Issue 4 | Volume 9 | Dec. 2023

Security Solutions

ADDRESSING THE NEEDS AND SECURING THE FUTURE

Helping secure your world

Editor's Note

Season's greeting to all our readers!
On behalf of the Management and staff of Amalgamated Security Services Limited we would like to take this opportunity to wish each and everyone a joyous Christmas and a bright and prosperous 2024. May the spirit of Christmas which brings joy, peace, faith, laughter and good will to all men continue into the New Year and beyond.

As the number one security company within the Caribbean region we take pride in advising our clients on security measures that can be implemented which can protect life and property. The first article written by our Non-Executive Director Mr. Brian Ramsey discusses the security of mobile devices as it relates to the work environment. He speaks on the issue where companies may lean to the alternative of allowing their employees to use their personal devices for work purposes, however in the long run this may cause greater problems with respect to securing company data.

Article two asks the question; is the microphone on your computer, tablet or Smartphone eavesdropping on your conversations, even when you're not using it? Here we learn how to block microphone eavesdropping by checking the setting on your microphone. The third article speaks about four data security mistakes you should avoid making such as failing to back up information, etc. In keeping with this theme, article number four speaks about information destruction and the laws governing it.

During the holiday season many families embark on vacations or persons may be out of town to spend time with love ones, most times leaving their home unattended for long periods of time. The next article discusses five measures to enhance home security such as not boasting on social media and fencing the periphery of your property to name a few. In the last article we discuss issues surrounding used vehicles and why before you buy a used car, check for odometer fraud. The purpose behind this type of fraud is that the perpetrator wants to make it seem the car has less wear and tear than it really does. After all, it's often hard to judge just by looking, you may end up spending more on a vehicle that isn't worth it.

In wrapping up the year 2023 we at Amalgamated Security Services marketing team do hope that our quarterly publication helped settle some of your security concerns. As in 2023 it was our goal in 2024 that this newsletter will help build awareness with respect to property and personal protection, we trust that this mandate was achieved.

Regards
ASSL Marketing Team

Security of Mobile Devices

By Brian Ramsey

Mobile devices are everywhere. At every turn you see people on their mobile phones and tablets sending texts, surfing the Internet, checking their email and doing all manner of activities that the various apps allow them to do. Giving into the wave of pressure from staff and recognizing the productivity improvements that are possible through the use of mobile devices, companies have increasingly begun arming their staff with mobile devices or allowed their staff to use their own devices in the performance of their work. Undoubtedly companies have experienced a performance boost as a result. No longer are customers told that that the person did not see the email because they were not in the office or that they will get a response on Monday when the person goes to the office.

Mobile devices are therefore a tremendous benefit to Caribbean companies but they carry a risk that many companies are not recognizing. This risk is compounded by the fact that employees often bring their own devices to work and use them for work purposes. Some employers view this BYOD approach as a cost savings to the organization because they think that now they do not have to incur the cost of purchasing and maintaining mobile devices for employees. The risk that some Caribbean companies are not recognizing is that mobile devices if not properly configured can open up unauthorized means of access to company information, which in turn can lead to damaged reputation, corporate espionage, loss of revenue and more. The unauthorized access can also lead to the introduction of viruses and malware on a Company's system which can actually shutdown a company's IT system and cripple a company's operations. The risk is further magnified by the fact that employees in seeking to reduce the usage of their data plans and thus save on their personal cost will frequently use any open wireless networks that they discover and often have their mobile devices configured to search for open wireless networks and use those first. Open public wireless networks however are often unsecured and so frequented by hackers looking for victims.

There are several measures that companies should have in place in they are allowing the use of mobile devices. The first and simplest method is that anybody who wants to use a mobile device to access the Internet and the company network should have installed and regularly updated antimalware software for their device. The second measure is that mobile devices should be configured to avoid unsecured wireless networks, and Bluetooth should be hidden from discovery. In fact, when not in active use for headsets and headphones, Bluetooth should be disabled altogether. These measures while good first steps are not the only protective actions that companies should take with mobile devices.

Increasingly individuals have realized that they cannot simply have mobile devices open to be picked up and used by anyone. People have caught on to the fact that if their mobile device is stolen anyone finding it will have access to their personal information and able to use their device and incur charges that they will have to pay. As such most individuals have configured their mobiles to require a password to be entered. Where a mobile is being used for work purposes the access granting should go beyond just a password to ensure that possession of a mobile device doesn't automatically grant access to important information and systems. Most modern mobile devices now include local security options such as built-in biometrics - fingerprint scanners, facial recognition, and voiceprint recognition and companies should require the use of one of these combined with the password.

