- EDITOR'S COMMENTS....1
- IT Security Unit.....2
- Information Security Controls 3
- Hotels & Identity Theft…....4
- Social Engineering…..5
- Network Security ….....6
- Entrance to Home…….8
- Information Security…10
- Protect Kids……...11
- Homeowner Association.12
- Scratch Cards ……14

ISSUE 7 | VOLUME 1 | September 2012

Security Solutions

ADDRESSING THE NEEDS AND SECURING THE FUTURE.

Helping secure your world

Recently I received a call about a problem with one of our trucks. After replacing the defective part the truck was still not operating properly. Eventually I was told the truck was repaired and when I enquired why the delay the mechanic informed me that they had entered the wrong settings in the truck's software. This drove home the extent to which our lives are dependent upon software so this issue is focused on IT security.

Our first article introduces the **ASSL Information Security Unit**, while our second article looks at **Options for Measuring Information Security Controls**.

With increasing numbers of persons travelling for work and also needing to be connected to work even when on holidays we all expect hotels in the Caribbean to provide Internet access. Very few persons however think about the possibility of **Identity Theft when using WiFi in Hotels**. Our third article therefore addresses that subject.

Very often when looking at Information Security, as our fourth article shows, it becomes apparent that the **Human Element is the Weakest Link**.

The firth article looks at some **Misconceptions about Network Security**.

We recognize that individuals are always surprised at how burglars select their targets. We have therefore included our sixth article, **How did they gain entrance to my Home**.

Our seventh article is also on **Information Security**. While our eitht article provides advice on **Protecting your Kids when you are not at home**.

Article Nine gives some advice on **Preventing Homeowner Association Fraud**.

Our final article, looks at a **Crime technique involving Scratch Cards** that murderers are now using.

Is there anyone who you think would benefit from receiving this magazine? Just send their name and email address to newsletter@assl.com and we would be happy to add them to our mailing list.

Brian Ramsey
Editor

ASSL Launches Information Security Unit

Amalgamated Security Services Limited is please to introduce our newest Business Line – the **Information Systems, Security & Intelligence Business Unit**; herein referred to as ISSIBU.

In Today's world, Information Technology lies at the heart of every business. No longer is IT merely for producing the Accounts, it is how the business communicates, how it tracks its performance, how it plans each action, how it records it activities. Information Technology today is a resource that is critical for the survival and success of every business.

As with every resource there are risks; disruptions to the availability of the resource can cripple a business, competitors gaining access to the information can out maneuver a company, criminals gaining access to the network can steal millions or cause a company to lose millions. Just as there are security measures for the protection of physical resources, so too there are security measures for the protection of Information Technology and for tracking illegal attempts at accessing that information.

The protection of Information has evolved to include next-generation mechanisms – inclusive of Cyber-Analytics, Cyber-Forensics, Electronic Fraud and Forensics and Bio-Informatics within the whole sphere of Cyber Risk/Intelligence.

To help companies protect and deal with the risks to their Information Technology, Amalgamated Security has launched its newest Business Line – the Information Systems, Security & Intelligence Business Unit (ISSIBU). The Unit provides companies with comprehensive and all-encompassing IT Solutions for their operations.

This unit specializes in Information Security and Cyber Intelligence activities as well as traditional core Information Technology services. We are confident that our keen knowledge of the Security industry has helped us develop solutions that answer the needs of companies.

Among the services we offer are;

1. IS Fraud & Forensics Managed Services
2. Security Incident Management
3. Enterprise Security Consulting
4. Social Networking & Web 2.0 threats
5. Website Protection
6. Cloud Cyber Security and Compliance
7. Countermeasures & Threat Assessments
8. Data Recovery & Business Continuity
9. Mobile Device Protection and Hardening
10. Unmanaged Mobile Devices
11. Critical Data and Infrastructure Protection
12. Audit, Compliance & Internal Controls
13. Crytographic Key Management
14. Technical Security Re-Architecture
15. Network & Security Operation Centres
16. SAP & ERP Security Guidance

ISSIBU has compiled an expertly qualified and experienced team with many designations, certifications and skill sets that makes it the singularly best qualified Information Security and Cyber Services oriented Unit in the Region.

