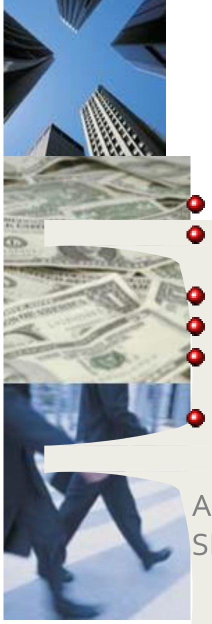


Issue 2 Volume 5 June 2019

ADDRESSING THE NEEDS AND SECURING THE FUTURE

Security *Solutions*

Helping secure your world

Editor's Note

In recent times our region was faced with an unprecedented number of computer-generated offences ranging from cyber crime, cyber bullying and identity theft to name a few. Due to this persons have adopted various methods of protecting themselves. This quarter, our newsletter will look into various methods of securing one's self when online.

With over 2.77 billion users, social media websites make a perfect platform for identity thefts. In article one, the writer discusses ten tips for keeping your personal data safe on social media. Given the huge user database of private information, it is the responsibility of social media platforms to keep personal information safe. Article two deals with the topic of scamming but when it takes the form of text messages. The reason is people trust text messages more than they do email, so they are more likely to fall for scammers who send text messages. One of the mediums used by hackers to access private information is public Wi-Fi. It can be used by the sinister minded to steal personal information, once you are connected to the internet; here you are at constant risk of spying and spoofing and all of your personal data can be easily accessible and vulnerable to hackers, this issue is detailed in article number three and it also details now to prevent this from occurring.

Article four addresses why cyber bullying occurs, how to prevent it, and how to address such attacks when they happen. In today's world, cyber bullying can greatly affect businesses. The types that can occur include (but are not limited to) fictitious reviews, false claims and trolling/harassment. Upon reading this article you will gain a better understanding on how and why cyber bullying occurs, how to prevent it, and how to address such attacks when they happen. Lastly article five speaks to an age old device, the smoke alarm, and here the question is, are they getting smarter? The short answer is yes, and this is further discussed in the article.

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

Regards
ASSL Marketing Team

10 Tips for Keeping Your Personal Data Safe on Social Media

Strong passwords, two-factor authentication and good cyber hygiene will keep your personal information protected while browsing popular social media accounts.

By Susan Alexandra

Social media plays a vital role in our daily life. Websites like Facebook, Twitter, and Instagram are the most common social channels used to connect with our loved ones. With over **2.77 billion social media users** today, such social media websites make a perfect platform for identity thefts. With huge user database of private information, it is the responsibility of social media platforms to keep personal information safe.

Last week, news circulated regarding the most commonly used social media website **"Facebook" that stored "hundreds of millions" of account passwords** and left them unencrypted. All the passwords were in plain text and viewable to thousands of in-house employees. If companies like Facebook have these issues, how can we rely on other platforms?

Every year, millions of people fall victim to data breaches and identity theft. If you fall prey, it can cost you loss of personal data along with lots of stress. It happens when you let your guard down and depend so much on these platforms for your security. Online safety is the most onerous task, but few ways can help you stay safe on social media.

Here are ten ways to keep your personal information safe while still enjoying the benefits of making social media connections:

1. Use a strong password and use a password manager

People use multiple social accounts for various purposes. Nevertheless, if your password is weak, your account's security gets compromised. Also, if you are using the same password for different accounts, all your accounts can get hacked by hackers.

Make sure to use a unique and strong password for every social account. Your password must include numbers, words, upper and lowercase letters, and special characters. The stronger password you use, harder for a hacker to crack your password. Change your password at least once a month. Try to keep different passwords for different social media accounts. If you are having a problem to manage your passwords, you can use password managers.

2. Add two-factor authentication for every social account

If you are using two-factor authentication on your social accounts, it will add an extra layer of security to them. When someone logs into your account from new location, device or browser; you will be sent a password that needs to be entered for logging into your social account. This means that every time you log in, you'll also need to enter a unique code sent on your phone by the social media website. Many people think it's time-consuming, but if you are seriously concerned about your privacy, you need to apply two-factor authentication on your each and every social account.

3. Setup security answers and update your privacy settings

All social media platforms give you the option to limit your audience. But many people are unaware of its importance. It is necessary for every user to explore, try and overview those settings. You can also set up security questions on your accounts. Instead of setting common questions like “What is your mother’s name?” or “From where you are?”, use questions that are hard for everyone to think about.