Most experts recommend that "all mobile device communications be encrypted as a matter of course, simply because wireless communications are so easy to intercept and snoop on. Those same experts go one step further to recommend that any communications between a mobile device and a company or cloud-based system or service require use of a VPN for access to be allowed to occur. VPNs not only include strong encryption, they also provide opportunities for logging, management and strong authentication of users who wish to use a mobile device to access applications, services or remote desktops or systems”.

The difficulty that is faced when companies opt to go the BYOD route is that the user owns the device, not the organization, which makes security somewhat trickier for IT to establish and maintain. Other experts have therefore recommended that in those situations, companies should “require such users to log into a remote virtual work environment. Then, the only information that goes to the mobile device is the screen output from work applications and systems”. As only screen output goes to the device the data does not remain on the device once the connection to the company’s network is terminated. Since accessing a remote virtual work environment invariably occurs through VPN connections, communications are secure as well.

For companies that want to go further they can implement mobile DLP technologies. These DLP applications provide data classification features to label messages and documents (metadata labeling), as well as features that analyze content and filter it when a mobile device interacts with a corporate server. This they can prevent information that has been classified as Sensitive or certain types of emails from downloading to a mobile device. Some of the DLP products prevent sensitive information from being transferred to devices based on a user or group rather than a device ID.

Along with the technological measures, companies need to educate users on the dangers of data leakage. Employees should be taught what is considered sensitive and confidential information and about security of devices. Employees should also be taught about the implications of data leakage not only to the organization but ultimately the danger to their own job security. Most employees will help protect an organization's assets once they understand what constitutes "confidential" information and the consequences of its leakage plus the risks that organizations face through unauthorized mobile access.

About the Author

Brian Ramsey has a B.A. in Accounting & Management, along with an M.B.A. in Finance and over 35 years in the Caribbean security field. He is a Non-Executive Director for Amalgamated Security Services Limited which operates in Grenada, Barbados, St Lucia, Guyana, Antigua, St. Vincent, Jamaica 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

How to Block Microphone Eavesdropping

Is the microphone on your computer, tablet or smartphone eavesdropping on your conversations, even when you're not using it?

During the past few years, reports of devices and programs listening in to nearby conversations have repeatedly surfaced. At the same time, numerous devices, apps and even hackers are known to have the ability to switch your mic on when you're using your device, both for legitimate and dubious purposes. Obviously, there may be plenty of occasions when you need and want to use the microphone -- making Skype-type voice-over-internet calls, for example, or using built-in virtual assistants such as Siri (Apple devices), Cortana (Windows) and Alexa (Amazon). Then there are programs like speech-to-text, voice recognition software, and apps that let you instruct them instead of using your keyboard. Even Google's Chrome browser has the ability to act on voice commands -- if it's switched on. Provided you're in control of when your mic is active and that whoever (or whatever) is listening in is doing so because you invited them is all well and good.

But that's not always the case. Sometimes you don't realize your microphone is on -- you may even think you switched it off -- and sometimes people are listening in for questionable purposes. For instance, computer users have, from time to time, reported speaking words in online conversations that subsequently seem to trigger pop-up advertisements on certain web pages and social media networks, though these claims are usually denied.

It has not always been clear to what extent some legitimate apps, like Microsoft's Cortana, gather information about what you're saying, leading to genuine privacy concerns. And, on the other side of the law, hackers have demonstrated how they can trick their way into computers and smartphones to switch on microphones without users being aware.

A couple of years ago, computer security firm Panda identified spyware that could switch on a phone's mic, identify where the device was located, record conversations and track the user all day. This sort of eavesdropping goes hand-in-hand with illegal or questionable remote accessing of web cameras, which we reported on in an earlier issue.

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

There's no better evidence that the risk of this spying is real than the recent publication of a photo of Facebook founder Mark Zuckerberg, whose laptop, in the background of the photo, was seen to have tape placed over both the camera and mic.