Mr. Ricardo Ramdhan – the Head of ISSIBU is formally trained in the Defense Sector in USA and Canada, and has been attached to such organizations as the Royal Canadian Mounted Police (RCMP) and Vancouver Police Department (VPD), as well as Canadian Forces over the past 7 years. He is an approved and registered Cyber Security & Intelligence contractor with both the Departments of Defense of the USA and Canada as well as NATO. The other members of the ISSIBU team all possess unique variations relating to Information Systems and Security, and with this team, that ASSL is confident that we can and would rival any service provider currently existing in our market.

Customers learn more about our investigations unit by visiting our web site at www.assl.com/investigations.htm

Are Your Information Security Controls Effective?

By Lee Hezzlewood

Pretty much all modern businesses deal with information of some description. Whether its basic day-to-day accounting data on your own business, financial records of other businesses and individuals, or detailed personal and medical files on thousands of people, information exists within your business.

Unfortunately, whatever information you have in your business there's a pretty good chance that someone else wants it. These people could be simple criminals out to make a fast buck, organized crime gangs running a profitable if somewhat corrupt operation, competitors willing to try a little industrial espionage, or even nation states using your business to gain international advantage.

And your size and stature doesn't always have to be substantial - indeed the Information Commissioner's Office here in the UK considers smaller businesses a weak link precisely because they are small and often unwilling to invest in effective information security controls, and because they frequently supply to or work on behalf of major corporations.

So we've established that your business handles information, and that a threat exists to that information. The next question is what are you currently doing about it?

If you have existing security controls in-place, are they effective, both in terms of costs and protection? Do your staff understand their role in protecting information? And can and should you be doing more?

Now unless you have an effective system for testing and assessing your information security controls it's doubtful you can answer these questions with any degree of certainty.

So how do you go about measuring the level of information security within your business?

The 1st option is to trust in fate and hope that you never experience a breach. The problem with this approach is that it relies on your organisation never being targeted. Now of course it may indeed never be targeted directly. But I'm sure you would agree that's not the most sensible approach. Especially when all evidence suggests such attacks are on the increase.

Another option is to implement a process of measuring your own security controls. If you have the skills and resources this might appear the best solution and that way you're not exposing your soft underbelly to 3rd parties. The downside of this is that like any internal process, you may be the victim of politics where the judgments and test results end up being skewed by internal issues and rivalries, making the results unreliable.

In addition, if reduced risk and improved security is your goal, with a long-term objective of possibly gaining some kind of certification (such as ISO-27001), then you really need an objective, unbiased opinion from a trusted business partner.

Which brings us to the 3rd option - find a suitable security assessment provider and have them do an assessment of your business.

Now obviously there are a number of solutions in this area. Many companies have fixed-price services that are primarily designed for small- and medium-sized organisations. If you are a large business or need something more thorough you might opt for an assessment performed on a consultative basis by an experienced individual or business.

If you wish to go down the route of certification you might need help in choosing an appropriate certifying body and then assistance implementing the

controls, policies and systems needed to obtain certification.

Whichever option you go for in the end you are far better off ensuring you properly assess your information security controls than simply crossing your fingers and hoping for the best. Your business and your customers are depending on you!

Lee Hezzlewood is the founder of Secure Thinking, a UK company providing specialist services in Data Protection and Cyber-Security. For more information on information security for SME businesses take a look at our Managed Security Services.

Article Source: Reprinted from EzineArtilces.com

Hotels, Laptops and Identity Theft!

By Dave Ostler

When people travel, it is not uncommon for them to take their laptops or other wireless devices with them. Whether they may be travelling for business purposes or for a family vacation, they may want to receive email, stream media, or work on presentations. Most of these activities require some sort of connection to the Internet. For those with smartphones, the connection is already in place. But for many others, a laptop or iPad is really the preferred tool, and connecting to the hotel's free wireless Internet connection is their best option, as to not use up precious data minutes through their wireless provider.