4. Be careful what you share
Avoid sharing personal information online because your information, including your email address, phone number, and social security number, is worth a lot of money to hackers and data mining companies.

Take a look at your social media profiles and try to keep them barren—the people who need to know your birth date, email address and phone number already have them.

5. Use a VPN

If you want to keep your conversations, messages, and calls secure; you can use an encryption tool which is called VPN. A VPN helps you to keep your communication encrypted and secure. All your information will be passed through a secure tunnel between the websites and your VPN services provider.

If you are really concerned about your privacy, you might have a question; how do VPNs protect my data? As mentioned here “Even though all the information going to and from the customer to the VPN is encrypted, all the information being sent through the outgoing VPN server is subject to the regular rules of the wild internet.”

6. Keep system up to date with antivirus

Keep your system updated with the latest antivirus. Never operate an internet-enabled computer without installing anti-malware and antivirus software. There are many paid and unpaid antivirus software available. To secure mobile devices, use antivirus apps to secure your online activity and important data.

You have a friend request.

Jane Doe (St. Louis, MO)

You have 3 friends in common.

7. Verify friend requests and block fake accounts

Platforms like Facebook and Instagram are full of fake profiles. Those fake accounts can be a hacker, a suspicious organization or even a frenemy who wants to monitor your activities.

Don’t accept any friend request without verification. If someone is disturbing you, it's good to report and block such profiles.

8. Regular check your mailbox to check suspicious login attempts

Keep a habit of checking your emails regularly. Many people ignore emails from Facebook, Twitter or other social accounts. They might think that it's a notification from their friends, but it could be login attempt by a hacker, and your social platform wants to inform you about it.

If you got a suspicious email or login attempt to your account, change your password as soon as possible.

9. Use an updated browser
Use an updated browser for a pleasant browsing experience. Make sure to use the latest version of the browser that is not vulnerable to hackers. Also, don't save your passwords on your browser because if your system gets compromised, hackers can easily read your saved passwords from the browser in just a few clicks.

10. Log off to your accounts when used.

The last important and good practice is, always log off to your system when you are done with it.

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

Scammers Turn to Smishing for ID Theft

Phishing, the scam that involves tricking people into giving away confidential information, is surging via text messaging, posing a greater than ever risk of identity theft. The reason? People trust text messages more than they do email, so they're more likely to fall for the scam.

This type of phishing, better known as "smishing," has been around for years but because consumers have wised-up to email tricks and, in fact, are using email less and less for simple messages, scammers have switched their focus to SMS texts to target their victims.

According to computer blogger Luke Larsen, the crime "has come full-force to texting, and it carries even more potential danger than it does through email." Writing for the online tech site Digital Trends, he says that cyber crooks are buying up smart phone numbers from databases on the dark web and then targeting them to trick users into giving up personal info.

The text usually contains a link that downloads malware, which steals as much data as it can find. And therein lies the threat:

"Your smartphone knows a lot more about you than your PC, so an installed piece of malware might steal the phone numbers in your contact list and spread the virus in hopes to exponentially multiply," Larsen says. "Even important bits of personal data, like banking credentials or your tracking location, can be at risk."

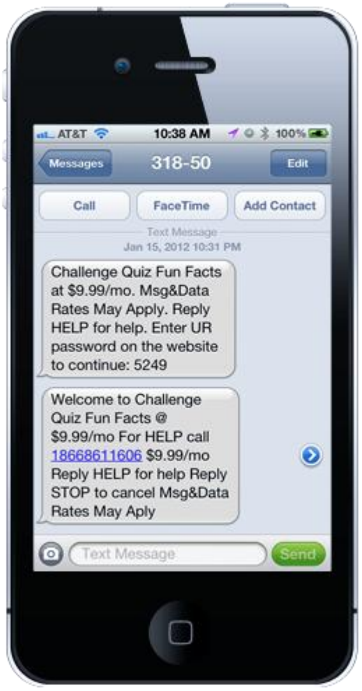
Insider View

His views are echoed by industry insider Ruby Gonzales, communications director of NordVPN, which recently published a report on the trend. She says that, as personal use of email is falling, legitimate marketing companies have turned to SMS and some social media sites to sell their products and services.

