

A close-up, slightly blurred image of police vehicle emergency lights. On the left, there are red lights, and on the right, there are blue lights. The lights are glowing and creating a sense of urgency.

STAYING SAFE

From serial killers to
identity thieves, a primer
to keep you out of
criminals' crosshairs

FBI Profiler

MARK SAFARIK

ALAN JACOBSON

National Bestselling Author

DANGER

STAYING SAFE

**From serial killers to
identity thieves,
a primer to keep you
out of criminals' crosshairs**

MARK SAFARIK

FBI Supervisory Special Agent (ret.)

ALAN JACOBSON

National Bestselling Author

Copyright © 2007-13. **Important notice:** The authors grant permission for the dissemination of this eBook, provided it is used in its entirety and without alteration.

Contents

Staying Safe: An Introduction	4
<i>Why this information is important</i>	
Background concepts of crime	5
<i>Known acquaintance vs. stranger-on-stranger crime</i>	
Human behavior and violent crime	6
<i>Understanding who these people are and why they do what they do</i>	
Measuring your risk	9
<i>The concept of risk levels</i>	
Personal Safety Checklist	11
<i>Keeping yourself and your loved ones safe</i>	
Home Safety Checklist	21
<i>Your home is your castle. You don't need a moat, but some common sense tips can work wonders.</i>	
Protecting yourself from identity theft	26
<i>Who does it, what it means to you and your life; prevention</i>	
Keeping your online presence secure	40
<i>Creating and using passwords and PINS properly</i>	
In closing	43
<i>An ounce of prevention is worth a pound of cure</i>	
About the authors	44
<i>Who we are, what we do</i>	

Mark Safarik is a recently retired senior profiler with the FBI's Behavioral Analysis Unit who has dedicated his career to helping law enforcement agencies worldwide catch serial offenders. Alan Jacobson is the national bestselling author of several novels, including the critically acclaimed thriller series featuring the enigmatic FBI profiler Karen Vail. Jacobson spent seven years researching serial killers with Safarik and other members of the FBI profiling unit.

We go about our lives doing those things we deem necessary: we lock our houses and we lock our car doors. We keep a front porch light on at night. And we watch our children when they're scurrying about the local playground. But sometimes there are others watching our loved ones, too. Nefarious individuals who are out for no good, whose sole purpose in life is to satisfy their needs by committing violent crime. Or to cause property damage, or take from you that which is not theirs.

Staying safe is a mindset as much as it is a checklist of things to do. We have to be aware that these criminals walk among us, and we have to take this risk seriously. Does this mean we have to walk around constantly checking over our shoulder, waiting for something bad to happen? Absolutely not. But the FBI likes to say that a little paranoia can be a healthy thing.

We're going to share principles with you that will help keep you and your loved ones safe. This is merely a

primer, because the topic is far ranging and there's no way to cover every scenario that could arise. There are a million variables that can come into play. But if you can glean some lessons from what we're about to outline below, you'll begin to understand what you can do, and how you can protect yourself.

The old saying is that it's not enough to give a hungry person a piece of fish; instead, give him a pole and teach him how to fish. That's what we're going to do. Below is your pole, and a figurative instruction manual on how to use it.

Background concepts of crime

Known acquaintance vs. stranger-on-stranger crime

According to studies conducted by the FBI and other law enforcement agencies, the majority of violent crimes are committed by people who have some level of relationship with their victims. That's the good news, because we have some degree of control over the situation. If we know someone has a violent history, we can choose not to socialize with that individual; or if we know he shows violent tendencies when he drinks alcohol, we can avoid him in those settings. Clearly, this is a simplification—we can't always choose the time and place where we interact with people. But by and large, we have some modicum of control over this type of violence.

In the late seventies, research was published in an area called "routine activities theory." The theory holds that people often travel in fairly consistent patterns. They go to work, go shopping, visit relatives, go to the health club, and go home. Everyone has his or her own pattern of activity. When two different people's activities intersect and one is inclined to act out violently, that act of violence may occur when your activities intersect with theirs.

The closer the relationship between two people, the greater likelihood their daily activity patterns will intersect with, or overlap, one another. During this overlap, should one party act out violently, there is a greater likelihood that injury will result to the other person. This is why most of the violent crime occurs between people who have some level of relationship. The probability that they will be in the vicinity of the person committing a violent crime is high. In many cases, it is *the interaction between them* that sparks the violence.

This is clearly the case in domestic violence events where an argument escalates to physical confrontation—which escalates further to serious injury or death. Another example would be a bar fight where two individuals have intersected in an atmosphere that fosters violent confrontations: male posturing may enter into the equation, loud music, or "gang behavior" in which someone is around his friends and feels the need to act out. Further, the use of alcohol lowers one's

inhibitions to using violence to solve a perceived problem.

As noted earlier, the situations described above afford us some degree of control over situations because we know the players involved. However, stranger-on-stranger crimes are much more difficult to manage, both from a victim's perspective in defending oneself, and from law enforcement's perspective in trying to find the perpetrator.

Human behavior and violent crime

Understanding who these people are and why they do what they do

It's important for us to think about crime the way criminals do. It's not merely a random act with a finite goal in mind. In other words, it's often more than just "I need something, so I'm going to find out where I can steal it." People who engage in criminal acts are repeat offenders. They commit a crime, and should they find success (they don't get caught), the belief they can repeat the act is reinforced.

Clearly, the more times they successfully complete their crimes and come away with the spoils of their efforts, the more motivated they become to continue these acts. As a result, the life of crime becomes their "occupation," and some of them study and treat their "trade" as if it was a legitimate business enterprise. They study us all the while we are unaware, scoping out our houses,

businesses, vehicles, possessions...and us, including our children.

