

Personal Security in the 21st Century

A family guide to staying secure



Overview

This booklet is designed to provide your family with security-minded “best practices” to keep them safe from scam artists, cyber hackers, social engineering scams, or criminals that prey upon unsuspecting victims. Everything contained within this booklet is unclassified / open source and may be shared freely with your friends and neighbors. Although this material is current as of the time of its creation, criminals are constantly changing their tactics to prey upon their victims (and make money) – however, the adoption of a security-minded mentality will reduce the likelihood of your becoming a victim.

Disclaimer

Viewpoints, company names, and product names contained within this awareness product do not constitute an endorsement of or a recommendation by the Defense Threat Reduction Agency (DTRA) or the Department of Defense (DOD). Information presented within this document is provided “as-is”, with no guarantee of not being superseded by more current safety / security recommendations after its publishing date.

Contents

Overview	1
Disclaimer.....	1
Active Shooter.....	3
Automated Teller Machine (ATM) Fraud	4
Automobile Safety	6
Cell Phone Security	7
Crime.....	8
Cyber Threats	11
Facebook Smart Card	13
Google+ Smart Card	15
LinkedIn.Com Smart Card	17
Twitter Smart Card.....	19
Drugs	21
Fire Extinguishers	24
Firearm Safety	25
Gangs.....	27
Hotel Security.....	29
Identity Theft	30
School Vulnerabilities.....	31
Terrorism in the U.S.	32
Source Index.....	34

Active Shooter

Columbine High School, CO; Virginia Tech, VA; Ft. Hood, TX; Tucson, AZ; Albuquerque, NM – what common thread do these places share? They all experienced Active Shooter incidents. You might be asking yourself “What is an active shooter and why was it important to me?” Per Wikipedia.com, “Active Shooter” is defined as: “... an armed person who has used deadly physical force on other persons and continues to do so while having unrestricted access to additional victims”. A **VERY** serious situation indeed and something that could impact your family regardless of where they are at or what they are doing. Long story short, you never know if an individual might walk into the building that you (or your family) are currently inside of and decide to kill people. Sometimes, the shooter is a former employee who feels they were treated improperly; other times, the building is chosen at random – the majority of the time, the killing is indiscriminate and victims are shot simply because they are visible to the shooter.

Active Shooter events are not a recent phenomenon; our ever-increasing methods of receiving news (e.g. Twitter) makes them better known. Some examples of Active Shooter incidents would include: on 18 Jul 1984, James Oliver Huberty killed 21 people inside of a McDonald’s restaurant before being fatally wounded by SWAT. On 16 Oct 1991, George Hennard drove his truck through a Luby’s Cafeteria and shot and killed 22 people, wounded 20 additional, and then committed suicide. More recently, on 18 Oct 2012, a gunman walked into a Wisconsin beauty salon and shot and killed three women (including his estranged wife – she worked at the salon), injured four another woman, fled the crime scene and committed suicide at a nearby house. His estranged wife had filed a restraining order against him a few days prior to this tragic incident.

Albuquerque has not been immune to Active Shooter events. On 12 Jul 2010, Robert Reza, a former Emcore Corporation employee, returned to his former workplace, shot and killed two people, wounded four others before committing suicide. More recently, four students at the Middle School located in Belen, NM, planned to enter their school on 12 Dec 2012, “shoot up” the school, and then kill themselves. Thankfully, fellow students overheard the student’s discussing their plans, notified school leadership of their intentions, and authorities were able to intervene.


Some potential signs that a former / current co-worker might commit an Active Shooter incident include:




- Increased use of alcohol and / or drugs
- Unexplained increase in absenteeism and / or vague physical complaints
- Depression / withdrawal
- Increased severe mood swings and noticeably unstable or emotional responses
- Increasing mentions of problems at home, school or work
- Increase in unsolicited comments about violence, firearms and other dangerous weapons and violent crime

The city of Houston Mayor’s Office of Public Safety and Homeland Security developed an excellent five-minute video that addresses Active Shooter concerns – the video is viewable on their web site in either English or Spanish. The web site address is: <http://www.readyhouston.tx.gov> or you can search Youtube for the video titled “RUN. HIDE. FIGHT.” Key points of the video are:

- Run if a safe path is available. Always try and escape or evacuate even if others insist on staying.
- Encourage others to leave with you but don’t let the indecision of others slow down your own effort to escape.
- Once you are out of the line of fire, try to prevent others from walking into the danger zone and call 9-1-1.
- If you can’t get out safely, find a place to hide.
- When hiding, turn out lights, remember to lock doors and silence your ringer and vibration mode on your cell phone
- As a last resort, working together or alone, act with aggression, use improvised weapons and fight.

Automated Teller Machine (ATM) Fraud

 <p>A false card slot is affixed over the original card slot. The false slot holds an additional card reader used to copy card information.</p>	<p>Criminal places a molded plastic “faceplate” over the top of the ATM – when the victim inserts their card the bogus faceplate reads the back of the card before it reaches the legitimate card reader.</p> <p>A small camera is nearby (usually placed inside of a document holder that has an unobstructed view of the keypad) to obtain the victim’s PIN number.</p> <p>The criminal can now make a duplicate of the compromised card!</p>
	<p>A slip of electrical tape or x-ray film can be shoved into the card slot and prevent the card from coming out – when the victim goes inside to complain the criminal retrieves the card.</p> <p>Normally the criminal is standing nearby to watch the victim type in their PIN</p>
 <div style="display: flex; justify-content: space-around;"> <div data-bbox="167 1396 406 1430"> <p>A normal ATM device.</p> </div> <div data-bbox="505 1396 883 1560"> <p>ATM with skimming device attached in front of card slot. Notice how the card slot is no longer inset into the machine, but “bulges” outward.</p> </div> </div>	<p>A variation of the faceplate scam [note: if possible, use ATM machines with the same banking institution so you will become knowledgeable to how their faceplates normally look like – and easily spot if a false faceplate has been added]</p>

	<p>Another variation of the faceplate scam; this one uses a fake numeric keypad (placed on top of the legitimate numeric keypad) to record the PIN when the victim enters their PIN</p>
	<p>A criminal can apply fast-drying glue to three keys on the ATM's keypad. The victim can't cancel the transaction (because the keys are glued) – when the victim goes inside to complain, the criminal will apply a solvent to dissolve the glue, complete the transaction, and steal the cash</p>
	<p>Kleenex can be jammed into the money slot, thus preventing the victim from obtaining their cash. When they go inside to complain, the criminal uses a hook to retrieve the money</p>

SECURITY BEST PRACTICES

- Be suspicious of anyone standing beside / behind you – they could be watching you enter PIN number or be waiting to snatch your cash / cash out of your hand
- If an individual walks up behind you and gets uncomfortably close, it might be best to cancel the transaction and locate a different ATM
- Carefully inspect the front of the ATM (especially the keypad and card insert slot); gently “tug” on them to determine if a skimming device has been attached to the legitimate machine
- If the ATM “eats” your card do NOT immediately run inside to complain – a criminal could be waiting for you to leave and retrieve your cash / card. Instead, ask someone nearby to notify a bank employee to come outside to address the problem
- ATMs located outdoors are usually much easier to attach a skimming device to; if possible, go inside of a bank to conduct your banking needs
- Avoid ATM machines that are located in unusual places for convenience (e.g. a swap meet; a trade show) – those machines are usually independently owned and normally don't encrypt your information before using a dialup modem to process the transaction
- Avoid ATMs that are located in isolated / deserted locations – a criminal can easily walk up behind you, produce a weapon, and demand your money / card

Automobile Safety

Driving is one of the most dangerous activities that U.S. citizens regularly participate in. Here are some considerations to make before sitting down behind the steering wheel:

	DUI / DWI: If you observe a vehicle that is being driven erratically, and you have a cell phone with you, dial #DWI or #394. Do NOT engage with the vehicle's driver, as they could become enraged at you or accidentally / purposely swerve into your vehicle. [Note: that police must observe the erratic driving to stop the vehicle and determine if a sobriety test is warranted – they cannot stop the car based upon your testimony alone!]
	Emergency Kit: Ensure your vehicle has an "emergency bag" that is filled with items you will need should your car become disabled / stranded. Items could include: flares; reflective triangle; water; blanket; energy bars; jumper cables; cell phone recharging cable; miscellaneous tools / clamps / hoses; antifreeze; motor oil; small shovel; sand; ice scraper.
	Garage Door Opener: If you park your car in your driveway and have a garage door opener inside of the vehicle (e.g. clipped to the sun visor) a criminal can use it to get inside of your garage (and then possibly inside of your home). If your vehicle has the capability of programming it's electronics to open your garage door for you that creates an exploitable vulnerability. Your name and address are printed on your vehicle's registration – if your car is stolen and your garage door opener is inside of that car, they now possess two key pieces of information to enter your home.
	Hitchhikers: Even an innocent-appearing hitchhiker could have ill intentions. Most of New Mexico's prisons are located near major roads / highways, and signs are posted to never pick up hitchhikers (because they could be an escaped convict). Unless you know the hitchhiker, it is best to not pick up a stranger and give them a ride; don't even slow down / stop to ask the questions either, as they could force you out of your vehicle with a weapon.
	Interior: Never leave ANYTHING of value plainly visible inside of your car's interior (e.g. radar detectors; cell phones; MP3 players; laptop computer). Criminals look inside of parked cars for valuables to steal – it takes seconds to smash a window and steal the valuable(s), and car alarms will not deter a criminal from making a quick buck! BTW – the suction cups used to affix a radar detector or GPS to your windshield leave circle marks on the glass that tells a criminal that electronics COULD be stored inside!
	Packages: Whenever you have bags / packages to carry in your vehicle, ALWAYS place them inside of your vehicle's trunk before you drive away. Criminals watch parking lots – if they see you place a bag / package into the trunk before you walk inside of a building they will know that the trunk contains something of value.
	Parking: Always try to park your vehicle in an area that is visible from the building that you are inside of. Areas that are dark, unlighted, or secluded provide car thieves / criminals with opportunities to break into (or steal) your vehicle or be waiting for you to return to your car. Always walk with purpose to your vehicle and have your car keys in your hand, ready to unlock the vehicle, as you approach your car.
	Tires: Ensure that each tire is filled with air per the manufacturer's specifications (some vehicles have a plate inside of the door jamb that will give the PSI recommendation; otherwise, consult the car's manual) – do NOT use the PSI number that is molded into the tire. If you have a flat tire, ALWAYS try to mount the spare tire on the left rear of the car – mounting the spare on the front will negatively affect your car's steering, and rear wheel drive cars use the right rear tire to push the car forwards / backwards.

Cell Phone Security

If you've been around long enough to remember the "brick phones" from the 1980's, you will agree that portable phone technology has come a LONG way in a very short amount of time. Brick phones became flip phones that fit into your pocket, and now 80% of Americans own smartphones. This technological wonder has transformed how people communicate with each other and access the Internet – landlines in homes are being abandoned, and telephone booths are a distant memory for most cities. A smartphone has more raw computing power, and more storage space, than the majority of personal computers sold to consumers in the 1980s. In fact, the Apple iPhone 4 can perform two BILLION multiplications per second – the world's first supercomputer (the ENIAC; developed in 1946) could only perform [385 multiplications per second](#)!

And therein is the problem...

Smartphones are actually pocket sized computers that consumers use to manage their daily lives. People store contact information, detailed personal information, and important information (e.g. family birthdates, social security numbers, wedding anniversaries – you know, all of the things that you typically forget) in their phone. They log into Internet web sites using their smartphone to conduct online banking; check their on-hand balances; conduct money transfers. What people forget is their smartphone SAVES all of the information inside of their phone. Criminals / hackers, on the other hand, DON'T forget that fact; instead, they are HOPING that you leave your phone in a location where they can steal it, locate all of your personal information, and use your information to steal your identity / steal your money / target your friends and family members. Smartphones have become a booming business for the bad guys – and they are making **millions** of dollars every year via smartphones.

Which means YOU have to be smarter than the criminal, be aware of how information stored on your phone is stolen, and take defensive measures to protect yourself and your family from this 21st century problem.