Whenever a computer or other wireless device connects to the Internet, many of the software applications installed on the device search their "homebase" for updates. In fact, most applications are programmed to do so. When an application finds an available update, it prompts the user to install the update. In general, software updates are desirable. Updates provide critical patches for security vulnerabilities and bug fixes for other glitches, all in an effort to provide the user with a safer, more secure, and better user experience.

Recently, some hotel guests are finding that simple updates via hotel wireless networks are leading to big headaches, and that is because the updates are not from the software provider; they are from criminals!

How an Attack Works:

While staying at a hotel, a user connects to the hotel wireless Internet and soon gets a popup for a popularly installed application claiming it is out of date and that there is an update available. The user decides to go ahead and install the update, but instead, what they are really installing is malicious software that criminals use to steal their personally identifiable information and commit fraud.

Cyber criminals have cleverly infiltrated the hotel's wireless Internet connection and routinely scan for newly connected devices. Once they find one, they will display a popup window for a piece of software commonly found on all computers or devices in hopes to entrap the user. If the user proceeds with the update, the malicious software now places them at risk for identity theft.

How to Defend Yourself:

Whether you find yourself travelling a great deal or only occasionally, you can defend yourself against this type of attack. When you receive a popup prompting you to update software, check the certificate to see if it is registered to the actual software vendor. If it is not, do not install the update. You can also visit the software vendor's website to see what the latest software version is. Does it match what the popup claims? If not, don't trust it.

If at all possible, you should always wait until you return home or to work where you will have a trusted and safe Internet connection by which you can download and install the update.

One way to protect yourself while traveling from unsecured hotel networks is to use a personal network of your own called a virtual private network, or VPN. A virtual private network is a dedicated connection between networks. A VPN creates a secure tunnel and encrypts your data through the dangerous cloud of the Internet. A VPN changes your virtual location by assigning you a different IP address. A VPN controls the traffic to and from your computer, keeping your online information activity secure, private and anonymous. VPNs also provide Antivirus, Malware and Trojan infiltration protection as well as encrypting your data. A VPN is much more secure than a typical public network because fewer people are using your specific VPN, and even if someone does get unauthorized entry, the attacker will not be able to read the data because it is encrypted at such a high encryption rate.

If you are interested in setting up a VPN simply do a web search for "VPN" and the most popular VPNs will pull up in your browser. VPNs are easy to use and are available for computers, smartphones and tablets.

In addition, if your home's wireless network is not secure, you should make every effort to secure it before you proceed any further. By not having a safe and secure network you open yourself up to these types of attacks.

Another way to protect yourself is to update your system before you travel on vacation. This will allow you to know that your system is already up-to-date and that the popup you see is probably bogus.

Whichever route you take, be sure to stay alert. It is rather easy to fall victim to this type attack, especially if you like to keep your system or devices up-to-date. When in doubt, ask yourself if you could survive without the update until you return home. Chances are you probably can.

Article Source: Reprinted from EzineArticles,com

Social Engineering and Operations Security: How the Human Element Is the Weakest Link

By Dean Soto

When businesses start planning their security strategy, especially information technology security, the tendency is to put an emphasis on technical measures. That is, we think that having the latest firewalls, intrusion detection devices, and solid security management processes are going to be the foundation that keeps the organization safe from the bad guys. Well, the truth is that no matter how many cool gadgets and tools you have in your arsenal, you will always have one gaping hole that puts your company at risk - your people.

The two big concepts that this article is going to touch on are Social Engineering and Operations Security. Although different, they both play a major role in the success of a security program or its demise.

Social Engineering, in essence, is the use of psychological and sociological methods to gain information that would otherwise be off limits to unauthorized individuals. These methods may range from a simple email to a more complex ruse that involves multiple attempts to gain information. A large-scale example of this occurred in early 2012 in which there was a rash of people being telephoned by individuals claiming to be "Windows" and that their computer had a virus that needed to be removed right away. The caller would then lead the unsuspecting employee to a website that would download malware, or have them pay for fake anti-virus software.