Like you go to your office and clock in to sit at your desk to get work done, they spend hours each day trolling, observing, and looking for openings where they can strike in ways that will net them their booty.

They assess you as their target. For the criminal offender, the most dangerous time is when he first makes physical contact with you. He doesn't know how you are going to react when confronted, and his goal is to gain control of you quickly. If he is unable to do so, his risk level greatly elevates because now he has to use force, a weapon, or threats to induce or force you to comply—all of which involve more risk on his part. (The concept of risk levels will be discussed in more detail below.)

When selecting a victim, an offender looks for someone who gives off an aura of being a victim. That is, he's watching for an individual who does not radiate self-confidence, who looks afraid, timid, disengaged, preoccupied, and unobservant. This potential victim does not carry herself with authority and confidence. How do you avoid projecting these qualities? Be observant, look around and be aware of the space around you. Be cognizant of people behind you or coming toward you. This does not mean you should be afraid; quite the opposite. Bottom line: awareness is the key. (More on this later.)

Unbeknownst to you, some offenders study your habits, note your comings and goings, and watch your house. Now, with services such as Google Earth, they can do their work in the comfort of their own home, prowling online for homes in areas that provide clean getaway routes. They can evaluate your property from above, zoom in and see what shrubbery you have that obscures view from neighbors or police.

Others are acting because an opportunity has presented itself: you're alone, it's dark, your car is parked in an isolated area and you've entered a geographic area they've targeted. It isn't that they've targeted you personally; you're the next person to enter the area they have selected.

Offenders are not interested in ethical or moral issues of what is right or wrong. They are only concerned with what's good for them. They seek instant gratification—whether that's the feeling they get when using drugs purchased with money stolen from you, or from the challenge and act of stealing, it's all about obtaining the most—with the least amount of effort.

Measuring your risk

The concept of risk levels

Everyone is at some risk for becoming the victim of a violent crime. Most of us are at a low risk. That is because we do not engage in high risk behaviors like criminal activity, illegal drug activity, hitchhiking,

prostitution, and walking alone in desolate and isolated areas.

Risk cuts both ways. Offenders also need to engage in some level of risk in order to commit a crime. The higher the level of risk for them, the greater the reward needs to be for them to take that risk. Ideally, we want to be at a low risk level—while forcing offenders into thinking their risk level for choosing us as a victim will be high. Unfortunately, despite our best efforts, sometimes we find ourselves in situations that elevate our risk, or what criminal profilers call "situational risk."

Examples of situational risk might include your car breaking down on the highway or having to park in an outlying area of a parking garage or mall, or traveling at night in isolated locations, especially on foot; another example would be unexpectedly returning home late at night and having to walk to your residence in the dark in relatively secluded areas.

If you recognize that in such situations your risk level is elevated, you can take proactive steps to minimize your risk. You can have people meet you so you don't have to walk alone. You can ask security personnel to accompany you to your cars if the area is dark or isolated. You can be more aware of cars or vans parked around or adjacent to your vehicle in a parking lot, and you can become more aware of your personal space when you are in public. (More on these safety steps below.)

If you understand that crimes are not generally chance occurrences, you can become aware of those things you should be doing to protect yourself. Below are **safety checklists**—precautions you can take, along with actions that will increase your chances of surviving an attack. These are not exhaustive lists. During the course of your daily life, if you think of something that's not on this list, please send us an [email](#) so we can share the information with others.

Spend some time thinking about the items below. They will help you form a common sense approach to making your everyday habits safer for you and your family.

Personal Safety Checklist

Keeping yourself and your loved ones safe

First and foremost, don't put yourself in dangerous situations. What does this mean? Generally, it means understanding what we outlined above and applying common sense. Specifically:

1. Do not go places alone at night when you're able to avoid it. You may be an individual who goes about his or her daily activities in a manner that makes you a "low risk" target. But if you alter this behavior in certain ways, you can inadvertently elevate your risk level. An example would be the mother who needs milk for her baby at night. She's a low risk individual because she doesn't

engage in the type of behavior or activities that put her in harm's way: she doesn't frequent places where nefarious individuals hang out, she doesn't use drugs or drink excessively.

Yet here she is, running out to the local store at ten o'clock at night, figuring it's okay to do so because she lives in a safe neighborhood. But she's just elevated her risk level. If she should get a flat tire, have car trouble—or any number of scenarios that could intervene while she's on the road alone—she is now prey to individuals whose desire is to do harm. Avoid putting yourself in these situations. It's not worth the risk.

2. Don't carry your money in a manner that makes it clear to others that you're carrying cash. In short, don't give a criminal a reason to look at you as prey—don't "flash the cash." Pull out your wallet, quickly extract the needed bills, and pay. Then put your money away before walking out of the store.
3. Don't wear expensive jewelry—even expensive-*looking* jewelry—when it's not necessary. Remember, criminals are watching and observing, and if you are walking around wearing items that could net them a quick "score," you are increasing the chances you'll be victimized. Ladies, if you're intent on wearing jewelry for a formal event, put it in your pocket or purse while

en route. When you arrive, go to the restroom and put it on. That keeps you from attracting attention out in the street or in the parking lot.