Some tips to get you started:

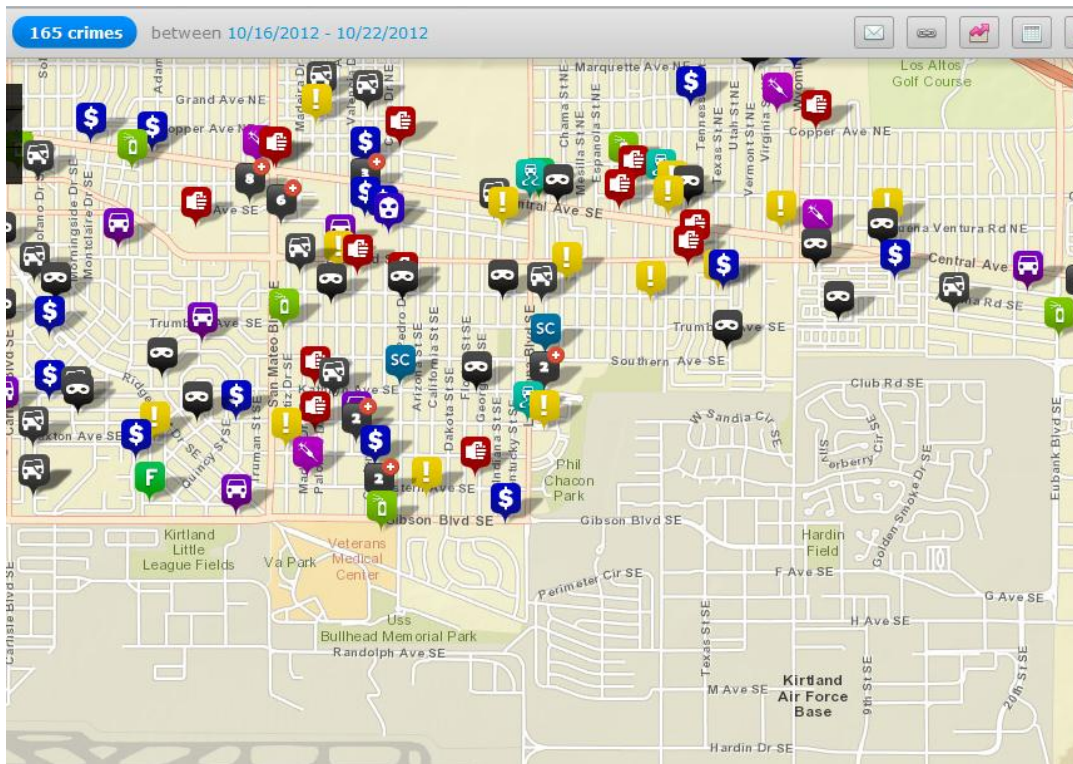
- Password protect (or activate swipe security on) your phone
- Turn off the Wi-Fi feature of your phone; a hacker can use that to gain unauthorized access to your phone
- If your phone is lost / stolen IMMEDIATELY contact your phone carrier to have it deactivated
 - If you can remotely delete / reset your phone DO IT
 - If you can remotely track your phone (e.g. the Apple iPhone has this capability via Apple Care) DO IT
- Be VERY careful on which apps that is downloaded / installed onto your smartphone. A growing number of malicious applications are finding their way onto the Apple Store / phone companies Apps Stores. Once installed, you'll never detect their activity, and you will become an Identity Theft victim
- Consider installing anti-virus software for your smartphone
- Review your monthly telephone bill for unusual activity (e.g. excessive billing charges)
- Ensure you wipe the phone's internal storage before giving it away / selling it / trading it in

Some web sites for additional information:

- D-I-Y Life tips: [click HERE](#)
- Information Week mobile security tips: [click HERE](#)
- T-Mobile web page for mobile phone security: [click HERE](#)
- TechChunks 18 Mobile Security Tips: [click HERE](#)
- TopTenReviews for mobile phone security software: [click HERE](#)
- US-CERT Cell Phone / PDA Threat Advisory: [click HERE](#)
- Verizon cell phone security tips: [click HERE](#)

Crime

There are a couple of web sites that can help you identify criminal activity occurring within any part of Albuquerque. Point your web browser to this address: <http://www.spotcrime.com/nm/albuquerque> - you can define a range of dates to display a map of crimes reported to city police, and optionally have reports sent to you via email (e.g. criminal activity occurring near your home or business). You can also use the CrimeMapping.com web site to also build a detailed map of Albuquerque to identify criminal activity in a particular section of town at this address: <http://www.crimemapping.com/map.aspx?aid=6d325d92-98e5-4c2c-9b55-f6d867510c50> - an example of the map that you can generate resembles:



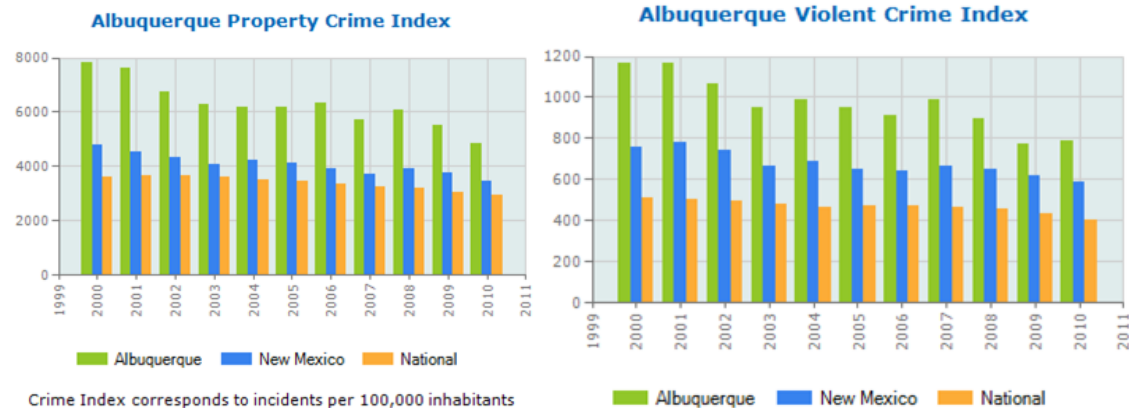
Detailed crime statistics for Albuquerque between 2000 and 2008 are available on the City of Albuquerque [web site](#).

Per the Disaster Center [web site](#), New Mexico's crime rates between 2000 and 2010 were:

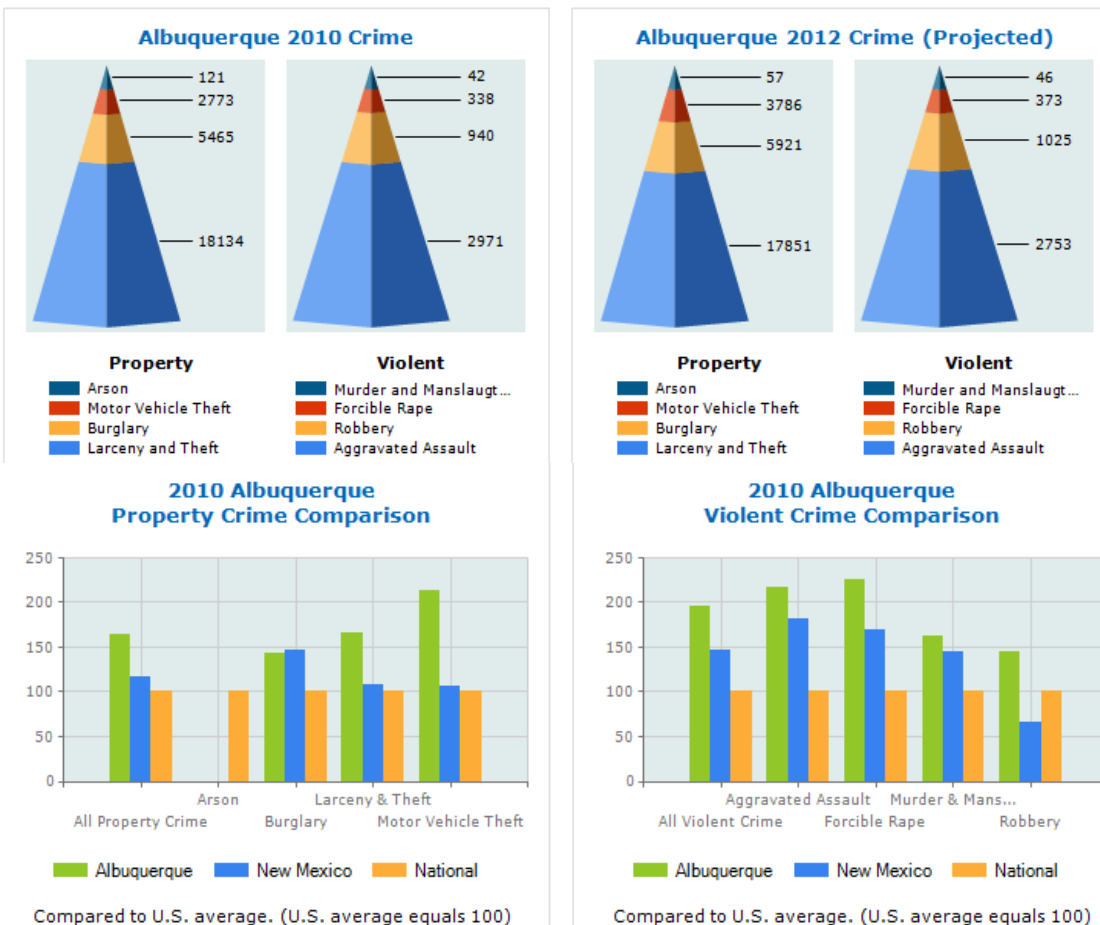
New Mexico Crime Rates 1960 - 2010

Year	Population	Index	Violent	Property	Murder	Forcible Rape	Robbery	Aggravated assault	Burglary	Larceny-Theft	Vehicle Theft
2000	1,819,046	100,391	13,786	86,605	135	922	2,499	10,230	21,339	57,925	7,341
2001	1,830,935	97,383	14,288	83,095	99	850	2,695	10,644	19,552	56,406	7,137
2002	1,852,044	94,196	13,719	80,477	152	1,027	2,206	10,334	19,634	53,406	7,437
2003	1,878,562	89,351	12,535	76,816	116	940	1,937	9,542	18,997	50,595	7,224
2004	1,903,006	92,976	13,081	79,895	169	1,039	2,062	9,811	19,924	52,069	7,902
2005	1,925,985	92,033	12,448	79,575	144	1,041	1,893	9,370	20,939	50,707	7,929
2006	1,954,599	89,528	12,572	76,956	132	1,094	2,105	9,241	20,909	46,822	9,225
2007	1,969,915	86,479	13,085	73,394	162	1,032	2,321	9,570	18,992	45,463	8,939
2008	1,986,763	88,760	13,010	75,750	150	1,114	2,152	9,594	20,720	47,004	8,026
2009	2,009,671	87,348	12,709	74,639	198	1,069	1,932	9,510	21,955	46,182	6,502
2010	2,059,179	82,868	12,126	70,742	142	958	1,614	9,412	21,014	44,481	5,247

Per the CityRating [web site](#), Albuquerque's crime rates in 2010 were:



Actual versus Projected Crime Totals



Per the Rocky Mountain Insurance Information Association [web site](#), Albuquerque ranked in the nation's top ten cities for car theft in 2007, 2008 and 2009. Auto theft continues to be a booming business for car thieves in NM. Factors that influence the high car theft rate is the city's proximity to the Mexico / US border and the proliferation of "chop shops" that sell parts cannibalized from stolen vehicles. In 2009, then-Governor Richardson signed legislation that strengthened

UNCLASSIFIED

penalties for auto theft and created new crime categories for embezzlement and fraud for auto theft. Albuquerque Police Department has enacted a “decoy vehicle” program, where they place a specially outfitted vehicle in areas that experience high rates of vehicle theft to catch car thieves. Some additional statistics from their web site:

New Mexico Auto Theft by Location in 2011 (NICB)

Each year, the [National Insurance Crime Bureau](#) (NICB) studies Metropolitan Statistical Areas (MSAs), or major metropolitan areas to compare the number of vehicle thefts per 100,000 people.

