Issue 1 | Volume 5 | March 2019

ADDRESSING THE NEEDS AND SECURING THE FUTURE

Security Solutions

Helping secure your world

Editor's Note

As is habitual with our first issue of the New Year, we at Amalgamated Security Services Limited would like to extend a heartfelt Happy New Year to all our subscribers and readers. We do hope that 2019 would be a blessed year of success and prosperity for you.

We begin this issue with an article that speaks to new and potential home owners about Gated communities and their security. Mr. Brian Ramsey – Regional Development Director of ASSL explores this topic and speaks to how we can identify a secure gated community. Article two speaks to arguably the most powerful individuals and an influential group in our business society; Chief Executive Officers. Many times Executive Management gets bombarded with unsolicited mail from external parties and sometimes this mail is an attempt to gain entry to be able to impersonate the CEOs. The article CEO Swindle shows the steps in a targeted attack where a fraudster impersonates the CEO or another senior executive within the organization and instructs a member of the finance department to make an urgent payment to a particular account for a specific reason. Article number three stays within the workplace with the Clean Desk Test. We see that most workspaces hold sensitive documents and information that you don't want to get into the wrong hands. A little care and a few good habits such as, locking your computer, taking items out the printer even a securing a USB stick can go a long way toward keeping everything secure.

Article four clarifies a misunderstanding that many persons have as to what a personal alarm is designed to do. The primary purpose of these devices is not to attract attention, but to make the attacker stop what they are doing. With technological advances and improvements businesses may be encouraged to purchase and upgrade their machinery and software and they all depend on a steady supply of electricity but a single minute without electricity can translate to interruption, threat to secure data, damage to equipment or chaos. Learn more about selecting the correct UPS in article five. The focus on security of business data continues in the last article where the best internet security solutions of 2018 are discussed.

At **Amalgamated Security Services Limited** we will continue to fulfill our commitment to provide quality service for all customers and in keeping with this commitment we do hope you find these articles and the safety tips helpful.

Regards
ASSL Marketing Team

Gated Communities – Are they really secure?

By Brian Ramsey

A spreading phenomenon throughout the Caribbean are gated residential communities.

The growth of crime or more exactly the growing fear of crime is leading to an expansion in the number of these communities.

Many individuals, particularly older persons, are opting to live in these complexes, often selling their existing homes to purchase houses in gated developments.

For most of these persons the rationale is that these communities are seen as secure but the question is, are they really secure?

The answer to this question is important not simply because it underlies the reason why individuals bought property within the community but also, although individuals may not realize it, because thieves often target gated communities.

All developers of gated communities seek to give the community an attractive appearance and that gives the impression that the people who live in those communities are wealthy. Once an area has the appearance of wealth it becomes a target for thieves and so gated complexes are frequent targets of thieves.

The answer to the question of if gated communities are secure is that it depends. So what are the factors that might make a gated community not secure.
To answer that question one must first start by defining what is considered a gated community.

Most individuals simply look at the fact that there is a gate that must be opened to gain entrance to the community and define the community as a gated community. That very thinking is what often causes a community that has been called a gated community to not be secure.

In trying to decide if a gated residential complex would be secure you have to examine if there is access into the community from other points. Can a person simply go to the back of the community and walk in?

A few years ago the son of a friend of the writer was robbed in their home in a gated community. This home is built on a hill side in a community with a locked guarded gate at the entrance to the area but you can climb the hill from another community, walk across and then descend into the gated community. This is precisely the route that the intruders took to be able to rob.

So a residential complex that merely has a locked gate at the entrance is not really a secure complex.

It therefore stands to reason that to begin considering a gated community as being secure the entire community has to be enclosed.

However one needs to ask if those gated communities that are completely enclosed either by wall or fence are they secure?

Part of the answer to that question rests with the issue of how high is the wall or how impenetrable is the fence, such that it can prevent intruders from gaining easy entry.
Another part of the answer to that question lies in another question. Who is patrolling the compound to see that no one is climbing over the wall from outside?
An associated question is, can the patrol see the entire

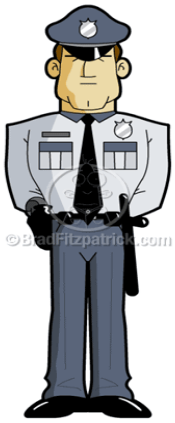
perimeter of the compound or is their view blocked by the houses within the compound.