4. Don't enter parking garages alone unless they're properly lit. If a garage is unusually dark, it could be because the lights have been purposely tampered with—to make you an easy mark when you enter, headed to your car. If a garage is suspiciously dark, find someone you know and trust to walk you to your car—or ask for security personnel to escort you if there are any in the vicinity. If you still must enter alone, be alert and aware of your surroundings (refer to numbers 6 and 9).
5. When you're out at night, walk in the middle of sidewalks—that is, away from buildings, and away from the curb. This prevents someone laying in wait from grabbing you as you pass. Some kidnappers or killers use vans with side-opening doors. They snatch and grab, pull you into the van, and leave the scene before anyone has taken notice. Again, these people have perfected their art, so they know what they're doing, and they know how to quickly subdue you. Avoid alleys or dark entrances where you can't see if there is a nefarious individual lurking.
6. When walking the streets, through parking lots, or to/from a place of business, particularly at night or in isolated areas, carry a weapon. No,

we're not advocating you walk around with a pistol in your pocket...but a car or house key, carried in a closed fist with the shaft of the key protruding between your index and middle fingers, makes a relatively effective and unexpected weapon that can cut and wound someone who grabs you from behind. If your key ring permits it, splay more than one key between all your fingers and strike with a closed fit.

7. Don't sit in your garage with the door open while chatting on your cell phone. You don't want to get out of your car and find someone standing there, ready to strike. Take the call inside—or close the garage door (and shut your engine) immediately upon entering.
8. Don't accompany strangers, no matter how harmless they may seem. Ted Bundy, one of the most notorious serial killers, looked like a clean-cut, well-mannered man. He was bright and preyed on women who let down their guard around him. He was less threatening than a shaved-head, bearded, tattoo-riddled biker, but he was infinitely more dangerous. Thus, if a stranger asks you to accompany him, for any reason—even if it's to lend needed assistance—politely decline. He can call 911 if he needs help that badly.

This situation is akin to parents telling their children not to go with strangers who claim

they've lost their puppy and need help finding it. We know to tell our children to avoid these people, but adult to adult, we don't always see the same danger lurking.

9. Be aware of your surroundings. Remember, criminals prey on easy targets. The easier the target you are, the more likely you'll be chosen as the victim compared with someone else who follows these safety steps. So what kinds of things make a criminal's job easier? Remember, this is their profession—they've likely done this before and have perfected their approach, so they know what works and what doesn't. Simply put, they're looking for a situation that will net them the highest chance of success. To combat this, be aware of your surroundings. If you're not, they can approach you without concern over you screaming, yelling, running, or striking out at them. Watch for people who are following you. If you're suspicious of a person, cross the street; if they still appear to be shadowing you, quickly find a lighted place where people are congregated. If you make yourself a more difficult mark, the criminal will hopefully leave you alone and will, undoubtedly, look for someone else who is more vulnerable.
10. Use the panic button on your car's key fob remote, if it's so equipped. This button sets off your car alarm and will disorient an offender. When walking to your vehicle alone, have the

remote handy so you can press the panic button immediately. The first few seconds when it goes off may be all you need to survive. If you return to your car with an armload of packages, or if you have young children to strap into car seats, stay aware of your surroundings. Keep glancing around to ensure no one is approaching you.

11. Pepper spray can be an effective deterrent as well. It's readily available and classes on proper usage can be found at your local police department, community college, or self-defense stores. YouTube has videos demonstrating proper techniques.
12. If you're going out alone, make sure someone knows where you're going and who'll you'll be with.
13. Carry a cell phone with a charged battery. Better yet, buy a spare battery and keep it charged and in your purse or pocket. Unfortunately, many cell phones go into "roam" mode when reception is diminished. The phone constantly searches for a nearby cell tower; if it finds a tower owned by a different provider, it goes into "roam," which often uses an analog signal. Both the constant searching and roaming on another provider's network drains the battery extremely fast. Thus, you may have left your home with five "bars" of battery power, but when you pull out your phone to call for help because you have a flat tire or see

someone suspicious, your phone is dead. If you have a spare (charged) battery, pop it in and you're good to go in a matter of a minute.

That said, today's smartphones often don't have removable batteries. The solution is a bit more cumbersome than carrying a thin, spare battery, but it does work well. A portable external battery backup plugs into your device via a USB port and charges up your phone's battery. They're inexpensive and work quickly.

14. Know where you're going before leaving your house or restaurant. Get directions ahead of time. This prevents you from wandering around and appearing lost. The same goes for driving in your car. If you don't know where you're going, or if you're driving in unfamiliar areas, you could easily make wrong turns and end up in neighborhoods that are not safe.
15. Appear confident and able. Walk tall, make eye contact, and project a sense of confidence. The opposite of this gives the impression you're an easy mark who won't put up a fight.
16. Put up a fight. If you're approached by someone, and you sense that something is not right, don't wait for it to "go south" before acting. Look them confidently in the eye and ask them what the hell they're doing—and say it loud. Don't be afraid to scream. Yell. Make noise. Personal safety expert

Michael Bloom says, "It's better to be rude and wrong than polite and right—that is, injured."

17. If you find yourself in a dangerous situation with an offender, making noise might not be enough if the individual has gotten you in a place where he has time to subdue you. You must then fight like you've never fought before. Kick, bite, pinch, poke, thrash...and yell—in a loud and dominating tone. Yelling focuses your mind, gives you confidence, and attracts attention.

Do whatever you must, as fast as you can do it. Do not think it's better to wait for a better opportunity—because there won't be one. Don't believe what you read in books or see on TV. Once an evil-doer has gotten you in his car, or in his grasp, your chances of survival have significantly diminished. So fight and don't stop until he relents or help comes—and mean it. Tear skin. If you're biting, bite to draw blood. Your life really does depend on it. You have roughly four to eight seconds to act—as that's about the time it takes an offender to strike, grab, subdue you and take complete control (get you into a trunk or a van, a cellar, or a backroom).