Metropolitan Statistical Area (MSA)	2011 Rank, out of 366 MSAs	2011 Auto Theft Rate per 100,000 people	2010 Auto Theft Rate per 100,000 people
Albuquerque	15	429.65	435.36
Las Cruces	130	197.10	188.31
Santa Fe	138	192.24	209.47
Farmington	295	89.70	113.81

New Mexico 's Top Ten Stolen Vehicles in 2011 (NICB)

1. 2006 Ford Pick-Up (Full Size)
2. 1996 Honda Accord
3. 2005 Chevrolet Pick-Up (Full Size)
4. 1998 Honda Civic
5. 2001 Dodge Pick-Up (Full Size)
6. 1991 Toyota Camry
7. 1995 Saturn SL
8. 1998 Ford Pick-Up (Small Size)
9. 1999 GMC Pick-Up (Full Size)
10. 1999 Chevrolet Pick-Up (Small Size)

Per the 2012 [FBI Uniform Crime Report](#):





CATEGORY	2010	2011	Change
Burglary	5,465	5,985	+9.5%
Larceny	18,134	19,168	+5.7%
Auto Theft	2,773	2,823	+1.8%
Arson	121	133	+9.9%
Murder	49	35	-28.6%
Rape	228	264	+15.8%
Aggravated Assault	2,971	2,910	-2.1%
Robbery	940	998	+6.2%




Some easily implemented, proactive security measures to protect yourself and your possessions:

- Have your car’s windows etched with its VIN number [note: several times a year, the Albuquerque Police Department conducts free VIN etching – check local newspapers for dates / times]
- Don’t park your vehicle in dark areas. Never leave your car running unattended (e.g. warming up the car in your driveway during the winter)
- Always walk “with purpose” – keep your head pointed upwards and maintain situational awareness of your surroundings (especially in parking lots, shopping malls, “Old Town”)
- Never walk away from your vehicle before rolling up windows / locking all doors / hiding all goodies inside of the vehicle within the trunk or glove box
- Remove shrubs near your home’s windows (which provides concealment to burglars)
- Place ladders inside of your garage – don’t give burglars easy access to second story windows
- Add emergency phone numbers to all of your family’s cell phones
- Set up “safe houses” with your neighbors so children have somewhere to go if they feel threatened
- Ensure your home’s [deadbolt](#) inserts at least 1” into the door’s frame – most deadbolts can be pried out of the frame with a screwdriver (due to the doorframe expanding / contracting with humidity)
- If your house has an attached garage, ensure the door between the home and garage is always locked – otherwise, anyone who gains access to your garage can then walk directly into your home
- Conduct a 100% inventory of your possessions; if a valuable doesn’t have a serial number etch a unique identifier onto it. Take pictures / video footage of the items. Upload the data to your email for safekeeping

Cyber Threats

Computer automation is the wave of the future; large aspects of our daily lives are already automated. Imagine how drastically your life would be changed if you no longer had access to the Internet at home, or if your laptop computer was stolen, or your email was blocked? The conveniences that modern technologies bring into our daily lives are significant; unfortunately, criminals ALSO know how the value of accessing YOUR Internet connection; YOUR home computer; YOUR data. It is absolutely vital for you to protect yourself, and your family, in a 21st century cyber world - otherwise, your identity can be stolen, your bank account(s) drained, and your life turned upside down.

	<p>Anti-virus software: Studies have repeatedly shown that the average computer, when plugged into the Internet for the first time, is likely to become infected with computer virus' (aka: malware) within minutes. There are numerous anti-virus solutions available to you – many are free. Do your homework, choose wisely, and ensure that it is scanning EVERY file on your computer's hard drive(s) at <u>least</u> weekly; that it is updating properly; that it scans inbound emails; that it will alert you if it finds malware on your computer.</p>
	<p>Desktop password: Every recent version of Windows allows for each user account to be password protected – to gain access to that user's information that is stored on the computer's hard drive the correct password has to be entered. Screen savers can also be configured to demand the currently logged in user's password to be entered to gain access to their data. If your computer isn't password protected, and that machine is lost or stolen, anyone else can easily access your data. Granted, these passwords can be broken / bypassed by a computer expert, but they "keep honest people honest" – and a password is your first line of defense to protect your stored information.</p>
	<p>Laptop computer security: Laptop computers are praised for their portability; which, ironically enough, is its biggest security problem! It takes only a few seconds for an individual to walk away with your expensive laptop computer – even if your laptop's internal hard drive is encrypted / password protected, they can swap its internal hard drive with a new one, and for less than \$100 they now own a laptop computer! This means that you not only have to pay more attention to where your laptop is, but also ensure that EVERY time you use it that it's tethered with a Kensington Lock to an immovable object to prevent it from disappearing. Always use a backpack type of laptop bag to transport the computer versus using a laptop carry bag (which announces to the world that the bag contains a laptop computer). You can also purchase "Lojack" types of software to help you recover a lost / stolen laptop computer.</p>
	<p>Secure web sites: If you do ANY shopping on the Internet you normally must create a user account on that web site (a username, password, your full name, mailing address, phone number, and email account). When it comes time to pay for the item(s) you must enter your credit card number, its CCV number, the name displayed on the card and its expiration date. If you entered all of that information into a web page that isn't encrypted, and a criminal / hacker is able to intercept that information, odds are nearly 100% that you will become an identity theft victim. Before you start entering your billing / credit card information you MUST check two things:</p> <ol style="list-style-type: none"> 1. The website URL starts with "HTTPS://" instead of "HTTP://" 2. The web browser shows a gold-colored lock icon in its status bar <p>Amazon.Com has a good tutorial on secure web purchases: click HERE for more info!</p>

	<p>Software updates: Most hackers will gain access to your computer (via the Internet) by learning what software is installed on it's hard drive, find an exploitable vulnerability for that software (e.g. Adobe Acrobat Reader), and then create an opportunity for you to download / install that malware onto your computer to target that vulnerability. Once the malware is installed, they can access every file saved on your computer. Ensure you regularly run the Windows Update application to download / install Microsoft's patches; if your other software applications don't have a means of auto-patching themselves; it becomes your responsibility to periodically check the vendor's web site to download software updates (and then install the patch to close the software backdoor).</p>
	<p>SPAM / Phishing: If you have an email account, then you know what SPAM is – it's the electronic equivalent to junk mail that you receive in your mailbox at home. SPAM (aka: unsolicited) email can also be used as a method to infect your computer with malware – once you open the SPAM email, behind the scenes malware is being installed onto your computer (that the criminal / hacker can then use to gain access to information stored on your computer's hard drive). Phishing is SPAM that has been slightly more "tailored" to a specific audience – for example, if the criminal / hacker can figure out what your gender is they can tailor the SPAM they send to you (e.g. if you're male, they will direct sports-related SPAM your direction, figuring you are more likely to open / read that type of email). It is important to NOT respond / reply to SPAM email – sometimes SPAM is "shot-gunned" out to as many email accounts as possible – if you reply to the SPAM, your email address is now confirmed as "active" and even more SPAM will be sent to you! Most email accounts / software have ways of filtering / identifying email as SPAM – if you report an email address as sending out SPAM then your email service provider can start blocking that email address at a higher level (thus preventing others from receiving emails from that email account) – sort of a "community effort" to reduce SPAM from a known SPAM email originator.</p>
	<p>Wireless router: Many people enjoy using wireless devices within their home – the ability to use a laptop computer on your back patio or stream music throughout your home is a very nice convenience. However, criminals / hackers know how to "leech" onto your wireless connection – not only can they use YOUR Internet (that you pay a hefty sum of money for each month), but they could use your Internet connection for illegal activities (e.g. download or share child pornography) or even gain access to information stored on every computer in your home network)! Even if you've password protected your wireless network, if you choose the wrong kind of router encryption (i.e. you are using WEP versus WPA encryption), or haven't changed your router's default password, or are using a weak password, the hacker / criminal can easily gain unauthorized access to your network. A good "how to" article on wireless security can be found on this Internet web site: http://compnetworking.about.com/od/wirelesssecurity/tp/wifisecurity.htm - another useful web site is here: http://www.ehow.com/wireless-router-security/ Another thing to consider when using "free" wireless Internet (e.g. a hotel lobby; the local coffee shop) is that a criminal / hacker could actually be the source of that wireless access point; or, the Internet service you are using has been compromised and in exchange for the "free" Internet that everything you've shared on your laptop is being accessed.</p>

Facebook Smart Card



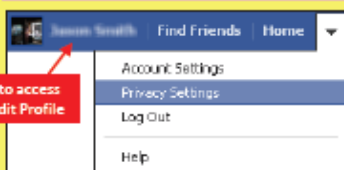
Facebook Smart Card

FB 121211_1800

Social Networks - Do's and Don'ts

- Only establish and maintain connections with people you know and trust. Review your connections often.
- Assume that **ANYONE** can see any information about your activities, personal life, or professional life that you post and share.
- Ensure that your family takes similar precautions with their accounts; their privacy and sharing settings can expose your personal data.
- Avoid posting or tagging images of you or your family that clearly show your face. Select pictures taken at a distance, at an angle, or otherwise concealed. Never post Smartphone photos and don't use your face as a profile photo, instead, use cartoons or avatars.
- Use secure browser settings when possible and monitor your browsing history to ensure that you recognize all access points.

Minimizing your Facebook Profile



Facebook has hundreds of privacy and sharing options. To control how your personal information is shared, you should use the settings shown below (such as *Only Me*, *Friends Only*) for (1) **Privacy**, (2) **Connecting**, (3) **Tags**, (4) **Apps/Websites**, (5) **Info Access through Friends**, and (6) **Past Posts**.

Control Your Default Privacy 1

This setting will apply to status updates and photos you post to your profile from a Facebook app that doesn't have the inline audience selector, like the Facebook App for iPhone.

Change to "Friends Only"

Public Friends Custom

How You Connect

Control how you connect with people you know. [Edit Settings](#)

How Tags Work

Control what happens when friends tag you or your content. [Edit Settings](#)

Apps and Websites

Control what gets shared with apps, games and websites. [Edit Settings](#)

Limit the Audience for Past Posts

Limit the audience for posts you shared with more than friends. [Manage Past Post Visibility](#)

Block Lists

Manage your lists of blocked people and apps. [Manage Block Lists](#)

How You Connect 2

Who can look-up your profile by name or contact info? Friends

Who can send you friend requests? Friends of Friends

Who can send you Facebook messages? Friends

Who can post on your Wall? Friends

Who can see Wall posts by others on your profile? Only Me

[Learn more](#) Done

Choose Your Privacy Settings > Apps, Games and Websites 4

Apps you use: You're using 1 app, game or website.

Facebook August 22 [Edit Settings](#)

Limit Use of Apps

How people bring your info to apps they use: People who can see your info can bring it with these apps. Use the setting to control the categories of info that can bring with them. [Edit Settings](#)

Uncheck ALL Boxes

Instant personalization: Lets you see relevant information about you arrive on select partner websites. [Edit Settings](#)

Disable Personalization

Public search: Shows a preview of your Facebook profile using a search engine. [Edit Settings](#)

Disable Public Search

How Tags Work 3

Profile Review of posts friends tag you in before they go on your profile (notes tags may still appear elsewhere on Facebook) On

Tag Review of tags that friends want to add to your posts On

Profile Visibility of posts you're tagged in once they're on your profile Friends

Tag Suggestions when friends upload photos that look like you Off

Friends Can Check You Into Places using the mobile Places app Off

Done

Limit The Audience for Old Posts on Your Profile 6

If you use this tool, content on your profile you've shared with more than your friends (no public posts) on your Wall will change to Friends. Remember: people who are tagged and their friends may see these posts as well.

You also have the option to individually change the audience of your posts. Just go to the post you want to change and choose a different audience.

[Learn about changing old posts](#) **Limit Old Posts to Friends Only** [Limit Old Posts](#) [Cancel](#)

Info accessible through your friends 5

Use the settings below to control which of your information is available to applications, games and websites when your friends use them. The more info you share, the more social the experience.

<input type="checkbox"/> Bio	<input type="checkbox"/> My videos
<input type="checkbox"/> Birthday	<input type="checkbox"/> My links
<input type="checkbox"/> Family and relationships	<input type="checkbox"/> My notes
<input type="checkbox"/> Interested in	<input type="checkbox"/> Photos and videos I'm tagged in
<input type="checkbox"/> Religious and political views	<input type="checkbox"/> Hometown
<input type="checkbox"/> My website	<input type="checkbox"/> Current city
<input type="checkbox"/> If I'm online	<input type="checkbox"/> Education and work
<input type="checkbox"/> My status updates	<input type="checkbox"/> Activities, interests, things I like
<input type="checkbox"/> My photos	<input type="checkbox"/> Places I check in to

[Save Changes](#) [Cancel](#)



Facebook Smart Card

FB 121211_1800



Do not login to or link third-party sites (e.g. twitter, bing) using your Facebook account. "Facebook Connect" shares your information, and your friends' information, with third party sites that may aggregate and misuse personal information. Also, use as few apps as possible. Apps such as Farmville access and share your personal data.

Profile Settings

Apply and save the Profile settings shown below to ensure that your information is visible to only people of your choosing.

Jason Smith
Born on May 25, 1970 · Add where you work · Add your school · Edit Profile

Work and Education Edit

Employers: Where have you worked? Change to Only Me

College/University: Where did you go to college/university? Change to Only Me

High School: Where did you go to high school? Change to Only Me

Arts and Entertainment Edit

Share Your Interests: Add Music, Add Books, Add Movies, Add TV Shows, Add Games

Activities and Interests Edit

Other: Salon, NPR Music, Words With Friends

Basic Information Edit

Sex: Male

Contact Information Edit

Email: jason.smith7825@yahoo.com Change to Only Me

IM Screen Names: Add / Remove Email Change to Only Me

Phone: Mobile Change to Friends Only

Address: Change to Only Me

City/Town: Change to Only Me

Zip: Change to Only Me

Neighborhood: Change to Only Me

Website: Change to Friends Only

Music Edit

What music do you like? Change to Friends Only

Books Edit

What books do you like? Change to Friends Only

Movies Edit

What movies do you like? Change to Friends Only

Television Edit

What TV shows do you like? Change to Friends Only

Games Edit

What games do you like? Change to Friends Only

Activities Edit

What do you like to do? Change to Friends Only

Interests Edit

What are your interests? Change to Friends Only

Current City Edit

Hometown: Change to Only Me

I Am: Male Change to Only Me

Show my sex in my profile

Birthday Edit

May 25 1970 Show Birthday

Show my full birthday in my profile

Interested In Edit

Women Men

Languages Edit

About Me Edit

Deactivating / Deleting Your Facebook Account

facebook Search

Security

Secure Browsing: Secure browsing is currently disabled. OK

Login Notifications: Login notifications are disabled. OK

Login Approvals: Approvals are not required when logging in from an unrecognized device. OK

Recognized Devices: No recognized devices. OK

Active Sessions: Logouts from New York, NY, US and 2 other locations. OK

[Deactivate your account](#)

To **deactivate your Facebook account**, go to Account Settings and select Security. To reactivate your account log in to Facebook with your email address and password.

