

- ▶ EDITOR'S COMMENTS.... 1
- ▶ Making IT your Business 2
- ▶ Security Doors in the Workplace..... 4
- ▶ Crash Course in Perimeter Security.... 6
- ▶ 5 Questions to ask before buying a Shredder 9
- ▶ 7 Common Mistakes People make when using the Internet 10
- ▶ Developing a Fire Escape Plan 12

○ ISSUE 3 | ○ VOLUME 1 | ○ April 2008

Security Solutions

ADDRESSING THE NEEDS AND SECURING THE FUTURE.

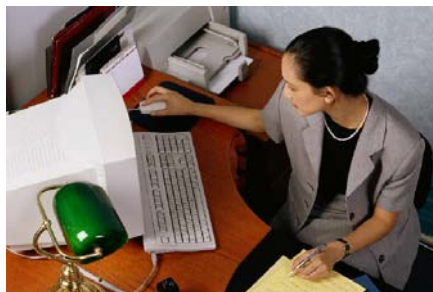
Helping secure your world

Murder, robbery, kidnapping, burglary, crime seems to be everywhere and everyday and indeed it is. In this situation it often seems as though there are no solutions, no measures that can reduce the impact of crime. There are however measures that can prevent you from being a victim of crime and that is the purpose of this magazine, **SECURITY SOLUTIONS**. We seek through this medium to alert you to developing crime trends and to provide you with measures for your protection.

Some individuals believe that only large companies can implement defined security policies and address all the risks that a business will face. They have the view that small businessmen do not have the time or resources to develop and implement security policies. In this issue, we

identify some of the basic components that a business should implement in establishing a security policy in the article, **Making It Your Business**.

One of the primary components of any protection system is the securing of the perimeter of the premises, whether that perimeter is a hedge, fence or door.



For most properties in the Caribbean, the perimeter is secured by a chain link fence or a wall. In an attempt to increase the protection, these are often topped by barbed or razor wire, however while these are deterrents they do not provide any notification if an intrusion takes place. The article, "**Crash Course in Perimeter Security Technology**" introduces electronic systems that provide such notification while the **Security Doors in the Workplace** article addresses the type of external door that you should have.

Advice on personal security issues is given in two articles that point out the **7 Common Mistakes that people make when using the Internet** that often leads to Identity Theft and **How to Develop a Fire Escape Plan**.

Brian Ramsey
Editor

Making IT Your Business

by Monte Robertson



Company security is everyone's responsibility

Sometimes it seems as if everything is about security these days. Homeland security, physical security, digital security—there's constantly a new security issue that needs attention.

The common thread, and threat, in all these areas is people. You can't lock up your staff or seal their mouths, so you need a process to keep your most valuable assets from turning into your worst nightmare. There was a lot of truth behind the old wartime saying "loose lips sink ships." Businesses have many areas of risk that are as vulnerable to careless behaviors and communication as the Atlantic convoys were during World War II.

Homeland security affects travelers and anyone near a critical area. Physical security

affects people who use keys to enter a facility or who must remember to shred a sensitive document. Digital security affects people every time they turn on computers and includes passwords, anti-virus software to protect systems online and backup systems to get users back on track if something happens.

While most people don't have a lot of individual control over homeland security issues, employees are able to control many aspects, both physical and digital, of their business security by creating and implementing a security policy—the glue that holds it all together and gives businesses a fighting chance at survival. The layered security model shows how important such policy is in securing a business.

Beyond Common Sense

Most actions taken are common sense, but it can be surprising how many small businesses skip one or more of the essentials. Whatever else you economize on, smoke detectors, an alarm system and a fireproof safe should not be among them. But what about the paper shredder? And do you keep a record of the number and distribution of master keys? Yes. If you don't know who has keys and where those keys are at all times, the door might as well be wide open.

Physical security starts with good insurance. It's important that the insurance policies you choose to protect your

business are the right ones. Help your insurance agent understand your business and what is most valuable to you. Most insurance policies offer discounts on a sliding scale, depending on what you do to protect the business.

Physical security also is essential for critical servers and other computers. A motivated person with physical access can get into any Windows®-based device without knowing the user name or password—something you need to remember when putting a basic security policy together.