Remember, the offender wants immediate control and it's your job to prevent him from getting it—by any means possible. He will try to minimize the resistance by saying he only wants your money, that he won't hurt you. Don't

believe it. He's saying this to calm you and to gain control. Never, ever give up control!

The most effective approach, according to Bloom, is using your knees, elbows, nails, and fists with keys (as described above). Use short staccato strikes with the weight of your whole body behind them. Strike through the target, and don't stop until the police pull you off him.

18. A car pulls up behind you with flashing lights. It looks like a police car. But you're in a location where it's dark and deserted. Do not pull over. Instead, acknowledge them with a hand signal and indicate that you're going to keep driving. When you find a well-lighted place with people around, pull over. If it's a legitimate law enforcement officer, he will understand and will not have a problem with you doing this. If he's an imposter, he will not likely want to pursue you in a populated area. Lock the door, roll the window down only an inch or so and ask for their law enforcement ID. Keep the engine running in case you need to bolt. Call the officer's police department, if in doubt, to verify his identity. Do not let down your guard until you are sure the officer is legitimate.

19. Child safety. An entire book can be written on this, but it's important to note that most crimes, particularly against kids, are perpetrated by family, friends, teachers, clergy, neighbors, co-

workers, etc.—that is, someone you or your children know and trust. This is a difficult concept for children to grasp. You don't want them to be afraid of adults, but it's important for them to know there are dangers out there. For older children, stress the importance of communication. If you're dealing with teenagers, who often express their independence by not sharing their whereabouts with their parents, explain the need for them to keep you posted on their comings and goings. Cell phones make this easier than in the past—but tell them that if you call them, they should take the call and not ignore it. They should also notify you if their plans change (when getting a ride home from someone, for example, they should call or text you and let you know).

20. The profiling unit has a division devoted to child abductions. The best defense is, obviously, to prevent an abduction before it happens. For younger children, role play with them so they understand they are never to talk to strangers. Make them aware of the typical ploys criminals use, wherein a stranger will offer candy (or some other inducement) if they come with them, or who will claim he needs help finding his lost puppy. Another tactic is for the offender to approach the child and tell him he's a friend of his mother's, and that his father was hurt in an accident. He tells the child his mother asked him to pick up the child and take him to the hospital.

The overriding rule for your children: they are never to go anywhere with a stranger. Ever. Rather, they should yell and run in the opposite direction. And as with an adult, if they're grabbed, they need to fight back—loudly—in any way possible.

Home Safety Checklist

Your home is your castle. You don't need a moat, but common sense tips can work wonders.

Back when you were a kid playing "tag," you could always run to "home base" and escape from your pursuers. It was where you were safe, where no one could, literally, touch you. In reality, your home should be a place where your ultimate safety lies. If you pay attention to some simple steps, you can maximize the chances it'll remain that safe haven you want it to be.

1. Lock your doors *and* windows. If you have a ground floor or live on the first floor, do not leave your windows open when you leave the room. This is easy entrance for any criminal: an open window is like an unlocked door, only worse—because it's plainly visible as an easy mark from the outside. A criminal doesn't know a door is unlocked unless he tries the knob.

2. Get a dog. Dogs bark, they make noise, and they protect you. Simply put, you're their meal ticket. Thus, even the laziest and least intelligent of dogs are motivated, at an innate level, to keep you around. And they protect their turf. Their hearing is five times better than humans, so they will sense a trespasser before you would even know he is in the vicinity. Beyond that, a dog represents an obstacle the criminal must weigh when determining if he wants to target you. For the offender, there will always be another home that does not have a dog—making the choice to leave yours alone an easy one.
3. Install good lighting around your house. If someone wants to steal from you or do harm after dark, they certainly would prefer not to do it in the light, which increases their chances of getting caught. If you're concerned about electricity usage, putting the lights on motion sensors is helpful because it turns the lights on when movement is detected. Alternatively, you can put the lights on light sensors so they come on when dusk sets in and go off when the sun rises.
4. Trim bushes to a low level, to give clear line of sight of the immediate area. If you make it difficult for a criminally inclined individual to hide or lay in wait, they may choose somewhere else to "hit" that's an easier mark.

5. Draw curtains, blinds or shutters when night falls. When it's dark outside and the lights are on inside, the interior of a home is easily seen. Closing window coverings prevents offenders from seeing into your home and taking note of who is at home, how many people are there, the ages of your children, where you're located, etc.
6. Install a burglar alarm. The costs of an alarm have come down significantly because of wireless technology, which has largely eliminated the need for running wires. If you can afford to have it monitored by an outside agency, they will notify the police if your alarm goes off. At the very least, even without monitoring, a blaring alarm increases the risk a criminal will get caught. Most offenders would thus prefer to find a house with lesser risk—that is, no alarm.
7. Place a security camera in plain view at your front door and, if possible, at other points around the house. These have become significantly less expensive recently, and you can now buy wireless cameras. But—even if they are not hooked into anything (i.e., they are "dummy" cameras)—the criminal may not know this. Hopefully, the presence of cameras will motivate him to seek out other targets.

8. Install a fisheye lens in your front door. They're inexpensive and easy to install in most doors. They allow you the ability to see who's at your door without opening it. Whatever you do, DO NOT open that door unless you know the person standing there. Even if you're expecting someone to arrive shortly, take a look through the lens before turning that knob. It might not be who you think it is.
9. Are people really who they appear to be? Appearances can be deceiving—which is why this is a successful tactic used by criminals. If someone in uniform (law enforcement or a utility worker—gas, electric, water, etc.) comes to your door unexpectedly, without an appointment, ask for identification before you open your door. Call the department or company's home office to ask if they sent this particular individual to your home—then schedule another time for the individual to return.