To **delete your Facebook account**, go to Help Center from the account menu. Type Delete into the search box. Select How do I permanently delete my account then scroll down to submit your request here. Verify that you want to delete your account. Click Submit. FB will remove your data after 14 days post security check.

Useful Links

A Parent's Guide to Internet Safety
Wired Kids
Microsoft Safety & Security
OnGuard Online

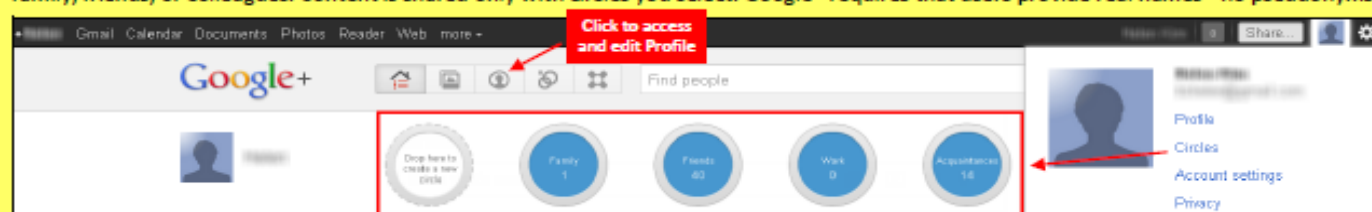
www.fbi.gov/stats-services/publications/parent-guide
www.wiredkids.org/
www.microsoft.com/security/online-privacy/social-networking.aspx
www.onguardonline.gov/topics/social-networking-sites.aspx

Google+ Smart Card

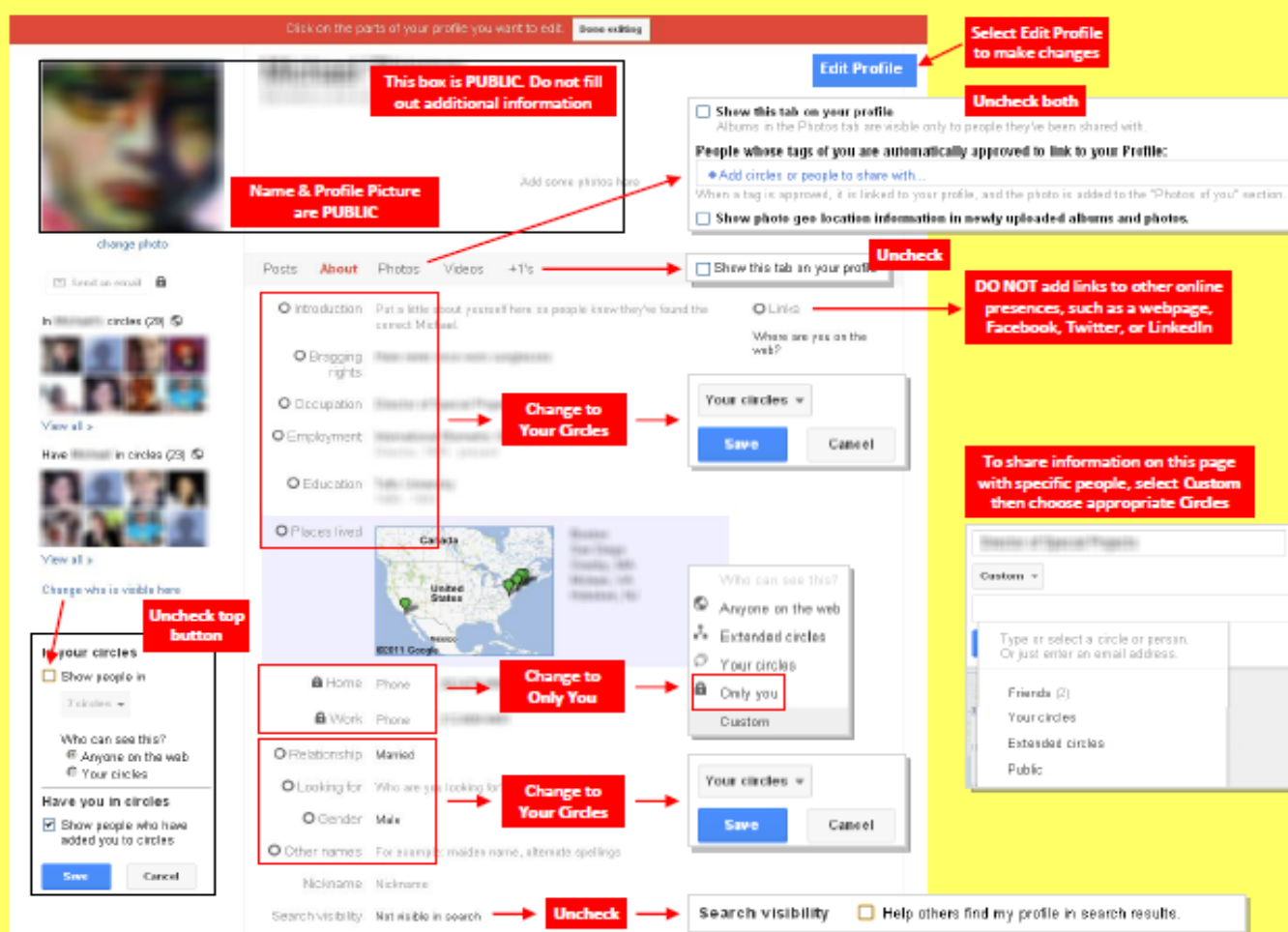
Social Networks - Do's and Don'ts

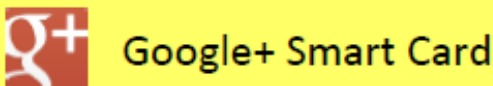
- Only establish and maintain connections with people you know and trust. Review your connections often.
- Assume that ANYONE can see any information about your activities, personal life, or professional life that you post and share.
- Ensure that your family takes similar precautions with their accounts; their privacy and sharing settings can expose your personal data.
- Avoid posting or tagging images of you or your family that clearly show your face. Select pictures taken at a distance, at an angle, or otherwise concealed. **Never post Smartphone photos and don't use your face as a profile photo, instead, use cartoons or avatars.**
- Use secure browser settings when possible and monitor your browsing history to ensure that you recognize all access points.

Google+ provides privacy and sharing options using Circles. Circles are groups that users create for different types of connections, such as family, friends, or colleagues. Content is shared only with circles you select. Google+ requires that users provide real names - no pseudonyms.



Apply and save the Profile settings shown below to ensure that your information is visible to only people of your choosing.





G+ 121911 2000

Account Settings & Minimizing Your Activities

Apply the Account settings shown with arrows below to ensure that your information is shared in a limited fashion.

Account overview

Profile and privacy

Google+

Language

Data liberation

Connected accounts

Change as indicated

Google+

[Back to Google+](#)

Who can interact with you and your posts

Who can send you notifications? [Learn more](#) See circles

Who can comment on your public posts? [Learn more](#) See circles

Who can start a Messenger conversation with you? Circle

Notification delivery

Email: ishelen@gmail.com

Phone: [Add phone number](#) **Don't Add Phone Number**

☐ Push notifications ☐ Don't notify me

Manage email subscriptions **Uncheck**

Occasional updates about Google+ activity and friend suggestions









- Account settings can be accessed under **Account Settings > Google+**.
- Maintain a small Google+ "footprint". Select only important Google+ notifications as shown in the box to the left.
- Limit notifications to email as opposed to text.
- Do not connect your mobile phone to Google+ or use the Google+ mobile application, and **Disable +1** on non-Google Websites
- Do not allow contacts to tag you then automatically link to your profile
- Disable your circles from accessing your photo tags prior to you

Google +1
+1 on non-Google sites Off [Edit](#) [Change to "Off"](#)

Google+ Pages
☐ Automatically add a Google+ page to my circles if I search for + followed by the page's [Uncheck](#)

Photos
☐ Show photo geo location information in newly uploaded albums and photos. [Uncheck](#)
☐ Allow viewers to download my photos [Uncheck](#)
☐ Find my face in photos and prompt people I know to tag me. [Learn more](#) [Uncheck](#)

People whose tags of you are automatically approved to link to your Profile:
[+ Add circles or people to share with...](#) [Remove Everyone](#)
When a tag is approved, it is linked to your profile, and the photo is added to the "Tagged" section.


Receive notifications		Check as indicated
Notify me by email or SMS when someone...		
Posts and mentions of my name	 Email	 Phone
Mentions me in a post	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Shares a post with me directly	<input type="checkbox"/>	<input type="checkbox"/>
Comments on a post I created	<input type="checkbox"/>	<input type="checkbox"/>
Comments on a post after I comment on it	<input type="checkbox"/>	<input type="checkbox"/>
Circles	 Email	 Phone
Adds me to a circle	<input type="checkbox"/>	<input type="checkbox"/>
Photos	 Email	 Phone
Tags me in a photo	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Tags one of my photos	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Comments on a photo after I comment on it	<input type="checkbox"/>	<input type="checkbox"/>
Comments on a photo I am tagged in	<input type="checkbox"/>	<input type="checkbox"/>
Comments on a photo I tagged	<input type="checkbox"/>	<input type="checkbox"/>
Messenger	 Email	 Phone
Starts a conversation with me	<input type="checkbox"/>	<input checked="" type="checkbox"/>


The screenshot shows the 'Connected accounts' section of a Google account settings page. On the left, a sidebar contains links: 'Account overview', 'Profile and privacy', 'Google+', 'Language', 'Data download', and 'Connected accounts' (highlighted with a red box). The main content area is titled 'Connected accounts' and includes a message: 'You can improve your Google experience by connecting your accounts from other services.' Below this, there are two rows of account connections. The first row shows 'YouTube public' with buttons for 'Disconnect this account' and 'Link', and a red 'Uncheck' button. The second row shows 'Twitter' with a checkbox for 'Add this link to my public Google Profile, too' and a red 'Uncheck' button. A large red box with the text 'Do not add outside accounts' is overlaid on the Twitter connection options. Below the connections, there is a section titled 'Connecting your accounts' with three bullet points: 'When you search, you can see relevant results your friends share on the web.', 'You enable it easier for them to find the stuff you share on the web.', and 'You can choose which accounts to show as [your public Google Profile](#).' A note states: 'Remember, Google won't share your searches or other private information with third-party services without your consent.' At the bottom, there is a checkbox for 'Use my Google contact information to suggest accounts from other sites' and a red 'Uncheck' button.


By default, Google+ uses your Google contact information to link your accounts from other online services, aggregating your online identity in one location. To disable this feature:


- Go to Account Settings > Connected Accounts
- Click "No" to Google-suggested 3rd-party accounts
- Disable Google+ access to your contact information
- Do not manually connect other online accounts using Google+


Deleting Your Google+ Profile Information or Account



Account overview



 Profile and privacy



 Google+


 Language


 Data liberation


 Connected accounts


Account overview



[View your info](#)
[Edit profile](#)

Services

Delete profile and Google+ features
Delete entire Google account
View, enable, or disable web history

Delete profile and remove associated Google+ features
Close entire account and delete all services and info associated with it
Go to web history

[Go to Account Settings](#)
[> Account Overview](#)

- **Delete Google+ Content** removes Google+ related information such as circles, +1's, posts, and comments
- **Delete your entire Google profile** removes all user data from Google services, including your Gmail
- **Disable web history** to prevent accumulation of your digital footprint

Useful Links

A Parent's Guide to Internet Safety	www.fbi.gov/stats-services/publications/parent-guide
Wired Kids	www.wiredkids.org/
Microsoft Safety & Security	www.microsoft.com/security/online-privacy/social-networking.aspx
OnGuard Online	www.onguardonline.gov/topics/social-networking-sites.aspx

LinkedIn.Com Smart Card



LinkedIn Smart Card

UJ 121911_1400

Social Networks -Do's and Don'ts

- Only establish and maintain connections with people you know and trust. Review your connections often.
- Assume that ANYONE can see any information about your activities, personal life, or professional life that you post and share.
- Ensure that your family takes similar precautions with their accounts; their privacy and sharing settings can expose your personal data.
- Avoid posting or tagging images of you or your family that clearly show your face. Select pictures taken at a distance, at an angle, or otherwise concealed. **Never post Smartphone photos and don't use your face as a profile photo, instead, use cartoons or avatars.**
- Use secure browser settings when possible and monitor your browsing history to ensure that you recognize all access points.