Users have become accustomed to receiving offers by text, including clickable links. They're also less likely to have spam filters on their texting service, like they do with email, and it's often difficult to check whether links inside SMS messages are valid or not. "It's a wider channel for criminals," Gonzales says, "and they are trying to exploit it in the same way as all other channels that are opening."

Scammers are also using texts to pose as tax authorities, not just in the US but also in the UK and Canada. The tactic creates a false sense of realism because many people don't realize that text messages can be a threat.

"They say that the user is due a tax refund or needs to provide more information," she explains. "Basically, they try to get users' information, and that can be used for stealing their money."



Challenge Quiz Fun Facts at $9.99/mo. Msg&Data Rates May Apply. Reply HELP for help. Enter UR password on the website to continue: 5249

Welcome to Challenge Quiz Fun Facts @ $9.99/mo For HELP call 18668611606 $9.99/mo Reply HELP for help Reply STOP to cancel Msg&Data Rates May Aply

Dangerous messages sometimes use shortcodes -- one-word responses users are asked to key in to acknowledge they got it. That can be enough to trigger a malware download.

For example, scam messages posing as donation requests from charities may provide a single word response that immediately forwards a donation. Scammers have used the same tactic, Larsen says, to steal money right out of bank accounts. You might also end up with additional charges on your phone bill, according to a recent warning from the Federal Trade Commission (FTC).

Research suggests as many as one in three smartphone users had been targeted by a smishing attempt in just six months last year, although the actual number is likely to be higher since most people don't report scam attempts.

What to Do

The best thing you can do to avoid falling victim is to never click on a link inside a text message.

Certainly, you should never respond to a request for a password or other confidential information. Instead, visit the real website of the organization that seems to be asking and check if it's a genuine request.

You should also use extreme caution even if the message asks you to send the word "Stop" to stop receiving messages, as many do, unless you're 100% sure that it's genuine. Sending a "Stop" message may not land you in immediate trouble but it signals to a phishing scammer that there's a bite on the line.

In fact, for the same reason, you should never reply to text messages from someone you don't know. It simply opens the door for an onslaught of spam. In most cases, it's actually illegal for businesses to send unsolicited texts to mobile devices without your permission. So, if you get one, that's a big red flag.

Block the sender if you can. But otherwise, just delete the message.

And don't share your cell phone number on social media.

In addition, it's wise to install an anti-malware app on your phone.

Contrary to what many people believe, Gonzalez says, phones are more susceptible to malicious software than PCs. "Specifically, Android phones," she warns, "because Android is a more open system."

To learn more about smishing, check out this article from Internet security company Kaspersky: https://usa.kaspersky.com/resource-center/threats/what-is-smishing-and-how-to-defend-against-it

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

How to Stay Safe on Public Wi-Fi Networks: A Detailed Guide

All of your personal data can be easily accessible and vulnerable to hackers.

By Susan Alexandra

The internet is not the safe haven for users. It’s a world which is full of hackers and other bad guys. Once you are connected to internet; specifically through public Wi-Fi, you are at constant risk of spying and spoofing. All of your personal data can be easily accessible and vulnerable to hackers.

Connecting to public Wi-Fi is very easy and people love to connect it. From restaurants to malls, hospitals to libraries, each place is nowadays equipped with the Wi-Fi. Some Wi-Fi does require a password to connect while others are open for all. You can get access to them freely and perform various tasks on the internet without paying a single penny.

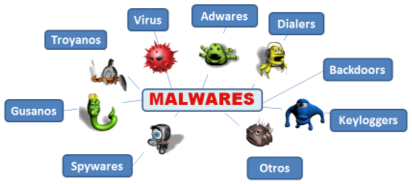
But in reality, nothing in the world is free. Even if it appears to be free, it has a price to be paid and for public Wi-Fi, it has a disguised price that you are paying by risking your own security and data, as well as the security of people associated with you.

According to the recent study of **Kaspersky**, about 70 percent of tablet owners and 53 percent of mobile phone users use free public WiFi hotspots to go online.

Risks Associated with Public Wi-Fi

Public Wi-Fi is open networks and is accessed not only by regular users but it is a hub of spies and hackers too. Whether you opt for a password secured public Wi-Fi or get connected with an open one, it makes your online existence vulnerable. To stay safe, it is essential to be well aware of the plausible threats associated with public Wi-Fi while using the one.