New Challenges

Passwords need to be hard to guess and changed frequently, which all too often means that people write their passwords down. For every manager who keeps his or her passwords in a "little black book" that's stored in the fireproof safe, there are 10 employees whose desks are littered with password-inscribed Post-it® notes.

Passwords go some way toward protecting laptops left in taxicabs, for example, but a better way to go is to make it policy to encrypt laptop hard drives. Encryption software is easy to use, widely available and inexpensive. It will nearly guarantee that a thief can't access the data stored on the machine. It's also about the easiest way there is to ensure that your business is in compliance with government regulations regarding data protection and privacy.

You've probably figured out how to manage virus, spyware and spam problems. But what's going on now on the Web is entirely different. The game has changed dramatically—and so have the risks.

Organized crime has taken to the Web in a big way. The criminals—and their digital weapons—can be completely invisible. One pixel on the screen can hold a poison dart that can exploit a common software application like Internet Explorer and steal information without anyone noticing. Microsoft's much-vaunted "Patch Tuesday," when security fixes are released, is now routinely followed by "Exploit Wednesday."

Your employees also are busy adding new programs to their systems that make them even more susceptible to security breaches. Social networks like Facebook and IM and VoIP applications like Skype are tunneling into and out of your business. If you thought keeping control of spam and stopping users from opening e-mail attachments was tough, welcome to the brave new world of Web 2.0.

Web 2.0 is all about two-way, synchronous communication. All of the abovementioned activities might be convenient for getting business done, and can save a considerable amount of money, but they come at a cost.

Saving money means a trade-off elsewhere. And in the case of these real-time activities, the big downside is lack of security. Sharing data and keeping that data secure is like mixing oil and water. You can either share data or secure data, but not both. And while it would be nice to simply lock everything down and block consumer driven applications, it's simply not realistic to expect users to live with that level of inflexibility—or they'll be spending half their time trying to get around it.

Computer security is an ever-changing landscape. At a minimum, users need antivirus, anti-spyware, anti-exploit, antispyware, anti-exploit, antispyware, firewall, encryption and backup— and everything needs to be kept up to date at all times. Plus, security measures need to be as transparent to your users as possible. If security gets in the way of working, users will work around it.

If you're like most small businesses, you simply don't have the bandwidth, the manpower or the expertise to deal with all of this. So you need a reseller or consultancy with security expertise to help guide you through this security maze.

The Human Factor

People security starts with the hiring process. It's so easy these days to check a person's history online that there's no reason not to do it, and there are plenty of reasons why you should. There are firms that

will do this for you, as well, but be sure that when you search under the term "background checks" the site you click on is not dishing out malicious code.



Make security part of the new-hire orientation process. If you can educate your people to understand the risks they are exposing the business to with some of their behaviors, there is a good chance you can start to tilt the balance in your favor. It only takes one weak link to break the security chain and potentially expose everyone to the risk.

The big roadblock for businesses implementing training and awareness programs is time. Security training is crucial to business. Since time also is crucial, find a way to make ongoing security training relevant and fun. Make it worth the employees' time to understand why security is so important to the business.

Tying it All Together

Security awareness really needs to be embedded in the fabric of your business, which means policies must be in place for all aspects of security. Make security part of everyone's routine by

establishing security policies in writing and making sure they're implemented correctly. Repetition, consequences and follow-through will pay off.

The section of the policy on physical security needs to cover, at a minimum, essentials like who has keys to what, the process for issuing new or replacement keys, changing smoke alarm batteries, alarm-setting and maintenance responsibilities, and the factors that determine which documents should be shredded and when.

The section on digital security should cover password management and electronic acceptable-use policy. Every employee should be provided with a standard computer setup to minimize the number of configurations that need to be managed and maintained—any employee wanting additional applications should be required to make a business justification for that application or install that application himself.

Some applications require users to have administrative rights—rarely a good thing when you think of what users can do with those rights—so be careful when choosing which applications to allow.

In some ways, digital security policy is easier to manage than physical security, because much of it can be enforced from the server. If you still have a peer-to-peer network, move to a managed

domain as soon as possible. Windows Active Directory allows different usage policies to be applied to different users so, for example, financial records are only accessible to the accounting department and senior management, whereas documents like the employee handbook are accessible to everyone.



If you don't have the time or expertise in-house to create and implement server based policies, find an expert to help. But make the time to determine who can have access to what applications and under which circumstances. No one can implement a policy, standard or guideline for your business if they don't know what is critical to the business. Remember, too, that this is all a work in progress and must remain flexible.

