



▶ EDITOR'S COMMENTS..... 1

▶ Intellectual Property 2



▶ Creating Plastic Id Cards 4

▶ Protecting your Business against Fraud or Theft 5



▶ Help, my computer has been stolen 6

▶ Best Practices for using Public WIFI 8

▶ Residential Window Security & the Impenetrable Fortress 9

○ ISSUE 2

○ VOLUME 1

○ February 2008

Security Solutions

ADDRESSING THE NEEDS AND SECURING THE FUTURE.

Helping secure your world

As we produced the eight issue of **SECURITY SOLUTIONS**, we were reflecting on the importance of intellectual property. This thinking is undoubtedly influenced by the clamor that is made each year at Carnival about the impact that music pirates have on the incomes of our soca artistes through theft of their intellectual property. Most companies also have intellectual property and it is important to protect it. Our [first article](#) therefore explores this theme.

An important component of security protection is controlling access to the premises. The use of ID badges is generally an integral part of that control, so we provide some advice on the creation of ID badges.

The recent losses suffered by Socete Generale have thrust the risk of fraud on the worldwide stage. Businesses, both big and small should address this risk and the article Protecting Your Business against Fraud or Theft provides some of the measures that you should implement.



Advice on personal security issues is given in three articles that show you how to minimize damage if your computer is stolen, how to protect your information when using public Wifi and how to keep your windows secure.

As always our aim is on alerting you to security issues that can have a harmful impact, as well as providing you with practical implementable solutions for security issues in both your corporate and personal life.

If any additional persons in your organisation would like to receive this email newsletter, just send an email to newsletter@assl.com with the words "Subscribe Newsletter" in the subject line and the email address, name and organization in the body. To opt out of the mailing list send an email with the words "Unsubscribe Newsletter".

Brian Ramsey Editor

Intellectual Property - Trade Secrets, Copyrights and Trademarks

by Marjorie Geiser



Many professionals have a lot of questions about protecting their materials and name. What they are concerned with is what we call 'intellectual property'. Intellectual property can represent 70% of a company's value, so it is important to not only understand it, but to also understand how best to protect it. This article will address what intellectual property is, explain each in a bit of detail, discuss how the Internet has impacted it, and how to protect it.

Intellectual Property - what it is

The definition of intellectual property is basically any knowledge, information or ideas that is important to a business for competitive success. Examples include a business name, a logo,

a graphic, a tag line, advertising materials, product literature, software, an invention. Even such things as customer lists or vendor lists can be considered intellectual property.

Trade Secrets - keep it hidden!

A trade secret is any information, including a formula, pattern, compilation, program, device, method, technique, or process that provides a business with a competitive advantage that others don't have access to. To qualify as a trade secret, the company/owner must take reasonable efforts to keep it secret. Sales and marketing plans can be considered trade secrets, as are computer files sales data. Probably the best example of a trade secret is the formula for Coca-Cola. For health and fitness professionals, a trade secret might be a particular bit of survey information that has helped them discover a need in the market that no one else has discovered, yet. This information must not be generally known to be considered a trade secret. However, once the professional has taken steps to market to that audience, as a result of the survey, it will no longer be a secret.

Another example of a trade secret might be a particular program for clients that are different than what others have ever created. It may be a particular workout, or a particular eating plan; some type of program or method that is unique and not generally known or discoverable by others.

Copyrights - do you really need them?

Of more importance to health

and fitness professionals is the law of copyrights. Many clients ask me about this when they are creating handouts and the answer depends on how much you feel your materials need protection. Copyright law applies to pieces of work such as books, works of art, software, websites, musical recordings, magazines, plays, dramatic performances, and movies. An easy way to informally protect works is to include the "©" symbol, followed by the name of the author/publisher, the year of publication. You can also include the phrase, "All rights reserved".

Copyright protection gives the original author exclusive legal rights to economic benefits from the work. They can reproduce copies, develop derivative works based on the original product, such as workshops, for example, distribute copies, perform it publicly, and display it publicly. Of most importance is that copyrighting the work prevents others from copying, distributing, performing or displaying the work without permission from the author/publisher.

