Bahamas, Assassination of Haitian Consul
- 1976, Barbados, Bombing of Cubana Airplane & Bombing of BWIA office
- 1976, Trinidad, Bombing of Guyana Consulate-General
- 1976. Bahamas, Attack on Soviet Ship
- 1980, Guadeloupe, Bombing at airport
- 1985, Guadeloupe, Bombing of Ford dealership
- 1987 Dominican Republic, Bombing of Peace Corp office
- 1988, Dominican Republic, Bombing of U.S. Centre
- 1989, Dominican Republic, Bombing of G.T.E subsidiary
- 1990, Suriname, Bombing of Alcoa subsidiary
- 2006, Trinidad, Bombings in the streets
- 2007, Trinidad, Guyana, JFK bomb plot



Apart from these direct on-islands terrorist activities there have been Cyber attacks by persons linked to ISIS on the government computers of Jamaica and St Vincent & the Grenadines. In addition there are clear indications that persons from Trinidad have gone to the Middle East to fight with ISIS and the production of a recruitment video aimed directly at attracting persons from this region to join ISIS. One of the aspects of terrorist group operations and particularly noticeable with ISIS is the propensity to expand their affiliations and so join with groups in other territories. In addition with ISIS fighters being drawn from many countries around the world there is need to be concerned about ISIS fighters returning to their home countries and terrorist cells beginning operations in new countries.

The impact of Terrorism in the Caribbean is therefore a valid concern and one which Caribbean businesses should be addressing.

Terrorism has direct multi-layered implications for Caribbean businesses which include;

- Direct implications for companies as a potential target
- Direct implications for personnel employed in companies
- Collateral damage implications as a business may be located near to a terrorist target

Companies may become a target because of their name e.g. British American Tobacco or British American Insurance. Companies may become a target because of a perceived link to a terrorist enemy. Companies may also become a target if they are seen as symbols e.g. McDonalds, Citibank, Royal Bank of Canada etc. It is interesting to note that one of the suicide bombers chose the McDonalds restaurant outside the Stade de

France in which to detonate his vest and it is believed that he picked this restaurant because it is a symbol of America.

Given that Caribbean companies need to be concerned about terrorism, the issue becomes what should businesses do independent of what actions the State should take for dealing with terrorism.

One of the first actions that every business should undertake is to conduct a security assessment that should specifically incorporate a terrorism assessment. That assessment should particularly look at the risk profile of the company both in terms of being a direct target and also the possibility of collateral damage implications because of the company's location. The assessment should identify the level of risk and how robust are the company's arrangements to assist it in preventing a terrorist attack. While it is important to do an initial assessment, it is equally important that the assessments are regularly reviewed, at least every 3 years and also after any major incident.

In seeking to reduce the possibility of a terrorist incident affecting your business, a critical aspect is staff awareness. Companies must make security awareness part of their organization's culture. Employees are the eyes and ears of a company; they know who is a regular customer and who is not, they know when something is out of place in their environment and so can quickly identify when action needs to be taken. It is also important that when hiring staff or contractors that thorough background checks are conducted on the individuals.

The control of access in a business is also another vital part of any company's terrorism prevention actions. This is of course complicated by the nature of the business and the extent to which the business caters directly to the public. It is certainly easier for an organization involved in warehousing and distribution to strictly control access when compared to a restaurant or a hotel. Nevertheless regardless of the nature of the business, public areas should be clearly defined and all other areas restricted to staff or authorized visitors only. Such actions help reduce the risk to specific clearly demarcated areas. In restricting access, the days of simply placing a sign saying no access or authorized persons only as the method of access control are over, especially if the concern is terrorism as terrorists will not be deterred by just signs. Businesses must invest in automatically closing doors and electronic access control systems whether card or biometric access control.