Without regular patrols that can view the entire perimeter an enclosed gated community is not truly secure.

In search of the factors that might make a gated community not secure, let us return to the gate at the entrance to the community. How is that gate opened - Does everyone have a remote for opening the gate or is there a common code to enter into a panel that will allow the gate to be opened.

Often with gated communities where a code has to be entered in a panel, the requirements of daily living force them to give the code to the maid, baby sitter and gardener or the residents get lazy finding it too troublesome to come to the gate to receive deliveries and so give the code to the pizza delivery man. Eventually the code becomes common knowledge among persons who do not live in the community and can eventually be known by thieves.

A more secure community would have a guard at the gate who controls access but even with such a measure there can be shortcomings. How does the guard know who should be allowed to enter the compound? Is there a system where the residents must provide the names of any visitors so that the guard would know who to admit?



One gated community in West Palm Beach Florida has such a system but has added to it by requiring that visitors provide photo-identification so that the guard can know that the visitor is indeed the person that the resident is expecting and that photo-identification is scanned and stored as a permanent record of the visit.

So the answer to the question of if gated communities are truly secure really is that it depends and it depends on if the other elements of security are also in place.

About the Author

Brian Ramsey has a B.A. in Accounting & Management, along with an M.B.A. in Finance and over 30 years in the Caribbean security field. He is the Regional Development Director for Amalgamated Security Services Limited which operates in Trinidad and Tobago, Grenada, Barbados, St Lucia, Guyana, Antigua. He is also the Chairman of the Caribbean Institute for Security and Public Safety. He can be contacted at bramsey@assl.com

CEO Swindle

A manufacturing firm transfers thousands to scam artists after falling victim to CEO fraud.

Social engineering involves the use of deception to manipulate individuals into carrying out a particular act, such as transferring money, handing over confidential information, or clicking on a malicious link, and it's causing serious financial harm to businesses around the world.

One of the most common types of social engineering is CEO fraud.

This is typically a targeted attack where a fraudster impersonates the CEO or another senior executive within the organization and instructs a member of the finance department to make an urgent payment to a particular account for a specific reason.

More often than not, the CEO or senior executive in question will have had their email account compromised. But you don't even need to be hacked in order for this kind *of* fraud to be carried out. Some fraudsters will go off publicly available information such as email addresses.

Any business that transfers funds electronically can be susceptible to losses of this nature.

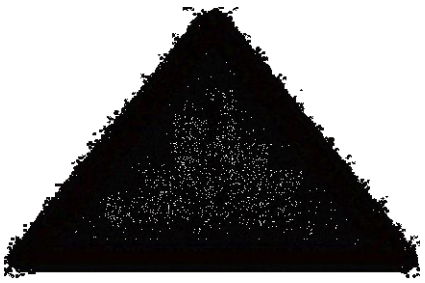
Phishing

One of our policyholders affected by a case of CEO fraud was a manufacturing company, specializing in the production of machinery used in the textile industry.

The scam all began when the CEO fell for a credential phishing email.

Credential phishing emails are used by malicious actors to try and trick individuals into voluntarily handing over their login details. Typically by directing them to a link that takes them through to a fake login page.

In this case the CEO received an email *from* what he thought was Microsoft. The email stated that his account details needed to be validated in order for him to continue to use the Outlook service without disruption. As the email appeared to have come from an official source, the CEO clicked on the link. The link took him through to a seemingly legitimate landing page, where he inputted his email login details. Assuming that his account had been validated, the CEO gave no further thought to the incident.



However, by inputting his credentials on this login page, he had actually passed on his details to a fraudster who could now access his account.

Gaining access to the CEO's email account allowed the fraudster to gather valuable information about how invoice payments were processed at this company. For example, it allowed the fraudster to take a look at previous Invoices that had been sent from the insured's contract manufacturers and suppliers and to identify the main Individual in the insured's finance department responsible for paying invoices and authorizing wire transfer requests.

What's more, it also allowed the fraudster to gain access to the CEO's Outlook calendar and establish what the CEO would be doing on any given work day.