The problem with social engineering is that it is very hard to defend against. The reason being is that, although a strong security education program may be in place, often the person doing the social engineering has

already researched the target organization to find holes in their armor. Often little pieces of information are collected from various personnel and are eventually put together in order to fully compromise a system and this is where Operations Security comes in.

Operations Security (OPSEC) focuses primarily on keeping small bits of seemingly harmless information out of the hands of those that wish to do harm to an organization. There is a systematic series of steps to follow in order to ensure a good implementation of OPSEC.

The first step is to identify critical information. Often, companies have no idea what systems or information is crucial to keeping their business afloat. That being said, once the mission critical items are identified, you can then start moving toward protecting them.

Second, you need to assess the threats. Who is out there that would want your information? Once you figure out the threats that are out there, you can start to understand how those threats may try to approach your employees and what information they might ask. You will also start to see how much support they may have, whether it is just a lone person or an entire state sponsored group trying to penetrate your organization.

Third, you must analyze the vulnerabilities to those critical assets. Having a realistic view of your security holes is vital to be able to implement any safeguards. Often, large amounts of data are leaked because lower level personnel have far too much access than is needed to do their job. Once a social engineer fools them and gains access to their system, the keys to the kingdom are theirs.

Fourth is an assessment of risk, which is often overlooked. Not all threats and vulnerabilities may need to be mitigated, and some threats may have a low probability of occurrence. Sometimes the cost of implementing a safeguard may be more than the cost of a compromise. The point is that there is a lot of stuff that *could* happen, but what's the likelihood that it will?

Lastly is the implementation of your OPSEC safeguards. This can only be done effectively when everything else has been appropriately analyzed.

When all is said and done, the human element in security will always be the weakest. The beauty of melding the knowledge of Social Engineering with OPSEC is that rather than just relying on security education of your employees, you can have a systematic way of mitigating the risk involved with Social Engineering.

Dean Soto is a business consultant that's passionate about sharing entrepreneur concepts. He also provides tools such to help you make your first sale. Download his simple but effective business proposal template!

Misconceptions About Your Businesses Network Security

By Dave Ostler

In a survey conducted by Ponemon Research on behalf of Juniper Networks, 90% of the respondents said their organizations' computers had been breached at least once by hackers over the past 12 months. Ponemon Research surveyed 583 companies located in the US with an average of 9.5 years of business experience. Nearly 60%

reported two or more breaches over the past year. More than 50% said they had little confidence of being able to thwart off further attacks over the next 12 months. Those numbers are significantly higher than findings in similar surveys, and they suggest that a growing number of enterprises are losing the battle to keep malicious intruders out of their networks.

"We expected a majority to say they had experienced a breach," said Johnnie Konstantas, director of product marketing at Juniper, a Sunnyvale, California based networking company. "But to have 90% saying they had experienced at least one breach, and more than 50% saying they had experienced two or more, is mind-blowing." Those findings suggest "that a breach has become almost a statistical certainty" these days, she said.

The organizations that participated in the Ponemon survey represented a wide cross-section of both the private and public sectors, ranging from small organizations with less than 500 employees to enterprises with workforces of more than 75,000. The online survey was conducted over a five-day period earlier this month.

Some of the findings are as follows:

· As a result of these multiple breaches, more 34% of respondents say they have low confidence in the ability of their organization's IT infrastructure to prevent a network security breach.

· Insufficient budgets are an issue for many organizations in our study. 52% of respondents say 10% or less of their IT budget is dedicated to security alone.

· The financial consequences can be severe. When asked to consider cash outlays, internal labor, overhead, revenue losses and other expenses related to the security breach, 41% of respondents report that it was $500,000 or more and 16% say they were not able to determine the amount.

· In the next 12 to 18 months, 47% say their organizations will spend the most IT security dollars on network security.

Roughly half of the respondents blamed resource constraints for their security woes, while about the same number cited network complexity as the primary challenge to implementing security controls. The Ponemon survey comes at a time of growing concern about the ability of companies to fend off sophisticated cyber attacks. Over the past several months, hackers have broken into numerous supposedly secure organizations, such as security vendor RSA, Lockheed Martin, Oak Ridge National Laboratories and the International Monetary Fund.