As a supplement to the protective measures a CCTV system that enables facial recognition should be considered. There must however be proactive use of the system. In the fight against terrorism one cannot simply have a CCTV system so that if a terrorist incident occurs you can possibly identify who committed the act. The objective for every business must be to prevent any terrorism incident occurring on their property. As such the business should aim to regularly review the footage of activities in and around their property, particularly if staff report that a strange individual was seen either within or in the vicinity of the business. The system must be such that it is easy to provide Government authorities with copies of the video so that they can investigate the individuals and possibly prevent an incident from occurring.

Apart from the overall good public image and hence enhanced revenues that may arise, maintaining an aesthetically pleasing appearance also has an anti-terrorism benefit. Companies should ensure good basic housekeeping throughout their premises. They should keep public areas tidy and well-lit, remove unnecessary furniture and keep garden areas clear. Where possible, they should not allow unauthorized vehicles close to their building. Each of these actions makes it easier to see if something is out of place

and so requiring immediate action.

The steps outlined above are some of the actions that businesses can take as part of a pro-active terrorism prevention strategy. It is however vital that there is constant monitoring of the various strategies implemented by the company. There is the tendency in the Caribbean to hurriedly implement measures but then not follow up to ensure that the measures are consistently applied and become part of a consistent ongoing operational methodology. Terrorists do not hurriedly plan their actions but spend time carefully examining a company for weaknesses and so implementing with no consistent follow up provides them with the weaknesses that they can exploit.

About the Author

Brian Ramsey has a B.A. in Accounting & Management, along with an M.B.A. in Finance and over 29 years in the Caribbean security field. He is the Regional Development Director for Amalgamated Security Services Limited which operates in Grenada, Barbados, St Lucia, Guyana and Trinidad and Tobago. He can be contacted at bramsey@assl.com.

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

Watch Out for these 5 Pokemon GO Scams

Scammers have swiftly latched onto the Pokemon GO game craze that's currently sweeping many countries.

Within days of its launch, it had already been downloaded onto smartphones tens of millions of times, but some versions of the game are virus-laden knock-offs, while the name itself is being used for scamming and spamming on a large scale.

For those who don't know -- and surely there can't be many -- "Pokemon" is shorthand for "pocket monster," but the creatures are actually Japanese cartoon characters, of which there are dozens of different types. The game's makers are able to place Pokemons onto player's smartphones so that they appear to be actually out in the real world when viewed through the phone's camera (a technique known as augmented reality). The game has captured the imagination and enthusiasm of players worldwide, as they go critter-hunting in streets, parks, forests and lots of other public, and some not-so-public, places.

The level of participation and the location of some of the characters have raised concerns about safety and several accidents have been reported. But it's also brought the scammers out in force. So, if you're a player, you need to be on the alert to these tricksters, especially as the nature of the scams seems to be constantly changing as the crooks identify new opportunities.

The basic game itself is actually free and can be downloaded from Apple (iOS) and Google (Android) app stores. Players can then pay for enhanced features such as a currency called Pokecoins, or a type of virtual attractant known as a "lure."

But it didn't take long before scammers stepped in with:

1. Virus-infected versions targeting Android devices installed via other download sites.

The malware is used to give scammers access to the victim's smartphone and possibly also to directly steal information.

2. A bogus monthly subscription service.

Players receive a message warning they have to pay for a $12.99 per month upgrade to continue playing.

Otherwise, the message says, the game will freeze within 24 hours. This it totally fake and nothing happens if recipients just ignore the message. The message contains links that take victims to a sign-on page where they're required to pay by credit card. All the information entered is then used for identity theft.

3. Spam campaigns offering lots of "free" Pokecoins for users who complete an online survey -- actually thinly disguised advertisements with no coins at all at the end.

Similarly, fake websites have been set up supposedly offering support, cheats and shortcut links in return for completion of these click-harvesting and product-pushing "surveys."

4. Lures that increase the likelihood of characters appearing in particular locations -- and then mugging players who turn up to "capture" the characters.

There are also concerns that lures may be used to draw children into unsafe locations and situations, though none had been reported at the time of this writing.

5. Various, dubious offers, usually on Craigslist, in which advertisers offer to help players locate Pokemon or increase their virtual wealth for a fee.

Some of these may be legitimate but there's no way of knowing that in advance.