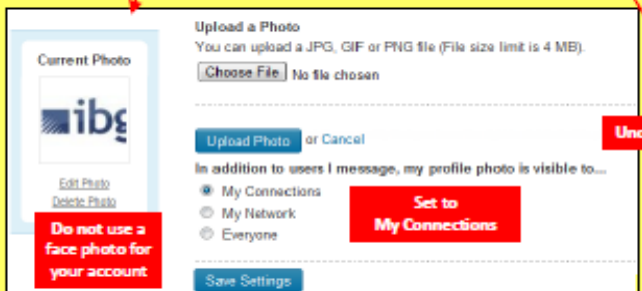
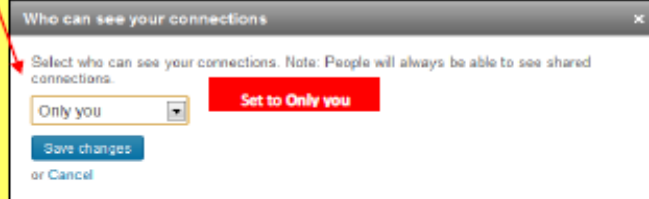
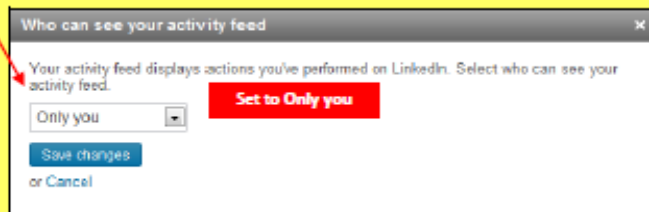
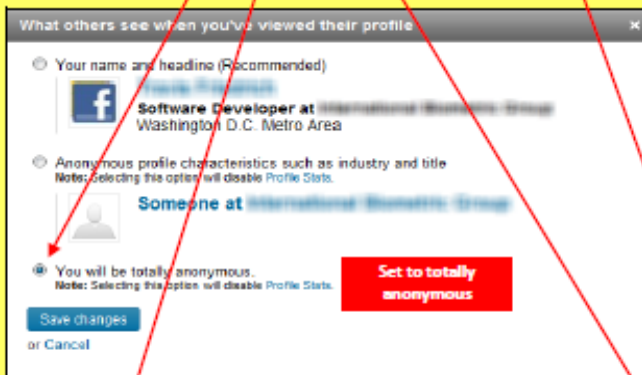
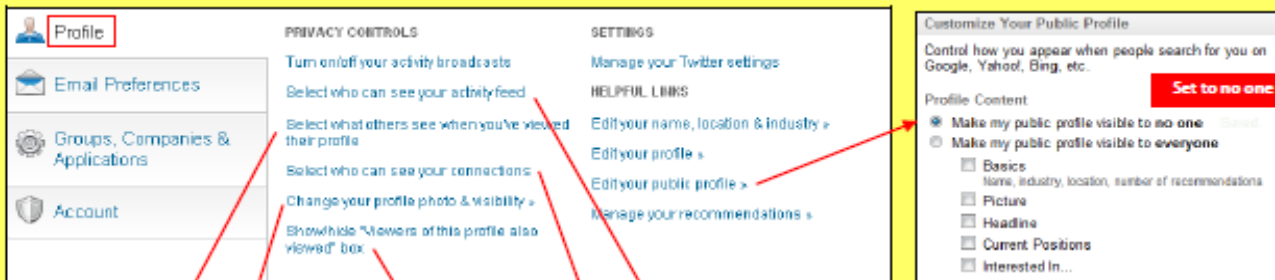
Managing Your LinkedIn Profile

LinkedIn is a professional networking site whose users establish connections with co-workers, customers, business contacts, and potential employees and employers. Users post and share information about current and previous employment, education, military activities, specialties, and interests. To limit exposure of your personal information, you can manage who can view your profile and activities.



Profile Settings

Apply the Profile settings shown with arrows below to ensure that your information is visible only to people of your choosing.



LinkedIn Quick Facts

- There are over 100 million LinkedIn users around the world. Aside from the US, LinkedIn is widely adopted in India, Brazil, and the UK.

- Users tend to share information related to their careers or jobs as opposed to photographs from parties or social events.
- LinkedIn profiles tend to be more visible and searchable than in social networks such as Facebook.
- Paid LinkedIn accounts have access to more information about other users, such as connections, than free accounts.
- The type of information users can see about each other depends on how closely they are connected (1st, 2nd, or 3rd degree).





LinkedIn Smart Card

U 121911_1400

Account Settings

Apply the Account settings shown with arrows below to ensure that your information is shared in a limited fashion.

<ul style="list-style-type: none"> Profile Email Preferences Groups, Companies & Applications Account 	PRIVACY CONTROLS Manage Social Advertising Manage Partner Advertising SETTINGS Change your profile photo & visibility > Show/hide profile photos of other members Customize the updates you see on your home page Select your language	EMAIL & PASSWORD Add & change email addresses Change password HELPFUL LINKS Upgrade your account > Close your account > Get LinkedIn content in an RSS feed >	Passwords Use a complex password with capital letters and numbers to ensure that attackers cannot access your account information.
	Closing Your LinkedIn Account If you no longer plan to use the LinkedIn service, you can close your account. Click Close your account and confirm that you want to take this action.		

Partner Advertising LinkedIn works with partner websites to show advertisements to LinkedIn members on their sites. This collection of partner sites is called the LinkedIn Audience Network. Read more... <input type="checkbox"/> LinkedIn may show me ads on its partner websites. Save changes or Cancel	Manage Social Advertising LinkedIn may sometimes pair an advertiser's message with social content from LinkedIn's network in order to make the ad more relevant. When LinkedIn members recommend people and services, follow companies, or take other actions, their name/photo may show up in related ads shown to you. Conversely, when you take these actions on LinkedIn, your name/photo may show up in related ads shown to LinkedIn members. By providing social context, we make it easy for our members to learn about products and services that the LinkedIn network is interacting with. <input type="checkbox"/> LinkedIn may use my name, photo in social advertising. Save or Cancel
--	---

Uncheck to opt out of Partner Advertising on third party websites

Uncheck to opt out of Social Advertising

Application Settings

Third-party applications and services can access most of your personal information once you grant them permission. You should limit your use of applications to ensure that third parties cannot collect, share, or misuse your personal information. Apply the Application setting shown with arrows below to ensure that your information is visible only to people of your choosing.

<ul style="list-style-type: none"> Profile Email Preferences Groups, Companies & Applications Account 	GROUPS Select your group display order > View your groups > Set the frequency of group digest emails Turn on/off group invitations COMPANIES View companies you're following >	APPLICATIONS View your applications > Add applications > PRIVACY CONTROLS Turn on/off data sharing with 3rd party applications Manage settings for LinkedIn plugins on third-party sites	Data sharing with third-party applications <input type="checkbox"/> Yes, share my data with third party applications. Save changes or Cancel
	Manage settings for LinkedIn plugins on third-party sites If you're signed in to LinkedIn when you view any page that uses our professional plugins, we receive information that you've visited that page. This allows us to improve your LinkedIn experience and provide you with insights from your professional network, like how many of your connections have shared an article into LinkedIn using the Share on LinkedIn plugin. <input type="checkbox"/> Yes, allow LinkedIn to receive information about my visits to pages that use LinkedIn plugins. Save changes or Cancel		Also, avoid using the LinkedIn smartphone app to prevent accidentally collecting and sharing location data. LinkedIn, by default, automatically retrieves information about the user on websites with LinkedIn Plug-In integration. Prevent sharing your activities on third-party websites with LinkedIn by unchecking the box.

Uncheck the box. Do not share your information on Third Parties with LinkedIn.

Useful Links

A Parent's Guide to Internet Safety	www.fbi.gov/stats-services/publications/parent-guide
Wired Kids	www.wiredkids.org/
Microsoft Safety & Security	www.microsoft.com/security/online-privacy/social-networking.aspx
OnGuard Online	www.onguardonline.gov/topics/social-networking-sites.aspx

Twitter Smart Card



Twitter Smart Card

Twitter 121511_1631

Social Networks -Do's and Don'ts

- Only establish and maintain connections with people you know and trust. Review your connections often.
- Assume that ANYONE can see any information about your activities, personal life, or professional life that you post and share.
- Ensure that your family takes similar precautions with their accounts; their privacy and sharing settings can expose your personal data.
- Avoid posting or tagging images of you or your family that clearly show your face. Select pictures taken at a distance, at an angle, or otherwise concealed. **Never post Smartphone photos and don't use your face as a profile photo, instead, use cartoons or avatars.**
- Use secure browser settings when possible and monitor your browsing history to ensure that you recognize all access points.

Managing your Twitter Account

Twitter is a social networking and microblogging site whose users send and read text-based posts online. The site surged to worldwide popularity with +300 million active users as of 2011, generating 300 million tweets and 1.6 billion search queries daily.

Home @ Connect # Discover Search Profile Compose

Jason Smith
View my profile page
0 TWEETS 11 FOLLOWING 1 FOLLOWERS

Tweets Stream of tweets from people you follow Use Settings to manage visibility

HP LatinoVoices @LatinoVoices
Are Gingrich and Marco Rubio getting closer? huff.to/10a3YM
Retweeted by Huffington Post
Each tweet is timestamped → 21h

Following are people you subscribe to. Followers subscribe to your tweets. Private tweets will only be visible to followers you approve.

Tweets

"Tweets" are short text-based messages – up to 140 characters – that users post to Twitter. "Tweet" can refer to a post as well or to the act of posting to Twitter. Tweets are public, indexed, and searchable unless protected by the user. Many users never Tweet, choosing only to follow persons or topics of interest.

Hashtags (#topic) are used to mark a keyword or topic in a Tweet. Posts with hashtag are categorized by topics in the Twitter search engine. Hashtagged words that become popular become Trending Topics (ex. #jan25, #egypt, #sxsw).

Mentions (@username) are used to tag a user in a Twitter update. When a public user mentions a private Twitter account, the link to the private account profile becomes public.

Gündüz Feneri Blog @gunduzfeneri
#BestHolidayMovies It's a wonderful life (46), a christmas carol (51), The Catalogue 5 (88), Miracle on 34th Street (47), love actually (03)
2h

@jessmchung
@Delta last word on the matter. \$DAL >6% down over a 24 hour period. You are lucky it is the weekend.
30 Sep

Profile Settings

Apply the Profile settings shown below to ensure that your information is visible only to people of your choosing.

JasonSmith7825's settings
Account Password Mobile Notifications **Profile** Design

Picture
Choose File No file chosen
Maximum size of 2MB. JPG, GIF, PNG.

Name
Jason Smith
Enter your real name.

Location
USA
Where in the world are you?

Web
http://
Have a homepage or a blog? Put the address here. (You can also add Twitter to your site here)

Bio
About yourself in fewer than 160 chars.

Facebook
Post your Tweets to Facebook
DO NOT connect to Facebook


Save

Jason Smith @JasonSmith7825
Edit your profile
1 TWEETS 11 FOLLOWING 5 FOLLOWERS

Tweets
Following Following Favorites Lists

Twitter Best Practices

- Avoid using hashtags (#) in updates to avoid being indexed and associated with a topic by Twitter Search.
- **Tweet responsibly.** Do not provide personal details regarding your whereabouts and activities in your post.
- Do NOT upload links to personal photos or websites on Twitter.
- Do NOT allow Twitter to use your location on mobile devices.
- Change your Twitter username periodically to limit account exposure.



Twitter Smart Card

Twitter 121511_1631

Account Settings

Apply the Account settings shown below to ensure that your information is shared in a limited fashion.

JasonSmith7825's settings

Account Password Mobile Notifications Profile Design

DO NOT connect your phone

Name: Jason Smith
You can change your name on your [profile settings](#).

Username: JasonSmith7825
Your public profile: <http://twitter.com/JasonSmith7825>
Change every ~6 months

Email: jason.smith7825@yahoo.com
Note: email will not be publicly displayed.
Uncheck ☐ Let others find me by my email address

Language: English
What language would you like to Twitter in?
Interested in helping translate Twitter? Check out the [Translation Center](#).