Man-In-The-Middle Attacks (MITM). The most common risk for public Wi-Fi users is that of the man in the middle attacks. There are high chances of hackers using the same network as yours and they work as the middleman. They receive all the information sent through your device before it reaches the targeted sites and vice versa. They can easily gain access to your important information like email addresses, bank details, photos, and crucial files if shared through this connection, and then use it for any unauthorized or illegal purpose.



Malware. Malware is a file containing viruses that can hijack your computer or any other device connected to the network and gain access to all the offline information saved on your device. These files are sent by hackers usually in the name of the system upgradation and once you download them your device is easily accessible by the host site or person. When you have file sharing option enabled in your device especially while using public Wi-Fi you are a prime target of malware.

FREE INTERNET
seattle
Wi Fi
hotspot
Connect Now...
Step 1: Open your wireless software
Step 2: Set your Network ID (SSID) to: SeattleWiFi
Step 3: Connect and open your web browser
Rainier Chamber of Commerce
City of Seattle

Rogue Wi-Fi Hotspots. Not all public Wi-Fi is hosted by authentic and legitimate networks. There is a high risk of fake networks offering free Wi-Fi with some reputable name that are actually created by cybercriminals. This is a common trick used by hackers to get easier access to the desired users account. Once you are connected to these rogue Wi-Fi hotspots, you have actually given yourself in the hands of the predators. Now not only your online activities are in danger but all your offline files and information are easily accessible for the hackers. They can even use your device for any unauthorized purpose and can carry out all online activities from it with the same legitimacy as yours and that too without you being getting notified.

Cookie Theft

Data encryption is not implied by all the host sites and Wi-Fi networks. When the data moving to and fro the site which is not encrypted and you are accessing it from public Wi-Fi there is a high risk of cookie theft. The unencrypted session data can be easily replicated by any third party and can be used with the same convenience as the real user.

Computer Worms. Computer worms are advanced versions of computer viruses but unlike viruses, they don't need any program to run. Computer worms usually transfer from one computer to another when they are sharing the same internet connection. With public Wi-Fi, the chances of getting infected by the worms are multifold as there are many different users accessing the network at the same time and if only one device is infected, worms can propagate to all the other devices connected especially the ones with no or minimum defense.

Packet Sniffing. Packet sniffer, also known as packet analyzer, is a small hardware tool that is installed to monitor the traffic on any given network. It also intercepts some parts of the data being transferred through the network. Though the sole purpose of installing these devices is to record the network traffic, it is a vulnerable tool and can be used by cybercriminals to trace the activities of any user on the network. The packet sniffing can be used as a tool for spying and spoofing the online activities of public Wi-Fi users and can be installed with ease.

Staying Safe on Public Wi-Fi Networks

Public Wi-Fi networks, though, appears to be unsafe and vulnerable but this doesn’t mean you cannot use it at all. After all, it’s a free service and is a blessing in states where internet connections are very expensive. It is certainly a good way to stay connected while being on the go or during vacations. The good news is that you are not defenseless against the threats of public Wi-Fi. All you have to do is stay vigilant and follow some security measures to stay safe while accessing the internet through public Wi-Fi.

1. Keep Auto Connection Turn Off

We have open public Wi-Fi networks around us most of the time we are in a commercial area or crowded place and they get automatically connected to your device if your Wi-Fi is on. In order to stay safe always keeps your Wi-Fi turned off when not in use especially at public places. It costs nothing but can save you from most of the rogue Wi-Fi hotspots.

2. Verify the Network

Whenever you log into a new public Wi-Fi, always verify the connection name with the employees or workers of the place around. There can be fake networks created by the predators with similar names and you can fall prey to that. It is even safer if the public Wi-Fi is protected by a password and is accessed by clients and employees only.

3. Disabled Sharing

Your devices usually have a file sharing option turned on by default. It allows files to be shared publicly on the network and is not a big issue until you decide to connect to a public Wi-Fi. Always turn off the file sharing option when you are using public Wi-Fi. Though it sounds simple, it is your best defense against malware so don't ignore this simple step and keep your devices safe.

4. Use VPN

VPN is your safest bet while using public Wi-Fi. It is a Virtual Private Network that provides an encrypted tunnel for all your online activities. It keeps all the data to and fro your device and the host sites free from any spying or spooking. It provides a genuine end to end encryption leaving no loopholes for leaking of data through any means.

