ISSN 1938-1905

AWARENESS

Journal of Public Safety Studies in America

Volume 1 • Number 2 *Fall 2008*

awareness.hsfamerica.org

2008 President's Award for Excellence

Jeffrey D. Reynolds

is honored this September for his volunteer efforts to improve conditions in America today and for future generations. Mr. Reynolds has been awarded the "2008 President's Award for Excellence" for volunteering more than 500 hours this year, dedicating his time to several key initiatives, including U.S. Privacy Protection and Disaster Preparedness.

"Jeff, on behalf of the Homeland Security Foundation of America and the American Public, thank you for your commitment to the organization and this Nation. You are a great American."

– Eric Brown, President, HSFA

About Jeff...

Mr. Reynolds has over 20 years experience in research & development as a software engineering professional. Currently, he is the President of Strategy Technology, Inc. which has been a consulting firm since 1998. He has consulted in numerous start-up firms after success with KnowledgeWare, Inc. and Protellicess/Platinum Technology, Inc. both which turned into publicly held software companies.

Jeff is a HSFA volunteer technical engineer and project manager. He serves on HSFA's Board of Advisors and contributes as technical editor to "Awareness".

Jeff holds a B.S in Computer Science from Southern Polytechnic State University and is working on his M.S. from U.C Berkeley in Project Management. Jeff has two children - the oldest is currently attending the University of North Carolina where his late mother played basketball.

AWARENESS
Journal of Public Safety Studies in America

Volume 1 • Number 1 *Fall 2008*

CONTENTS

I. INTRODUCTION

II. CURRENT ISSUES

AWARENESS

Journal of Public Safety Studies in America

ISSN 1938-1905

Editor - Managing
Laura Billon - awareness@hsfamerica.org

Contributing Editor(s)
Jeffrey Reynolds - awareness@hsfamerica.org

Article Submissions: Submit articles or book reviews by e-mail to awareness@hsfamerica.org or to the Managing Editor above, or on disk by mail to HSFA at PO Box 2335, Powder Springs, GA 30127. Enclose author's e-mail and postal address and phone number, a short bio line and a personal photo and other photos and captions germane to your submission. Authors are responsible for obtaining permission to reproduce copyrighted material from other sources. By submission to this journal, authors grant HSFA the use of the article in printed, digital and/or electronic form for the educational purposes of the American public.

Clearance: Authors are responsible for compliance with restrictions and regulations regarding the publication and clearance of materials dealing with present or past employment.

Letters to the Editors: Letters are welcome by e-mail to any of the editors or by mail to HSFA at the address above. Note: All letters received are considered for publication, in whole or in part, unless the correspondent has clearly set forth wording indicating that permission to publish is withheld.

Disclaimer: The opinions expressed in this journal are those of the individual authors and do not represent the position of, or endorsement by, the Homeland Security Foundation of America, its directors, officers, volunteers, community partners, or any U.S. Government Agency. Advertising in this journal does not constitute an endorsement or approval by the publisher, editors, or editorial board, as to the quality or value of the product or services advertised or the claims made for it by its manufacturer.

The Homeland Security Foundation of America
PO Box 2335
Powder Springs, GA 30127

Web: www.hsfamerica.org,
E-mail: comments@hsfamerica.org
Tel: 877-859-6850
Fax: 678-890-9522

HSFA is a nonprofit, non-political public entity, incorporated in Georgia in 2002 and reorganized under IRS code 501(c)(3). HSFA conducts and provides support for public safety initiatives, focusing on homeland security, disaster preparedness, privacy protection, child safety, family safety and other national security related issues.


Suzanne Goodney Lea, Ph.D.

The Impact of 9/11 on University Students' World Views...

I chair the Criminal Justice Program at a small, liberal-arts institution in Washington, D.C. Trinity (Washington) University's College of Arts and Sciences serves about 800 female undergraduates. Classes are generally comprised of 20-30 students. Most of our students grew up in either Washington, D.C., or Baltimore, MD. Criminal Justice is a popular major: the number of majors has doubled in the last year alone, and I expect it will nearly double again this year. I spent some time at the start of this new school year talking with my law enforcement class about the impact 9/11/01 has had on their lives, world views, and career choices. Most of the students in the class are sophomores or juniors, meaning that they were in the early part of high school-- and possibly even in middle school-- when the attacks happened.