Having worked out the CEO's schedule from his calendar, the fraudster waited until the CEO was travelling abroad for a few weeks on a business trip. With the CEO out of the office and with the chances of the scam being uncovered much reduced; the fraudster chose his moment to strike.

The fraudster's plan involved posing as a member of the accounts department for one of the insured's contract manufacturers.

The fraudster's first step was to set up forwarding rules in the CEO's email account.

Forwarding rules are settings that can be applied to an email account which ensure that emails that fall within a certain criteria are automatically forwarded to a specific folder or to another email account.

In this case, the fraudster set up two rules to ensure that the CEO didn't come across any of the emails related to the scam whilst he was away on business.

The first rule that was created meant that any emails from the individual responsible for approving payments were immediately marked as read and sent directly into the account's deleted items folder.

The second rule meant that any email that included a keyword such as "invoice" or words used on this particular contract manufacturer's trading name, in the subject line was marked as read and automatically sent to the deleted items folder.

With the background work now done, the fraudster sent an email to the CEO purporting to be from the accounts department of the contract manufacturer, attaching an invoice *for* $47,500 and explaining that there had been a change of account details. To add an aura of authenticity to the scam, the fraudster used one *of* the actual contract manufacturer's invoices as a template.

So to all intents and purposes the invoice looked normal, it featured the contract manufacturer's logo and address on the heading of the invoice

and carried a breakdown of the work carried out. The only difference was that the account details had been altered by the fraudster.

As a result of the forwarding rules in place, this email was immediately marked as read and sent to the deleted items folder. The fraudster then logged into the CEO's account and, posing as the CEO, forwarded this email to the individual within the finance department responsible for authorizing payments and requested that the payment be made that day. As the CEO was out of the office and because the email requesting that the invoice be paid had come from his account, the employee in the finance department assumed that this was a legitimate request and duly paid the invoice.

Having seen that the ruse had worked, the fraudster decided to try their luck and now sent through another invoice a few days later.

On this occasion, due to the fact that it had only been a few days since the last invoice had been paid the employee in the finance department responded to the CEO about the request to check that this was correct. Because of the forwarding rules put in place, however, the CEO was oblivious to the employee's response- only the fraudster was aware of it. In the guise of the CEO, the fraudster responded and explained that all was in order and that the invoice should be paid.

With the employee in the finance department genuinely believing that they were in correspondence with the CEO and with any objections and queries about the payments being swiftly answered, the fraudster managed to get two further invoices approved, bringing the total amount paid out to $190,000.

It was only upon the CEO's return to the office that the payments came up in discussion and the scam was uncovered. Our policyholder reported the incident to local law enforcement and attempted to recover the funds from the recipient bank.

But all of the money had been moved out of the fraudulent account and the prospects of a successful recovery were deemed to be remote.

Thankfully for the insured however they had purchased cybercrime cover on their cyber policy with CFC and were able to recover the loss in full.

This claim highlights a few key points. Firstly, **it illustrates how CEOs and senior executives are prime targets for cybercriminals.** CEOs and senior executives usually act as the face of their respective companies and as a result they tend to have bigger profiles on company websites and social media accounts, allowing cybercriminals to gather valuable information about them.

In addition cybercriminals know that employees are instinctively less likely to question and more likely to act upon instructions from senior executives. CEOs and senior executives therefore need to be especially conscious of sticking to good cyber security practices, and **employees need to be particularly alert to suspicious emails from senior executives** and have robust call-back and authentication procedures in place.

Secondly, it shows that cybercriminals are becoming much more sophisticated. In the past. It was not uncommon to see blatant attempts at funds transfer fraud over email, with an urgent appeal for help or bogus prize giveaways being just two examples.

Now, however, we are seeing far more nuanced attacks. In this case the fraudster managed to trick the CEO into volunteering his email login details, identify who was responsible for authorizing payments and work out when the CEO was out of the office on a business trip, as well as setting up forwarding rules in the CEO's in box to avoid detection and making use of one of the Insured's genuine contract manufacturer's invoice templates to add authenticity to the scam.

Finally, this claim also discredits one of the most common objections that organizations have to purchasing cyber insurance: namely that by investing heavily in IT security, they have no need for cyber insurance. The fact IS that the vast majority of cyber incidents are a result of human error. With increasingly sophisticated attacks like this on the rise, it makes it very difficult for employees to tell the difference between a real email and a fake email or a real invoice and a fake invoice. Furthermore, with more and more financial transactions being carried out electronically, the number of opportunities for cybercriminals to steal these funds has never been greater.

