Issue 18 | Volume 1 | December 2015

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 2016. 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 very own Regional Director Mr. Brian Ramsey discusses proper alarm system design, within the article he highlights and clearly outlines how cutting corners can sometimes cost more. Article two speaks to applications of facial recognition which is a biometric software application which can identify a person through his/her digital image. The third article speaks to password management software and how it can help you keep your passwords and accounts safe. Some of you may have heard about Electronic Locks and maybe even Wi-Fi Locks, but what is a Wi-Fi Lock and how does it operate? Article number four answered this and many other questions on Wi-Fi Locks.

During the holiday season many families embark on vacations or persons may be out of town to spend time with love ones. Most times a hotel is the number one choice; however, hotels are most times a target due to the fact that they attract large volumes of travelers who may be unfamiliar with the area, and in many cases, unfamiliar with the country as a whole. The fifth article details why hotel security is so important.

As technology advances many persons no longer engage in the traditional shopping techniques, the internet and websites such as Amazon, Ebay, Macys and Sears to name a few have drawn a lot of Christmas shoppers away from the local malls and stores. With the growth with online shopping simultaneously a growth in online banking was experienced, however we must not forget to secure ourselves from criminal activities in cyber space and the real world as well. The sixth and seventh article speaks to this.

We do hope that our quarterly publication helped settle some of your security concerns. As in 2014 it was our goal in 2015 as well that this newsletter will help build awareness with respect to property and personal protection and we trust that this mandate was achieved.

Regards
ASSL Marketing Team

Proper Alarm System Design – Cutting Corners can sometimes cost more

By Brian Ramsey

In February 2015 there was a burglary of a Pawn Shop in Port of Spain, Trinidad, in which the burglars escaped with US $3.5 million in cash and jewels. The burglary was only discovered the following morning when the employees arrived for work and this is in spite of the fact that the premises had electronic security systems. No electronic security system can prevent a burglary as they are designed to alert individuals that a burglary is taking place or to provide evidence after the burglary has taken place. The issue then becomes how could the burglars have broken into the premises, taken the items and then left and no one was alerted. This incident highlights the increasing knowledge and consequent professional approach of Caribbean burglars and the fact that in the design of an electronic security system one has to take into account all possibilities.

Many times when persons are looking at premises they view a wall or roof or window and form the opinion that it is solid and therefore impenetrable. They then, when designing the electronic protection, do not electronically cover that area because of their opinion that the area is too hard for someone to get through. At times the non-coverage of an area is the result of a customer trying to reduce the cost of the electronic security protection or of a security company trying to lower the cost of their quotation so that they can get the job. Often the view of impenetrability is based on their opinion that they cannot break through the wall and so they assume that no one else can but the question should really be, can I break through that wall or window if I had the correct tools and sufficient time.

In the case of this particular burglary, the cash and jewels were in steel safes inside a concrete vault room.

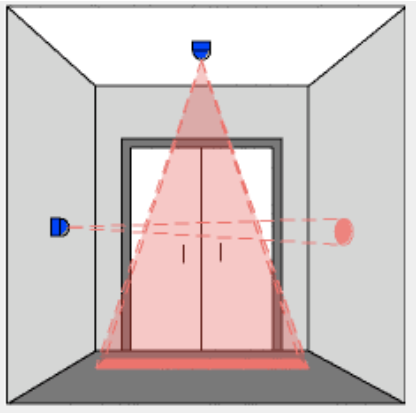
This vault room had electronic protection on the door leading into it and the premises had CCTV. So the uninitiated might again ask how could these burglars break in undetected and get to the valuables and then escape without the alarm system notifying anyone.

For this burglary the thieves came through the roof of the building and then used drills to bore a large hole through the slabs that form the top of the concrete vault room. Once inside they used portable blow torches to cut into the steel safes. After gaining access into the safes they removed the valuables and then left via the route that they had used for entry. Before making their exit they made sure to remove the DVR that contained the images from the CCTV cameras.

Many individuals would have thought that steel safes inside a completely concrete room provide a very secure environment, especially with alarm protection on the door to the room. Burglaries such as this one however demonstrate the weakness in thinking that steel and concrete alone are sufficient for protection. As we stated earlier in this article, the question to be asked by the designer of any security system is “can I break through that wall or window if I had the correct tools and sufficient time”. These burglars have shown that you can and it is to be noted that they did not interfere with the door that had the electronic protection thus not triggering the alarm system.