Time Zone: (GMT-06:00) Central Time (US & Canada)

Tweet Location: ☐ Add a location to your Tweets
Ever had something you wanted to share ("fireworks!", "party!", "ice cream truck", or "quicksand...") that would be better with a location? By turning on this feature, you can include location information like neighborhood, town, or exact point when you tweet.
When you tweet with a location, it will be added to your location history.
Uncheck
Click to delete all location data associated with your account
You may **delete all location information** from your past Tweets. This may take up to 30 minutes.

Protecting your tweets makes all your posts private. Only those who you approve can access your tweets.

Check ☒ Protect my Tweets
Only let people whom I approve follow me. If this is checked, your future Tweets previously may still be publicly visible.

Check ☒ Always use HTTPS
Use a secure connection where possible to encrypt your account information.

Save

Deactivate my account

Your pending follower requests

Jess M Chung @jessmchung
I spend a lot of time thinking about all the things I'd buy or eat. That and complaining.

Accept **Decline**

Deactivating / Delete Your Twitter Account

To deactivate your account, go to **Settings** and select **Account** page. At the bottom of the page, click **"Deactivate my account."** After deactivation, the user can reactivate the account within 30 days. After 30 days, the account is permanently deleted.

Notification & Application Settings

Maintain a small digital footprint by minimizing the number of notifications. Revoke access to unnecessary third party applications.

Notifications

Choose when and how often Twitter sends emails to itshehen@gmail.com (change).

Messages

Email me when: ☐ I'm sent a direct message **Direct message (DM) is never visible to the public**
☒ I'm sent a reply or mentioned

Activity

Email me when: ☒ I'm followed by someone new
☐ My Tweets are marked as favorites
☒ My Tweets are retweeted **Private tweets will become visible to the web when retweeted (RT) by a user with public account**

Updates

Email me with: ☐ Occasional updates about new Twitter products, features, and tips
☒ Product or service updates related to my Twitter account

Save

Applications

You've allowed the following applications to access your account

HootSuite by HootSuite
The social media dashboard which allows teams to broadcast, monitor and track results.
read, write, and direct messages access - Approved: Tue December 6, 2011 07:18:36 PM **Revoke Access**

Twitter for Android by Twitter, Inc.
Twitter for Android
read, write, and direct messages access - Approved: Sat February 26, 2011 07:16:46 PM **Revoke Access**

Samsung Mobile by Samsung
Samsung mobile own applications
read, write, and direct messages access - Approved: Thu February 10, 2011 12:15:07 AM **Revoke Access**

Block unknown or unwanted applications from accessing your account

Useful Links

A Parent's Guide to Internet Safety www.fbi.gov/stats-services/publications/parent-guide
Wired Kids www.wiredkids.org/
Microsoft Safety & Security www.microsoft.com/security/online-privacy/social-networking.aspx
OnGuard Online www.onguardonline.gov/topics/social-networking-sites.aspx

Drugs

Drug use / abuse is not a new phenomenon; what has changed over the past 20-30 years is the increased availability of drugs and the levels of peer pressure that our children experience, sometimes on a daily level, to try or use drugs. Drug manufacturers / drug cartels / drug dealers now cater their product with catchy names like “K2” and “Spice” to entice children to use their products. Some of these newer drugs are initially legal for consumption until side effects and / or fatalities start to occur – and then the U.S. government will ban those products.

Some statistics from the Drug and Enforcement Agency (DEA) web site (<http://www.getsmartaboutdrugs.com>):

- Seven out of the top eleven drugs used by twelfth graders are prescription / over-the-counter drugs
- Two in five teens abuse cough medicine to get high
- Everyday objects, to include magic markers, lipstick containers, and soda containers can be used as drug paraphernalia to conceal drug use
- Kids now use their cell phones, the Internet, and Twitter to warn their peers that parents are nearby and to conceal their drug use. Some acronyms to know:
P911 = Parents Alert; PAL = Parents Are Listening; PAW = Parents Are Watching; PIR = Parents In Room; POS = Parents Over Shoulders
- Kids obtain most of the drugs they need to get high from their home’s medicine cabinet
- One in five kids has used glue, aerosol sprays, or cleaning fluids to get high
- More than 60% of teens that are enrolled in a drug abuse program cited marijuana as their drug of choice
- Declining school grades are a strong indication of drug use

Marijuana (cannabis) is often coined the “gateway drug”, due to the misconception that it isn’t harmful. Marijuana users usually migrate to stronger drugs (e.g. cocaine; heroin) to induce more powerful “highs”. Some facts about this drug:


- Cannabis contains more than 400 chemicals, many of which are harmful.
- Cannabis smoke has more cancer-causing agents than cigarette smoke.
- The chemicals in cannabis smoke can remain in the body for up to a month.
- Cannabis affects co-ordination and slows down thinking and reflexes.
- Cannabis reduces people’s memory and affects comprehension.
- Cannabis smokers often lose interest in schoolwork, sports, and other extracurricular activities
- Smoking cannabis is especially harmful for young people because their bodies are still growing.
- Cannabis is psychologically addictive.

Per the 2011 “[New Mexico Substance Abuse Epidemiology Profile](#)” report, produced by the New Mexico Department of Health:





- Over the past 30 years, New Mexico has consistently had among the highest alcohol-related death rates in the United States; and it has had the highest alcohol-related death rate since 1997.
- New Mexico has the highest drug-induced death rate in the nation.
- From 1981-2007, New Mexico's suicide rate has consistently been among the highest in the nation -- 1.5 to 1.9 times the U.S. rate. Male suicide rates are more than three times female rates across the age range.
- In 2009, New Mexico public high school students were slightly more likely to report binge drinking than U.S. high school students; more commonly reported by upper grade students than lower grade students.
- In 2009, marijuana and cocaine use were more prevalent among New Mexico students than among U.S. students.

UNCLASSIFIED

Some things to know about drug paraphernalia and drugs commonly within New Mexico:

	<p>AROMA RUB</p> <p>Kids use surgical masks and vapor rubs in combination to enhance the effects of Ecstasy. The vapor rub is placed under the nose, and the mask is used to keep the rub from dissipating.</p>		<p>Glow Sticks</p> <p>People who attend Raves use glow sticks, laser lights and other light toys to enhance the hallucinogenic effect of Ecstasy. The lights are placed close to the users dilated pupils so they can see "trails" of light. This practice can cause long-term vision impairment.</p>
	<p>Surgical Masks</p> <p>Kids use surgical masks and vapor rubs in combination to enhance the effects of Ecstasy. The vapor rub is placed under the nose, and the mask is used to keep the rub from dissipating.</p>		<p>Crack Pipes</p> <p>Used to smoke crack cocaine. Crack users have been known to smoke through a soda can with small holes in the bottom, or a glass bottle with the bottom removed when a crack pipe is not available.</p>
	<p>Lipstick Container</p> <p>Used to conceal a pipe used to smoke marijuana. Also can be hollowed out and used as a drug pipe to smoke marijuana.</p>		<p>Hypodermic Needle</p> <p>Intravenous drug abusers, inject a liquid form of various drugs such as heroin, methamphetamine, methadone, or steroids into their bodies.</p>
	<p>Bong / Water Pipe</p> <p>A smoking device which is generally used to smoke cannabis (Marijuana) or Salvia. Used because the bong cools the smoke before it enters the smoker's lungs which makes it easier to smoke, and also allows a large amount of smoke to be inhaled quickly.</p>		<p>Home Made Bong</p> <p>Can be made out of soda cans, soda bottles, etc.</p>
 	<p>Marijuana</p> <p>Alias' include: Aunt Mary, BC Bud, Blunts, Boom, Chronic, Dope, Gangster, Ganja, Grass, Hash, Herb, Hydro, Indo, Joint, Kif, Mary Jane, Mota, Pot, Reefer, Sinsemilla, Skunk, Smoke, Weed, Yerba</p> <p>Marijuana is usually smoked as a cigarette (called a joint) or in a pipe or bong. It is also smoked in blunts, which are cigars that have been emptied of tobacco and refilled with marijuana, sometimes in combination with another drug. Marijuana is also mixed with foods or brewed as a tea.</p>		<p>Ecstasy</p> <p>Alias' include: Adam, Beans, Clarity, Disco Biscuit, E, Ecstasy, Eve, Go, Hug Drug, Lover's Speed, MDMA, Peace, STP, X, XTC</p> <p>K2 or "Spice" is a mixture of herbs and spices that is typically sprayed with synthetic marijuana. The colorful pills are often hidden among colorful candies. MDMA is also distributed in capsules, powder, and liquid forms.</p>
	<p>Inhalants</p> <p>Inhalants and solvents are ordinary household products that are inhaled or sniffed by a user to get high. There are hundreds of household and industrial products on the market are used as inhalants. Examples of inhalants include model airplane glue, leather glue, nail polish remover, cleaning fluids, gasoline, spray paint, fabric protector, air conditioner fluid (Freon) among others. These products are sniffed, snorted, bagged (fumes inhaled from a plastic bag), or "huffed" (inhalant-soaked rag, sock, or roll of toilet paper in the mouth) to achieve a high. Inhalants are also sniffed directly from the container.</p>	 	<p>Heroin</p> <p>Alias' include: Big H, Black Tar, Chiva, Hell Dust, Horse, Negra, Smack, Thunder</p> <p>Heroin can be injected, smoked, or sniffed/snorted. High purity heroin is usually snorted or smoked.</p> <p>Heroin is commonly distributed within aluminum foil; the drug user will use the foil to heat up the drug and then either smoke or inject it. Finding small pieces of aluminum foil is a strong indicator of heroin use – after the heroin is smoked within the foil there will be a yellow colored stain where the drug evaporated, with a black stain to the side.</p> <p>Finding spoons with a burned / scorched bottom is another indicator of heroin use</p>

UNCLASSIFIED

	<p>K2 / Spice Alias's include: Zohai, Genie, K3, Bliss, Nice, Black Mamba, Incense, and even fake weed.</p> <p>Youth believe this drug to be legal – it is not legal for sale / use in the country. At one time, tattoo shops would sell this drug. Tests concluded the active ingredients (HU-210) are between 100 to 800 times more potent than marijuana.</p>		<p>Bath Salts Alias's include: "Ivory Wave," "Purple Wave," "Vanilla Sky," and "Bliss".</p> <p>In 2012, the DEA deemed Bath Salts to be an "imminent threat to public safety" and made it illegal to possess / sell / use this drug.</p>
	<p>Peyote / Mescaline Alias' include: Buttons, Cactus, Mesc, Peyoto</p> <p>Peyote is a small, spineless cactus. The active ingredient in peyote is the hallucinogen mescaline.</p> <p>The fresh or dried buttons are chewed or soaked in water to produce an intoxicating liquid. Peyote buttons may also be ground into a powder that can be placed inside gelatin capsules to be swallowed, or smoked with a leaf material such as cannabis or tobacco.</p>		<p>Ketamine Cat Tranquilizer, Cat Valium, Jet, Jet K, K, Kit Kat, Purple, Special K, Special La Coke, Super Acid, Super K, Vitamin K</p> <p>Popular among teens and young adults at dance clubs and "raves." Ketamine is manufactured commercially as a powder or liquid. Powdered ketamine is also formed from pharmaceutical ketamine by evaporating the liquid using hot plates, warming trays, or microwave ovens, a process that results in the formation of crystals, which are then ground into powder. Powdered ketamine is cut into lines known as bumps and snorted, or it is smoked, typically in marijuana or tobacco cigarettes. Liquid ketamine is injected or mixed into drinks. Ketamine is found by itself or often in combination with MDMA, amphetamine, methamphetamine, or cocaine.</p>

Simple Reminders:

- Pay attention to materiel indicators (listed above) that your children might be experimenting with drugs.
- Be mindful of personality changes; unexplainable mood swings; declining school grades.
- Lock up prescription medication – properly dispose of unneeded medication.
- There are dozens of drug testing facilities throughout Albuquerque that can test your child for drug use – do an Internet search for "Albuquerque drug testing" to locate one nearest you.