Having good training and authentication procedures in place can certainly help reduce the risk of an event like this happening, but it's impossible for any business to be completely impervious to these kinds of attacks. This is why cyber insurance should be a part of any prudent organization's risk management program; acting as a valuable safety net should the worst happen.

Case Study performed by CFC

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

The Clean Desk Test

Ten ways a messy desk puts confidential information at risk.

By Joan Goodchild
Editor-in-Chief, CSO

Most workspaces hold sensitive documents and information that you don't want to get into the wrong hands. A little care and a few good habits can go a long way toward keeping everything secure.

Here are 10 things to tidy up.

Open computer
When you leave your desk, do you lock your computer to ensure no one else can look at what you are working on? While it's not always practical to constantly lock and close applications (or no one would get anything done), certain applications and documents should be given special attention and closed, minimized or locked before leaving a desk. A short auto-lock time for your screensaver can help.

Sticky notes with sensitive information
Your employer expects you to remember ALL of those different passwords? What better way to organize them than to write them all down on a sticky note, right?

Wrong. Even without spelling out exactly what those passwords are used for, an industrious criminal or hacker could use them to gain access to private accounts.

Don't write down passwords anywhere, especially not on display on your computer.
A password manager can get your passwords under control.

Confidential documents
Expense reports and client contracts are two types of documents that should not be left out for all eyes to see.
Private corporate and proprietary information is the kind of data a competitor would love to get their hands on.
Documents left out overnight, when cleaning crews or other outside contractors may be in the building, are of particular concern.
Do people really leave sensitive information lying around? Of course they do — we found violations right in CSO's offices.

Put any sensitive paperwork in a locked file or drawer when you're not working on it.

Forgotten printer document
How many times have you printed out a document and then neglected to retrieve if from the machine? In this example, the employee has left a bill for a toll-fees account out for all to see. Bank account information might be found on this document, as well as travel itinerary information that could be considered private.
Retrieve all documents from the printer immediately and store them in an appropriate, secure location.

Recycle bin
The recycle bin or wastebasket is another place where employees make security mistakes.
You'd be amazed at the stuff that gets carelessly thrown out.

Consider what you're throwing away before you pitch it. Many documents should be shredded for privacy and security reasons.

Smartphone left on desk
What kinds of texts or other information might be available to someone who picks up your smartphone? Have you received a text regarding an executive's travel plans? Your own? Corporate travel — particularly trips requiring executive protection — should not be available for just anyone to view.

Take your smartphone with you when you leave your desk. Always have it locked with a strong passcode to prevent compromise.

Keys
Do your keys open doors to server rooms, document storage or other places that should have good access controls in place? Car keys clearly show what brand of car they belong to. If the lot is fairly empty, how long until an ambitious car thief finds their way to it?

Store keys in your pocket or purse.

Bag sitting out
What's in your bag? A wallet? Sensitive corporate documents? A laptop not docked and in use? Chances are this bag has plenty of goodies that thieves would love to get their hands on.
If your bag contains valuables, keep it with you or lock it up.

Easy access to files and folders
It would take a motivated thief mere seconds to grab and dash away with files left in unlocked storage spaces.

Make their job just a little harder by locking your document storage areas, such as cabinets and drawers.

Vulnerable USB stick
USB sticks may hold many rewards for a thief. Is there private data on there? Proprietary information that might be valuable to a competitor? All the thief needs to do is grab it and stick it in a pocket to find out.

USB sticks, like bags, purses and sensitive documents, need to be locked up and secured when not in use.

Access card
Leaving your access card out on your desk means unauthorized individuals might take it and use it to access your building after hours. Or it could be used to get into secure parts of the building that only you, and others with privileged-access rights, are allowed to enter.

Keep your access card with you in your pocket or purse. Many people use clips or lanyards to keep it easily accessible when moving about the building.

Whiteboard covered with writing
Does your whiteboard include names from a client list or financial figures that you might not want to fall into a competitors hands? Is it easily viewed from outside the office, open for anyone to see?
Use whiteboards appropriately and privately. Clean off information that could be considered sensitive. Consider the position of your desk and workspace when it comes to windows and doors. Could someone easily spy on you?
Reprinted from csoonline.com

Do Personal Alarms Work?