The events of 9/11 and their aftermath have had a significant impact on my students' world views. Despite this, all of the students asserted that the 9/11 attacks did not affect their choice of career. Most of the students in the class are criminal justice majors and have chosen the major based upon broader interests in criminal cases, personal experiences, and/or the influence of family members or friends who work in the criminal justice field. Still, most students felt that 9/11 had very much impacted their lives. Several either themselves felt reticence about flying or knew close friends or family members that did. Much more common was the feeling that flying has become too much of a hassle. Students felt that the measures taken by airport security are understandable, but worried that they were (a) reactive to past incidents and not anticipatory of possible future attack methods and (b) ineffective-- several students recalled times when they had inadvertently taken a prohibited item through security only to have the TSA workers miss it. None of the students reported having an emergency preparedness kit. Observed one, "My grandmother has one." As younger people, they generally seemed to feel this level of preparedness to be an overreaction. Several wryly noted that their purse has everything they would need in case of an emergency.

Students expressed some concern over several trends since 9/11/01. Most felt that the "report suspicious behavior" signs were generally useless. Some have observed little old ladies on the subway reporting "problem youth" that were simply nuisances. We wondered how often such reports are made and if such white noise might hide valid reports and concerns. There was also concern expressed regarding how one would call to report truly troublesome behavior if there was a real problem. You cannot always call 911 if an event is happening-- for instance, if you are taken hostage. Maybe 911 could be better equipped to receive text messages, wondered others. This might be especially useful for people who cannot communicate clearly by voice such as deaf individuals or people whose ability to speak is otherwise compromised. Finally, there was the observation that people often tend to think that they would have acted differently if they had been on the plane or involved in something like the Virginia Tech shootings. In fact, they likely would not have-- and mostly people would surely have missed what others missed during an era when there had not been a hijacking of an American airliner for more than a decade. At least the heightened awareness may have created a norm in which citizens are more aware.

That said, students also expressed concern over racial profiling, feeling strongly that the approach does not work very well. Most of my students are either African-American or Latina. Many have themselves been victim to racial profiling or have known people close to them who have. While it was observed that 9/11/01 has diminished the attention paid to profiling Blacks and Latinos, there was some feeling that efforts to profile Arab men might be misleading. The Islamic world is much broader than the Arab world, and women, it was noted, can be terrorists as well. Additionally, some students felt that profiling efforts are still seemingly used more against certain minority groups (such as African Americans and Latinos) than might be statistically likely.

Perhaps the most intriguing remark made by my students was that they are actually more concerned with domestic terrorism than with international threats. They were not sure how readily international terrorists could pull off a 9/11-styled attack since it apparently took about a decade to plan. Meanwhile, as vast resources are being poured into stopping another such attack, what is being done to stop another Columbine or another Virginia Tech? A few students noted that such attacks are now increasingly being constructed as terrorist attacks and that this may allow for more resources being put toward preventing such incidents. Still, much of the response to such events is a matter of judgment by authorities. My students still find it remarkable that Virginia Tech administrators did not respond more aggressively to a deadly shooting in one of their dormitories. At the end of the day, this may be the key lesson that my students have gleaned: you can throw piles of resources at an issue, but if there is not sufficient judgment by airport security, university administrators, or citizens reporting suspicious behavior, it will not matter. As an educator, it is my strong belief that relevant, critically-minded education is the building block of that judgment.

Dr. Suzanne Goodney Lea is the Chair of the Criminal Justice Department at Trinity University in Washington, D.C. She has a Ph.D..in sociology with an emphasis on Criminal Justice from Indiana University. She has taught many classes exploring violence in America, domestic terrorism, behavioral profiling and cold cases. She is very active in many professional organizations around the world when she has sat on many Boards and Committees. She is on the Board of Advisors to HSFA.

CONTEXT

Laura Billon, Editor In Chief

Welcome to the first edition of Awareness, "Of the people, by the people, for the people…" Awareness is the official newsletter of the Homeland Security Foundation of America! Our goal of this publication is to provide information that the everyday, average American can use to improve their life. We strive to do this by disseminating information, helpful hints or ideas about things that affect all of us. The Homeland Security Foundation of America (http://www.hsfamerica.org) works hard to protect the well being of our citizens through disaster preparedness, child safety, protecting our civil liberties, identification theft, crime prevention, general safety, etc. In keeping with the organization's mission of non-partisanship, the information that we present will address all these issues and many more to compliment the busy lives that we all lead.