About the author

Monte Robertson
Monte Robertson is the

founder and CEO of Software Security Solutions.

**Reprinted from
Security Products**
February 2008

Security Doors in the Workplace - Wood or Steel Security Doors?

By Lee Jackson

For any business considering an investment in high security doors and unsure whether to opt for wood or steel doors the following real life story will help make that decision;

A high-rise apartment building wished to offer residents the highest possible security. Double steel security doors were installed in every unit. One day whilst out and about, an elderly tenant had an accident and was taken to the hospital.

Neighbours became worried when they noticed his untouched newspaper outside his apartment the following day and called the police to break in to see if the elderly gentleman was in trouble. The police and fire departments thought the door was a painted wooden one and attempted to break their way in. Upon realising it was a steel security door, they sent for additional assistance. After almost an hour using two determined workers with special tools the rescue team pried the steel framework apart enough to disengage the locks on this 30 year old steel door. The high security steel doors had done their job!

Statistics reflect that more than 70% of burglars focus on a building's door to gain entry. No matter how high quality the locks may be, if a wooden door can be broken the locks are useless, unlike steel doors.



If the workplace consists of several offices/rooms in a commercial building open to the public a business is at even greater risk and security alarms often do not bring authorities until 10 or 15 minutes have passed. This is plenty of time for a wooden door or doorframe to be broken, the workplace entered, and valuables taken. There is a reason that most safes and safe deposit boxes aren't made of wood!

With steel security doors tests on their strength are an industry requirement. These tests guarantee buyers that steel doors cannot be broken into in such a manner.

Every aspect of steel security doors' design, manufacture and installation guarantee that a buyer is obtaining the optimum in security. This offers a peace of mind that is hard to find with other types of high security doors, and should be a priority to most business owners. Plus, although "fire doors" can be purchased, businesses still receive excellent protection

against the spread of fire with steel security doors. (Providers should have their doors' fire ratings and fire resistance standards available for discussion.) Steel doors also provide increased energy efficiency, since they insulate the cold air from outside up to 4 times better than wooden doors.



Steel doors are made to a building's specifications, with many factors measured for an exact fit. Openings for the locks are expertly engineered with no room for error. The metal framework fits perfectly to eliminate any space in which to slide the slimmest tool or crowbars. Installers take special measures to ensure the heavy doors are hung with perfect balance and all hardware is flush with surrounding surfaces. The entire process, including manufacture and delivery, can take several weeks, and the installation can require 5 hours, but the steel security door can last forever. It can't rot, warp or otherwise change shape, thus

eliminating a potentially dangerous situation!

There are many choices open to a business which is considering steel security doors, and after discussing the many options with a professional supplier, the buyer will know that they are getting a door that meets their unique needs. However, there are some aspects of high security doors that are standard, such as protections from rust and corrosion, various designs and finishes (most which require no maintenance), and the opportunity to choose locking mechanisms and the direction of swing. Some doors offer anti-lever cover plates, anti-crushing surfaces, anti-jimmy strips and reinforced steel edges to further enhance protection. With more than 65% of homeowners choosing entry doors made of steel, it makes sense for a business to consider them as well! Since every kind of steel security door can be accommodated by existing structures, even a business located in an old garage, carriage house, or condominium can take advantage of the protection it offers. Materials used in construction include galvanized or zintec steel. A few points to remember are that, when comparing types of steel, the stronger the steel, the lower the gauge number it carries. (Plus, the stronger it is, the more the steel will resist dents.) This number should be referred to as "true gauge" and not "nominal", since the latter means it's not quite at the rating it's carrying. In addition, hot-dip galvanizing appears to offer more protection against rust than electro-

galvanizing, which may leave some areas uncovered.

A steel door specialist can discuss what may be best for a buyer's needs, and can explain the guarantee of parts, manufacture and anti-perforation abilities. He or she can also explain the pricing options; steel security doors range greatly in price, depending on customer choice. However, it is possible to purchase a high quality, high security door for less than expected. Although it may be a little more expensive than a standard wooden door, the benefits are definitely worth it!