By Neil Savin

If you read reviews of personal attack alarms, you will find that some people say that the alarms are not loud enough. The truth is that many people misunderstand what a personal alarm is designed to do. The primary purpose of these devices is not to attract attention, but to make the attacker stop what they are doing and run away.

How Loud Are Personal Alarms?
Most personal alarms are in the region of 110dB to 140dB. To put that in perspective, a power saw is 110dB at three feet away, and a jet engine is 140dB at 100 feet away. However, sound doesn't travel too well through solid objects. That's why shutting your windows will partially block out the sound of traffic in the street below. This simple fact applies to alarms as well. If you set one off, it won't seem very loud if you are in the next room. But, if you were to hold one up to your ear, you could damage your hearing.

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

How Do Personal Alarms Work Then?
Thieves, muggers and other types of criminals don't want to get caught. They want to commit their crime and get away with it. If someone triggers a loud alarm when they are attacked, the perpetrator will be surprised, confused, and is likely to become concerned that they will be caught in the act. The loud siren of an alarm may attract attention. Unfortunately, though, bystanders may not always react to it. This is simply because we have all become somewhat accustomed to hearing sirens. A criminal, though, won't want to risk getting caught. So, the sound will be enough to scare them away.

What About Other Self-Defense Products?

There are other non-lethal self-defense products that you can use. One of the most popular of these is the pepper spray. The potential problem with pepper sprays is that you can't take them everywhere with you. They are prohibited on commercial airlines, and you are not allowed to carry a pepper spray in some public areas and buildings. If you are going on an overseas vacation, you also need to be aware that

is illegal to carry pepper sprays in some countries.

In What Circumstances Will a Personal Alarm Not Work?
Personal alarms are effective in any situations where the attacker thinks that the noise may attract attention. For that reason, using one on a hiking trip into a remote region probably wouldn't have the desired effect. Their effectiveness can also be limited by background noise. If you were at a rock concert, for example, an alarm siren probably wouldn't be heard. In most situations, though, the fear that the alarm might bring help will be enough to deter an attacker.

What Type of Personal Alarm Is the Most Effective?
You can find personal alarms on sale in stores and online. They do vary quite a lot in quality though. Some of the very cheap models may have batteries that you can't replace, and the batteries may not last very long. It's best to avoid the very cheap devices and go for a well-known brand, like Vigilant or Sabre. Even the best personal makes, though, will only set you back about $20.

Article
Source: http://EzineArticles.com/expert/Neil_Savin/2156456

Choosing the Right UPS from CVT Manufactures to Befit Any Building

By Uma Nathan

Homes, hospitals, businesses, clinics, airports - the list of places that depend on a steady supply of electricity is long, varied and weighted. Even a single minute without electricity can translate to interruption of business, threat to secure data, damage to equipment or chaos. Therefore, it behooves to be proactive.

A straightforward and inexpensive method of preparing for the incoming weather is Uninterruptible Power Supply. A UPS is a reliable source of power that is entirely affordable and offered in a variety of options. It is the safest method of protecting assets, investments, equipment, and data.

A UPS:

1. Supplies a consistent flow of power to devices
2. Keeps in check the spike or fall in electricity and safeguards technology

Awareness of the benefits a UPS delivers to a business or home is not enough. It is essential to know the right kind of UPS that fits the requirements of the building and the technology it contains.

Illuminated below are practical counsels for selecting the precise UPS for a residence or commercial place.

- **Categories - Recognize Them All**

For mobiles, there are tens of brands with hundreds of models within each. Any product present in the market has endless options, and a UPS is no different. Just like when purchasing any technology, gathering data on it is crucial before buying a UPS so it is vital to know about all the categories. Be aware of every system offered by different companies and the features of it. Randomly purchasing a unit from one of the socomec ups dealers nearby is not the right solution because each UPS has its own specialties.

For example, a useful UPS for a home PC would be a standby UPS. They work offline and are ideal when power cuts are small and infrequent. On the other hand, a data centre that wants protection against hackers

should invest in a line-interactive UPS. Not every UPS can support every gadget. Do due diligence on the possibilities available to you.