Everything contained in the following pages is about YOU. What you read will provide insight, recommendations, opinions, solutions and guidance from individuals from all walks of life and from sea to shining sea. Help us to make this newsletter even better: our panel of editors would love to review something that you contribute to our publication. At any time you can submit an article through our website that you think may be beneficial to your fellow Americans. This newsletter is all about America and how we can continue to improve this great nation. We look forward to hearing from you!

"Of the people, by the people, for the people."

"Freedom is not the right to do what we want, but what we ought. Let us have faith that right makes might and in that faith let us; to the end, dare to do our duty as we understand it."

- Abraham Lincoln, President of the United States

The Homeland Security Foundation of America, HSFA, is a non-profit, non-political, public entity, incorporated in Georgia in 2002 and reorganized as a tax-exempt organization under Internal Revenue Service code 501(c)(3). HSFA's mission is to advance homeland security while preserving American's civil liberties. HSFA's principal objective is to improve public safety by focusing on counterterrorism, disaster preparedness, privacy protection, family and child protection, energy and other homeland security related issues. HSFA conducts and provides support for nationwide and community safety initiatives designed to help EDUCATE, SERVE and PROTECT the public.

Each day, security experts, emergency managers, engineers, educators, scientists and business and community leaders from all walks of life come together, donating their time, experience and resources to further HSFA's mission. The HSFA team incorporates innovation, forward-thinking, determination and a unique ability to engage the public in an "all hands on deck" approach to improving key areas of public safety in America.

HSFA is a public entity, owned by America and run by the people. Any U.S. citizen over the age of 18 is eligible to run for office. To date, no HSFA staff member, director, or advisor has been paid for their tireless efforts. HSFA is actively fundraising, and, when resources permit, staff members will be reasonably compensated for services rendered; however, Members of our Board of Directors and Board of Advisors are elected and will continue to serve voluntarily without compensation. This selfless commitment is representative of their collective patriotism, excellence and dedication.

The men and women who support HSFA understand public service and demonstrate an unwavering commitment to their duty as Americans. Together they ensure the continued strength and vitality of this organization which has already impacted so many lives in a country revered by millions at home and abroad. HSFA will continue being a force for good in the community, helping secure FREEDOM, SAFETY and PROSPERITY for all.

Programs and Events

U.S. Privacy Protection Initiative, Phase 1 (USP-I) is designed to help combat computer crimes by introducing secure authentication technology into the small to medium-sized business (SMB) market at no cost, eliminating a major source of privacy violations for employees and consumers.

The National Ready Program provides each household in America with a copy of their local Emergency Operations Plan (EOP) brochure and a copy of our disaster preparedness and first aid manual.

Forsyth County, GA Safety Day
October 4, 2008, 9:30 a.m. – 12:00 p.m., Eastern Time
HSFA will be onsite at the Forsyth County, GA Safety Day providing free digital KIDSAFE IDs, copies of "Awareness" and information on how families can best protect against fraud, ID theft, terrorism, disasters and more.

Theft from Auto

by Phil Sumner

Theft from Auto (TFA) is a crime which continues to grow in communities around the country, primarily due to ease-of-access. In our busy society, it's not uncommon for people to leave items of value in their cars while they go work out at the gym, take a class or attend an event. Many thefts occur after hours while most folks are asleep, or in business parking structures during the day when they are at work. There are few worse feelings than walking up to your car in a parking lot only to find you're the victim of a TFA. That's where the nightmare begins.

When we look at routine crime, specifically theft, the important thing to remember is criminals are NOT stupid – nearly all criminals use the Risk vs. Reward formula when scoping out a target. Simply put, they determine the required level of effort and weigh the potential profit with the risk of jail time if they fail. The key to combating theft, especially TFA, lies in this formula. First, let us take a moment to understand the primary factors thieves consider before they strike.

1. Most victims don't believe they are a target of thieves
2. Most victims leave items of value in cars in plain sight
3. Most victims leave their car for more than 30 minutes
4. Most thieves will not break into a car to go window shopping, they will actually steal what they find

When you consider these factors, you can probably imagine how easy it is for an experienced criminal to spot a laptop on the back seat of your car, use a punch tool, Slim-Jim or maybe a brick to break into your vehicle for the "prize". This presents loss that is two-fold. First, a valuable item has been stolen and must be replaced; secondly, and more importantly, a thief, in stealing your wallet or purse, laptop, cell phone, iPod, PDA, or daytimer, may have just gained access to your personal information, such as your name, address, social security number, driver's license and more. There's one thing that is known, when there's money to be taken, criminals work together. Not only does the thief now have a useful device they can fence, they have your personal data that can fetch a much bigger payoff. It is not uncommon for victims of theft from auto to have a high risk of identity theft and fraud.