One should not lose hope however and think that it is impossible to protect their valuables; it merely requires the appropriate design of the electronic security system. In this situation it appears that the designer only considered the

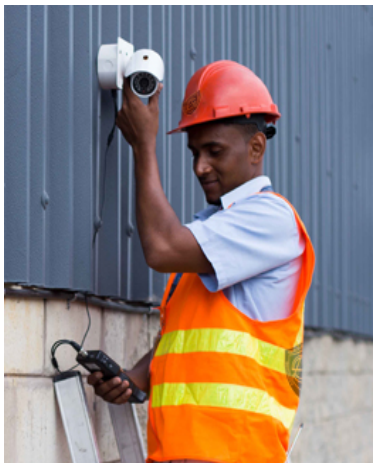
possibility of someone breaking into the room through the door. If however an electronic security system includes vibration sensors on the walls and roof then the burglars would be detected as soon as they attempt to drill through the concrete roof. Thus there would have been notification of the burglary attempt before the thieves manage to enter the room and so give responding agencies the opportunity to be on the scene before the thieves can get to the valuables.



Another detection device that could be incorporated into the design would be a PIR) Beam placed inside to room to detect anyone who enters the room from any side once the alarm has been turned on. We would not however recommend relying solely on a PIR as this detects when the intruders are already inside and they could "grab and go" before response arrives.

Often in the urban areas in the Caribbean there is significant building rumble as a result of the passage of heavily laden trucks and/or vehicles with excessively loud sound systems. Some persons are concerned about the high number of false alarms that may be caused by this passing external vibration and so are reluctant to recommend or install vibration sensors in commercial urban settings. While this may be a valid concern it should not deter persons from using such sensors as these sensors can be adjusted to reduce their sensitivity to such external vibration. Where the sensors are set with reduced sensitivity then they should definitely be combined with another internal detection device such as a PIR, so that there is double layer protection.

There are also other detection devices that can be incorporated into the security system to provide the protection through alerting of intrusion attempts. The overriding theme however must be that one should not assume that because you cannot determine how to break into a place that no one can, rather one should identify all possible entry points and seek to ensure that these are covered.



About the Author

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

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

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

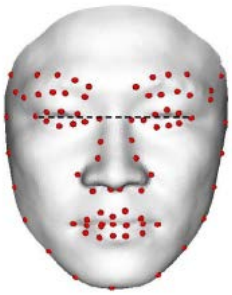
Response Services
Alarm Monitoring
Guarding Services
Electronic Service
Courier Services
Assess Controls
Data Services
Cash Services
Investigations

Applications of Facial Recognition Biometrics

By Fahad A. Khan |

Facial recognition is a biometric software application which can identify a person through his/her digital image. Digital image here means the facial components of a person like lip size, cheekbone shape etc. They are primarily used for security reasons but current trends indicate its application in multiple spheres like online shopping, gaming etc.

How does it work?
Facial recognition works on the principle that the various face pointers are differentiated by the shape and size of the face. A facial recognition system identifies these differences as Nodal Points. Every human face has approximately 80 nodal points. These are measured in terms of:
Nose width
Lip size
Jaw line length
Eye socket depths
Distance between eyes
Cheekbone shape



The nodal points are then measured creating a numerical code known as Faceprint that represents the face in the database.

Some Applications
Since Facial Recognition System (FRS) is innovative and reliable, its use and applications are increasing with government and private firms backing it.

Financial Security
Banks and financial institutions are using this technology to remove the usual PIN and password protection methods which could be counterfeited. FRS can also safeguard vaults and deposit boxes against loots.
E-commerce
It helps verify the identity of shoppers and fastens the shopping and transaction process.
Immigration
This serves as a stronghold against international terrorists who want to unleash terror in foreign soil. The effectiveness to identify a threat increases five-fold as it's difficult for human eyes to identify people with just a photograph.

Law Enforcement
An FRS application includes acclaimed CABS-computerized arrest, booking system and child protection measures. This is used globally to recover missing and exploited children. This helps verify molesters and traffickers.

Access Control
FRS can help identify a person on their identity claims. It eliminates the risk of people obtaining false keys and access cards.

Surveillance/scene analysis
FRS has the ability to extract, categorize and search for non-facial imagery like scars, tattoos, marks etc. The software is capable of identifying the exact people it wants to find in a crowd. It can analyze scenes from archived videos for the precise faces.

