This is my first major submission for publication, so please be patient. You need to know that I am almost completely computer illiterate and that my hacks are probably what most of you would consider to be relics from the Pleistocene epoch, but if I understand the term correctly, a hack is neither about modernity nor technological sophistication. Rather, it is a way of thinking about and looking at the world. The way most self-described hackers, not to mention the publishers and editors of this magazine, use the word, it is someone who circumvents obstacles, or even more broadly, solves problems. It is someone driven by curiosity to discover how something works and, depending on the circumstances, either improves it or neutralizes it.

I am serving 292 months for a terrorism-related offense, and have written a book entitled *Framed* about my experiences. In it, I detailed some hacks that either I or somebody else used in the real world between 1990 and 1999.

On the rare occasions when professionals from the intelligence community comment publicly on these techniques, they usually roll their eyes and imply that such activities are embarrassing comic-book anachronisms. The truth is, these techniques are still taught and practiced by every major intelligence and counterintelligence service in the world. Collectively, these techniques are referred to as “tradecraft” and continue to be part of modern espionage curriculum because A) they are simple; B) they are cheap; and C) they still work. I found out the hard way what works and what doesn’t. Learn from my mistakes.

When I first wrote this article, I thought I could be both inclusive and concise, but I was over 3,000 words and wasn’t half finished, so I will have to cut it down to just a couple of hacks that I used successfully, or otherwise.

One of my favorite hacks which I used frequently, albeit unintentionally, was to habitually ditch FBI tails. In their reports to their superiors, they breathlessly informed them that I was “surveillance conscious,” but it was really just the way I drove. I hate being tailgated or feeling rushed, so I regularly took back roads and drove comparatively slowly, so they were continually having to “terminate surveillance.” This simple technique really works; get in the habit of using it. Other common vehicular counter-surveillance techniques are frequently pulling over (ostensibly to consult a map), executing U-turns, pulling into driveways, and doubling back - and, if you are really suspicious, prepositioned observers surreptitiously watch your progress for tails. This can be done in either rural or urban settings.

A simple but effective counter-surveillance method I always liked was originated by Whittaker Chambers, the Communist spy turned informer who helped put Richard Nixon on the map. This method is best used in a suburban setting. Albert is walking south on Elm Street, while Ben is walking toward him northbound, also on Elm. They can each see for several blocks behind one another and can mutually observe any tails, either vehicular or on foot. When they are parallel to each other and there is no surveillance detected, they give one another a prearranged signal, (scratching nose, pushing up glasses, coughing, etc.). If surveillance has been detected, they pass no signal at all. It is confusing, but a signal means all clear, no signal means you have a possible tail. To be doubly sure, they can check one another for tails again by proceeding in the same direction on Elm for a couple of blocks, then each turning east (or west), proceeding on two more blocks to Broadway, and again turning towards each other. This time Albert headed north and Ben is headed south. If the same person or vehicle is still trailing either of them, there is a problem. The process of losing a physical tail is called “dry cleaning.”

In my original article, I profiled many more examples of tradecraft, but there just is not sufficient space. Therefore, trimming as much as possible on the subject of secure communications, a good rule of thumb to remember is the faster and more convenient it is, the less secure it is. In descending order of security, they are dead drops, face-to-face meetings, radio, mail, telephone, and Internet. I understand that this is
difficult advice to follow for a magazine whose readership consists of the hacker community, but if you want to stay out of trouble, keep off the phone and computer.

A dead drop is a physical site where information is dropped off for future retrieval without any interpersonal contact. For this reason, most professional spies prefer the dead drop. They can be in a rural or remote setting or in the middle of a city. During the Cold War, Central Park in New York City was a favorite dead drop venue for Communist bloc spies using the UN as a diplomatic cover. Cemeteries are also popular sites because they are usually sparsely populated and yet being in one arouses no particular suspicion. The usual procedure is for the person delivering the data to drop it off at the site, quickly move on, and be nowhere in the vicinity when it is picked up. This is so neither party can recognize or identify the other.

Face-to-face meetings are the next in order of security. If the person you are meeting is not betraying you and the meeting is not being monitored, you should be safe. Of course, if your contact is betraying you, no security measures are adequate. An old favorite trick for face-to-face meetings is to provide your contact with cheap nylon or canvas gym bags or similar accessories which are identical to your own. If you meet in a public venue, both of you bring your bags and exchange them, and of course their contents, during the course of the meeting. This can be easily done and is difficult to detect. If you set up such a meeting in a restaurant, library, public transportation, movie theater, or similar venue, make an effort to sit in an area away from concentrations of people. If someone enters shortly after you do and walks past more convenient seating in an apparent effort to sit near you, both of you get up and leave and go to a place selected randomly out of the phone book. Remember what the possible eavesdropper looked like; if you see him later, you are being tailed.

Radio is your next most secure means of communication. I saw a method of radio communication with which I was very impressed at a seminar in 1993. I am sure it is much more highly evolved now. The exhibitor had a laptop computer hooked up to a handheld ham radio transceiver. A typed message was sent via radio in what was even then a very brief transmission and received by a similar rig a mile away. Spies refer to such a compressed transmission as a "squirt." I doubt if the motivation of the inventor was circumventing surveillance - it was probably just reducing time between transmissions - but the effect is the same. Using encryption and techniques such as troposcatter, such transmissions can be almost impossible to detect, much less counter. If you do choose this method to communicate, do not transmit from your house. That is why you are using handheld transceivers and if you devise a set of random locations from which to transmit, make sure your house is not in the geographic center of the circle, triangle, quadrangle, or other geometric shape your transmissions are generating. I thought very highly of this system and the only drawbacks I could see were cost and the fact that you must be licensed and registered with the FCC in order to transmit on ham frequencies. Of course, the penalties are negligible and the chance of apprehension is remote, but I still don't like it. If you are a prepper, make your ham base station out of heavy, clunky old vacuum tube transceivers from the 50s and 60s. They are almost indestructible and will withstand an EMP burst even if they are turned on and in use during a nuclear strike. The handhelds won't.