The good news is that if a criminal sees a caper as too high a risk, they will most likely avoid it. There are a few simple steps you can take to drastically decrease the risk associated with TFA and lower the opportunity for criminals to commit the crime:

1. Upon exiting your vehicle, lock the doors. A locked door, in many cases, will deter thieves.
2. Never leave valuable items in plain sight.
3. If parking in a lot or structure at night, try to park in a well lighted area.
4. For high-end media systems, be sure to opt for stereo units that have a removable face plate.
5. When working out at the gym or visiting your local spa where you may use a locker, do not take the keyless remote / alarm system remote for your vehicle inside with you. Thieves will break into your locker and use these kinds of devices to activate your alarm system to search the lot and find your car quickly. Instead, remove the key from the remote and leave the remote in your glove box or console.
6. When you come home at night, take everything of value inside your home. Do this each and every night. Do not risk leaving an important item of value in your vehicle. Doing so will make it easier for thieves to strike while you're sleeping at night.
7. If you are licensed to carry a firearm, never store your firearm in your vehicle.

You don't have to be a victim…Remember the Risk vs. Reward formula. A thief will not break into your car to go window shopping. They spot what they want, something in plain sight, and then go for it. If you remove all your valuable items from your car, you've taken the first step to a safer community. If thieves don't see anything of value, they will not waste their time and they'll move on to the next opportunity.

Phil Sumner is a former combat engineer, U.S. Army Reserve, and has spearheaded mission critical advanced technology projects, developing space shuttle components and munitions systems, including solid propellant rockets and the TOW, Stinger and Cruise missile weapon systems. Sumner is Vice President of the Homeland Security Foundation of America (HSFA) and serves as Vice Chairman of the Board.

Arming The Stateside Counterinsurgent

Anna T. Cianciolo, Ph.D.

"Must effort to enhance homeland security focus solely on attack response and prevention?"

American military commanders in Iraq and Afghanistan are taught that the key to success (and survival!) is to know their Area of Operations, or "know the AO." Knowing the AO involves gaining a detailed understanding of the social networks of families, tribes, and religious groups that influence whether someone will support U.S. efforts to promote self-governance and rule of law. The expertise of civilian specialists – their knowledge of culture, language, and the challenges of developing countries – is especially valued for its importance in building the personal relationships that foster cooperation. Mutual understanding, respect, and trust serve as indirect metrics for success in neutralizing insurgents who oppose American interests in the Middle East.

In the interest of enhancing homeland security, one wonders: How might these lessons learned overseas apply to Americans stateside who share a concern about the threat of terrorism? Must effort to enhance homeland security focus solely on attack response and prevention? Or, following the wisdom gained abroad, might we not achieve success in neutralizing terrorism by also creating the social conditions, the personal relationships that preclude the growth of hostile sentiment? Military counterinsurgency doctrine suggests our answer.

Like deployed soldiers and civilians, each of us might consider knowing our own "AO"—learning more about the social relationships that give rise to the way we and others behave so that we may build personal relationships, mutual understanding, respect, and, yes, even trust with people of different social groups (e.g., different religions, different socioeconomic status, different race or ethnic identity, and so on). As social psychologists and military scientists agree, personal relationships foster social connections to one another that transcend stereotypes and pave the way to collaboration. In other words, the best way to defeat the enemy is to make a friend.

When you consider what you can do today to enhance homeland security, consider visiting a mosque or Islamic association, try learning a new language and practicing it with native speakers, volunteer to assist the economically disadvantaged. Reflect on how many friends, true friends, you have with people of different nationality, race, religion, or even political party. As Americans overseas can attest, change doesn't happen in a day, or even weeks or months, but social knowledge and personal relationships wield tremendous power to make positive change. Remember, friends are not just people you know, but more importantly, people who will do you no harm.

Dr. Cianciolo earned her Ph.D. in engineering psychology from Georgia Institute of Technology, where she studied how the characteristics of a task influence the abilities people need to achieve and maintain advanced levels of performance. After graduating from GA Tech, Dr. Cianciolo served as a two-year postdoctoral research associate at the Yale University Center for the Study of the Psychology of Abilities, Competency, and Expertise (PACE Center). While at the PACE Center, Dr. Cianciolo continued her study of performance development with a focus on understanding how to assess and develop experience-based, or tacit, knowledge. After completing her postdoc, Dr. Cianciolo served as the Senior Scientist of Instructional Technology at Global Information Systems Technology for two years before founding CPResearch. Dr. Cianciolo also is an adjunct assistant professor for the Institute of Aviation, Human Factors Division at the University of Illinois, Urbana-Champaign.