Health and fitness professionals often ask if they can legally copy materials to give to their clients, and the answer is, "it depends". Many educational materials will include the statement that they can be reproduced for educational purposes, and other materials will include a statement that as long as original author and contact information is included, materials can be copied and distributed. If a person is unsure, they should contact the author or publisher.

If you have educational material, should you go through the process of formally copyrighting it? Well, to decide this, you need to first determine if it qualifies. There are three basic requirements for copyright protection: 1) the work must be fixed in a tangible medium (written on paper, on a computer disc, or recorded on tape), 2) the work must be original, and 3) it must contain some bit of creativity. Legally, once a work has been fixed onto a tangible medium, it is copyrighted; a notice on the material is not even required! However, if the author wanted to prove infringement in court in the US, the owner of the copyright must have it registered with the Register of Copyrights, in Washington, DC. The process is simple and very affordable, so the author just needs to determine to what extent they need to protect their work.

Examples where just listing the copyright protection should be enough are educational handouts or any other similar materials for the education of clients. If a professional has created a particular of work that he would like to expand into workshops, or is something he would like to eventually license, it would probably be worthwhile to formally copyright. If you are unsure if your work should be copyrighted, it would be wise to consult with a copyright attorney, but it's not necessary to use an attorney to apply for copyright protection. Books are definitely copyrighted, however, and the most recent court ruling on royalties due authors who publish their works on the internet indicates that authors

who wish to be paid for such works should register, also.

Protecting your name with a trademark

Trademark protection is a huge business! Consider companies such as Nike with their 'trademark' swoosh, or the golden arches of McDonalds. A trademark is any word, phrase, name, symbol, sound or device that identifies and distinguishes one company's products or services from another.

When you consider trademark protection, you can trademark just in your state or federally. It is generally recommended to go for the federal trademark, for wide protection, but then also file for state trademark while you wait through the federal process. Not all trademarks are eligible for federal registration, however, such as descriptive marks. If you are starting a company and have created a unique name that you would like to protect for years to come, it may be a strategy you wish to take. However, the process of obtaining a federal trademark can be complex and it is recommended to use an experienced attorney for the process. Examples of what you might want to trademark could also include a particular logo, tag line or phrase.

The Internet

On the internet, domain names, which are website addresses, are given on a first-come, first-served basis. As a result, some people started to buy up domains of names that were trademarked by large companies and then tried to sell those domains to the companies for large amounts of money. There was no protection

of trademarked names when it came to domain names. Anyone could use the domain name of Ford.com, for instance.

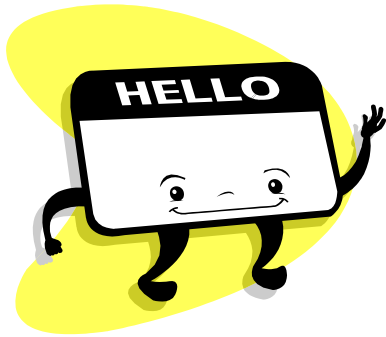
As a result, Congress passed the Anticybersquatting Consumer Protection Act of 1999 to make it illegal for a person to register a domain name, with bad-faith intent to profit from the name, if the domain is identical or very similar to a distinctive trademark or identical or similar to a famous trademark.

In order to properly protect your intellectual property, you should register or take specific steps to protect it. It is ultimately up to you to know the law when concerned about protecting what you created. When deciding on how far to take your protection, be sure to consider to what extent this property is important to supporting your revenue and competitive advantage. Sometimes it may not be important, such as a simple informational handout, but other times it may be extremely important, such as writing a book and planning to create workshops and programs around that book. As you develop your business, it is important to understand the role that your creation will play in the growth of that business.