You can usually tell if your camera is in use because most of them have a tiny light next to the lens that switches on with the camera. But with a microphone, there's generally no visible signal. It's also reportedly possible in some circumstances for headphones and even speakers to be used to collect conversation, even when a microphone is turned off or disconnected.

It's all this uncertainty over whether, how and why speech is being eavesdropped that creates user concern.

So, what can you do about it?

While we can't guarantee to make you soundproof, there are a number of key actions you can take to minimize the risk of being overheard or recorded, or of your microphone being activated without your knowledge.

Here's a quick rundown:

Learn how to manually disable

the microphone setting on your device, or search out software that will do this automatically for you. Then, disable the mic when you don't need it.

- You can also physically disable a microphone by plugging a cheap, wired mic into the microphone extension socket and then snipping the wire. The extension is activated as the default input source but there's no microphone.

- If you have a combined headphone/mic outlet, you would need a combination headset and again, snip the wire just below the microphone.

  (Note, however, that hackers may be able to switch your default setting back to the built-in microphone.)

- When installing programs, especially smartphone apps, check if they require access to your mic. Many apps will request permission, at least during first use. Deny it unless you're really going to need it.

- For programs and apps that are already installed, use their "settings" feature to check if they can access the microphone, or check the "microphone" or "privacy" listing in your settings.

  For example, if you use an iPad or iPhone, visit settings/privacy/microphone to see which apps use your mic.

  The same sequence in Windows 10 will perform the same task, with the ability to switch off the microphone altogether or to deny access to individual apps.

- Search online for how to do this on other devices.

- Keep your Internet security software up to date to keep hackers out or to alert you when programs behave suspiciously.

  By the way, tests suggest that Mark Zuckerberg's attempt to limit microphone access by using masking take doesn't work. It might muffle the sound but it probably wouldn't keep the eavesdroppers out!

Alert of the Week: Do you have an outlook.com email address? If so, beware of a message from "Outlook Administrator" that arrives in your inbox with the subject line: "Microsoft account unusual sign-in activity."

The message goes on to warn:

"We detected something unusual about a recent activity to the Microsoft account. To help keep you safe, we required an extra security challenge. You will need to verify your Microsoft email account below to confirm that the recent activity was yours and to regain access and enjoy our unlimited service."

It's quite a convincing phishing attempt to get your Microsoft sign-on details and, although the scam has been around for a while, there's been a resurgence in recent weeks.

Delete it!

Reprinted from Scambusters.org

4 Data Security Mistakes You Should Avoid Making

By Satvik Mittal

Data security is of great importance whether you are a journalist, whistleblower, investigator or a small company. While most people know that they need to protect their data, few take it seriously. To help you out, here are some of the most common data security mistakes that many people make and how to avoid them:

Failing to back up the information

Most people store their data on the cloud or on their devices. This isn't enough. Your device can get damaged or lost. The cloud storage may also be tempered with. In addition to storing your data in these areas, you should also back it up in other devices such as external hard disks. To spread the risk, experts recommend that you avoid backing up all of your data in one device. For peace of mind, you should regularly test the backups to ensure that they are working perfectly.

Mixing personal and professional devices

This is a common mistake made by startups. Due to insufficient resources, most startups allow their employees to use their devices in the workplace. The employees use their phones and computers to handle work related projects. While this is highly convenient as the employees can carry the work home, it puts your data at risk. When an employee leaves the organization, he/she can still get access to the corporate information which is dangerous for your organization especially if the information is sensitive.

Not taking mobile security seriously

Due to the commonality of mobile phones, many people don't take them seriously. Studies show that many people don't recognize that mobile phones are a security threat to their information. There are many things that can go wrong with your mobile phone: someone can pick it and obtain your sensitive information, you can lose your phone or a hacker can get access to the information. Due to these risks, it's imperative that you take the security of your device seriously. To keep off the regular snooper your phone should always have a password. To protect your data from hackers or when it gets lost you should install software that compartmentalizes your sensitive information.

Carelessly storing data

People will back up their information but fail to store it properly. One of the improper ways I have observed is people carrying sensitive data on a USB thumb drive. If you are like most people, you have the thumb drive in your car rings that you carry with you almost everywhere. If someone is interested in getting your information he/she only needs to get access to the thumb drive which is easy as you are always with it even in public areas. To protect your information you should store the device carrying sensitive information in a safe place and never carry it around. If you have to carry the drive with you, you should make heavy use of encryption. You should also make use of BitLocker, BitLocker, and other tools that offer additional protection.