In addition to these five scams, privacy concerns have been raised about the game.

At the outset, security experts claimed the game was capable of capturing and recording users' Google sign-on information as well as providing access to their email accounts. The makers of the game subsequently announced that although this was technically possible, the game didn't actually access this information and that they would now remove this feature.

Avoiding these scams is a matter of common sense. In particular:

* Don't let children download and play the game without your involvement.

* Beware of visiting isolated, lonely or exposed locations where you could be targeted for theft.

According to security firm Symantec, the game's makers say: "We encourage all people playing Pokemon GO to be aware of their surroundings and to play with friends when going to new or unfamiliar places. Please remember to be safe and alert at all times."

* Make time to read and check the game's terms and conditions, especially relating to its privacy policies.

* Don't download the game from unofficial sites or game repositories.

* Don't provide payment or confidential information to anyone or to any organization other than through the in-app payment arrangements.

* Don't be tempted to use online game-cheat tools. They may contain malware.

* If you are using an Android device, make sure you have up-to-date security software installed.

According to a recent news report, Pokemon-hunting players in Europe were spotted wandering into a real minefield in Bosnia -- a legacy of the war there in the 90s. Thankfully, no one was injured but the story illustrates how caution and common sense sometimes go out of the window when enthusiasts get caught up in a game.

You may not be near a real minefield, but when you play Pokemon GO, make sure you look out for other hazards -- and stay safe.

Reprinted from Scambusters.org

Latest Lottery Scam Tricks More Convincing Than Ever

Lottery scams cost Americans an estimated $300 million every year.

That's the amount that victims -- mostly seniors and other vulnerable individuals -- shell out in advance for supposed taxation and processing charges so they can pick up their "winnings," which, of course, never arrive. And despite stories appearing in local media every day about these costly con tricks, there's apparently no shortage of people still prepared to believe they've really won.

In one instance last November, a Jamaican man was sentenced to 20 years in jail in North Dakota for selling lists of gullible targets for lottery scams. He was also ordered to pay more than $5 million in restitution to victims who had paid money to enter non-existent lottery competitions.

Even attempts by family and friends to warn potential victims that they're on the receiving end of a scam sometimes fail to convince some of them.

One reason is that the crooks are getting even better at tricking people into believing them, notably by using the name of one of the best-known legitimate names in the prize-draw business, Publishers Clearing House, which we've written about previously.

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

Car Trick

A new example of how far these tricksters will go to convince victims happened recently in Idaho.

According to the Idaho Statesmen, a scammer posing as the son of a couple, told a car dealer his folks would be in later that day to select a car that he (the son/crook) would be paying for later as a surprise.

He seems to have asked the dealer not to mention that he would be paying. The couple showed up and selected their car, leaving it to be detailed for future collection. The crook called the dealer again saying he didn't have time to make the payment but would do it the following day.

But when they were ready to collect, the couple told the dealer they had won the vehicle as part of a lottery prize and had just paid their fees to the supposed lottery organizer. The dealer then had the tough job of telling them that the car hadn't been paid for and that he'd thought their son was buying it for them. At this point, they confessed that because it all seemed so real, especially as they'd had to select a car, they had wired the scammers $14,000.

In fact, lottery tricksters often use the lure of a car prize to add to the credibility of their story, usually a Mercedes, often because a car is a tangible thing -- we can all picture one in our minds, which somehow makes it seem more real.

Money Mule

Another sneaky trick we've encountered recently happens when the victim doesn't have enough accessible cash to pay the bogus processing fees. First, the crooks will often try to convince the victim to borrow the money and, if that doesn't work, they've been known to try to rope them into their scheme.

For example, a California woman was told she could work off the $20,000 fee she needed to pay to get her winnings by cashing checks for the non-

existent lottery company. In reality, she was being set up to become a money-mule -- a third party who would receive checks from other victims, cash them and then wire the money untraceably to the crooks. The victim allegedly agreed to do this but was eventually caught out when one of the checks she received bounced and her bank held her responsible for the money she'd withdrawn to wire to the scammers.