Marjorie Geiser is a nutritionist, registered dietitian, certified personal trainer, life coach, and MBA student. Marjorie has been the owner of a successful small business, MEG Fitness, since 1996, and now helps other professionals start up or grow their own small business through MEG Enterprises.com. To learn more about the services Margie offers, go to her website at

Creating Plastic ID Cards? First Review These Four Considerations

By Allen Richardson



When creating identification cards for your organization, there are four factors that you should consider before beginning your design. There are many uses of ID cards throughout the world and being in the industry and developed cards for thousands of customers, we have seen and experienced several of the benefits and downfalls of their use. Regardless of your reason for creating a photo ID card these factors should at least be reviewed.



Portrait VS Landscape

The primary method of the card being used is the first thing to consider when it comes to the orientation of your card. You may want your cards to be worn at a specific event or function and if so, then a portrait card would best suit your staff. If you want your members or staff to carry the card in their wallet then commonly it's best to choose a landscape card giving you more room for personal information and lengthy titles.

If you want your staff to wear their identification on their jacket, lapel or worn on a lanyard, then it's best to use a portrait setup. Wearing a landscape card commonly gets in the way because of its width. Also, it doesn't seem to stay as upright and keep your staff looking as sharp. A portrait card hangs better simply because of the effects of gravity. Also when you want your staff to wear a card, you should consider what information you want to be displayed to the world on their credentials.

Individual's Personal Information

When it comes to the information you want your staff to have on their photo id cards, it should be limited to the information you want the readers to have access

to. If your purpose is for the person to wear, then it's best to keep the information limited to the individuals name and title. If the card will be carried in a purse or wallet, then you can put more information on the card since the card will only be displayed when the person chooses to show the ID card. Items such as height, sex, and weight can help better describe the carrier.



If you are working in an industry that has mandated or suggested that your staff have company identification, then you should be sure to check their guidelines. An example of this is for police identification cards. Legislation has dictated what is required for law enforcement officers in several states. Another example is for individuals doing contract work on another's premises. Commonly these organizations have some suggested guidelines that should be followed. Be sure to check any requirements set or suggested by these organizations.

Overall, we suggest that you limit the amount of personal information for corporate identification cards. The exception is for individuals that need personal information in case of an emergency such as fireman, police, or any hazardous industry or profession. In these cases, we even suggest placing any pertinent medical information that would be useful

in the event of a medical emergency.

Back Side of the ID Card

The back side of the card can be used as valuable real estate that many do not use wisely. If the card is formatted in a landscape fashion, many organizations choose to put additional personal information about the carrier. If the card is going to be worn, then it can be used for the company's mission statement or the company's statement of purpose. Even adding the company's mailing address to the back of the card can be beneficial in the event of loss. We have seen the post office deliver cards just because someone dropped the card into a mailbox.

Other things we have seen this real estate used for are things such as important phone numbers, barcodes for job tracking or time clock tracking.



Other Uses

Before you begin to design your card it's best to consider what other uses you might be able to make of your companies new

identification cards. There are time clock applications that can use the cards by adding a simple barcode. There are more sophisticated solutions that have to do with access control, but this commonly adds a much larger investment for the hardware to read the cards and unlock access to secure areas.

In summary, it's most important to start with the primary reason you need identifications cards for your organization. Their benefits come in many ways ranging from corporate reorganization and branding, to having critical medical information available for individuals in hazardous industries.

Being the founder of Virtual Tournament Director and <http://www.FullIdentity.com> Allen Richardson has developed solutions for registration and identification cards for over seven years. Additionally, he has served as a consultant to Burlington Northern Sante Fe Railway, Southwest Airlines and many other organization.