At CryptKey we are developing an application that works alongside an implantable technology thus ensuring maximum protection for your information. To know more visit https://cryptkey.org

Article Source: http://EzineArticles.com/expert/Satvik_Mittal/1728302

Information Destruction, It's The Law

By James Dowse

Businesses serve the needs of its clients and this is achieved through the efficient and secure collection and utilization of information that is used to provide goods and services. This information is often confidential and sensitive. The responsibility to protect this information while it is necessary and securely destroy it when it is no longer needed has ethical and legal obligations.

Every business has the responsibility to protect its clients, employees and itself by ensuring the security of the information under their control.

Beyond the personal responsibility is the legal responsibility. Federal laws such as FACTA, The Red Flag Rule, The FACTA Disposal Rule, FTC Safeguards Rule, Fair Credit Reporting Act, Gramm-Leach-Bliley Financial Services Modernization Act, Identity Theft Penalty Enhancement Act, Sarbanes Oxley Act, HIPAA-Health Insurance Portability and Accountability Act, HITECH-The Health Information Technology For Economic And Clinical Health Act, have a commonality concerning what needs to be done for Information security and destruction, they are summarized as follows;

- Develop and implement a Written Information Security Plan
- Included in the plan must be Information Disposal Policy

    1. Destruction must be by Shredding, Burning or Pulverizing
    2. Electronic files must be destroyed by physically or erasing methods

    3. Perform due diligence when hiring a document destruction vendor or hire a vendor certified by a recognized trade association.

- Train all employees

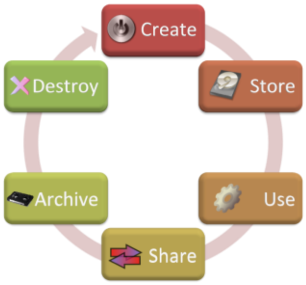
    1. Have employees sign an agreement to follow the company's policy

    2. Regular reminders and retraining of employees on the company's policy

    3. Imposing disciplinary measures for violations

- Monitor and test the plan
- Evaluate adjust and update the plan
- Document all information destructions
- Advise all employees of any changes or adjustment to the plan

You must be able to prove your compliance. Your plan must all be documented and available to Federal or State agencies when requested.



What next?

First and foremost, recognize information security as a priority.

Second, designate someone to be in charge of information security. This individual should be someone with a senior authority level, who has the authority regarding information security aspects of the organization's programs, policies and any new initiatives.

Third, find a document destruction vendor that is certified to assist you with development and implementation of a Written Information Destruction Plan.

Fourth, develop appropriate policies and procedures to safeguard the information. Be aware of Federal and State requirements.

Fifth, give the authority to your information security officer to oversee the implementation of and compliance with the written information security policies.

Sixth, train all staff members. Ensure that all staff is re-trained periodically on your policies and best practices for protecting information.

Seventh, hire a qualified document destruction vendor that has been certified by a nationally recognized trade organization (NAID-The National Association of Information Destruction).

Need more information? Need document shredding services? Call FileShred at 860-261-9595

Article Source: http://EzineArticles.com/expert/James_Dowse/2324935

5 Measures to Enhance Home Security

By [Lee Mark](#)

With the increase in illicit activities happening around, it becomes vital for everyone to take extra care of things that matter the most to you. The well-being of your family and the place where you dwell in would undoubtedly be the top on the list.

Following are the measures which will indubitably help in enhancing the safety of your home and consequently, strengthening the protection of your loved ones:

1) Boasting on Social Media is a big NO!

While you are on a vacation or going out on an official trip or visiting a relative, you tend to post the same on social media in form of departures, check-ins, or pictures of the new locations. This should be avoided as it will attract and update the burglars about your recent activities. If you are really enthusiastic to talk about your trip, you may post the images after coming back home.

2) Never, Ever

Most of us have a habit of leaving a message on the voicemail informing the person on the other side about the reason for not being able to attend the call, for instance, 'Away on vacation', 'Will be back in four days', and so on. Never disclose for how long you are out or away from your home. Keep your messages simple and generic for every situation, such as 'Hello! Thanks for calling. Will get back to you as soon as possible', 'Hey there! I'm occupied with something right now. Will call back soon', and likewise.