VPN also provides you with anonymous proxies which means you can alter the location of your server while being in some other place. This way you can fool the host site about your actual location and can enjoy surfing the net as an anonymous person from the server's id. It eliminates the risk of being traced or tracked through your online presence. But which VPN to trust?

There are different VPNs available. Some of them are less reliable and secured as compare to the industry leaders. According to **VPNpro**, the VPN market is set to hit $54 billion by 2024. On the analysis of 100 VPNs, the research shows the 10 most popular VPNs on the market today.

5. Use SSL Connections

SSL is the Secure Sockets Layer that ensures that your host site is encrypted. All sites with SSL connection uses HTTP before its address and often a lock symbol displays in the address bar which indicates that the data shared on these sites is completely safe and secured. Never use a site which is no encrypted especially while using public Wi-Fi. This can be a trap from the cybercriminals and can risk your security. Though SSL connected sites do not leak your information they don't provide any defense against man-in-the-middle attacks.

6. Enable Security Apps on Your Device

No matter how secured your network is, device security is essential too. There are various anti-viruses and anti-malware apps that detect any fishy activity in your computer and alerts you. It is an added layer of security and acts as a barrier between invading viruses and your device. It is better to always keep your device secured with latest and updated versions of your anti-virus software and it becomes crucial if you are using public Wi-Fi on your device.

7. Be Cautious While Browsing

The major risk associated with the use of public Wi-Fi is the **theft of important information** and spying. Even if your device is completely secured and you have taken all the essential safety measures but still never carry out any financial transactions through public Wi-Fi. It can be extremely dangerous and can cause you an irreversible loss.

8. Keep Your Accounts Secured

Apart from online banking and shopping transactions, it is also necessary to keep your email and **social media accounts secure** as well. Always use two-factor identification for your accounts to prevent any unauthorized access. Be extra vigilant while using public Wi-Fi and never opt for remember password option or auto log in and sign out of your account as soon as your task is done. Also, limit your browsing with public Wi-Fi to stay safe.

9. Remove Public Wi-Fi

Once you have connected your device on a particular Wi-Fi, your device retains its information and connects you with the network whenever it is approached. For security purpose always delete the public Wi-Fi and chose to forget password option once you are done with your task. Networks can also get hacked and old users often stuck in the trap of cybercriminals.

To Conclude

The Internet has become an essential part of our everyday life. Whether it's a matter of business or job or need for entertainment or infotainment internet has become a necessity. People from all over the world and belonging from the different socio-economic background are online most hours of the day and night. Wi-Fi is installed in every place be it school or university, hospital or restaurants, public libraries or private buildings, homes or offices as it has become a crucial part of our lives. Many places even offer free Wi-Fi which sounds very appealing and appears as a blessing when you are not in your hometown but there are many threats associated with it.

You definitely cannot avoid public Wi-Fi completely but taking some safety precautions can save you from a lot of troubles in the future. Most of the security leaks are the result of mere ignorance and can be rectified with little vigilance. Remember no matter how many layers of security you use for your device and how cautious you are about online transactions, public Wi-Fi will still remain vulnerable though to a much lesser extent.

"How to Prevent Cyber bullying From Hurting Your Business"

- Negotiation Tip of the Week

By Greg Williams

In today's interconnected world, #cyberbullying can greatly affect businesses. The types of cyberbullying that can occur, such as fictitious reviews, false claims and trolling/harassment can arise for reasons of retribution or corporate positioning for a negotiation. This article addresses why cyberbullying occurs, how to prevent it, and how to address such attacks when they happen. The information applies to businesses, but it can also apply to individuals.

Cyberbullying - Why?
Bullies tend to target those they sense as being vulnerable and weaker than themselves. In business, corporations of any size may target another organization for numerous reasons. They may do so to affect that business' revenues, its employee morale, or to diminish the company's reputation.

When negotiating (you're always negotiating), cyberbullying can be a tactic employed to soften an entity prior to a negotiation. This can occur by anonymously placing false stories about that entity in social media outlets, or having allies serve as its proxy. In either case, such actions can give the appearance of a corporation under siege from multiple points and sources.

Companies remain vigilant about social media activities because they're aware of the impact that negative postings can have on their business. A corporation can even be susceptible to cyber blackmail. That's another form of cyberbullying that leaves corporations in a precarious position.