Article Source:
EzineArticles.com

Small Business Security - Protecting Your Business Against Fraud and Theft

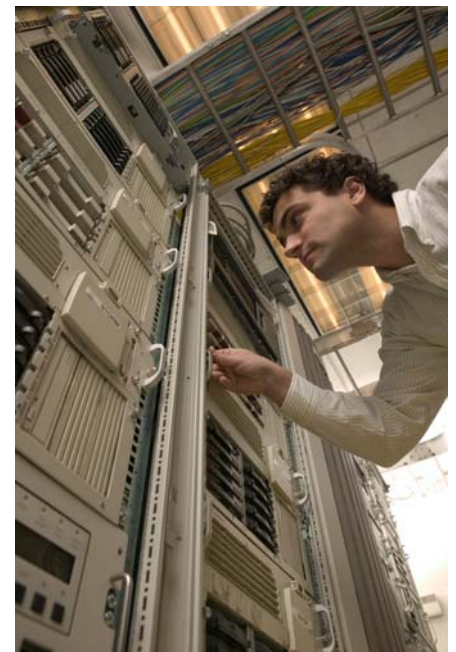
By C. Worrall ★

When I first co-founded a business many years ago, we did not spend much time thinking about security. We were too busy trying to get everything else done. This changed when we raised money from venture capitalists who insisted that our

security be increased to protect their investment.

In general, a few tips for reducing threats:

Check out your employees before you hire them, check references and do a background check. Like most preventative measures, it is less expensive than dealing with the consequences, but it does take time.



Limit access that employees have to data and to your server. If your server room is locked, but the person in charge of the backups keeps the key in his desk in his cubicle - your server is not secure! If your HR person has access to all the digital employee files, but keeps his or her password taped to the side of the computer, that data is not secure.

Require that your employees use strong passwords and changed them regularly. This will cause much grousing, but it's your business and their jobs, so they will have to live with it.

Backup your data regularly.

You should back up your data daily. Every week you should have a week end backup that is taken off site and stored. Annually backup your data and keep it in a safe deposit box or with your attorney.

Have virus protection software and digital intrusion detection software installed and reviewed regularly. If you outsource your IT, the company providing these services should be able to provide this for you.



Lock your doors, even during business hours. This is why Home Depot sells those wireless door bells. They are cheap. I am always amazed when I can walk into a business with no receptionist and wander the halls freely.

Get security cameras. This is both security for your business and for your employees.

Assign one of your senior management as security officer. This person is in charge of understanding possible threats and determining the best prevention. He or she should also receive training in what to do in case of an intrusion, digital or otherwise.

Another area of security is internal fraud, specifically employees stealing from you. As the security officer of one previous company, I was required to take a class on internal fraud. The characteristics of the offender tended to be (1) male, (2) in his 20s, (3) college educated, and (4) had never committed a crime before. Not to say that a 50 year old female, high school drop-out criminal will not commit the crime, but statistically those were the characteristics that came up most often.

Usually what happens is the perpetrator is in a bind, can't make a car payment, rent, doctor's bill, and he starts with just "borrowing" money or items to pawn from the company. He has full intentions of "paying it back." But the reason he got stuck in the first place still exists, so he have to steal more to cover up the first crime, and on and on it goes.

To prevent this type of fraud, have strong accounting policies and procedures. Have revenue checks come to a PO Box. Have a different person sign the checks than the one who creates them. Allow only one person to do the ordering for the company and keep an inventory of what each employee has. For instance, memory sticks disappear really easily. Yes, an occasional one gets lost, but some one who loses them constantly may have a problem.

Ask your accountant for assistance is creating these policies and procedures and have your books audited or reviewed at least annually.

Although it is possible to go overboard on security, I know very few companies that actually do and most don't even come close to basic security. Make sure your company is not one that gets caught saying "but she seemed so trustworthy, I can't believe that she stole from us."

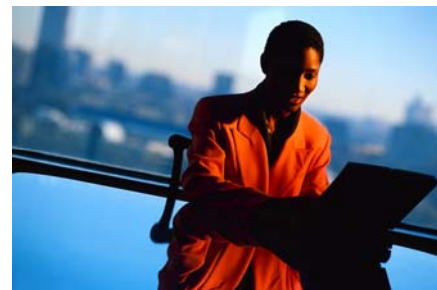
Please visit my website for more small business finance advice: <http://cfoyourself.com>

Article Source: EzineArticles.com

Help! My Computer's Been Stolen!