Homeland Defense
Homeland defense is a major part of a country's development. Countries around the world are making sure that this system helps them prevent terrorists from boarding aircraft, protecting critical infrastructure like dams, temples, bridges, energy plants etc.

Aviation Security
Airports are slowly rooting towards this technology for obvious reasons. Apart from the usual metal detectors and fortifications, FRS use can help

identify and nab suspects without much hard work. Since most terrorists arrive either through planes or ships, aviation becomes an important sphere to protect.

Voter Verification
It verifies various government officials prior to voting and election campaigns. Also, it stops forged and repeated voting.
Facial recognition is one of the most popular biometric technologies along with Iris and Fingerprint scanning. The applications of FRS are however on a rise and have found their way into the gaming industry as well. Because of the excellent features, its dominance grows and will grow until each and every necessary sphere hasn't been included by this technology.
Star Link is the pioneering manufacturer of biometric devices in India. Why don't you pay them a visit?
http://www.starlinkindia.com/

Article Source:
http://EzineArticles.com/expert/Fahad_A._Khan/2057675

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

How Password Management Software Can Help You Keep Your Passwords and Accounts Safe

By Terrence Lewis |

With the many attainments in technology, hacking is no more a difficult job, especially when passwords are in a vulnerable state. Fortunately, password managers are introduced to provide security to accounts. These password management applications are nothing but programs that function to manage and secure your various logins and passwords.

These tools enable you to store passwords securely in a particular location to ensure that they are recalled with just a few clicks. Aside from that they are free, encrypted, secured and easy to use. The best part about them is that they can be sync across numerous devices. Thus, having them installed will ensure that you never lose your password even if you lose your operating device.

Why Consider Using Password Management Software?

Recent studies proved that most users make two common mistakes. First, they use simple passwords and second they create similar passwords for multiple accounts. In case one account is hacked the others too become vulnerable. This is the reason why considering using these password managers can help you keep your accounts safe and secured. Also, they can be integrated with web browser to handle tasks such as secure navigation and automatic login input.

Password Management Software: Key Features

These software programs come with innumerable features allowing you to keep your logins and passwords safe and secured. They are;

• Flexible Access: They can be accessed from anywhere. Whether you are at your home, office or travelling, these password managers can be accessed easily.

• Synchronize across Various Platforms: Be it your Windows or Android phone, personal computer or laptop, they can be synchronized across all these platforms.

• Easy to Use: While using these managers you just have to remember one password and that's it. Generally, these kinds

of software encrypt your data needing one master password for accessing the others.

• Unlimited Storage: One of the most significant features of these managers is that they offer unlimited password storage facility. Aside from giving details about the login and password of your account, they also supply additional information.

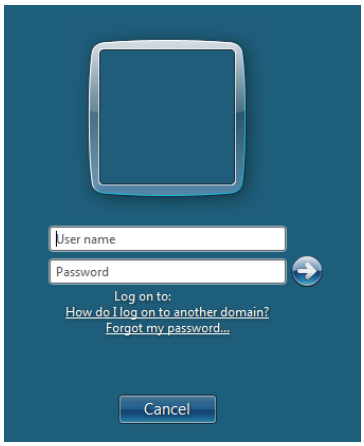
• Easy to Search Interface: As they allow full-text search, you can find information quickly. All you need to do is put in related data in text box and press enter and you will receive the information immediately.

• Record Different Types of Passwords: Not only they record generic passwords, but also store e-mail account passwords, software registration codes so on and so forth.

• Generate Multiple Passwords: These managers create some random passwords depending on the requirements of the users ensuring that they are hard to crack.

• Data Safety Safeguards: They ensure that the information stored is fully protected. They encrypt the master password by SHA algorithm, which is irreversible and has the highest encryption strength in the world.

Looking for a password management software to secure all your login credentials? To install password manager programs, look into our online store.



Article Source: http://EzineArticles.com/?expert=Terrence_Lewis

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

Wi-Fi Door Locks

By George Uliano |

You all have heard about Electronic Locks and maybe even Wi-Fi Locks, but what is a Wi-Fi Lock and how does it operate? I will explain the function of these locks and how they operate in this article. Wi-Fi locks operate like or even the same as electronic locks, the main difference is how they communicate and how they use that communication to operate and function.