[NPM-Sinoph Steel Security Doors](http://www.npm-sinoph.com)

<http://www.npm-sinoph.com>

Article Source:

http://EzineArticles.com/?expert=Lee_Jackson

Crash Course in Perimeter Security Technology

Technologies are merging to combat security threats, especially those created by vehicles

The establishment of a secure perimeter is possibly the most foundational concept in the security industry. Whether the task is to apply Crime Prevention Through Environmental Design (CPTED) principles to a new campus environment or to protect Class A national assets, the secure perimeter identifies that point at which the security program is initiated.

The technological tools that are applied at the perimeter can vary according to a number of factors, such as the specific

purpose of the perimeter, the characteristics of the site and the nature of the asset.

Three Categories of Perimeter Security

It may be helpful to think about perimeter types in three categories. First, security perimeters define a line of demarcation from a public to a non-public area. Once the perimeter is crossed, new rules are in force as promulgated by the property owner or the authority having jurisdiction. In some instances, this is the only defined perimeter for a facility — college campuses generally fall into this category. As an individual turns off the public street and onto the campus, signage is normally used to inform the individual that they are now on university property, to obey posted speed limits, etc. In CPTED terms, the university is establishing territoriality. Everything else on campus is largely open to the visitor.

A second type of perimeter also establishes a line of demarcation but with an ability to detect those that violate that line. Reliable perimeter intrusion detection has been and is an essential component of security systems for the protection of assets. These perimeters provide for authorized passage through access control portals for both personnel and vehicles; however, an unauthorized penetration initiates an alarm, which signals the malevolent intent of the intruder and simultaneously initiates response activities. Depending on the facility, the response could range from notification of the local law enforcement agency to activation of an armed response team.



A third type of perimeter is defined and designed to physically deny unauthorized access. Almost exclusively focused on vehicle-borne threats, this approach arose out of the vehicle bomb attacks on U.S. Department of State (DOS) and Department of Defense (DoD) facilities beginning in the mid-1980s. The importance of this type of protection has been reemphasized with events such as the Khobar Towers bombing in the mid-1990s and, of course, recent events in Iraq. These perimeters are typically characterized by systems that can absorb the kinetic energy of a fully loaded truck traveling at high speeds; and intrusion detection systems are typically not deployed (or needed) in these circumstances.

It logically follows that different technological solutions are employed to achieve the different goals implied by the second and third perimeter types discussed above.

Types of Sensors

Perimeter intrusion detection is a well-developed and, in some ways, mature technological offering. These types of sensors typically fall into three categories.

The first and possibly the most common type of sensor is fastened to and thus supported by the fence (normally chain link), defining the secure boundary. Current fence sensor offerings have overcome some

of the limitations of previously available sensors, such as:



- **Disturbance Location:** Current fence sensor products such as the Southwest Microwave Intrepid can locate the source of the intrusion-indicating disturbance to within approximately three meters. From an overall system design standpoint, this is a significant improvement over the 100-meter zone differentiation of a few years ago. This capability also affects the functional requirements of the associated CCTV assessment system. Instead of the traditional fixed CCTV camera viewing an entire 100-meter zone, the improved signal discrimination capabilities opens up the option of using pan-tilt-zoom (PTZ) with pre-set views or tracking software for alarm assessment and adversary tracking.

- **Zone Configuration:** Zones are constructed based on software definition and not physical cable construction. This allows cost effective tailoring of the zones to the specific site configuration.

- **Integrated Power Distribution:** Many sensors of this type distribute power to the distributed processing electronics through the sensor cable, eliminating the expense of a separate power distribution system.

- **Reduced Nuisance Alarm Rate:** The digital processing

and segmented calibration of the sensor cable has reduced the nuisance alarm rate associated with these types of sensors.

Free-standing sensors do not rely on a fence for support. These products range from single-technology microwave sensors (bistatic and monostatic) offered by firms such as Southwest Microwave; to the G-Line II and the veteran taut wire system offered by Magal Senstar. In broad terms, these sensor systems have also benefited from digital signal processing resulting in reduced nuisance alarm rates.

Buried sensors allow for high probability of detection in undulating terrain, a bane to most perimeter intrusion detection systems. Similar to the fence-mounted sensors, digital processing has allowed target location discrimination to well below three meters, as well as meter-by-meter sensitivity adjustments through the signal processing software. The performance of current buried sensor products is less dependent on soil type and burial depth than offerings of just a few years ago. These features are characteristic of products offered by both Southwest Microwave (MicroTrack) and Magal Senstar (OmniTrax).