We the People...

by Jeff Davis

Ways We Can Make Our "Digital Self" More Protected

We the people… What a great start to a great nation. Unfortunately, that encapsulates the malicious people as well. We are all running to catch up in the digital age and sometimes our awareness falls by the wayside. HSFA is trying to bring awareness back and we owe that to ourselves, family, and most importantly our children, as they are the minds of tomorrow. I'd like to describe a few ways we can make our "digital self" more protected. Be advised that this pertains only to personal computers. If you have a company owned computer, consult your system administrator for solutions and do not install any product without reading all of the terms of agreement. Research each product for yourself. Below are some helpful hints:

Microsoft Updates – Occasionally on a computer you will see a balloon pop up in the bottom right hand corner of the screen prompting you to install updates. These updates are usually from Microsoft and are very important. Most of the desktop world belongs to Microsoft and there are people with too much time on their hands that are trying to find "holes" in Microsoft software. When a hole is found, these people try to write their own software that will exploit this hole and wreak havoc on your computer or your company's network. We know them better as viruses. Viruses are simply software that is written for malicious purposes that usually ends up in a destructive ending. To protect us from these exploits, Microsoft responds very quickly with patches, service packs, or hot-fixes to remedy these vulnerabilities in the form of updates. The next time you see the balloon (you can wait until you get ready to leave for lunch or go home), click on it and install the updates. You can also get the latest updates by visiting http://windowsupdate.microsoft.com.

Spyware – Spyware is very similar to viruses and can cause just as much damage to our computers. Everyone should be or already is running some type of anti-spyware program. What a lot of people do not know is that they have to keep it up to date just like an anti-virus. These updates alert the anti-spyware program to the different kinds of spyware so it will know the patterns to look for, identify, and cleanse. I personally have used, with great success, Spybot Search and Destroy (http://www.spybot.com), which is a free program, to protect myself and my clients from spyware attacks. Remember to keep it up to date and run a full weekly scan.

Anti-Virus – To touch briefly on viruses, as we have all probably been subject to a virus attack and the pain of cleaning it, viruses are no more than a software program written to independently or run in conjunction with another application to wreak havoc on a pc. Viruses have been around for a long time and will probably remain a constant for a long time to come. AVG (http://free.avg.com) is a free anti-virus software that you can run on your pc and help protect you from viruses. Remember to keep it up to date and run a full weekly scan. These are just a few weapons to keep in your arsenal to protect you, your family, and your pc. Know that the malicious people out there have their own weapons and they are seeking you out. HSFA is now, and will continue to seek out new forms of awareness to keep the American people in the know and up to date.

Jeff Davis has worked in the IT field since 1992 actively working in project management, technical consulting, system administration, network engineering and project implementation. Mr. Davis is Certified as a Microsoft System Engineer and Cisco Certified Network Associate. He serves on the HSFA Board of Advisors.

Safe Escape

by Laura Billon

"Make sure that your family is protected by knowing what to do should there be a fire in your home"

A man's castle is his kingdom, his shrine, his home. But what do you when your castle is burning? We have all seen the recent devastation as wildfires wreaked havoc across our country, images of structures, homes, landmarks and businesses going up in flames. No amount of preparation can help you deal with the fact that your home was there one day and gone the next. Certainly in terms of a fire, this is one of the most difficult and trying things you will have to experience. Wildfires leave little standing in their path save a bunch of memories and debris.

On a smaller scale, and unlike a brushfire when you can see the fire as it heads towards your location, fire company personnel are knocking on your door telling you to leave, public service announcements identify evacuation locations and shelters, what do you do in your own home?

Recent findings published from the US Fire Administration show that over seventy-two percent of fire injuries to civilians occur in residential structures, with thirty-nine percent of those occurring from residents attempting to control or extinguish the fires themselves. While it is understandable to want to extinguish the fire yourself and keep it confined to a small portion of your home, more often than not, failure to immediately evacuate and therefore delay the response of emergency responders, results in increased damage, injuries or death due to inhalation of toxic fumes and gases.

It is crucial to know how to escape from your residence. Do not attempt to suppress the fire yourself – unless it is small and absolutely controllable. Leave the fire fighting to those who are professionally trained. Instead, make your way out of the building as determined by a preset, preplanned, and often practiced evacuation route.