The first thing to discuss is the mechanical parts of the lock. All locks must have some type of mechanical components to function. In this article we are talking about door locks, which could be either a knob/lever lock or a deadbolt lock. In either case a locking bolt must be moved to the open position. This can occur by a motor, solenoid or mechanically and still be considered a Wi-Fi lock. The difference is how the manufacturer designs the lock, in other words, does he put just the minimal amount of mechanical components, how will the lock communicate and what type of batteries to use, to name a few.

For the electronic part of the lock the design has a lot to do with how communications to it will occur. For this article we are going to discuss Wi-Fi and the communication method. We all already know what Wi-Fi is and how it works, a lot of us use it every day. A Wi-Fi lock will communicate through your modem just like your laptop or smartphone. Once set up, you will be able to control your lock through your smart phone or tablet. Again, the amount of control and features are up to the manufacturer and what they build into their software.

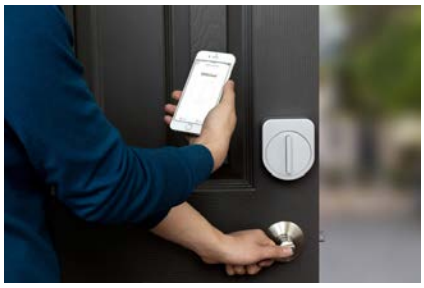
At the very least you should be able set up users, set up temporary user codes and lock out users. You may also be able to unlock and lock your front door remotely. Some models will store access history, so you could see who locked or unlocked the door in the past. You could also set it so that any time the door is opened you will get an alert. If you tie a camera to the lock you would be able to see who is at your front door.

The real difference in W-Fi locks is the software and what it is able to do and how well it works with other devices like the camera. The very first thing that you should do if you get a Wi-Fi lock is to set up security and passwords, if that lock doesn't have this ability buy another one.

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



If you are interested in learning more about our home security systems visit our website at: http://esis.assl.com/alarms-electronic-products/cctv-systems

Why Is Hotel Security So Important?

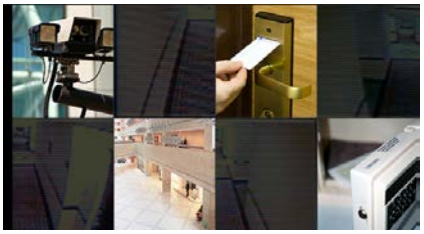
By Oded Loulay | Submitted On October 27, 2015

For many different businesses around the globe, having adequate security in place is essential to make sure that the assets, employees and customers of a business are protected. This often requires a blend of investing in security guards for hire, as well as implementing surveillance systems to monitor the premises.

We are all familiar with having CCTV cameras directed at us when entering and exiting a hotel, along with seeing the security guards that patrol the premises taking care of any problematic encounters with guests. But just how important is hotel security and how does its implementation affect the welfare of this particular type of business?

Firstly, it is important to note that hotels can be a particular target for thieves and other criminals for a number of reasons, which makes it so important to have sufficient security systems in place. One of the reasons for this is that these venues are easily accessible, with potentially hundreds of individuals exiting and entering the building each and every day.

Although hotel staff may be familiar with long term guests as well as other employees of the hotel, it is easy for people entering and leaving the hotel to retain their anonymity amongst larger groups and therefore more easily get away with committing crime.



Hotels are also a target because they attract large volumes of travellers who may be unfamiliar with the area, and in many cases, unfamiliar with the country as a whole. Travellers can make particularly easy targets for crimes such as thefts and assault, simply because they are less aware of their surroundings and especially vulnerable.

Those who are travelling also tend to carry large amounts of money with them and other valuable belongings such as cameras, mobile phones, passports and, in the case of businessmen and women, laptops for their work. This again makes them the ideal targets for thefts and muggings.

Some hotels may even play host to high profile guests, including celebrities, politicians and well-known business executives. These individuals can be the targets of many different types of crime, and although they are likely to have their own close protection, employing security guards for hire at the hotel itself can provide an extra level of safety for these people.

With that said, it can be argued that investing in security services is essential for ensuring the safety and security of guests, whether they are members of the general public or are very high profile clients. Not only is manned guarding an excellent deterrent to crime, but security guards can also provide a physical response to challenging and dangerous situations.

Whereas CCTV cameras can capture faces and actions carried out by the perpetrators of crime, it is the intervention of security guards in various circumstances which can be most effective at protecting and helping guests that find themselves the target of crime.