By Barry Sparling

Computers will always be targets for thieves. This advice will help you prepare for the worst - and protect your valuable data.



Having your computer stolen or losing your data is more than just an annoyance - the information on it may be irreplaceable or of value to the thief. Be prepared for the worst-case scenario to minimize the fallout. If you've lost your laptop on a trip, or your computer has been stolen from your home, notify the police and your insurer immediately.

What About My Personal Information - Is It Safe?

Unless you have taken precautions, everything on your computer is available for a thief to access - that includes address books, personal files, financial information and stored passwords. It is a good idea to have an inventory of the types of information on your computer, so you know what action to take.

Where appropriate, you need to change all your online passwords (for example, email accounts and online shopping). If necessary, tell your employer so they can change your access password. If you kept sensitive financial data such as bank or credit card statements, or tax returns on your machine, you may need to take appropriate steps to guard against identity theft.

As a precaution, you should never keep passwords stored on your computer, or any other information that can be used to steal your identity (e.g. mother's maiden name). Resist the temptation to click 'yes' when Internet Explorer asks you if you want it to remember a password.



If I Bank Online, Will The Thief Be Able To Access My Account?

Probably not. As a rule, banks and financial institutions only ask for parts of a password and often want other information as well, which means a criminal won't be able to automatically access your account. As long as you haven't left your passwords lying around the place - or on the computer - your accounts should be safe. If you think your passwords may be compromised, alert your bank immediately. As a basic security measure, change your passwords on a regular basis, creating them from a combination of letters, numerals and characters - never easily remembered words. And above all, don't use the same password for all your online services.

So How Can I Protect My Personal My Information?

For a start, keep an eye on the information kept on your computer - personal data that doesn't exist can't be stolen. Use

a cable lock when using a laptop in a public place to prevent theft.

Using a password for the computer will discourage the undetermined thief who simply wants to sell the machine or the parts. A savvy criminal can circumvent passwords, or simply remove the hard drive with all your information on it and access it from another computer. Criminals are increasingly aware that your personal information is more valuable to them than the value of the hardware.

The surest way to protect data is to encrypt it, so it is unreadable. In fact, anyone using their computer for online banking or similar services would be advised to encrypt their computer. Encryption is available on high-end Microsoft Vista and recent Mac operating systems, or you can buy additional software that can do the job.

What About All My Photos And Music Files

The only way to protect against data loss is to back up files on a regular basis. External hard drives are large enough to store everything on your computer and are easy to use. Recordable CDs and DVDs can also be used, but are less practical if you have a large amount of data to back up. Experts recommend using two backups, especially if one is kept on the same premises as the computer. Consider an online storage site, at least for your most valuable data.

How Can I Get My Computer Back?

In the UK, police recommend marking goods so they can be returned if recovered, and it will also help if you have records of serial numbers of your equipment. There are companies that can track the whereabouts of stolen computers as soon as they connect to the internet - you install their software and pay a small yearly subscription for the service. They provide you with the information needed to track down the machine's location and thief's identity - however, it is up to you to alert the police, and if the computer has been taken abroad, recovery will be difficult. The software also allows you to take control of the stolen computer when it is online, so you can remotely delete sensitive information.

For more useful information please visit [<http://mycomputersbeenstolen.blogspot.com/>]this webpage, where you will find more helpful advice on what to do if your computer is stolen... and ways to prevent it happening in the first place!

Barry is an ex-IT professional who now writes articles related to computers, gaming and many of his other interests.

Article Source:
EzineArticles.com

Amalgamated Security provides a full range of security services, which include:
Cash Services
Electronic Security
Access Control
Data Storage
Courier Services
Guarding Services
Alarm Monitoring
Response Services

Best Practices For Using Public Wi-Fi

November 16, 2007



AirDefense recently unveiled a list of 'best practices' for consumers to use to protect their identity, credit card numbers and other personal information while using wireless devices at locations offering Wi-Fi this holiday season. These spots include: airports, bookstores, coffee shops, convention centers, hotels, libraries and train stations. According to the Electronic Retail Association (ERA), consumers are expected to spend nearly \$25 billion online at their favorite retailer during the holiday shopping season. Often times, consumers become unsuspecting victims of consumer identity theft and fraud as they let their guard down.