Sources: <http://www.nacada.go.ke/drugs/marijuana/>
<http://www.getsmartaboutdrugs.com/identify/drugs.html>
<http://www.dare.com/>
http://www.getsmartaboutdrugs.com/Files/File/DEApillbook_1_5_08.pdf
<http://www.saynoheroine.org/HAC1.html>
http://nmhealth.org/erd/HealthData/substance_abuse.shtml

Fire Extinguishers

Very easy to use, but if have never used one before it could be confusing – and if your possessions are on fire every second counts to pull the pin and squeeze the handle. You also need to purchase the right type of fire extinguisher:

1. HOLD EXTINGUISHER UPRIGHT AND PULL THE RING (SAFETY) PIN



2. STAND BACK FROM THE FIRE AND AIM AT THE BASE OF THE FIRE NEAREST YOU







3. SQUEEZE HANDLES TOGETHER AND SWEEP THE EXTINGUISHER STREAM SIDE TO SIDE



REMEMBER THIS SIMPLE WORD -
P A S S

PULL AIM SQUEEZE SWEEP

Fire Extinguisher Chart

Extinguisher		Type of Fire				
Colour	Type	Solids (wood, paper, cloth, etc)	Flammable Liquids	Flammable Gasses	Electrical Equipment	Cooking Oils & Fats
	Water	✓ Yes	✗ No	✗ No	✗ No	✗ No
	Foam	✓ Yes	✓ Yes	✗ No	✗ No	✓ Yes
	Dry Powder	✓ Yes	✓ Yes	✓ Yes	✓ Yes	✗ No
	Carbon Dioxide (CO2)	✗ No	✓ Yes	✗ No	✓ Yes	✓ Yes

Fire extinguishers are very affordable; most places sell a 2-pack of extinguishers for under \$40. Places to consider placing a fire extinguisher:






- Laundry room (if your dryer catches fire due to lint build up)
- Kitchen (stove fires; dishwasher heating element causes a fire)
- Living room (near your fireplace)
- Patio (for BBQ fires)
- Garage (where combustibles are stored)
- Classic cars (carburetor catches fire)

Firearm Safety



Whether or not your household personally believes in owning / using firearms, there is no guarantee that:

- Every household that your family visits doesn't contain at least one firearm
- That the household that one of your family members is visiting has properly secured their firearm(s)
- That the household member(s) has properly trained THEIR family on how to properly handle firearms

It therefore becomes important for YOUR family to know how to react when introduced to firearms. The basics are VERY simple to learn, and once learned they can literally save a life:

 <p>An example of a POOR choice of a target backstop!</p>	<p>Always keep a gun pointed in a safe direction</p> <ul style="list-style-type: none"> • NEVER point it at something unless you intend to shoot it • Bullet size doesn't matter – a BB gun can shoot a BB between 325 to 1100 feet per second <ul style="list-style-type: none"> ○ Even the weakest BB gun can still shoot out an eye ○ A .177 caliber pellet gun is dangerous out to 450 yards! • If you can see buildings / cars / people in the distance pick a different direction to shoot the gun • The area behind what you are shooting at is called a "backstop" – it's very important to know what the backstop is!
	<ul style="list-style-type: none"> • Always keep your finger off of the trigger until you are ready to shoot the firearm <ul style="list-style-type: none"> ○ One of the most basic, yet important, gun rules • The picture at left shows the PROPER way to hold a gun <ul style="list-style-type: none"> ○ The trigger finger is placed along the gun's frame until the shooter is ready to shoot
	<ul style="list-style-type: none"> • Always keep the gun unloaded until ready to use <ul style="list-style-type: none"> ○ A gun can't be accidentally fired if it is unloaded • A revolver (picture to the left) is easy to see if it is unloaded <ul style="list-style-type: none"> ○ The cylinder "swings" out to the side to remove / insert ammunition
	<ul style="list-style-type: none"> • A semi-automatic is a little more difficult to check if loaded <ul style="list-style-type: none"> ○ One round is still in the chamber if the clip is removed; the slide has to be slid backwards to eject that cartridge
	<ul style="list-style-type: none"> • Never handle / fire a gun if you are using alcohol or drugs <ul style="list-style-type: none"> ○ You don't drive drunk or incapacitated – the same goes for handling guns

UNCLASSIFIED

	<ul style="list-style-type: none"> • Before cleaning a gun double check that it is unloaded prior to cleaning <ul style="list-style-type: none"> ○ A basic rule of thumb that many forget – and they wind up shooting themselves!
	<ul style="list-style-type: none"> • Store guns so they can't be accessed by unauthorized persons <ul style="list-style-type: none"> ○ ALWAYS use a trigger lock or place the gun(s) in a safe so they can't be found by snooping <ul style="list-style-type: none"> ▪ Hiding the gun under a mattress / desk drawer / closet NEVER works – and children are usually the ones who find the unsecured weapon • There are many ways to secure your personal firearm(s) <ul style="list-style-type: none"> ○ Gun safe ○ Trigger lock ○ Cable ran through the magazine well / breech

And the most BASIC rule of all: **TREAT EVERY FIREARM AS IF IT IS LOADED!** If you are handed a firearm, and if the cylinder (for a revolver) isn't swung open to show it is unloaded or handed a semi-automatic whose clip is ejected and the slide is locked backwards, **TREAT THE GUN AS IF IT IS LOADED** and then personally check the weapon to determine if it is loaded or not. **NEVER ASSUME** a gun is unloaded!

Albuquerque has several ways to obtain firearms safety training:

- Gun shops
- National Rifle Association (NRA) sponsored training courses
- Shooting ranges

Click [HERE](#) for some Internet resources for gun safety / marksmanship courses throughout New Mexico.

Gangs

The National Gang Intelligence Center (NGIC)([website](#)) publishes an annual assessment of gang activity within the United States. Highlights of the 2011 report include:

- Gangs are expanding, evolving and posing an increasing threat to US communities nationwide.
- Many gangs are sophisticated criminal networks with members who are violent, distribute wholesale quantities of drugs, and develop and maintain close working relationships with members and associates of transnational criminal/drug trafficking organizations.
- Gangs are becoming more violent while engaging in less typical and lower-risk crime, such as prostitution and white-collar crime.
- Gangs are more adaptable, organized, sophisticated, and opportunistic, exploiting new and advanced technology as a means to recruit, communicate discretely, target their rivals, and perpetuate their criminal activity.
- There are approximately 1.4 million Active Street, prison, and OMG gang members comprising more than 33,000 gangs in the United States. Gang membership increased most significantly in the Northeast and Southeast regions, although the West and Great Lakes regions boast the highest number of gang members. Neighborhood-based gangs, hybrid gang members, and national-level gangs such as the Sureños are rapidly expanding in many jurisdictions. Many communities are also experiencing an increase in ethnic-based gangs such as African, Asian, Caribbean, and Eurasian gangs.
- Gangs are responsible for an average of 48 percent of violent crime in most jurisdictions and up to 90 percent in several others, according to NGIC analysis. Major cities and suburban areas experience the most gang-related violence. Local neighborhood-based gangs and drug crews continue to pose the most significant criminal threat in most communities.
- Aggressive recruitment of juveniles and immigrants, alliances and conflict between gangs, the release of incarcerated gang members from prison, advancements in technology and communication, and Mexican Drug Trafficking Organization (MDTO) involvement in drug distribution have resulted in gang expansion and violence in a number of jurisdictions.
- Gangs are increasingly engaging in non-traditional gang-related crime, such as alien smuggling, human trafficking, and prostitution. Gangs are also engaging in white collar crime such as counterfeiting, identity theft, and mortgage fraud, primarily due to the high profitability and much lower visibility and risk of detection and punishment than drug and weapons trafficking.
- Many gang members continue to engage in gang activity while incarcerated. Family members play pivotal roles in assisting or facilitating gang activities and recruitment during a gang members' incarceration. Gang members in some correctional facilities are adopting radical religious views while incarcerated.
- Gang infiltration of the military continues to pose a significant criminal threat, as members of at least 53 gangs have been identified on both domestic and international military installations. Gang members who learn advanced weaponry and combat techniques in the military are at risk of employing these skills on the street when they return to their communities.
- Gangs on Indian Reservations often emulate national-level gangs and adopt names and identifiers from nationally recognized urban gangs. Gang members on some Indian Reservations are associating with gang members in the community to commit crime.
- Many jurisdictions are experiencing an increase in juvenile gangs and violence, which is often attributed, in part, to the increased incarceration rates of older members and the aggressive recruitment of juveniles in schools. Gangs have traditionally targeted youths because of their vulnerability and susceptibility to recruitment tactics, as well as their likelihood of avoiding harsh criminal sentencing and willingness to engage in violence.

Here are two nationwide statistical charts that show gang member footprint and gang-related drug activity:

Figure 1. Estimated Nationwide Gang Presence per Capita per State

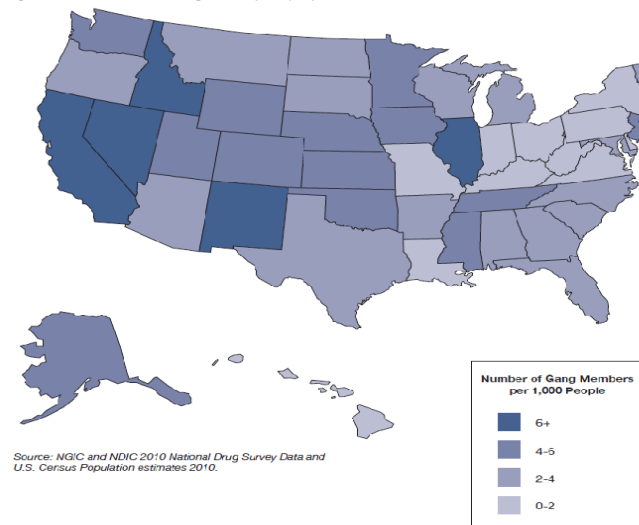


Figure 2. Major Cities Reporting Gang-Related Drug Activity in 2010:



The first gang in New Mexico was created in 1957 by a group of incarcerated Chicano street gang members. Since that time, the number of gangs in Albuquerque has swelled to **178 active gangs**.

If you have children that have started attending school, odds are they walk amongst gang members; they might even be occasionally pressured to join a gang. The ABQGANGS.ORG web site (<http://stopabqgangs.org>) has an excellent [web page](#) to educate kids about the dangers of joining a gang – how the gang member(s) will try to recruit new members; their initiation process (which often turns deadly), and how becoming a gang member will negatively affect not only the child, but also their family.


Graffiti is the most common type of property vandalism, which affects 35% of community members (per the [DOJ](#)). When an area is repeatedly targeted by gang members / taggers with graffiti, citizens feel their community isn't safe and oftentimes the graffiti serves as a welcome mat to more serious crime. Oftentimes, graffiti is painted onto walls / mailboxes / curbs for a gang to "mark" their territory – and serve as a warning to other gangs to stay away of suffer the consequences. Houses and community members within that area are then preyed upon by that gang.

To report graffiti (and then have the graffiti removed by city workers):

- Albuquerque: 505-768-4725 or 311 / [web site](#) / [email](#)
- Bernalillo: 505-243-7273
- Rio Rancho: 505-891-7224 / [web site](#)

Hotel Security

Regardless of the hotel being located stateside or overseas, there are security considerations to keep in mind as you travel alone or with your family:

	COMPUTER: Never travel with a laptop computer without bringing a Kensington Lock (approximately \$30 at Wal-Mart, Best Buy, etc.). Locate an immovable object (e.g. inside of the closet), loop the Kensington Lock through it, and tether your laptop computer to that immovable object to prevent it from being stolen.
	EXITS: Ensure each traveler knows where the emergency exits are located nearest to your hotel room.
	INTERNET: If you choose to use the hotel-provided internet with your computer, IMMEDIATELY terminate your Internet connection if you see any popup windows that ask you to install ANY type of software – that would be malware that is trying to steal your information! The only popup you should experience is one popup window that asks if you are willing to bill the daily Internet usage fee to your room number, and that the Internet access will expire in 24 hours – any demands to install software onto your computer is MALWARE!
	PARKING: Park your vehicle as close to the front of the hotel as possible to minimize its chances of being burglarized or stolen.
	PEEPHOLE: Make sure your hotel room's door has a peephole installed and you can actually see into the hallway from inside of your room with it. If the peephole is blocked / murky / cloudy, demand another hotel room.
	ROOM SERVICE: If you didn't order it, don't accept it if you hear a knock on your hotel room's door and hear "room service!" Instead, call the hotel's front desk, give them your room number, and allow their security personnel (or Manager) to "talk" with the individual located outside of your door.
	ROOM SELECTION: Choose a room between the second and tenth floors. Ground level rooms could allow a criminal to enter your room from the parking lot; floors above the tenth floor are too high for a fire department's ladder truck to reach you.
	SAFE: If you are traveling with a passport or valuables, make use of your hotel room's safe (or the safe located in the hotel's office) to secure those items from theft / pickpocketing / purse snatching.
	TIDINESS: Before you leave your hotel room unattended for a considerable length of time, push in all dresser drawers and, if applicable, shut the closet door. When you return to your hotel room, if a dresser drawer / closet door is not fully closed, your belongings were possibly rifled through. Immediately conduct an inventory of your possessions and notify hotel management if anything is missing.

Identity Theft

One of the fastest growing criminal industries is “identity theft”, which occurs when someone uses your personally identifiable information (PII), like your Social Security Number, home address, birth date, without your permission, to commit fraud or other crimes. The Federal Trade Commission estimates that as many as 9 million Americans have their identities stolen each year. Identity theft is a serious problem – while some victims can resolve their problems quickly, others spend hundreds of dollars and many days repairing damage to their good name and credit record.