This added level of protection has other benefits for the hotel business, and one of these is that guests may be encouraged to stay there more often. This is especially true of high profile guests, who may be understandably concerned about their own welfare if staying in a hotel with an inadequate security system in place.

Along with increased levels of business, this can then influence the success of the hotel in other ways, such as encouraging outside investment in the hotel and increasing shareholder value. The hotel can build a strong name for itself both among the general public and investors, which can pave the way for significant future growth.

With that said, it is important that all security guards that hotels hire should have adequate training in hospitality as well as in providing security services. All good security companies will be able to make sure that not only is a high level of protection provided, but also that all officers act in a manner that is in line with the hotel's image.

1GS Services are one of the fastest growing security companies in London, providing expertly assessed and highly personalised security solutions to a wide variety of clients in both the public and private sectors. With over 40 years' combined experience, the team at 1GS Services aims to meet the highest industry standards and is fully qualified to meet all security needs. 1GS Services also ensures that

clients receive ongoing support and updates during the course of a job, and detailed reports and evaluations once the work is completed. Services include: Manned Guarding, CCTV Installation and Monitoring, Retail Security, Corporate Security, School Security, Residential Security and many more. For more information and a free quote, please visit: http://www.1gsservices.co.uk/

Article Source: http://EzineArticles.com/expert/Oded_Loulay/2134435

7 Tips for Safer Online Banking and Account Security

It's fast, it's incredibly convenient but is online banking safe?

As usual, it depends. That is, it depends on you and how you safeguard your privacy. Considerably more than half of all Americans use their PCs, Macs, and mobile devices to transact business with their banks. But, as we all know, we're not the only ones who want to use our bank accounts. Hackers and scammers will also use them if they can only get their hands on our account details.

And even if you don't bank online, the information you store on your computer or mobile device can still open the door to the fraudsters.

Mostly, we tend to think of credit card fraud as being the main target for financial fraudsters but non-card fraud costs financial institutions and their customers more than $5 billion a year. As the financial website bankrate.com recently put it: "If it's got money in it, someone is trying to steal it." That's a good way of thinking about your bank account, whether you handle it online or not.

Now, the Federal Deposit Insurance Corporation (FDIC) has issued a list of computer security tips for bank customers. The FDIC, which we mostly think of as the organization that insures our deposit accounts against bank failure, says: "While federally insured financial institutions are required to have vigorous information security programs to safeguard financial data, consumers also need to know how to protect and maintain their computer systems so they can steer clear of fraudsters."

In fact, just a handful of basic computer/mobile security practices will go a long way towards keeping your account out of harm's reach.

Here are 7 key actions built around the FDIC's own checklist:

1. Protect your computer with security software including anti-virus and a firewall. These days, security software is built into most computer operating systems like Windows but not smartphones -- and some smartphones and tablets (i.e. Android devices) are more vulnerable than others (i.e. iPhones and iPads). Invest some time in researching which is the best security software -- free or paid for -- for your device(s).

2. Safeguard your mobile device, especially when using it for banking or shopping. Use apps that come from official device stores, cellular providers or the official site of your bank. Keep security and banking software up to date and don't leave your device unattended. "In case your device does get lost or stolen, use a password or other security feature to restrict access," says the FDIC.

"You should enable the time-out or auto-lock feature on your mobile device to secure it when it's not used for a period of time."

3. Get to know and understand your Internet safety features according to the sites you use. Do your bank and other sites where you use sensitive information scramble or encrypt data when it moves between your device and the website? Do you see the padlock icon and "https" that indicate secure access in your browser address bar?

4. Be careful about where and how you connect to the Internet. Public or other computers that aren't yours may not have up-to-date security. And don't use public Wi-Fi for banking and other secure transactions in case someone is "watching" or recording your activity.

5. Be extremely wary about clicking on links or attachments in unsolicited emails, even from people you know (whose own devices may have been compromised). They could download malware that steals your banking information. "Your best bet is to ignore any unsolicited request for immediate action or personal information, no matter how genuine it looks," says Michael Benardo, Manager of the FDIC's Cyber Fraud and Financial Crimes Section. "If you decide to validate the request by contacting the party that it is supposedly from, use a phone number or email address that you have used before or otherwise know to be correct. Don't rely on the one provided in the email."

6. Use strong IDs and passwords and keep them secret. We've written on this subject so many times. For example:

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

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

Yet, despite all the advice from us and many others, people still use easy-to-guess passwords, fail to update them or use the same password on multiple sites -- all highly dangerous behaviors.