Mail is probably the least appealing method to a high-tech readership, but it has the advantages of extreme elasticity, reasonable speed, and reliability along with fairly high security. One mail hack I used successfully was to send a postcard of a certain well-known local landmark to all of the members of my group, with a coded message on the back. At the next meeting, they were all greatly mystified about the strange postcard they had received. I explained that I sent it and that it was a simple arrangement for a rendezvous. The photograph on the front of the postcard specified the location of the meeting, and the text of the note on the back specified the time. On this occasion, at least, the message was received with 100 percent reliability.

While on the subject of using the mail for covert communications, allow me to give you some strange advice: don't throw out your junk mail! On the contrary, make an effort to accumulate as much as possible. Dozens of businesses have thoughtfully provided you with bulk mail envelopes with your name and address on them. Gather them up and distribute them among your contacts, and have them do the same with you. You can steam open the junk mail envelopes, insert any message you wish, reseal them, and drop them in the nearest mailbox. The post office will obligingly deliver the message to your contact in the most non-threatening format imaginable.

If the FBI or USPS are doing a mail cover on you, all they will do is record the name and address of the sender and possibly photocopy.
the envelope. Junk mail from magazines, charities, politicians, and others will not get a second look. A warrant to actually open mail is much harder to get, but junk mail will still receive a low priority. Concerning rescaling envelopes, if you use egg whites as an adhesive and allow it to dry, the envelope cannot be steamed open.

One of my favorite methods of using the mails was originated by organized crime. The FBI had been monitoring the communications of several suspects for a long period and the only common denominator among them was that they all used the same dry cleaner in Las Vegas. The FBI intercepted the parcels and minutely examined them, but could find no messages. The only thing the parcels contained were dirty clothes. The solution smells like the work of an informant rather than painstaking police work to me, but eventually it turned out that the clothes themselves were the message. Number and color of shirts, short or long sleeves, cotton or linen, size, missing buttons, etc. all comprised the coded message. But the wise guys were too wise by half. Think about it: why would someone in Williamsburg or Cicero even need to use a dry cleaner in Las Vegas? It was way too elaborate, but you can use the same principle successfully. Instead of sending dirty clothes, let the letter itself be the message. Size and color of envelope, size and color of paper, watermarks, number of pages, writing on one or both sides, color of ink; machine printed, hand printed or written in cursive, font type, and even odors can be used to convey the message. This way the entire gestalt of the letter becomes the message, not the content of the text. In fact, the actual text can be used to confuse, misdirect, and disinform.

Telephone communications are so easily compromised that I can only recommend two simple hacks in good conscience, neither one of which involves actual conversation. The first is the ring code, which at prearranged times the called party allows the phone to ring without picking it up. The number of rings is the code. If you have Caller ID, the ring code can be used at any time. Let the phone ring twice, exhibiting the incoming number as an authenticator, then immediately call back with the ring code. This method has obvious limitations.

The second telephone code is the “silent call.” In this case, the called party answers the phone and is met with silence. The duration of the silence is the message; the caller terminates the message by hanging up after the appropriate interval creating a dial tone. In a country with a properly functioning criminal justice system, intercepted wiretaps of such events would not be allowed into evidence; they are simply too ambiguous. Unfortunately, that does not describe 21st Century America. Why do you think the book is entitled Framed? The coded calls will probably be admitted, but their significance can only be speculated upon. Ultimately, there is only silence.

I know this next part is heresy if not blasphemy, but to me the Internet seems as if it were deliberately designed to be compromised. I would not use it for any but the most innocuous, vanilla communications. Yes, I know about encryption and steganography, but I still do not trust it.

My last hack is probably the most important and definitely the most low-tech. In fact, it is no-tech. It predates the wheel. It predates fire. It is your own instincts. I knew something was wrong every time the CRI (Confidential Reliable Informant) brought up the subject (and he always brought it up - I never did). I got a painful knot in the pit of my stomach. Like Captain Ahab, all good angels were mobbing me with warnings, but I foolishly allowed the veneer of sophisticated modernity with which I was brought up to drown out the vocalizing primate that was shrieking away inside my cranium.

There is nothing supernatural or irrational about this. In fact, it is the most natural and rational phenomenon in the world. It is hundreds of thousands of years of hard-learned survival instincts trying to break through the shell of rationalization and denial. It was my subconscious trying to assert itself and picking up on the rat's own subconscious cues.

You know yourself. You know the difference between nervous excitement or the thrill of the chase and a feeling of dread and impending doom. If I had listened to these hacks, I would not be here now. Listen to your instincts; they are still there in spite of all of the high-technology double-edged swords with which you are smothered. Those long dormant urges and hunches may be wiser than your deepest conscious thoughts. If something seems wrong, something is wrong.

I apologize for exceeding my allotted space, and I hope these examples meet with your definition of the word hack, and that you may profit from them. Good luck, and all hail the New World Order.

**HACKER PERSPECTIVE submissions are closed for now. We will open them again in the future so have your submission ready!**