"Today, more and more consumers provide hackers with personal information through free, unsecured and pervasive WIFI offered by a growing number of venues and cities across the country," said Dr. Amit Sinha, chief technology officer, AirDefense. "Though wireless hotspots are convenient and often times free or accessible by paying a nominal fee, consumers should guard their identity, credit card numbers and social security

numbers as closely as they would their wallet or car keys."

Consumers should follow this 'best practices' list to minimize risk during the online holiday shopping season:

Turn off the wireless card when not in use.

If shopping online, ensure that all wireless devices have their internal firewall and antivirus/malware turned on.

If forced to shop at a public hotspot, consumers should use online providers where they have existing accounts. This might prevent an attacker from getting all of a consumer's personal information, such as billing address, name or credit card numbers.

Only log onto known wireless access points and do not bank or shop online with any frequency from a hot spot such as an airport lounge, coffee shop or library.

Beware of slow networks, browser error and/or transactions not working because many of these could show signs that someone is trying to take over the hotspot.

Use your corporate VPN to setup a secure tunnel when connecting at risky and open wireless networks before going on the Internet.

Enable phishing filters on your browser. Make sure you use the latest and patched version of Internet browsers.

Use prepaid wireless cards or accounts and register before you use the hotspot.

Avoid busy hotspots, as these are locations most desirable to setup attacks.

Residential Window Security and the Impenetrable Fortress

By Scott Hares



Securing residential windows against home burglary is every bit as important the doorways. In fact, your homes windows are just as vulnerable as your normal doorways. Consider this question - if you locked yourself out of your house, would you be able to get in through a window?

It's not difficult to secure your home against burglars. A good security system should eliminate any possible burglary methods from all but the most determined and professional burglars - of which, most of us are probably not a target. Most of us are targets of opportunistic burglars and those damnable crank-head, tweaker speed-freaks. Here are some steps you can take to keep them out.

1. Window frame security - make sure your these frames are constructed of top quality materials, lumber, pvc, or metals. Although the British Standards Institute considers performance in its ratings, security is not considered a performance factor.

2. Any window frames that are broken should be repaired - especially wood frames, which if broken, cracked, or exposed, can allow moisture to enter, rotting the wood, and allowing easy access for crank-head burglars.

3. Check for any corrosion of metal frames. This problem should be corrected immediately. Corroded metals, especially aluminum can become brittle and easily removed with one hand. Metal latches should also be inspected for the same conditions.

4. Enhance residential window safety with supplemental locks. Even if you do use electronic systems to secure your homes windows, supplemental locks are relatively inexpensive and offer a real obstacle to the crank headed burglar - the general biggest threat to us all of any income or status level.

5. Laminated glass is a great product for increasing residential safety. It offers great protection because of its high durability, and it reduces the risk of accidental emergencies when the kids get rowdy.



6. Search for products that pass accreditation with PAS - Product Approval Specification. If their logo is present in the hardware you purchase, then you know it uses some of the best features available today.

7. Finally, there's tried and true - advice from others. Solicit friends, family and neighbors who have gone through the process of window replacement. Call local installers to ask these questions, and evaluate their ability to articulate versus their dodgy-ness - ie - bragging about being in business for 110 years.

There you have it, an outline of some do's, don'ts, and some questions to ask the professionals about your home security whether you're replacing windows, or just reviewing your homes safety.

Protect your home and families security with appropriate [<http://vinyl-window.net/window-security/window-security-systems.htm>] residential window security precautions - brought to

you by [<http://vinyl-window.net/>]

Article Source: EzineArticles.com

Amalgamated Security provides a full range of security services, which include:
Cash Services
Electronic Security
Access Control
Data Storage
Courier Services
Guarding Services
Alarm Monitoring
Response Services



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