Many of the attacks have involved the use of sophisticated malware and social engineering techniques designed to evade easy detection by conventional security tools. The attacks have highlighted what analysts say is a growing need for enterprises to implement controls for the quick detection and containment of security breaches. Instead of focusing only on protecting against attacks, companies need to prepare for what comes after a targeted breach.

The survey results suggest that some organizations have begun moving in that direction. About 32% of the respondents said their primary security focus was on preventing attacks, but about 16% claimed the primary focus of their security efforts was on quick detection of and response to security incidents. About one out of four respondents said their focus was on aligning security controls with industry best practices.

Ponemon Research believes their research provides evidence that many organizations are lacking the right strategy to prevent cyber attacks against networks and enterprise systems. Their study suggests conventional network security methods need to improve in order to curtail internal and external threats.

Ponemon Research believes organizations should consider incorporating the following recommendation in their network security strategy:

· Understand the risk employees' mobile devices create in the workplace. The largest problem is created when laptops or other wireless devices are connected to an unsecure network; breaches occur involving lost of sensitive data. In addition, stolen laptop computers or other mobile data-bearing devices remain a consistent and expensive threat.

Studies consistently show that the cost of cyber attacks is increasing in the US; in fact it's

the largest growing crime in the US. Reducing an organization's vulnerability to such attacks through the utilization of a virtual private network, and a combination of proper staffing, enabling protection technologies and training programs can help prevent the pattern of multiple breaches experienced by so many companies in the survey.

Article Source: Reprinted from EzineArticles.com

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

How Did They Gain Entrance to My Home?

By Douglas Harper

We want to think burglars are stupid, so stupid they can't get a real job. We want to believe they are lazy. Not true, burglars are just misdirected in the use of their talents and believe me some of them are very talented. I will act as the burglar and tell you how I got into your house and why I choose you.

- You know me, I delivered your refrigerator, cleaned your carpets and painted the trim on your house.
- I saw your alarm control panel at the front door through the decorative glass.
- I watched your house for newspapers piling up.
- I was the first to notice your lawn was not trimmed for over a week.
- When you didn't remove the flyers I taped to your front door, I knew you were not home.
- I hate alarms over the sink and motion detectors, and even worse I hate window alarms on the second floor, thanks for not installing them.
- Without an alarm system you actually gave me a few more minutes to select the items I wanted to steal, and those alarms wake the neighbors and get the police involved.
- I'm glad you had no security cameras, I hate that the police use video surveillance system recordings as evidence.
- Thanks for hiding your valuables in the sock drawer and medicine cabinet. Did you really think I wouldn't lift the mattress? You should have gotten a diversion safe.
- Thanks for turning off all radios and televisions. I like working when it's quiet.
- Didn't you tell your neighbors to watch over the house and didn't get one of those dog alarms. I hate nosey neighbors and dogs.
- When I saw that 60" flat screen TV carton by your trash can, I selected your house to rob.
- Thanks for the extension-ladder in the backyard; I had no trouble getting into the second story window.
- You forgot to set that alarm system because you were only going to be gone for a few hours. Thank you!
- I'll tell if your home by knocking and pretending to offer handy man services. You don't need to check me out or notify the police, as I would never rob you.

- Nasty day, rain, cold weather and you are in a hurry to get going. Forgot to lock the door? I work in good or bad weather, I really don't care.
- If you hadn't let me use your bathroom last week when I was working in your yard, I couldn't have unlocked the bathroom window.
- You live in a safe neighborhood, so don't worry about remembering to lock the door. I knocked and you didn't answer, I tried the knob and got lucky.
- Thanks for leaving all window blinds and shades open for me so I could select the items I wanted to steal.
- Remember you announced your vacation on Facebook; it was very easy for me to look up your address.
- You had a safe! I'm glad you didn't bolt it down, so it was easy for me to pick up and carry it out.
- When you saw me in your backyard, it was all right, because I had a clipboard.
- When you bought that diversion safe, I'm glad you didn't put it into the kid's room as I hardly ever take time to go there. It was so handy on the counter looking out-of-place.
- Before you left, you cracked a couple windows open for fresh air. I would have closed them if I suspected rain.