There is no doubt that current intrusion detection products can provide a high probability of detection with a low nuisance alarm rate when properly installed, calibrated and maintained. However, perimeter intrusion detection systems should be augmented by a CCTV assessment system in order to ascertain and verify the source of the alarm and to

initiate and coordinate response activities.



The next level in perimeter IDS will be to replace the intrusion detection sensors with video analytic-equipped cameras, thus combining two necessary and supporting systems into one. This technology is currently in use with mixed results. This is the exclusive topic of an article in next month's issue.

Vehicular Threats

Industry veterans are familiar with the wedge-type, pop-up barriers developed by a variety of manufacturers beginning in the mid-1980s. Delta Scientific continues to provide the broadest selection of barriers evaluated to Department of State (DOS) requirements as defined in "SD-STD-02.01, Vehicle Crash Testing of Perimeter Barriers and Gates, March 2003," however, other manufacturers such as Nasakta, Robotic Security Systems Inc., B&B ARMR, and Boon Edam Tomsed Inc., are also listed on the DOS list of certified barriers. While the basic principles and design of these types of barriers have remained somewhat constant, significant improvements have been made in deployment times and power efficiency. For example, RSSI and Norshield are currently marketing a K12-rated, pop-up-type barrier that

deploys using a set of internal springs. Upon loss of prime power, this particular model can operate for approximately 200 cycles on the internal battery backup module provided with the barrier system. These types of engineering innovations and efficiencies allow for enhanced cost-effectiveness in the deployment of these barriers.

One of the concerns surrounding the development of these types of barriers is the potential for accidental or otherwise inappropriate barrier activation and the danger this poses to normal, non-threatening vehicular traffic. This has spawned a significant amount of effort to define effective strategies to heighten the safety of automated vehicle barrier (AVB) installations. These safety schemes can involve the complete range of signs, warning lights, and vehicle presence detection devices. Specific guidance on the use of AVBs in the DoD environment can be found in the Unified Facility Guide Specification UFGS 34 41 26.00 10 and in Entry Control Facilities/Access Control Points, UFC 4-022-01.

Partially in response to these safety concerns, an energy-absorbing technology is being marketed by Universal Safety Response Inc. (USR) — the GRAB-sp barrier. The barrier's patented energy absorbing pistons reduce the vehicle speed, injury to vehicle occupants, and structural damage to the vehicle with zero penetration. With 70 real-world impacts under its belt with no injuries, the barrier has been tested and certified by the DOS, rated at K8 and K12. The ongoing U.S. Army Access Control Point (ACP) Program represents an interesting

approach to denying unauthorized vehicle access to Army installations. As shown in Figure 1 (above), vehicular approaches to an Army installation are divided into three segments: the approach zone, the identification credential check and verification zone, and the response zone. One or more automated crash rated vehicle barriers (AVB) are located at the end of the response zone. Activities in the ID/credential check area validate the authorization of an individual (and associated vehicle) to enter a given site at the specific location, day and time the credential is presented. In a properly designed access control point, those individuals/vehicles not possessing the proper credentials are directed to leave the site via a designated turnaround (U-turn) area; conversely, those with the proper credentials are granted site access.

One of the threat scenarios considered by the ACP Program is a vehicle proceeding normally to the turnaround area and then immediately accelerating in an attempt to enter the site. Upon detection of this action by the security forces in the ID/credential check area, their responsibility is to initiate AVB deployment. Due to safety features designed into the AVB logic circuit, there is a three to four second delay between the time the button is pushed and the barrier raises. In addition to this barrier deployment time, there is a certain amount of time needed for the security officer to identify the malevolent action (accelerating into the site instead of turning around), determine the proper response (need to push the button to deploy the barrier), and initiate

barrier deployment (push the button); this total response time is the time the adversary has to drive from the turnaround area to the location of the AVB.

During the design phase, the location of the AVB is determined based on certain assumptions regarding incoming speed of the threat vehicle, its maximum rate of acceleration, the response time of the security offices, and the barrier deployment time.

A second scenario assumes the threat vehicle enters the ID/credential check area at a high rate of speed and continues on toward the AVB in an attempt to clear the AVB before it can be deployed. As before, the location of the AVB is determined based on certain assumptions about the maximum speed at which a vehicle can successfully pass through the ID/credential check area, and the maximum rate of acceleration of the vehicle once clear of the ID/credential check area, the response time of the security officers, and the barrier deployment time.