No one should enter your house without a prearranged appointment unless it's an emergency. And if it's an emergency, and there's a police officer at your door, he or she will understand if you have to call their department to confirm the need for them to be there. Another common tactic is for an

imposter to ask to use your restroom or your telephone, or to get a drink of water on a hot day. Sorry—the answer *must* be no. No exceptions, no matter what they say.

10. Do not open your door to solicitors, no matter how many pages of official looking papers they hold up to your fisheye lens. Many of the companies who hire these armies of solicitors do not do background checks on the people they hire as independent contractors to solicit you. They bus them around the country and then unleash them on your neighborhood. There are documented cases of women being raped by people working for these companies. Once you open your door and give them entry to your home, you're at a distinct disadvantage.
11. When no one is home, put your lights on timers. Timers plug into the wall and your lamp plugs into the device. You then set the times for when the lamp will turn on and off. Spend a little extra for the kind that allows you to have the light go on/off multiple times through the evening hours and put a timer in different rooms of your house. Varying the times gives the appearance that someone is at home. This is not foolproof, but it's better than a darkened house that yells "No one's home."

12. Ask your neighbor to pick up newspapers and flyers left in front of your house. A pile of newspapers is a telltale sign you're away. It's better to have this neighbor take in your mail as well. It's possible to place a hold on your mail and newspapers, but keep in mind that sometimes criminals work in tandem with people who work at companies/post offices that take vacation requests for newspaper and mail holds. Placing holds is better than having the papers pile up at your house, but there is some risk involved.
13. When being picked up by a car service for the airport, if you live in a residential neighborhood, keep in mind that the driver now knows what house you live in and that you're headed out of town for a period of time. Bad deal. It's better to wheel your suitcases down the street from your house and have them pick you up there. And don't give your address when scheduling the car. Give them the intersection where you'll be waiting for them.

Protecting yourself from identity theft

Who does it, what it means to you and your life; prevention

Identity theft is a continuing problem. To give you an idea of its scope, between eight and ten million Americans fall victim each year, at a cost to individuals

and businesses of between \$37 and \$56 billion. How mainstream has identity theft become? Social Security numbers ("SSN") have been auctioned on eBay, and an Internet search for "fake ID" yields dozens of offshore operations hawking holographic identification cards that look authentic.

Who is behind this? The usual cast of characters: crack addicts, methamphetamine users, organized crime, nefarious individuals...and other governments. Identity theft has become an international problem: rings of thieves based in countries such as Russia steal, and then sell, your personal information in vast networks of organized crime circles. Law enforcement recently busted a professionally organized syndicate that utilized a corporate executive structure and a web-based login system that allowed criminals to purchase blocks of stolen identity information for predetermined prices.

A more recent problem is country-sanctioned computer hacking. These hackers aren't your old-time pimple-faced geeks holed away in a basement. They are government-sponsored "hacker armies" who plant malware on computers worldwide designed to commandeer your credit card and identify information; they park stolen information on the PCs and Macs of innocent people, then pick up the information at a later date. This stolen identity information is used to fund terrorism and government operations. Although China has denied it, industry security professionals have identified them as one of the prime culprits.

Thus, the problem is multi-faceted. First, a variety of personal information is exposed on the web by individuals, companies, and government agencies. Identity thieves find this data using search engines in a technique known as "Google hacking." In one study, using Google for less than an hour, participants exposed sensitive information on nearly 25 million people. They unearthed names, birthdates, SSNs, and credit-card information. Google hacking has inspired the creation of how-to web sites and books, which outline the process of submitting targeted search queries with specific commands to elicit sensitive information. Using one of the guidebooks, a computer user with average experience could master the skill in less than an hour.

Companies that aggregate personal information on you must take reasonable steps to protect that data to preserve your privacy. Some free email services have come under fire in the past because they search email messages for data that they then aggregate and sell to companies who market targeted ads to you. You may think that's fine (everyone is different), but the problem is that once that data is collected and tied to you, it can be used for means we can't even conceive of at present because the technology to exploit that information hasn't yet been invented.

Another area of concern is a newer tracking technology that you probably haven't heard much about—nor has Congress, apparently, because they have not yet outlawed it. At present, it's impossible to protect yourself from it, since it's tied to a unique combination

of identifiers from your computer's hardware. At the time of this writing, it's just now being studied in terms of potential abuses and what can be done to prevent it from being used as a tracking device. The point is, with technology changing weekly, challenges will continue to confront us.

Another threat comes from foreign countries that have been regularly launching cyberattacks against the US and its companies. This has been in the news the past year or so, but it's been going on much longer. The problem is that they've gotten more pervasive, and they're being launched successfully by enemy states (e.g., Iran). The offenders' goals are to: steal corporate secrets; get into government sites in preparation for future attacks; launch denial of service attacks; steal personal information (which facilitates identity theft); compromise our national security. These attacks occur daily, and most go unreported because no one wants to declare that their systems have been hacked—it's bad for business and it's bad for the government to admit it's been compromised. China, unfortunately, is a major offender, even though they continue to deny it. The US has stepped up its defenses, but FBI executive assistant director Shawn Henry stated in April 2012 that cyber criminals are too smart, and our defensive measures too weak, to stop them. He stated that a secure unclassified computer network does not exist in the US.