Some tips on how to prevent Identity Theft from impacting you:

- Limit the amount of PII that you post onto the Internet.
 - Conduct an Internet search of your name to determine how MUCH information exists about you online.
 - If possible, remove your PII from online social networking web sites, blogs, etc.
- Purchase a paper shredder for your home and shred ALL documents that contain PII
- Be cautious about unsolicited offers that ask for PII – legitimate offers shouldn’t require that level of information from you in the “introductory” stage
- Be cautious about SPAM email that requests you to click on an embedded hyperlink to “update” your account – even if the email looks official and appears legitimate, it is ALWAYS best to manually open the business’ web site and then access your account – NEVER trust the hyperlink!
- Pay careful attention to your checking / savings / credit card balances for unauthorized purchases
- If you believe you’ve been victimized by Identity Theft IMMEDIATELY address the issue! Every moment wasted is another moment the criminal(s) could be impacting your name and financial status!

There are numerous web sites that can provide more detailed information on this topic:

- Federal Deposit Insurance Corporation web site: click [HERE](#)
- Federal Trade Commission’s Identity Theft web site: click [HERE](#) or [HERE](#)
- Department of Justice web site: click [HERE](#)
- IDtheft.Gov web site: click [HERE](#)
- Identity Theft protection web sites: click [HERE](#)
- Social Security Administration web site: click [HERE](#)

School Vulnerabilities

The 21st century school environment is far removed from the more “innocent” Cold War era that most of today’s parents grew up with – the days of practicing nuclear war drills and having “only” fist fights off campus are long gone. Today’s youth contend with:

- Active Shooter incidents ([educational web site HERE](#))
- Assaults against school faculty by other students ([educational web site HERE](#) or [HERE](#))
- Bomb threats made against the school ([educational web site HERE](#))
- Bullying ([educational web site HERE](#) or [HERE](#))
- Burglary ([News articles HERE](#))
- Carrying weapons on school property ([info HERE](#), [HERE](#))
- Drug dealing or drug use in / around schools ([educational web site HERE](#))
- False fire alarms ([News article HERE](#))
- Fighting (to include videotaping of fights)([educational web site HERE](#))
- Gang recruitment / violence ([educational web site HERE](#))
- Graffiti in schools / on school property ([educational web site HERE](#) or [HERE](#))
- Hate crimes ([educational web site HERE](#))
- Hazing ([educational web site HERE](#))
- Peer pressure ([educational web site HERE](#))
- Sexting ([educational web site HERE](#))
- Stalking (either by students or by students against teachers) ([educational web site HERE](#))
- Teenage pregnancy ([educational web site HERE](#))
- Vandalism / theft of school property ([educational web site HERE](#))

These 21st century “realities” for America’s present-day schoolchildren are a complex challenge for parents. Peer pressure to participate in these undesirable / disruptive activities is enormous; some parents are left with no choice but to transfer their children to another school to keep them out of harm’s way.

Parents need to assist schools / school teachers / school counselors with providing their children with fact-based information on the threat categories listed. Simply telling children to “just say no” when a peer asks them to experiment with drugs or join a gang isn’t adequate – children need substantially more “tools in their toolbox” to deal with sometimes relentless peer pressure, stand their ground, and then stubbornly refuse to do something illegal.

Some indicators that a child might be experiencing peer-related difficulties at school include:

- Plummeting grades
- Resistance / outright unwillingness to attend school
- Ditching / showing up late for class
- Dramatic personality changes (e.g. isolationism)
- Dramatic changes to their dress and appearance
- Sudden and repeated injuries / bruising / abrasions / cuts on their body
- Signs of alcohol / drug use (e.g. dilated pupils; slurring of words; profuse sweating; constant chewing on fingernails or placing items in their mouth; smell of smoke or alcohol)

Terrorism in the U.S.

Here is a challenge for you: see how many days in a row that you can check your favorite news agency's web page and **NOT** read about an act of terrorism being committed somewhere around the world. Odds are you won't achieve two days in a row. People sometimes forget is that terrorism is not a new phenomenon – in the 1st century AD the [Sicarii extremist group](#) targeted temple priests and wealthy elites. Every century has experienced noteworthy acts of terrorism; and the 21st century arguably has more terrorist activity than ever before. The United States has experienced its own fair share of terrorism activity; some [notable examples](#) include:

- 1910 Oct 1: The Los Angeles Times building was destroyed by TNT – 21 killed. Two brothers planted the bomb in retaliation for the paper's opposition to unionization of its employees.
- 1915 Jul 2: A German professor wanted to prevent the U.S. from supporting allies in WWI – he exploded a bomb in the reception room of the U.S. Senate; the next morning he tried to assassinate J.P. Morgan.
- 1933 Oct 10: A Boeing 247 is destroyed midflight over Indiana by a nitroglycerin bomb. This is the first incident of air sabotage in the history of aviation.
- 1940-1956: George Metesky, aka "The Mad Bomber", placed over 30 bombs in NYC in public places (e.g. Grand Central Station; Paramount Theater) to protest the high rates of a local electric company.
- 1960: The "Sunday Bomber" set off a series of bombs in NYC subways and ferries during Sundays and holidays; he killed one woman and injured 51 other commuters.
- 1974 Summer: The "Alphabet Bomber" bombed the Pan Am Terminal at Los Angeles International airport; fire bombed the houses of a judge and two police commissioners; burned down two apartment buildings and threatened Los Angeles with a gas attack. He wanted an end to immigration / naturalization laws.
- 1975 Dec 29: LaGuardia Airport is bombed; 11 dead and 75 injured.
- 1980 Jun 3: the Statue of Liberty's Story Room was bombed.
- 1984: the Rajneesh movement spread salmonella in salad bars at 10 restaurants in Dalles, OR to influence a local election. 751 people were sickened and over 40 were hospitalized.
- 1993 Feb 26: Ramzi Yousef, a member of Al Qaeda, bombed the World Trade Center; 6 dead and 1000 injured.
- 1995 Apr 19: Timothy McVeigh and Terry Nichols detonated a truck bomb at the Alfred Murray federal building in Oklahoma City, OK. 168 people were killed.
- 2001 May 21: ELF burned down the Center for Urban Horticulture at the University of Washington.
- 2009 Jun 1: a radicalized Muslim shot and killed one military recruiter and wounded a second at a Little Rock, AR Army/Navy Career Center. He was upset over U.S. killing of Muslims in Iraq and Afghanistan.

Between 1980 and 2000, there were [335 terrorism incidents](#) on U.S. soil; 250 of these incidents were categorized by the FBI as Domestic Terrorism (i.e. an act of terrorism committed by a U.S. citizen). The remaining 85 terrorism incidents were categorized as International Terrorism (i.e. an act of terrorism committed by a foreign national / foreign group).

Although the United States has its military forces, government agencies and police forces actively engaged in identifying and lawfully pursuing terrorist groups / members, they don't possess the resources to be everywhere. Oftentimes, the best investigative leads that law enforcement agencies receive come from our country's citizens, who observe or come into knowledge of activities that are suspicious. Oftentimes, these suspicious activities have innocent explanations; however, it is **ALWAYS** better to report the anomaly and let the trained professionals make a determination instead of *not* reporting the information and it **DOES** turn out to be a terrorism indicator.

Listed below are some of the terrorism indicators that various law enforcement agencies have put together; it is not a 100% complete listing of possible terrorism indicators, but will give you an idea of what types of suspicious activities warrant contacting the police or FBI:

UNCLASSIFIED

- Talk knowingly about a future terrorist event, as if they have inside information
- Statement of intent to commit (or threatening to commit) a terrorist act
- Statements of having a bomb / biological / chemical weapon; about having or getting the materials to make such a device, or about learning how to make or use any such device
- Collecting of unclassified information that might be useful to someone planning a terrorist attack (e.g. pipeline locations, airport control procedures, building blueprints, etc.)
- Physical surveillance (photography, videotaping, take notes of patterns of activity at various times) of any site that is a potential target (to include any building of symbolic importance to the government or economy, large public gathering, transportation center, bridge, power plant, communication center, military installation)
- Deliberate probing of security responses, such as deliberately causing a false alarm, faked accidental entry to an unauthorized area, or other suspicious activity designed to test security responses
- Possessing or seeking items that may be useful for a terrorist but are inconsistent with the person's known hobbies or job requirements (e.g. explosives, uniforms, high powered weapons, books / literature on how to make a harmful device, multiple or fraudulent identification documents)
- Statements of support for suicide bombers who have attacked the U.S. or U.S. personnel / interests abroad
- Individual's residence contains little or no furniture besides a bed / mattress, a table and chair, etc.
- Individual possessed blueprints / maps / photographs of sensitive locations and potential targets
- Individual's residence contains police manuals, military training manuals, flight manuals, first-responder radio scanners or other communications equipment, surveillance equipment (night-vision goggles, GPS devices)
- Presence of ID card manufacturing equipment (e.g. lamination machine; plastic card stock)
- Arranged marriages to facilitate U.S. citizenship
- Possession of identification documents bearing more than one identity
- Possession of passport photos of other individuals
- Invalid or unusual explanations of visitor, employment or student status
- Exclusive use of public telephones and / or telephone cards even though they have a land line / cell phone
- Use of a distant post office rather than one closer to their work / home
- Cache(s) of funds, some of which may be held by unwitting associates
- Presence in a residence of military-grade (or unusual quantity of) weapons
- Inability to provide personal background information beyond that contained in identification documents or they provide answers that seem practiced or rehearsed
- Jihadist literature, training manuals, security plans, encoded materials, or instructions for the use of codes and ciphers inside of their residence / vehicle

Contact numbers to report suspicious behavior / anomalies:

- Albuquerque FBI: 505-889-1300
- Albuquerque Police Department: 911 or 242-COPS
- Kirtland AFB Command Post: 505-846-3777

Source Index

The following Internet sources were used in the creation of this awareness product:

Page Number(s)	Internet Source(s)
3 (Active Shooter)	http://www.google.com/url?sa=t&rct=j&q=&esrc=s&frm=1&source=web&cd=3&cad=rja&ved=0CDkQFjAC&url=http%3A%2F%2Fwww.cbsnews.com%2F8301-504083_162-20010291-504083.html&ei=fH-iUM-oMYr29gS3-4CoAw&usg=AFQjCNEvT8i67CmvZL4APqoBoir2gSQKkw ; http://www.readyhouston.tx.gov/
4 (ATM Fraud pictures)	https://www.google.com/search?q=emcore+active+shooter&hl=en&tbo=d&source=lnms&tbn=isch&sa=X&ei=fH-iUM-oMYr29gS3-4CoAw&ved=0CAQQ_AUoAA&biw=1280&bih=790&hl=en&tbo=d&tbn=isch&sa=1&q=atm+fraud&oq=atm+fraud&gs_l=img.3..0l3j0i5j0i24l6.1029.2121.0.2231.9.8.0.0.0.0.156.780.2j5.7.0...0.0...1c.1.rfDbNmDURMs&bav=on.2.or.r_gc.r_pw.r_qf.&fp=bf2828e5e7694d9a&bpc=38093640&biw=1280&bih=790
PICTURES 6 (Automobile Safety) 11-12 (Cyber Threat) 24 (Fire Extinguishers) 25-26 (Firearm Safety) 29 (Hotel Security)	https://www.google.com/imghp?hl=en&tab=wi
7 (Cell Phone Security)	http://www.bitrebels.com/technology/power-in-your-palm-the-computing-power-in-todays-smartphones/
8-10 (Crime)	http://www.spotcrime.com ; http://www.crimemapping.com ; http://www.disastercenter.com/crime/nmcrimn.htm ; http://www.cityrating.com/crime-statistics/new-mexico/albuquerque.html ; http://www.rmia.org/auto/auto_theft/new_mexico_auto_theft_statistics.asp ; http://www.wacrimstats.com/fbi-uniform-crime-report-2012/
13-14 (Facebook Smart Card)	http://www.amc.af.mil/shared/media/document/AFD-120504-122.pdf
15-16 (Google+ Smart Card)	http://sasit.rutgers.edu/component/docman/doc_download/494-smart-card-google?Itemid=
17-18 (Linkedin Smart Card)	www.amc.af.mil/shared/media/document/AFD-120504-124.pdf
19-20 (Twitter Smart Card)	http://www.umassd.edu/media/umassdartmouth/publicsafety/pdfs/Twitter_Smart_Card.pdf
21-23 (Drugs)	http://www.getsmartaboutdrugs.com/ ; https://www.google.com/imghp?hl=en&tab=wi ; http://nmhealth.org/ERD/SubstanceAbuse/2011%20New%20Mexico%20Substance%20Abuse%20Epidemiology%20Profile.pdf ;
27-28 (Gangs)	http://www.nationalgangcenter.gov/ ; http://stopabggangs.org/
32-33 (Terrorism in the U.S.)	http://en.wikipedia.org/wiki/Terrorism ; http://en.wikipedia.org/wiki/Terrorism in the United States ; http://en.wikipedia.org/wiki/Domestic terrorism in the United States