Fake Stationery
A third new trick uses the names of U.S. government departments as a tactic to try to convince victims.

Using stationery with logos from the FBI, General Accounting Office and Internal Revenue Service, they tell victims they've won millions in the "Gold Rush International Senior Citizens Sweepstakes."

Once again, victims are told they must pay tax on their winnings first. In some cases, phony U.S. Treasury checks seem to have been used to convince recipients of their authenticity.

There are many ways of avoiding a lottery scam but, as always, there's one golden rule that will always keep you in the clear:

Never pay money to receive competition winnings because no genuine competition organizer works that way. While you may have to pay taxes on winnings, these are either deducted from winnings before they are paid to you, or you pay the IRS after collecting your prize.
Avoiding a lottery scam is as simple as that.

Alert of the Week
The FBI has warned of a huge increase in CEO fraud, where hackers spoof an email to a key financial employee from their boss, telling them to redirect a payment - straight to the scammers.

The crime has lost firms more than $2.3 billion in more than 17,000 scams during the past three years and in the past year alone incidents have rocketed by 230%.

If you get this type of message seemingly from your boss, double check it with them.

Reprinted from Scambusters.org

Prevent Identity Theft with Your Router

One of the most overlooked ways to prevent identity theft is right in front of you -- your router

One of the best ways to prevent identity theft is your router. It is also one of the most overlooked methods of protecting yourself against online identity theft. Here's some information to help you get the most protection out of your router.

Setting your router for protection

If you have more than one computer in your home, chances are you already have a router. Don't know what a router is? It's that piece of equipment between your cable or phone modem and your computer. This is what allows your other computers in the house to operate wirelessly.

Computer hackers can hack into your computer and steal your personal information such as bank accounts, savings accounts, credit card numbers, social security numbers, birth dates, etc. By hacking your computer, they can get all the information they need to steal your identity.

If you have a router, it will have its own IP address. This stops information from leaving your computer. Anyone trying to hack your computer will reach the router and to the hacker, it appears that they have reached a computer and can't get any information. Even if you set you router up straight out of the box and didn't set any security settings, the router is already protecting you.

To be sure you have this protection, install a router on your computer even if you don't need it to connect other computers in your home. The router is like an extra firewall between you and identity thieves.

For further protection, use the proper user codes and passwords. Your router will come with instructions for encryption that can stop even the most determined hacker. While most routers come with these instructions, they don't usually emphasize why it's important to use them. Because of this, many people install their router and never take advantage of the protection that is already available to them.

When protecting yourself again identity theft, take advantage of tools you can find -- identity theft protection programs, checking your credit reports regularly, and proven identity theft software are good places to start. Using your router for protection is just one more tool you have to prevent identity theft.

Safety Items You Should Always Have at Home

By Joie M Gahum | Submitted On May 29, 2016

A safe home is a stress free home that not only protects you from the potential threats and dangers outdoors but as well as the potential accidents and dangers you may also encounter inside your homes. Fire, strangulation, chemical burns, boils and cuts are just a few of the accidents one may encounter at home. Thus having the basic personal protective equipment that may help in protecting or reducing the effect of harm to you and the rest of your household is a must.

Here are some of the basic safety items you should have at home.

Masks and respirators

Dusts and chemical fumes can be inhaled even while staying indoors. It is important to always have masks and respirators handy especially when cleaning areas in your home to prevent you from inhaling anything potentially dangerous for your respiratory system. Examples would be dust and other foreign materials when dusting your floors or other areas in your home as well as chemical fumes that you might inhale while cleaning your bathrooms. Masks are often disposed after use while filters in respirators should be replaced from time to time to remain efficient.

Chemical Cabinets

It is essential to tuck away chemicals and other dangerous liquids and items away from children's reach in a chemical cabinets. Chemical cabinets unlike other type of cabinets are more durable and can withstand chemical reactions that can be a potential risk when using ordinary wooden cabinets or plastic storage boxes for your chemicals. Hiding this cabinet in an area far from heat, fire and other triggers that my cause combustion or chemical reaction is also a must.