Now let's look at what we can do to deter a burglar from entering your house and stealing your possessions. First make sure all windows are locked and use a door brace on sliding glass doors. Install dead-bolt locks on the doors and use the locks that require a key from both sides. Get a couple timers for lights to make it look like someone is occupying the house at night. Trim your hedges around windows and mow your lawn just prior to leaving. Get a security camera or camera system. The security camera's presence will deter a burglar, but if they ignore the camera, you have a video record to take to the police. Fake dummy cameras can make your video system seem bigger than it really is and a barking dog alarm will deter a burglar. Enhance your video security with "Beware of Dog" signs and security system stickers. Obtain diversion safes for money, valuables and jewelry.

Upgrade your outdoor lighting with motion sensing lights. Keep your garage door closed and if you purchase high dollar items, keep the boxes in the garage until you can cut them up or drop them off at a commercial disposal site. Lock ladders to the wall with a chain and lock up any pry bars, crowbars and other "tools of entry" in your toolbox. Don't make it easy for them to rob you.

If you have purchase and existing home or rent your home or apartment, a wireless alarm system is easy to install and very inexpensive. The wireless alarm system can dial the police and others to alert them of an intrusion. Glass breakage or window alarms and motion detectors are a necessity to make the alarm fully effective. If you have a friend or relative you can trust, have them stop by the house to collect mail, put out the trash and check the premises at least twice a week while you are gone.

If you have a rather large home or detached buildings with tools and equipment you can purchase a Voice alert system to tell you someone has entered a part of the house that is vacant or one of your out buildings. This alarm can be set to give you different messages such as "car entering driveway", "person entering the pool" or "someone entered the garage". You can put the receiver in your bedroom, home office or kitchen to give you a feeling of security while you focus on other things.

If you have been robbed, you are very likely to be robbed again, unless you change things.

Whatever it was that attracted them in the first place makes you a target to be robbed again. A typical home can be equipped with a video camera security system, a wireless alarm system, door braces and a voice alert system for under $1,000.00. This is very inexpensive insurance for your valuables, and should bring the cost of home insurance down to help you pay for all this equipment.

Doug Harper is a former Marine having served in Viet Nam, later becoming a drug and prisoner transport officer and an airline pilot. Doug retired from the airlines in 2011 and opened Harper Stores, LLC that owns Sharper Safety http://www.sharpersafety.com and Sharper Defense http://www.sharperdefense.com.

Article Source: Reprinted from EzineArticles.com

Information Security Programme Management and Your Business

By Andrew Leith

The management of an information security programme is a significant project for a business owner or manager, and will not happen of its own accord. When you plan your project, it is important to be clear about both where you are at the moment and also what you wish to achieve. The best results by far are gained by implementing and managing security as an overall programme, rather than adding occasional unrelated security countermeasures (such as a firewall) on an ad hoc basis.

Information security programme management is often viewed by managers as something that "just happens" of its own accord. Nothing could be further from the truth. In fact, it reaches into so many disparate business functions, and involves so many people, that it is arguably one of the most complex areas to manage successfully. Ideally, the Chief Information Security Officer (CISO) needs all of the following attributes:

• In-depth knowledge of specialised technology, such as firewall types, computer network configurations, and cryptographic algorithms, for the purposes of computer security.
• In-depth knowledge of recognised standards (such as ISO 27001) to a level which enables the CISO to implement the standards in full for a given organisation.
• Experience of writing customised policies and procedures for a given organisation, based on the CISO's experience of industry best practice.
• Knowledge of relevant legislation and industry regulations, and how to comply with them, together with experience of liaising with the company's legal department.
• Familiarity with methods of workplace training and awareness-raising, plus experience of liaison with the HR department concerning contractual clauses.
• A working knowledge of human psychology as applied to workplace behaviour and computer security.
• Experience of conducting IT audits and liaising with external auditors and consultants.
• Experience of managing an information security team (for larger organisations).
• Experience of managing a significant budget and liaising with vendors.