A home filled with smoke is a dangerous and often deadly place. It is often too late before you recognize the affects of the gases you are taking into your lungs. Vision becomes hindered and the inhalation of the toxic gases will lead to dizziness followed by disorientation. It was not uncommon for our suppression crews to find bodies near exit doors, people who were unable to make their escape before they were asphyxiated and succumbed to the fire.

Ensure that your smoke alarms are functioning properly and while planning your escape route, make sure you have two ways out. If there is only one door in or out of your home, plan and practice a way out by means of a window, recognizing that an escape ladder may be necessary. Blocked exits or individuals being trapped below or above a fire contribute to injuries sustained in fires. Have procedures in place for those requiring assistance such as small children or elderly citizens. Getting out as quickly and safely as possible is the priority. If a pet will come with you freely and not hamper your evacuation, take them with you. If you cannot do so, tell the suppression teams that you have pets in the building.

DO NOT GO BACK INSIDE THE BUILDING! Once you are out, stay out, As difficult as it may be to imagine and comprehend, THINGS can be replaced, you and your family cannot be replaced. Have a designated meeting place that is established and identifiable by all family members – the old Oak tree around the block, the mailbox one block over. Practice your plan regularly; ensure that each person knows the way out. Always remember to call 911 from a location other than your own home.

With fire season upon us and the winter months following quickly behind, make sure that your family is protected by knowing what to do should there be a fire in your home.

Laura Billon has a Masters Degree in Forensic Science and is a Certified Fire Investigator. She has been in the Fire Service for over eighteen years in California and works as an evaluator for the Center For Arson Research. She is certified as a Hazardous Materials Technician and as a Hazardous Materials Investigator. She teaches in the Arson Department of the National Fire Academy in Emmitsburg, Maryland and is an adjunct professor of Fire Science at Miramar College in San Diego.

Identity Theft

by Jeffrey D. Reynolds

It can happen to you quickly but take years to discover!

Review the following two ID Theft scenarios, the first being fairly simplistic, the second more of a high tech sophistication. Note the varying degree of results.

Scenario 1: A large retailer had a clever employee that made a copy of a credit application. They then filled out the credit application again with a different address. This resulted in two credit cards under the same name and Social Security Number. The resulting extra card was unknown to the original applicant for two reasons: they never received a bill in the mail AND the abusing party used the card for months and made the payments on-time. Then one day original applicant was denied credit from a different institution. This was a surprise as they knew they had good credit. A free credit report inquiry was made. To their horror they found they had two retailer credit cards with different credit limits going to two different addresses. After almost a year of usage, the abuser simply stopped using the card and left a fairly large balance.

In less than one week the credit institution completed their investigation and the issue was resolved, which included a letter with an enclosed new credit report showing the removal.

Scenario 2: A large bank was offering favorable savings account rates. A large sum of money was deposited into the savings account. The account owner filed away the monthly statements in the home filing cabinet, never looking at the enclosed statement. The associated ATM card was still in the original envelope and had never left the house or been activated. After two years, the account owner needed some money and attempted to make a withdrawal from said account. Much to their surprise "It was gone!" How could this have happened?

The bank conducted a thorough investigation and identified a VERY high tech ID theft ring had somehow obtained information from the bank.

According to bank records, the ATM card was used to take out monies in January of 2005. The account owner denied this ever occurred and it went back and forth. Here is the interesting high tech part:

The depositor was on a business trip on that day in a small city (City X) outside Los Angeles. After checking into a major hotel with a different bank card, their ID was stolen within 30 minutes by usage of another ATM card used in a Casino bank in New England. Interestingly, the name of the city in New England has the same exact name as (City X).

Currently, the investigation has found a card was manufactured with a PIN number and used 30 minutes later. The investigators now group like ID thefts to find a pattern of this high tech theft.

How can you protect yourself from these types of crimes?

- Use the free credit reports online or by writing to various credit reporting institutions. This report lists ALL accounts and if something looks odd, call the credit card company immediately. You might find resistance as in this case, the two different addresses caused the agency to not want to close the account.
- Open your statements and read the balances each month even when you think you know how much is in an account.
- Be diligent and have a home shredding machine, they are inexpensive and easy to find.

These are two real world cases, not hypothetical situations. The first had a happy ending in a short timeframe. The second does not have a happy ending and is still pending investigation after two years of the infraction and 1 year of discovery. The depositor does not yet have the money, as it is being held in escrow pending the investigation.