Gloves

Gloves are also one of the basic protective accessories you should have at home. These include cloth gloves, plastic and heavy-duty plastic gloves. Cloth gloves can be used to protect the hand when handling equipment for gardening or when chopping wood. Cloth gloves are also perfect for use when applying paint. Plastic

gloves on the other hand are advisable for use when handling food items. Heavy duty gloves on the other hand are used when handling metal or when you do welding at home. Wearing rubber gloves on the other hand when doing the laundry by hand protects that skin from the harsh chemicals of the soap that you use.

Eye glasses

There are different kinds of eyeglasses that can be used as protective equipment at home. When clearing the lawn or dealing with saw dust, it is advisable to wear a clear eyeglass that covers up to the side of the eyes to prevent foreign material from entering the eyes. As for welding items, an appropriate eyeglass or face mask can be used to dull the spark that welding creates and protect the eye from any possible object that may enter the eye.

Fire extinguishers

Some chemicals during combustion cannot be put out with simple water. Having fire extinguishers, at least one in your home is necessary to be able to have a handy fire-fighting tool that can be used to clear fire, even those caused by chemicals. Remember the acronym PASS to be able to use your fire extinguishers properly. Pull the cap, Aim on the fire, Squeeze on your trigger and then Swipe across your target.

It is important to have basic safety equipment and accessories in your home to help you in dealing with unexpected emergencies as well as accidents that may happen indoors. Having these items allows you to instantly deal with potential threats you may encounter at home giving you more time to call for an expert or safety professional.

Consider investing in chemical cabinets via Big Safety for your working areas or sheds at home to be able to provide a safe, locked, and durable hiding place for household chemicals and other liquid items that you use in your home improvement your projects around the house. Having one decreases risks of possible digestion or burns that chemicals may cause to you and the rest of the family.

Article Source:
http://EzineArticles.com/expert/Joie_M_Gahum/2200904

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

Tips For Improving The Security Of Your PVC-U Windows And Doors

By Reeze Martin | Submitted On July 15, 2016

Windows and doors found on both residential and commercial properties can be constructed or made with various materials. They can be made of wood, steel, and even aluminum. One of the most popular materials many doors and windows are made of today is PVC-U.

PVC-u, also known as uPVC, stands for unplasticized polyvinyl chloride. Many building experts call this material rigid PVC because it is hard and does not flex. It is one of the safest construction materials around because it does not contain any phthalates or BPA. It is also one of the most stable and durable building materials as well. They are used for the production of cladding, fascias, and plumbing materials. They are also used in the

creation of window frames and sills and doors.

Windows and doors made of this material are considered innately secure. However, if your property has PVC-u windows and doors and want to improve the level or amount of security they provide, below are some tips you can follow:

• **Invest in window restrictors.** These are small additional catches that prevent the window from opening all the way. Restrictors prevent windows from fully opening. They won't make your windows unappealing since they are small and are not noticeable once they are fitted. This accessory won't prevent burglars from damaging the frame if they are determined to do so but it will make it far more difficult for them to gain access and they often act as an effective deterrent.

• **Replace poor-quality or worn-out PVC-u window locks.** Window locks are subject to wear and tear, too. Once they become overused, they will become easy to break. If you notice that they are already looking old and flimsy, have them replaced immediately. You can also consider having sash locks fitted into the windows since they are great deterrents against burglars as well. Sash locks, also called "sash jammers", work by stopping the window from opening even if the main handle or lock is unlocked. Sash jammers are released by using a separate key.

• **Add locks to sliding patio PVC-u doors.** Most modern patio doors have built-in locks which are tremendously effective. However, if the door is quite old already, consider replacing the current locks or have additional new ones fitted. You can have new locks fitted that can stop the doors from being lifted off the runners they sit on. You can also consider installing a simple bolt lock to prevent unauthorized entry in your home.

Read more about PVC-u windows here.

Article Source: http://EzineArticles.com/expert/Reeze_Martin/1873796

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

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