There's not a lot you can do about your personal data hanging out on the Internet and its resulting vulnerability. There are companies that you can pay to

monitor your financial accounts and alert you if there is a problem. But there are also things you can do to help yourself thwart identity thieves. Here are 24 tips; not all will apply to you, but many will prove invaluable:

1. **Obtain a locking mailbox.** Thieves troll neighborhoods looking for credit card statements, checks, credit card offers, and the like. An unlocked box is an invitation for years of headaches.
2. **Do not list your address or phone number on your checks.** Your names are sufficient and banks will comply with this request. (Note: if you use online banking, the address of record on your account will likely be printed on the checks the bank mails on your behalf.)
3. **Do not list your home address on your driver's license** or other ID in your wallet. Wallets are lost and stolen, and the last thing you want is for the thief to know where to find you should he want to return for more.
4. **Do not keep your home address or other personal information in your car.** Cars are broken into and stolen. Check your insurance and registration cards; if your address is there, cut it out.
5. **Do not carry your SSN in your wallet.** More on this later.

- 6. Obtain a shredder.** Did you know that your trash is sorted at state prisons? That means those pre-approved credit card solicitations you receive are passing through the hands of convicted criminals. Buy a cross shredder that slices and dices your sensitive paperwork and unwanted/old credit and ATM cards into confetti. Here's the litmus test: if a criminal came to your door, what wouldn't you want him absconding with? That's what you should shred, rather than just dumping it in your garbage. In short, shred all mailing labels that contain your name and address, any account numbers, paperwork with your kids' information (schools they attend, etc.), bank or brokerage statements...and those pesky credit card or loan solicitations.
- 7. Obtain a Private Mail Box ("PMB")** for use when ordering materials online or over the phone. This prevents you from listing your home address on a company's server—which may be hacked or otherwise compromised by shoddy security. (Change your credit card address to the PMB, because online orders will kick back your purchase if the shipping and billing addresses are different.)
- 8. Don't put personal information in emails.** Email is NOT secure. Home addresses, bank or investment account numbers, social security numbers, and passwords are best exchanged via

fax (careful of “public” fax machines; alert the recipient of its impending arrival) or by phone. Many financial institutions use secure email systems for communicating with you, if necessary. But don’t think that email is any different from passing around an unsealed envelope. Anyone who cares to look can do so. Likewise, your attached documents are not secure unless they are password protected.

That said, a word of caution: while Microsoft Office uses strong security algorithms to protect the contents of its documents, the encryption that Adobe Acrobat uses to lock down its PDFs is ineffective; Acrobat, in fact, tells you this the first time you password protect a file: it states that third party software (non-Adobe programs) might be able to open the “protected” document. Well, excuse us—that means it’s not secure at all. A much better alternative we’ve found is Foxit PhantomPDF. According to our cybersecurity cryptographer, this PDF software uses the same encryption that Windows uses, which is very strong.

9. **Your medical records are sometimes handled by an outsourced company**—which could be in India, Ireland, or Pakistan. While you sign a privacy agreement with your physician, a transcriptionist in Pakistan could be typing up his reports. What’s in your medical records? Personal

information. Only provide your doctor's office with need-to-know data. They don't need your SSN or driver's license number.

- 10. Do not click on a link in an email you receive from your financial institution.** In "Phishing," thieves send emails that purport to be from your bank asking you to log in to your account to verify/update information or correct an error. They include a link to the page where you can access your account; but this link takes you to a look-alike website that's logging every keystroke you make—and stealing your username and password. Protect yourself: go directly to the bank's website yourself or use a Favorite you've bookmarked.
- 11. Do not give out your SSN** unless you're dealing with the IRS or another government agency that demands it. For financial institutions that request it for identification, only give them the last four digits. They'll then ask for other identifiers they have in your record (birth date, mother's maiden name, etc.).
- 12. Call your credit card company or bank if a new card or an account statement is late.** A missing card or bill may mean someone called the company using your name and changed the billing address to prevent you from catching their shopping spree.

13. Order a **free copy of your credit reports** once a year to check for errors: Equifax (www.equifax.com), Experian (www.experian.com), and TransUnion (www.transunion.com).
14. Use a **credit rating monitoring service**. There are companies you can hire, for an annual fee, to monitor your credit. Thus, if someone attempts to open a credit card or take out a loan using your SSN, you will be alerted. These services are useful in protecting you from unauthorized access to your account.
15. If you suspect you've been victimized, **immediately file a report with local police**, or the police where the identity theft took place. Get a copy of the report (or report number), as you'll need it when filing a theft affidavit. Your bank, credit card company, and soon-to-descend collection agencies will require this affidavit for each fraudulent transaction incurred.
16. When choosing passwords, **don't use easily-obtained information** like your birth date or zip code. Do not use real words; include a symbol, a number, and a combination of capital and lowercase letters. This is called a "strong" password.

- 17. Watch your laptop or tablet.** Your computer contains more personal information than you think. Leaving the information unprotected—and your laptop unsecured in public places—is akin to giving a thief the keys to your private life, and personal data. Items to consider: LoJack for laptops, which places a piece of code in the computer BIOS (the computer's hardware operating system) that allows law enforcement to track the laptop if it's stolen.
- 18. Encryption software.** There are software programs that allow you to encrypt (scramble, and thus password protect) portions of your hard drive. Information saved in these folders is unavailable to the prying eyes of thieves unless they know your password. A good, free program is TrueCrypt, available at www.TrueCrypt.org. Don't forget about the easiest of all: Microsoft Word (version 2007 and later) use the newer .docx file format, which allows you to encrypt your important documents with a password. The former head of the Office software suite told us that Word encryption was excellent and very secure.
- 19. Shred electronic files with personal data.** With more banks and brokerages providing electronic delivery of documents, it's important to be careful when deleting, or throwing out, these statements (or other files containing personal information).