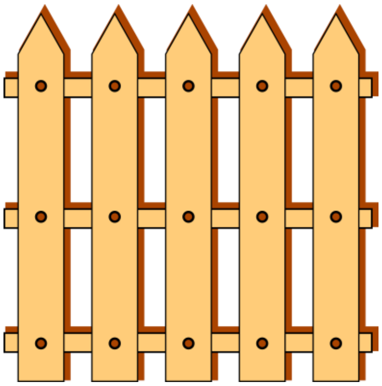
Moreover, don't even think of hiding your house keys under the doormat or in other obvious places. Intruders are smart enough and they already have the idea of all such places.

3) Eyes and Ears for your home: Security System

Technology has not only made our life simpler, but secured as well. If you live alone or stay in an isolated area, it is recommended that you should position a surveillance system (indoor security cameras and weatherproof outdoor surveillance cameras) at your home to ensure enhanced security. These gadgets are one of the best devices to monitor everything that is happening in and around your premises when you are at home or even when you are away from home.

4) Fencing the periphery

To restrict the entry and hence, make your abode more secured, you may go for the fencing option too. It is one of the most facile yet the strongest way to shield your dwelling. Various kinds of fences namely PVC, Wood, Bamboo, etc., are available in the market from which you can hand-pick the one as per your requirements.



5) Seal them to conceal things

The window shades are capable enough to conceal the whereabouts of inside. Windows with drapes or shades would certainly block outsiders to have any glimpse of inside. Also, be extra cautious and make sure to lock all your windows properly before leaving the house as the unsealed ones would offer quite a good welcome to the burglars.

Just implement these measures and reap the benefits of deepened security of your home!

Acknowledged for his security acumen, Rohan Sharma is a gadget wizard, an active blogger, and an eminent speaker. Having 10 years of experience to his credit, Rohan has always been a pertinent contributor towards the security industry with his area of expertise into the surveillance systems domain. He is closely associated with Revo America, a well renowned security products manufacturer and retailer.

Article Source: http://EzineArticles.com/expert/Lee_Mark/2266383

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

Before You Buy a Used Car, Check for Odometer Fraud

By Jessica Hunter

Odometer fraud, i.e. rolling a used car’s odometer back to make it appear less used, is sadly common. Here’s how to avoid it.

Any car, even a used one, is a huge investment — so you definitely don’t want to fall for something as avoidable as odometer fraud. While most cars made in the last few years use electronic odometers that are harder to jigger, fraud is still an issue for cars with mechanical odometers.

Here are some simple ways to check whether or not that honest-looking fellow trying to sell you that ’64 Nash with just 12,000 miles on the meter is on the up-and-up.

A Serious Issue

The goal of “busting miles,” as the Brits call it, is simple enough: the perpetrator wants to make it seem the car has less wear and tear than it really does. After all, it’s often hard to judge just by looking.

Odometer “clocking” is one of the most common consumer frauds out there. According to a study conducted by the National Highway Traffic Safety Administration in 2002, as many as 450,000 used cars with “clocked” odometers are sold each year in the U.S. alone.

That amounts to as much as $1 billion in costs to the people who bought them. Fortunately, with electronic odometers, the problem is slowing down somewhat.

Telltale Signs

While there are paperwork methods of checking for false odometer readings, such as obtaining a title or certificate of registration with an odometer history, or getting a Carfax report on the auto, they’re slow. For best results, you’ll need to be able to tell just by looking.

Do the numbers on the odometer line up properly? They shouldn’t contain any gaps or be crooked. The 10,000 mile digit is the most important to pay attention to. Next, bang on the dash; do any of the numbers jiggle? If so, they’re probably jiggered.

Other Indicators

Look closely at the area of the instrument panel immediately around the odometer. Do you see any scratches? That’s a dead giveaway. Next, examine the dash. Are there any loose or missing screws? If so, it could mean someone has taken the dash apart to get to the odometer.

Take the car for a test drive. Does the odometer stick at all?

Finally, give the whole car a good inspection, focusing on general wear. If the odometer claims 45,000 miles and the car seems too ragged out for that number of miles, that should tell you something…at the very least that a previous owner was too hard on it.

Bottom Line

If the odometer reading and the car’s condition don’t match up, or you notice oddities about the odometer or the dash, think twice about buying the car. You don’t have to accuse the seller of odometer fraud, but if you’re worried, just back off and go elsewhere.

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