This is a demanding set of requirements, and few people perform equally well on all points. Just as obviously, the tentacles of information security reach into every part of even a large organisation, making the job of the information security manager even more challenging than other managerial jobs.

However, help is available from several sources. Chief among them is the ISO 27001 standard, which specifies the design, implementation, monitoring and improvement of an information security management system. This standard and its sister standard ISO 27002 together represent the distillation of best practice in this area. Becoming compliant with these standards will go a long way towards easing the burden of information security programme management. In addition, help and advice can be obtained from professional networking events with one's peers in the same town or city, as they will be affected by exactly the same local conditions. Finally, reading relevant periodicals can help to provide insight into commonly-encountered problems.

In brief, information security programme management should be viewed as a substantial project in its own right, demanding an extraordinarily wide range of expertise and experience. Organisations need to budget resources to ensure the job is done properly, since it will not happen of its own accord.

Andrew Leith is a security consultant at commissum, a UK-based information security consultancy specialising in penetration testing, vulnerability assessment, ISO27001 consulting services, and security configuration of enterprise systems.

How to Keep Your Kids Protected When You Need To Leave Home

By Cori Baker

If you are a busy career man or woman, it might be quite challenging for you to balance your work and your responsibilities with your children. Some working parents might need to leave their homes for a certain amount of time. This means that they have to leave their kids alone or under the guidance of another adult.

Some parents consider this a daunting experience. Fortunately, you can still keep your kids safe and secure even if you are not there to personally take care of them. Before you leave, make sure that you have planned these things:

It might be necessary for you to make a schedule for your kids. If you are going to have another person take care of the children, this list can also be beneficial to him or her. Create this schedule as early as possible. Make sure that you have not forgotten anything. This schedule will include activities that the kids need to do at school or out of it. The tasks that they need to complete at home should also be added into this schedule. Making your kids stick to a schedule allows the temporary guardian to check if there are problems or if everything is alright.

The guardian of your kids has to be aware of the typical meal times, the time when your kids need to be in bed, the amount of time they have to play, etc. As much as possible, entrust your children to people that you know and those who are familiar with your family's schedule. If you are going to leave your children to a stranger, that might not be a very wise thing to do. Taking care of the children can be a very difficult task especially if they have not warmed up to the person who's going to be with them. Also, you might put your kids in danger.

Reinforce the safety measures that you have at home. If you think the locks in your doors won't be enough to keep intruders out, add a more effective lock. Repair damages on the doors and windows. If you have an alarm system, make sure that this is working perfectly.

You might have already taught your kids how they should react

if they sense danger when they are out of the house. However, you should also teach your children about the basics of staying safe while inside the house. Be stern about not inviting friends over to the property, except for friends and neighbors that you already know and trust. Make your kids realize about the possible dangers of their potential irresponsible behaviors. If they realize the threats that are present, they will know what correct things they should be doing.

As much as you can, check on your kids. With the variety of electronic communication devices that are present these days, there can be no plausible excuse for not checking on your children even if you are a thousand miles away. Set up regular meeting hours by which you and your children can talk on the phone or see each other through video call.

Cori Baker loves writing for beststungun.com/ which is a reliable source of information for pink taser as well as a host of related products.

Protect Yourself Against Homeowners' Association Fraud

Groups run by volunteers that hold money on behalf of all their members are increasingly vulnerable to insider scams, such as homeowners' association fraud.

Unscrupulous employees or board members exploit the fact that most volunteers likely know little or nothing about financial management to "cook the books" or channel money to contractors who pay them a kickback.

They know too that volunteers are often pressured for time and may not scrutinize activities in the way that paid officials would do.

In one recent example in Nevada, Federal investigators claim to have uncovered a single scam involving several homeowners' associations whose alleged crooked board members placed lucrative lawsuits and other work with attorneys and contractors involved in the scheme.

Even worse, the Feds contend the perpetrators used dishonest and threatening tactics to get their stooges elected to the boards, sometimes buying condos they never even lived in but which entitled them to stand for election.