Finally, the bulk of the perimeter of a fixed site often needs to be designed to prevent unauthorized vehicular penetration. Tests have clearly shown that chain link fences present no impediment to a vehicle. To address this category of perimeter security issues, various fence designs have been developed and subjected to DOS testing. The pioneer in this area is Ameristar Fence Company whose Impasse product satisfies the DOS K12 requirements using a tensioned cable and post design. As an added bonus, the Impasse design is considered to be less aesthetically intrusive than other fence designs.

Define Your Purpose

Establishment of a secure perimeter requires a clear conceptual framework defining the purpose of the perimeter as well as the physical and technological tools to achieve the desired functional performance. While much progress has been made in developing active vehicle denial barriers, the current challenge is implementing them safely and cost efficiently at existing sites. Securing the remainder of the perimeter against a variety of threats is also a reality with the DOS-listed fencing products. Finally, the available intrusion detection sensors offer cost effective and reliable detection in realistic exterior environments.

Randall R. Nason, PE, CPP is a corporate vice president and manager of the Security Consulting Group at C.H. Guernsey and Co. His experience spans a broad spectrum of the security profession including threat assessment, vulnerability analysis and master plan development through complete system design, construction management and design-led build projects. He has also designed and conducted full-scale emergency response exercises for a federal agency.

Reprinted from
Security Infowatch
February 2008

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**

Five Questions to Ask Before Buying a Shredder for Your Office

By Jeff McRitchie

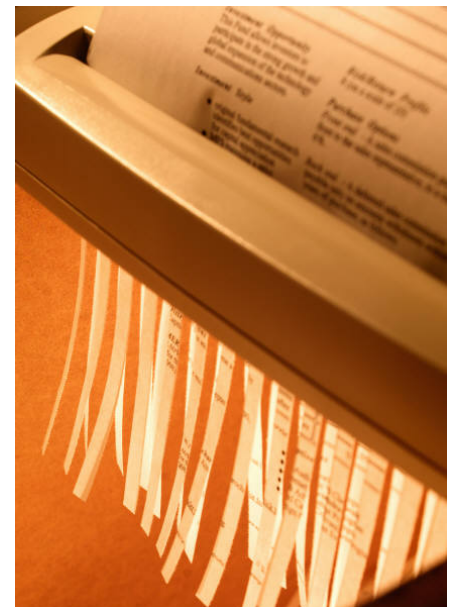
Data security is a huge concern for most organizations these days. Even the thought of client data and sensitive credit information slipping into the wrong hands is enough to make small business owners cringe. However, one of the best things that a company can do in order to secure its data is to buy a shredder for your office. A shredder can help to keep sensitive client information out of the hands of identity thieves and can protect the reputation of your business.

If you are considering the purchase of a paper shredder for your organization there are several things that you should consider. This article is designed to provide you with four questions that you should ask before purchasing a shredding machine. Here they are...

What types of materials do you need to shred? Obviously you are going to want to destroy paper documents. However, many companies need to destroy more than just paper. You will need to ask yourself if your sensitive documents have staples and paper clips? If they do, you are going to want to pick a machine that can handle these. You might also need to deal with computer disks, CD's, DVD's and continuous forms. Again, you should check to see if the device that you are interested in will handle these types of materials.

How many departments in your organization handle sensitive data? If your company has an accounting department, a marketing department and a sales department it is possible you might need to consider buying more than one device. Remember that if it is not convenient for your employees to use the shredder they will probably just throw things in the garbage.

How many people will need to share the same device? If you decide to purchase one larger shredding device for your entire office you will need to figure out just how many people will be using the machine. It is important to know this so that you can determine the correct size and capacity of machine that is most appropriate for your needs. After you have determined the approximate number of users that will be sharing the shredder you can get an estimate of the amount of sensitive information that needs to be shredded each day. Keep in mind that the actual amount is usually double the initial estimate.



What level of security do you need? For organizations that deal with large amounts of sensitive consumer data it is important to consider purchasing a machine that offers a greater level of security. The level of security offered by paper shredders is a reflection of the size of confetti or strips that it produces. Most low security devices will shred documents into long strips. As the security level rises, the machines will cut documents into smaller and smaller pieces. The ultimate in document security is offered by DOD or NSA approved devices which cut documents into such small pieces that they are approved for use in high security government facilities.