- **Runtime - Know Power Backup Period**

Let's say a clinic necessitates a power backup up to 60 minutes but the UPS installed renders a steady supply for just half an hour. Such a power backup is a useless entity because it fails to do its job.
An APC UPS has one primary responsibility - to provide continuous power in the event of load shedding so that the equipment doesn't switch off. Thus, it is imperative to be aware of the runtime of a unit before buying. Know the total backup period of the UPS you are considering purchasing.

Factors to Consider:-

1. Is the UPS wanted for a short duration so that data can be saved & gadget shut down?
2. Is the UPS required for the complete length of the outage?

- **Performance - Do Level Inspection**

A UPS that is incapable of bearing the load of the system it is linked to is impractical. The basic guideline is that the UPS should give 25% more power supply than that needed by all the devices and gadgets connected to it.

Two steps should be taken to check if UPS will perform as expected:

1. Calculate the total power that will be needed to operate all the equipment when there is a power cut. Add 25% more to it.
2. Compare all the UPS models you have shortlisted and inspect which one caters to the power level required.

Make an informed decision based on these calculations. Additionally, ensure that the UPS can balance out any electricity surges and overloads.

- **Outlets - Count The Number**

This pointer may seem like common sense, yet few individuals take the time to check it.
A UPS that needs to power 4 computers requires at least 4 outlets.

The tip is to pay attention to the number of power outlets and not just the price point of the UPS. Furthermore, make sure that every outlet is powered directly by the battery. There are many models that come with eight outlets, but only some of them are connected to the battery.

- **Warranty - An Essential Tip**

There is no machinery on the planet that is not prone to issues and wear and tear. It is, hence, vital to have a warranty which incorporates a majority of the problems that may arise. Always identify the duration of the warranty offered with the UPS and what factors it includes.

- **Last Decisive Recommendation**

To prevent dire consequences, power management has become a vital thread for all organizations. Blackouts, especially during extreme weather, are usual and sudden.

The only strategy to avoid disasters is to invest in a robust, dependable and excellent UPS that does not hamper the smooth functioning of the systems that are linked to it.

UPS systems warrant that a backup is in position during an emergency situation. A good UPS provides users the freedom to suitably save their work before electricity runs out.

Article
Source: http://EzineArticles.com/expert/Uma_Nathan/1246323
Reprinted from Ezinearticles.com

Best Internet Security Solution - What Kind of Protection Features Does the Program Offer?

By George Botwin

Having an internet security solution to protect your home and/or business is essential. There are so many potential threats these days that you'll need the best internet security to keep everything as safe and secure as possible.

Cyber attacks are becoming more and more sophisticated. It's not just the ole' virus and malware problems we have to worry about.

Cyber criminals are using methods to hack into webcams, steal personal information from smart phones, attack Wi-Fi networks, and even steal identities.

Since internet security solutions come with more features than the traditional antivirus software, the price is higher. However, as long as you choose the best suite, you'll have all of the peace of mind you'll ever need. If you're trying to protect your business, think of how much money you could lose if there is ever a cyber threat that compromises your clients' personal information. Your entire business could end up being destroyed with a security breach.

Even if you just want to protect your home PCs and smart phones from threats, it's a good idea to invest in the best internet security. It seems like every day there is another story in the news about a corporation or organization getting hacked. On top of that, there are always horror stories about individuals getting into a ransom ware situation.

The IT security companies are constantly putting out new software and updates to keep up with all of the newest threats. Even webcams are vulnerable to hackers. Someone could be spying on you through your webcam without you being aware. Regular antivirus programs don't offer webcam protection. It's crucial that you opt for a security suite that includes protection against illegal use of cams.

Top Features in the Best Internet Security

Here are some other features found in the best internet security:

- Anti-spam module
- Anti-ransomware module
- PC vulnerability detection
- Firewall
- Anti-phishing
- Remote wipe or lock function if the device is stolen or lost
- Parental controls
- Optimization module for the PC or Mac's speed
- Router and Wi-Fi protection
- Password protection and management
- Online banking and shopping security
- File shredder
- Rescue Mode
- VPN

There are also cyber security solutions that are ideal for small to medium sized businesses and provide end point and data center security.

Article Source: http://EzineArticles.com/expert/George_Botwin/1425000

Reprinted from ezinearticles.com