Protect yourself so that this does not happen to you!

Jeffrey D, Reynolds is on the Board of Advisors of the Homeland Security Foundation of America. He serves as a technical editor to Awareness and has over twenty years experience in the IT field.

Are You Prepared?

by Bill and Janet Liebsch

September is **National Preparedness Month** … are you ready?

Today marks the 7th anniversary of 9/11, reminding us that terrorist attacks are still a possible threat to our nation and our way of life. The thought of a chemical, biological or nuclear attack on our soil can be overwhelming, but we need to acknowledge the threats exist and prepare ourselves for the unexpected.

Keep in mind, a terrorist attack is a very low risk possibility. More common disasters that affect families and businesses year round are things like earthquakes, chemical spills forcing evacuations, fires, floods, power outages and injuries.

The Department of Homeland Security has designated September as National Preparedness Month to increase awareness as well as encourage individuals, families, businesses and communities to take action, make a plan and prepare for emergencies.

Planning is a fact of every day life. We plan and make lists for our chores, the kids' activities, shopping trips and vacations. But when it comes to planning for a disaster, many of us don't do it. A recent study by The Ad Council found "91% of Americans say it is important to be prepared for emergencies but only 55% have actually taken steps to prepare".

Unfortunately, disaster preparedness is often thought of moments before or immediately following some sort of crisis or emergency. For example, how many times have you seen images of people stocking up on water, canned goods and batteries just before the hurricane comes ashore? It'd be easier (and cheaper) to purchase things in advance and have them in a kit with other supplies. Planning for something that may never happen is difficult … but what if something does happen? Are you and your loved ones prepared?

BE AWARE... BE PREPARED... and HAVE A PLAN!

For 9 years our company has quietly been helping the country prepare with our book called "IT'S A DISASTER! …and what are YOU gonna do about it?" The 284-page reference manual helps families and businesses prepare for and respond to most types of emergencies, first aid needs, and natural or man-made disasters (including Terrorism).

We've worked with many government agencies, businesses and nonprofits to get hundreds of thousands of copies into the public's hands. This information needs to be in every home and business in America. We believe if more people would take responsibility and learn what to do in advance, it could alleviate a lot of problems, anxiety and loss.

Some important things you can do for National Preparedness Month include:

- Get a Disaster Supplies Kit for your home, office and car;
- Make a Family Emergency Plan;
- Learn about different types of disasters and emergencies;
- Get Involved in community efforts;
- And visit https://www.hsfamerica.org/RedBook to get copies of IT'S A DISASTER! for your family, friends, employees and customers … and help support HSFA in the process!

Bill & Janet Liebsch are co-founders of Fedhealth and co-authors of IT'S A DISASTER! …and what are YOU gonna do about it?

Dear valued customer we added ID Theft insurance to your account for only $30 extra each month... no worries!!!!

- Your friendly National Bank

The War on Computer Crimes

by Eric V. Brown

In the post-9/11 era, we face significant challenges in intelligence, counterintelligence and homeland security. With Islamic terrorism on the rise and a continued conflict abroad, we have significant areas of opportunity for information assurance at home, leaving the door wide open for routine crimes like ID theft to top the charts when it comes to national threats. ID theft, fraud and other computer crimes cost Americans billions of dollars each year, and the question we should be asking is who's getting all that green?

There's a direct link between routine crime and terrorism. Recent trends indicate terrorist groups launch unconventional, nonviolent attacks against Americans, profiting from criminal activities, including but not limited to theft, kidnapping, extortion, and cyber-financing in order to execute deadly attacks in the future. The impact of these crimes on our national security is great especially when numerous successful attacks are executed over a long period of time. This strategy has a three-part effect resulting in an immediate reduction in financial stability, increased burden on law enforcement, and diminished response and investigation capabilities for the real attack forthcoming.

ID theft in particular is a highly lucrative form of cyber-financing that can be originated anonymously outside our borders, and, despite recent indictments by the U.S. Justice department, can be nearly impossible to investigate. Most victims won't even know they've been violated for years, and by then, the damage is already done. This makes ID theft the perfect fundraising tool for terrorists.

This doesn't necessarily mean terrorists have connected all the dots, but consider for a moment the potential operational capabilities of a terrorist group such as Al Qaeda or Hezbollah if they no longer need to rely on funding centers or individuals to make donations that can be investigated. Keep in mind terrorist groups are not like routine criminals, i.e., drug dealers and kidnappers. Criminal gangs operate to make profit, but terrorist groups don't care about profit – their interest is not in taking money, but in taking lives, which means they can't be stopped or even slowed down by conventional deterrent methods that typically involve law enforcement putting the squeeze on financial resources. Simply put, when faced with such a challenge, they'll just find another way to fund their operations.