As you answer these questions, you should be able to narrow your search for the right shredding machine. As you get close, the final step is to balance your needs with your budget. Just remember, buying too small a device for your needs is way worse than buying too large a device.

Jeff McRitchie is the director of Marketing for <http://www.mybinding.com> He has written more than two hundred articles on topics related to binding machines, binding supplies, presentation covers, ring binders, index tabs, laminators, laminating pouches, roll film, shredders and paper handling equipment. If you have any questions about [Paper Shredders](#) or [GBC Shredmaster Shredders](#) check out MyBinding.com

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

7 Common Mistakes People Unknowingly Make When Using the Internet that Can Lead to Identity Theft



Identity theft was a little known crime even ten years ago. Today, it's one of the fastest growing evils, has topped our list of the worst scams each year, and is the topic subscribers are most interested in us writing about.

Unfortunately, it's very easy to become a victim of identity theft, especially on the Internet. So, we've put together a list of the seven most common mistakes people make that can lead to identity theft.

Mistake #1: Hand over personal details to a phisher.

Phishing -- grabbing your personal details by taking you to a phony website that often looks genuine -- is perhaps the biggest online cause of identity theft.

It usually starts with an email seemingly from an organization or someone you know, inviting you to click on a link that takes you to a site you'd expect to see. Here you'll be asked to

enter sensitive information about yourself, often supposedly to "confirm" your details.

Instead, you're really giving them away to a thief.

A recent study by the IBM Internet Security Systems X-Force found that in 2007, 19 of the top 20 companies that were the supposed senders of phishing emails were in the banking industry.

What to do: Don't click on any link in an email. Instead, visit the real website via your browser, or email or call your friend and confirm the contact. Be especially wary of emails that supposedly come from your bank.

You can find more about phishing scams here.

<http://www.scambusters.org/phishing.html>

Mistake #2: Give yourself away -- post personal information online.

Great. Now you're on Facebook, MySpace, and half a dozen other places where you can meet and interact with others. Unfortunately, so are the criminals intent on identity theft, and they'll scour your listing for anything they can use for crime.

Remember, identity theft isn't always about getting financial details. Fraudsters may be able to piece together enough to pass themselves off as you and commit another crime. They can screen-grab your photo too.

What to do: Use a nickname where possible. When you must use your name, such as on a school reunion site, never provide any other personal

details. And resist the temptation to post your photo.

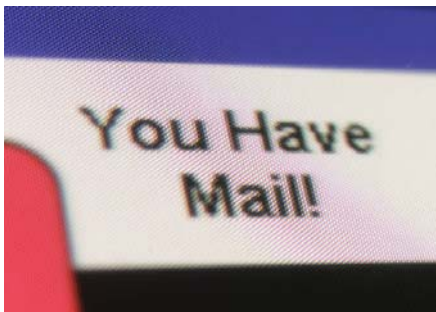
Mistake #3: Click on a pop-up and download spyware.

Ever been surfing when a pop-up message warns that your Internet security is at risk? Very often it's the first step to downloading and installing a program on your PC aimed at identity theft or spying. It may even download a keylogger that records every key you press and sends details to the scammer.

Some 'free' anti-spyware programs on the Internet actually include harmful spyware. Or you can pick up spyware by using shady music downloading sites or clicking on an email link that tells you a friend has sent an e-card greeting.

What to do: Don't click on any unexpected pop-up -- in fact, disable pop-ups in your browser if you can. Never just click on an e-card link if you don't know the sender -- and email any friend who supposedly sent you an e-card first for confirmation.

Mistake #4: Email your confidential information to thieves.



Did you know that, in its basic form, email is often not secure? Scammers bent on

Internet theft can and do intercept emails. They can also find out your email address, and often, they can make a good guess at your online email password. They can even hack into email servers and, if they are successful, read your email.

What to do: Never put personal or financial information in an email. Use the phone. Use a service where all your email is stored on your PC, and make sure addresses and passwords are hard to guess.

Finally, if you are at a site that requires an email address and you don't really want to give them yours, consider using one-time email addresses available at 10minutemail.com or an email address you can always turn off from [SneakEmail.com](http://sneakemail.com).