7. Play it safe on social networking sites. Crooks scour sites like Facebook and Twitter for innocently-provided information like birth dates, addresses, and pets' names (often misguidedly used as passwords). People you don't know, or imposters posing as someone you do know, may try to "friend" you and eventually persuade you to hand over confidential information or even money.

The FDIC has also produced an online video on how to guard against Internet thieves and electronic scams. See it here:

https://www.fdic.gov/consumers/consumer/guard/

And, of course, there are many other useful sources of information about online banking security.

Don't forget though, that new hack attacks and banking fraud schemes are happening all the time. Make sure you read Scambusters to stay up-to-date.

Reprinted from Scanbusters.org

Scammers Exploit Launch of New Chip Cards

Chip cards -- new-fangled credit and debit cards embedded with a microchip -- have been dropping into mailboxes across the U.S. for several months. The cards are supposed to make transactions more secure and reduce the risk of credit and debit card fraud -- something we obviously applaud. Many people have already received their replacements, but the rollout is expected to continue right through 2016 before everyone has them. That and other delays in distributing the new cards (sometimes called EMV cards after the names of the companies that created them) are being exploited by scammers.

It's easy to spot the chip on your card. It's a little gold or silver rectangle that looks like a very simple circuit board -- with a few, connected little black lines. Over time, they will replace the use of those black magnetic strips on the back of your card. Instead of swiping, chip card users place them into a slot on the payment card reader, which then interprets the encrypted information it finds on the chip. We won't go into why that makes the cards safer but, when the system works properly, trust us, it does.

The problems are that some card issuers have not yet sent them out to their customers, while other issuers haven't fully explained in understandable language why their cards have been changed. Either way, this gives scammers a golden opportunity to phone or email people explaining that their cards need to be updated or replaced, and then ask them to confirm card and account details.

The fact is that card issuers are not, repeat not, contacting users by phone or email to confirm card details, so any information you give out goes into the hands of the scammers and is used for identity theft. Emails may contain copied card logos to make them look real. And there are reports that some email messages contain links that lead to phishing pages or malware downloads.

The same processes are being used by crooks every time there's news of a security breach, in which retailers' computer systems have been hacked. Again, the scammers pretend to be from the credit card company or even the retailer, asking for confirmation of card numbers.

How to Play It Safe

To play it safe with all these tricks, here's what you need to know:

There's never any reason to give out your card information over the phone or online to anyone unless it's for a transaction you initiated.

* When you get your chip card, as with any other new credit or debit card, it will be accompanied by instructions on how to activate it. This is the only confirmation action you need to take -- and usually you will not be asked to re-key your card number.

* In every other respect, using a chip card is no different from the way you used your previous card. You still have to use your card and security number when buying online or over the phone -- what the card issuers call a "card not present" transaction.

* Your fraud protection rights -- where most card issuers only hold you responsible for $50 or less of any fraudulent

transactions -- are not affected by the change.

* Even if you have a chip on your card, the retailer may not be ready to use them and you'll still be expected to swipe your card. The old magnetic stripe is still there.

* Chip cards can still be counterfeited using stolen data and, because the magnetic strip is still there, information can be stolen from these too if they're swiped through a compromised card reader.

The FBI advises: "Consumers should closely safeguard the security of their EMV cards. This includes being vigilant in handling, signing, and activating a card as soon as it arrives in the mail; reviewing credit card statements for irregularities; and promptly reporting lost or stolen credit cards to the issuing bank."

Small Business Alert

Meantime, if you're a small business or store owner, you should know that the FBI has also issued a warning about the use of signature pads rather than PIN numbers, when customers use the new cards.

In most countries, especially in Western Europe, chip cards have been in use for many years and the use of PINs is prevalent; the cards are actually known as "chip and PIN" cards. Card numbers by themselves become worthless to crooks unless they also know the PIN, whereas signatures are easy to forge.

The FBI says: "Merchants are encouraged to require consumers to enter their PIN for each transaction in order to verify their identity. If a consumer uses a signature, merchants should also ask to see a government-issued photo identification card to verify the cardholder's identity."

Read the full FBI chip card warning here: https://www.fbi.gov/sandiego/press-releases/2015/fbi-warns-that-new-credit-cards-may-be-vulnerable-to-exploitation-by-fraudsters

Reprinted from Scambusters.org