Who's to blame for these activities? Just imagine the impact of a new-age, radically Islamic terrorist group with some working knowledge of U.S. intelligence culture effectively utilizing deception in its portrayal of itself while mastering the world's fastest growing anonymous crime. Imagine them committing ID theft against Americans, with little or no resistance, building a wealth of resources that they in turn use to launch coordinated, deadly attacks against the U.S. and her allies. In this scenario, it would be difficult to argue that America did not play a role in feeding the terrorists when little has been done to combat ID theft.

The "sweep-it-under-the-rug" approach big corporations take to dealing with ID theft and fraud leave the majority of Americans open to attack. There's little legislation and few lawmakers who can stay ahead of the curve when it comes to new scams and emerging technology. Furthermore, with the nature of the crime, there's little the average citizen

can do to prevent it. Many organizations have begun to offer special ID theft protection, credit monitoring and alerts and other pay-for-protection products, but these defenses offer a false sense of protection as most activate only after a crime has occurred and a report filed by the victim.

ID theft is a costly crime that's different from other types in which the victim may be able to give investigators a description of the perpetrators or recall recent suspicious activity in the neighborhood. In most cases where personal records have been compromised through security violations, the theft takes place outside the home in facilities controlled by private corporations and government agencies. Since 2005, there have been more than 230 million records compromised in incidents ranging from lost or stolen government laptops to complicated high-tech intrusions on unsecured corporate networks. The FBI has moved ID theft up to the number three spot on their priority list, but resources, specifically budget allocations and total number of agents assigned to the task, simply do not match up with the priority level.

Eric V. Brown

ID thieves target average, every day American citizens, many of whom are unaware how the theft occurs. So, how does it happen, and how do we stop it? I think the secrets to life's mysteries are revealed to us when we simplify the complicated, but in so doing, we must be careful not to complicate the simple. In the spirit of simplification, I believe the real threat, when it comes to attacks that originate offsite or offshore, exists at the point of Phishing. With the exception of low-tech violations, i.e., dumpster diving and surveillance, Phishing is the gateway for ID theft, fraud and other computer crimes. I believe the key to reducing potential loss associated with these crimes is eliminating Phishing.

By making Phishing a tool of yesterday, we will help prevent terrorists of tomorrow from expanding operational capabilities off "easy money" and advancing their planned acts of terror to the next level, which, without exaggeration, could involve detonating a low-yield nuclear device (suitcase bomb) on sovereign U.S. soil.

If we can potentially save millions of lives in the future simply by exploring the link between routine crime and terrorism, then it's incumbent upon us to take a serious look at ID theft and other security violations that offer high gains with low risk to terrorist groups.

There are many who might argue a nuclear attack inside U.S. borders is too grandiose a scenario to actually happen, and perhaps they're right – maybe it will never occur, but there are few experts who deny the potential for it to happen. In being right, we can't afford to travel down the same road of neglect that led to the devastating loss of life on the morning of 9/11. As we approach the 7-year anniversary of 9/11 and move forward to face new challenges, U.S. intelligence and law enforcement agents must consider all possibilities and develop reasonable strategies for defending against the unknown.

As an American and a potential target, what can you do to prevent terrorists from attacking? Not a whole lot, but the things you can do to ensure the future safety, security and prosperity of this great nation are many. First and most importantly, learn about your privacy rights – understand your rights and exercise them. Take notice of how businesses and websites use your private information and whether they'll sell it to the highest bidder. Keep a close watch on your social security number, driver's license and other forms of identification like military ID cards and Medicaid cards which still show your full social security number on the face of the card. Download training materials from the FTC and other trusted sources – share this information with your family and have an open dialogue about the importance of safeguarding private information. Never give your information to a stranger or over the phone in response to a direct mail piece that may promise free resources or give notification of sweepstakes winnings. Remember, if something appears too good to be true, it probably is.

Eric V. Brown is President of the Homeland Security Foundation of America (HSFA) and serves as Chairman of the Board. Brown is an experienced field operator and has conducted successful undercover campaigns for public and private operations. He is currently Department of Homeland Security / FEMA certified in homeland security, emergency management, and disaster preparedness and mitigation. His affiliations include the National Association of Investigative Specialists and the Association For Intelligence Officers.