Merely deleting the file does not delete it. It places that file in your recycle bin. But emptying the recycle bin does not delete it permanently, either. It merely removes the computer's reference to that file. It's equivalent to erasing a chapter's entry in a book's table of contents—but leaving the chapter in the book. You may not know where to locate it, but the chapter (your deleted file) is still there. Here's the fix: a free program called Eraser (from Heidi Computers at <http://www.heidi.ie/>) electronically shreds any personal information left on your PC by writing over the data multiple times with ones and zeroes.

- 20. Use anti-spyware software and internet browsers with anti-phishing filters.** Regardless of whether you use a PC or Mac, spyware and phishing are real threats. Internet Explorer (version 7 and later) has an anti-phishing filter. Good anti-spyware programs include Spybot - Search & Destroy and Ad-Aware personal edition. Both are free, but do not perform automatic scans (that is, you have to manually run them). Another excellent free program is Ccleaner, which securely removes cookies and temporary internet files as well a host of other data you leave behind on your hard drive. It can be set to automatically run when the PC starts. Spybot, Ad-Aware, and Ccleaner are all available to download from www.Download.com, a

reputable download site owned by CBS. Webroot's SpySweeper and Window Washer are paid programs that do the same thing, but require an annual subscription.

21. Use a secure browser. Internet Explorer 10 has special browsing modes called “InPrivate Browsing” and “InPrivate Filtering.” The former, also known as “Stealth Privacy Mode,” prevents the browser from storing your history, temporary files, cookies, passwords, etc. related to that browsing session. (Since some websites view this material on your PC, your data is not safe, or private.) The latter prevents websites from identifying you as having visited their site. The two can be used simultaneously.

22. Anti-virus software. A good (free) program is AVG Free, from Grisoft. Another highly rated free program is Microsoft Security Essentials. Both are available from www.Download.com. These programs perform automatic scans and real-time email scanning. There are other, paid, antivirus programs that work well and offer some additional benefits. Examples include TrendMicro PCcillin; McAfee; ZoneAlarm.

23. Keep current on privacy and identity theft issues. Consult www.worldprivacyforum.org, an excellent resource for keeping tabs on privacy information, issues, and pending legislation.

24. Read the privacy policies for your search engine, internet, and email providers. Pay attention to what's stated, as well as what isn't. There are a lot of choices for these services, so if what you read doesn't sound like the company is truly protecting your privacy rights, use a different provider. One clause to pay attention to is how they use your information—do they share it with (or sell it to) business partners, affiliates and subsidiaries? This is your personal information. You should be the one to choose how it's used and aggregated.

You may think it's okay if they store the search you made for that new car, but when companies aggregate your data, they build an extremely comprehensive profile of you that can be sold to others—your hobbies, purchases, beliefs, social activities, affiliations...there's virtually no end to the info they gather on you. This is the first time in world history so much information about individuals' private lives has been available for sale.

Have we crossed the line into paranoia? Consider this: a dozen years ago, when identity theft was beginning to become a problem, one of us moved into a new house. The home builder erected a plain mailbox, and shortly thereafter our bank mailed several boxes of new checks to us. We only received one.

The criminals, who drove around neighborhoods riffling through mailboxes for bills, credit cards, checks, and the like, stole the blank checks, created fake IDs, and used them at a variety of retailers including Safeway, Home Depot, and Wal-Mart. They then printed more checks via mail-order check printers using the bank account number. They sold these checks to other criminals. Because of alert staff at Home Depot, a woman attempting to write a check was caught and arrested. Not surprisingly, the thief was a methamphetamine addict who lived about 45 minutes away. It took a year and a half before credit agencies and debt collectors finally stopped their harassment.

The situation would have been far worse had they gotten hold of a social security number. If an identity thief gets your SSN, your credit is destroyed forever. In rare instances, the government has issued new SSNs, but your destroyed credit on your "old" number does not get eradicated. Identity theft victims with impeccable credit have been unable to buy homes, cars, and other large-ticket items.

It is our responsibility to take the necessary steps to protect our personal information. Just like we lock our doors when we leave home, we must lock the areas of entry into our personal information. Failure to do so could result in years, if not a lifetime, of headaches, wasted time, and ruined credit.

Keeping your online presence secure

We go about our normal day to day activities without much thought to the numbers and passcodes we use to access our financial accounts. But if a criminal obtains these passwords, he can unlock vast amounts of money housed in the your checking, savings, brokerage, and/or credit card accounts. These passcodes take two forms: PINS, or personal identification numbers, and passwords.

PINS are four digit numbers that have been used for decades in financial transactions. The way they're used, however, from newer, high tech ATM machines to the internet, has evolved. So has the technology behind them. This is both to our advantage and disadvantage; while we benefit from faster and better processing, the criminals have learned how to exploit these advances.

There's little you can do to prevent theft on the technology end. But there are a number of steps you can take on the mental end to thwart a thief from obtaining it:

- 1- First, and perhaps most importantly, choose a PIN that's not easily guessed. This seems obvious, but—as hard as it is to believe—nearly 11% of people use the PIN 1234. Other frequently used PINS are equally guessable: 1212, 7777, 9999, 0000...you get the picture. Don't make a criminal's job easier. Choose a number that has no commonly known relevance to you (like a birth year or anniversary year).