Cyberbullying Example and Handling:
A business associate that owns a diner recalled a time when several male professionals walked into his eatery. They were inebriated, boisterous and disrespectful to other customers and my associate's employees; my associate did not want to confront his rowdy patrons by calling the police because he didn't want to lose control of the situation. So, he informed the disorderly customers that his in-store security camera was filming their actions and if they didn't adopt a mannerable demeanor he'd have to release the video on social media. While he wasn't threatening them with cyberbullying, he was implying that he'd use cyberspace to 'out them' if they didn't correct their behavior. The men apologized to everyone in the establishment and no further actions were required. The threat of using social media was enough to back them down.

Cyberbullying Prevention, Combating, Overcoming:
As a business owner, to combat cyberbullying:

1. Be proactive on social media platforms and garner as many positive comments as possible. Then, if another organization attempts to bully your business, they'll stand out as an outlier compared to the glowing comments you've already received.

2. Have business allies and customers at the ready to post rebuttal comments to support your organization against a bully. In extreme cases, have your allies note the efforts that a cyberbully has engaged in, in other environments. Respond in a strong and swift manner to let the bully know that there's a high cost for him to incur for targeting your business. Remember, bullies

tend to pick on easy targets. To combat a bully successfully, insulate your business; don't make it an easy target.

3. In brick-and-mortar businesses, have camera systems installed that captures, in real-time, the actions that a bully might perpetrate in your establishment. Their in-person actions could be the prelude to cyberbullying. Being proactive with a video account of their in-person actions will allow others to see your side of the story more clearly.

Conclusion:
If you're someone that engages in cyberbullying, be mindful of who you attack. What you do to others can come back to harm you. It might do so at the most inopportune time.

As a business owner, be proactive to bullying attempts. Follow the suggestions above and ward off potential attacks before they occur... and everything will be right with the world.

Remember, you're always negotiating!

"Body Language Secrets To Win More Negotiations" will allow you to gain insight as to how you can negotiate better by being able to read the other negotiator's body language. In addition, the book goes deep into new negotiation strategies that you can use to disarm your negotiation opponent and increase your negotiation win rates.

Get "Body Language Secrets To Win More Negotiations" and start winning more negotiations while reading body language to do so!

https://www.amazon.com/Body-Language-Secrets-More-Negotiations/dp/1632650592/ref=sr_1_1?ie=UTF8&qid=1476818919&sr=8-1&keywords=body+language+secrets+to+win+more+negotiations

Article Source: https://EzineArticles.com/expert/Greg_Williams/98280

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

Are Smoke Alarms Getting Smarter

By George Uliano

The short answer to that question is yes; smoke alarms are getting smarter. Now let's take a look into why that is.

For years smoke, CO and fire alarms were those round white things on the ceilings in your house that woke you up in the middle of the night with beeps when the battery had to be changed. Those beeps were the only indication that something was working, unless you got out the ladder and climbed up to push the test button. How many people actually performed that monthly test?

I am not saying that these alarms are bad, they are most definitely better than nothing. But like all things electronic, the times and these devices are changing.

Smart smoke alarms or detectors offer the following benefits:

- They can detect smoke and CO2 faster
- They will tell you in plain English when their batteries need to be changed
- They can automatically test themselves
- They can be controlled by an APP from your phone
- They can provide visual cues that they are working

These are just some of the most important features. Different manufacturers will include other features. A company call NEST is the name that most people will recognize as a provider of these devices. Another important feature is if you have multiple alarms in your house they all network together. If an alarm goes off, it will force all alarms to sound. Some will then tell you in plain English what alarm is detecting the problem. If the problem turns out to be something like burnt toast, you would be able to turn off that alarm through the APP.

There are many features that the manufacturer can add through software updates sent directly to the alarm. That will keep your alarm updated with features for many years. Most smoke/CO2 alarms and detectors will have an expiration date of between 5 and 10 years. This means that the material inside the alarm which detects smoke or CO2 has exceeded its ability to detect smoke or CO2. These smart alarms will tell you when that time is, so you can replace your units.

Smart alarms can communicate with Alexa, Google Assistant and others This allows them to connect to devices such as thermostats, lights, doors, etc. In future years everything in your home will be connected. That said; always make sure that you control the equipment, not the other way around.

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

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

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

Reprinted for ezinearticles.com

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

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