<http://10minutemail.com>

<http://sneakemail.com>

Mistake #5: Reveal yourself on insecure websites.

By definition, a site that is not secure is accessible by hackers and scammers. Even if it's perfectly legit, if you enter personal details here, you could be an easy target for identity theft.

What to do: If you're asked to key in personal info, check that the details in the address bar of your browser begin with 'https' or 'shttp' (the 's' stands for 'secure'). There may also be a lock icon in the address or status bar. You can read more about this at our friend Leo Notenboom's excellent site, [Ask-Leo.com](http://ask-leo.com).

http://ask-leo.com/is_an_https_connection_really_all_that_safe.html

Mistake #6: Leave information on a public computer.



Whenever you walk away from a computer, you may leave part of your identity behind. If it's a public computer, or any computer someone else can access, they can use it for identity theft.

If you visited a secure site and didn't log out, you're likely still logged in. Even if you logged out, details of your activities are still stored on the PC.

What to do: Ideally, avoid using public computers for confidential purposes. They may even have key loggers installed to capture passwords. Always click the 'log out' button and frequently clean up the trail of your activities by using the options/security menu in your browser.

Mistake #7: Use easy-to-guess or easy-to-grab passwords.

Passwords -- the very things that are supposed to give us Internet security -- are often the weakest link in our Internet armor, leaving us wide open to identity theft. Using any single word, whether it's your pet's name or a random word from the dictionary, makes it easy. Using insecure password savers or storing them somewhere is also a giveaway.

What to do: Use mixtures of letters, numbers and even punctuation for your passwords; change them frequently and don't use programs that fill in your passwords unless they too are protected by a master password.

We've written a lot about creating secure passwords -- here is one article that will get you going.

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

Follow these tips and you'll go a long way towards beating identity theft. Also, please check out some of the previous ScamBusters articles on identity theft.

<http://www.scambusters.org/identitytheft.html>

Enjoy using the Internet and avoid identity theft -- make sure the only people who really know you are your friends!

Tips: Developing A Fire Escape Plan

January 30, 2008



Fire is a leading cause of preventable deaths in the home; but by being prepared to handle this emergency, you can help your family

safely exit your home in the event of a fire. Fire safety and survival begins with everyone in your household being prepared. In the year studied, The State of Home Safety in America report found that only 54 percent of families with children have discussed what to do in case of a home fire. The Home Safety Council recommends the following guidelines for developing a home fire escape plan:

- Have smoke alarms on every level of your home. Make sure a smoke alarm is inside or near every bedroom. For the best detection and notification protection, install both ionization- and photoelectric-type smoke alarms. Some models provide dual coverage. The type will be printed on the box or package.
 - Test each smoke alarm every month. Push the test button until you hear a loud noise.
 - Make a fire escape plan for your family. Sketch out a floor plan of your home, including all rooms, windows, interior and exterior doors, stairways, fire escapes and smoke alarms. Make sure that every family member familiar with the layout.
 - Make sure windows and doorways open easily. Make sure stair and doorways are never blocked. Look for things that could slow down your escape. Move or fix them.
 - If you have security bars on doors and windows, have a "quick-release" latch. This makes it easy to get outside in an emergency. Make sure everyone in your family knows how to use the latch.
- Find two ways out of every room -- the door and maybe the window. You might need an escape ladder to get out of upstairs bedroom windows. If so, they should be part of your fire drill, deployed safely from a ground-floor window for practice.
 - Select two escape routes from each room and mark them clearly on the plan.
 - Children and older people will need help escaping a fire. Plan for this. Know who needs help and pick someone to help them. If anyone in the household has a hearing impairment, purchase special smoke alarms that use strobes and/or vibrations to signal a fire.
 - Have a place to meet in front of your home. Use a portable phone or a neighbor's phone to call 911. Once you get out, stay out. Do not go back inside for any reason.
 - Make copies of the escape plan sketches and post them in each room until everyone becomes familiar with them.
 - Practice makes perfect. Every second counts during a real fire. Hold family fire drills frequently and at various times until the escape plans become second nature. Once you've mastered the escape process, hold a drill when family members are sleeping so you can test each family member's ability to waken and respond to the smoke alarm.
 - Young children might sleep through the sound of the smoke alarm. Be prepared for a family member to wake children for fire drills and in a real emergency.