- 2- Don't share your PIN with anyone other than your spouse; in fact, if you're speaking with your bank and they ask for your PIN, there's a problem because they don't need it to access your account. Rather than providing it, ask to speak with a supervisor.
- 3- Don't start your PIN with a zero or one, and don't repeat numbers (like 5776). In short, if it's easy to remember, it's probably easy to guess.
- 4- Don't write your PIN down, unless it's in a password-protected Word document or a secure password program; likewise, don't keep it in your wallet or car.
- 5- Although many financial institutions have taken steps to house ATMs inside semi-secure rooms, data entry terminals in stores are not protected as such. Bottom line: cover your hand while entering the pin on the keypad to prevent others from seeing the numerals that you're pressing.
- 6- Don't use the same PIN for multiple cards, or multiple devices (smartphone, iPad, etc.).
- 7- Perhaps most importantly in a booklet dealing with personal safety, if a criminal obtains your PIN (such as by watching your hand movements), you will become a target: this type of offender will likely be motivated by money, so his objective will be obtaining your wallet. But it's not worth putting yourself in danger.

Passwords, like PINS, are the keys to our transactional activities on the internet. But too many people opt for “weak” codes that are easily guessed, like “password” (no joke), “admin,” “qwerty,” or, as with PINS, the old “1234” standby.

Passwords that are easy to guess are considered “weak.” Likewise, those that are difficult to crack are called “strong.” Often, cybercriminals use password-cracking tools that utilize algorithms and patterns to break the code. So what can you do to avoid a weak password and how do you create a strong one?

- 1- Avoid using words that appear in any language dictionary. The aforementioned software does a quick search of known words. Eliminate this threat by using phrases that cannot be found in a database.
- 2- As with PINS, don’t use years or other numbers that have relevance to you, your family, or your life.
- 3- Avoid using the same password with multiple accounts. If an offender gains access to one, he would have access to the others, as well.
- 4- Don’t use words spelled backwards or common abbreviations.

- 5- Generally, you want to use both capital and lowercase letters, numbers, and symbols (for example, a dollar sign or an ampersand).
- 6- There are a number of conventions and tricks for creating strong passwords. Here's one: think of a sentence you remember from your childhood. Take the first letter of each word and then add a numeral for the number of words in the sentence. Thus: Mary Had A Little Lamb Whose Fleece Was White As Snow becomes Mhallwfwwas11. (Don't use this example as it's for illustration purposes only; it's too simple and the number of words is eleven, which is a repeated number.)

Other tricks like this one can be found on [Ascentor's website](#) or in this [Consumer Reports article](#). After you've created your masterpiece, go to [Microsoft's Safety & Security Center](#) to check its strength. Type it into the password field and it'll automatically judge how good it is.

- 7- Change your passwords periodically.

In closing

An ounce of prevention is worth a pound of cure.

So there you have it. There's a lot of information here—but remember, the concepts are important. If you understand how criminals think, you'll start to see things

differently—and figure out your own ways of protecting yourself.

One important caveat: if, for some reason, an offender targets you and is determined to do you harm, he will find a way to accomplish his goal. Unless there are special circumstances involved, most criminals are not committed to targeting you specifically, and will be deterred by the safety steps outlined above.

Consult this pamphlet periodically to refresh your memory regarding those items you may have forgotten. Most importantly, we give you permission to share this document with those you know and care about. **If you intend to forward, email, or post the article in any manner, it must be sent and/or posted in its entirety, and without alteration.**

The safety tips discussed above *do* save lives—and a lot of heartache. Keep in mind that you often don't know when you've been targeted, and when the steps you've taken have successfully warded off an offender. But whether or not you're aware of how these steps may have helped you, understand these are tried and true methods. And they may just keep you alive.

An ounce of prevention really is worth a pound of cure.

About the authors



Alan Jacobson

Alan Jacobson is the national bestselling author of the critically acclaimed thrillers *False Accusations*, *The Hunted*, *The 7th Victim*, *Crush*, *Velocity*, *Inmate 1577*, *Hard Target*, and *No Way Out*. Alan's novels have been named to numerous "Best Books of the Year" lists, including the "Top 10" for *Library Journal*, *The Strand Magazine*, *Suspense Magazine*, and the *Los Angeles Times*. Alan's eighteen years of research and training with the FBI, DEA, US Marshals Service, SWAT, and Scotland Yard have influenced him both personally and professionally, and have helped shape the stories he tells and the diverse characters that populate his novels. Several of his novels have been optioned by Hollywood.

Visit him at www.AlanJacobson.com and follow him on [Facebook](#) and [Twitter](#).



Mark Safarik

Supervisory Special Agent Mark Safarik recently retired as a senior member of the FBI's elite Behavioral Analysis Unit. Agent Safarik has over 30 years in law enforcement, 23 with the FBI and the last 12 as a Senior

Profiler. He is now Executive Director of Forensic Behavioral Services International, a consulting firm in Virginia specializing in the behavioral analysis of violent crimes. Agent Safarik was awarded the Jefferson Medal from the University of Virginia for his internationally renowned research on the sexual assault and homicide of elderly females. He is also a member of the Vidocq Society, a nonprofit group that assists law enforcement in resolving difficult, unsolved cases.

Agent Safarik has appeared on Dateline, Court TV, Forensic Files, The Discovery Channel and Nancy Grace's *Under Investigation* and has trained over 20,000 professionals in Europe, Africa, South America, Russia, the U.S. and Canada. His television series, *Killer Instinct*, aired on both NBC's Cloo network and Biography Channel, and is now available on iTunes. More information is available at www.FBSInternational.com.

● *The authors also wish to acknowledge the assistance of martial arts instructor and personal safety expert **Michael Bloom** with portions of this booklet.*