This may be an extreme example, but the fact is that any volunteer-led organization -- charitable organizations, trade associations and even religious groups -- runs the risk of an insider scam, although community association or homeowners' association fraud is the most widespread.

And it's not unusual for losses and liabilities to run into millions of dollars.

Donna Berger, executive director of the Community Advocacy Network, which represents homeowner associations said in a recent article in Florida's Sun-Sentinel newspaper: "Fraud is an ongoing threat to associations. And the likelihood of being a victim escalates during bad times.

"Association boards are run by volunteers who take time away from families, jobs and hobbies to serve. Con artists know these time constraints and divided attention might leave an opening."

Usually, the scam is not part of an organized plot but simply the action of an opportunist who is either greedy or in debt and often feels entitled in some way to help themselves (for instance, if they

have a grievance, such as feeling they've been treated unfairly).

These three characteristics -- opportunity, motivation and rationalization -- are what crime experts call the "fraud triangle."

As CPA Arlen Lasinsky told the Chicago Tribune: "The standard reasons someone commits fraud are drugs, alcohol, gambling, boyfriend, girlfriend and medical bills. Lately, with the recession, it's also to buy groceries and make the mortgage payment."

The crime comes in numerous forms, from dipping a hand into the petty cash or using an association credit card for personal purchases, to altered bank statements and checks or bogus invoices for work that has never been done.

The loss of money by this means it is not only a hit for the organization affected; it is also a potential threat to board members -- in the shape of lawsuits filed by aggrieved association members alleging breach of fiduciary duty.

Whether you are on the board or just a concerned member of such an organization, it's in your interests to ensure that all possible safeguards are in place.

Here are 10 things you can do, or encourage the board to do, to reduce the risk of fraud and/or protect the organization.

1. Ensure all board members and employees are thoroughly vetted and that the election or hiring process is "transparent" -- that is, not secretive.

2. Keep a wary eye out for a board member or employee who seems to be living beyond their means or who never takes vacations (because their crime might then be uncovered).

3. Question any delays in circulating financial statements and other organizational documents.

4. Segregate responsibilities -- that is, have different people responsible for signing and banking checks and a third person for reconciling the two. Require two signatures on all checks.

5. Require at least two original copies of bank statements (that is, direct from the bank, not photocopies provided by someone inside the organization).

Scrutinize statements, looking for individuals or companies with similar names (one may be a legitimate recipient, the other not).

6. Set up a "positive pay" arrangement with the homeowners' association bank. Under this system, you send your bank a list of checks that have been authorized and they then compare it with the actual checks they have.

7. Set a limit on invoice amounts that can be paid without full board authorization. Perform regular spot checks on invoices (from just one company but choosing a different company each time).

8. Download "Preventing Fraud: How to Safeguard Your Organization," a free useful guide aimed specifically at nonprofit organizations produced by the former National Center for Nonprofit Boards (now known as BoardSource).

Get it here (PDF reader required): http://clicks.aweber.com/y/ct/?l=EPyWa&m=JiC8WIMRgGtWfo&b=C2oOoJ1BQCH1.Q8lnEhpLg

9. Have your accounts independently and professionally audited, preferably every month but at least once a year.

10. Finally, just in case the worst happens, ensure you have full compensation protection through employee fidelity bonds, and directors and officers insurance (known as "D&O").

None of these measures individually will likely be strong enough to spot or stop homeowners' association or other nonprofit fraud, but when combined you'll find they create a formidable defense.

Article Source: Reprinted from Scambusters.com

Scratch Cards to throw off the Police

There is now a new technique used by robbers and carjackers to escape from arrest due to their criminal activities. They are collecting used scratch cards and once they abandon the stolen car or dump a dead body or bodies they leave the already used scratch card at the scene. Once the police arrive they naturally use the scratch card serial numbers to track on which phone number it was loaded then they start tracking the owner of that phone number. Already two people who fell victim of the trick had to answer several questions before they were released by the police.

To avoid being placed in this position, once you load airtime make sure you destroy the card before you dispose it to avoid such incidences.

Amalgamated Security has offices in Trinidad and Tobago, Barbados, St Lucia and Grenada.