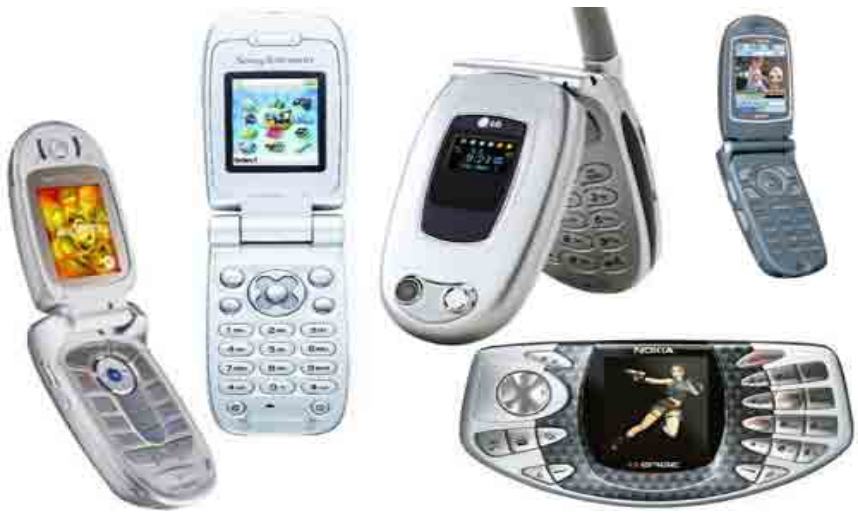
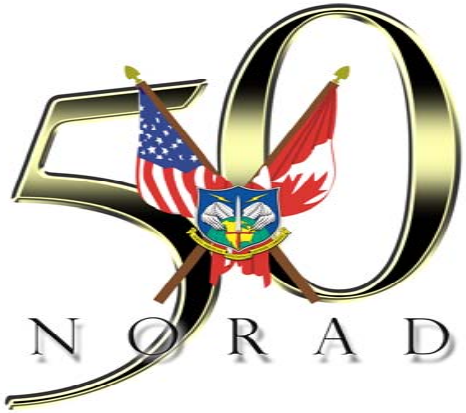
CELL PHONE

VULNERABILITIES!



Created By, And with Great Appreciation to:

Ms Cora Ann Metz
SOCSOUTH Command Security Manager

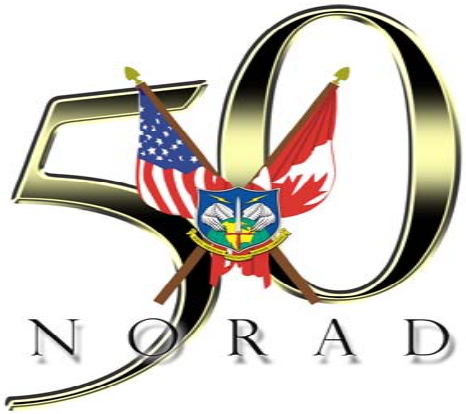


Be Aware! Your cell telephone has three major vulnerabilities

1. Vulnerability to monitoring of your conversations while using the phone.

2. Vulnerability of your phone being turned into a microphone to monitor conversations in the vicinity of your phone while your phone is inactive.

3. Vulnerability to "cloning," or the use of your phone number by others to make calls that are charged to your account.

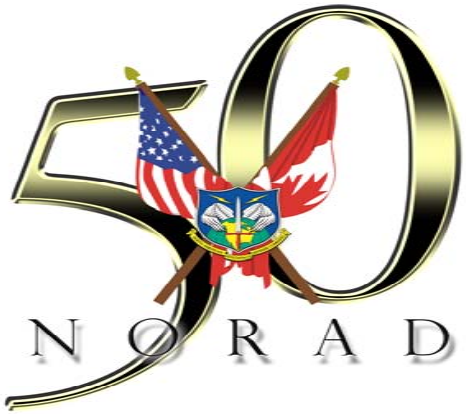


VULNERABILITY TO MONITORING:

- All cell telephones are radio transceivers. Your voice is transmitted through the air on radio waves.

- Radio waves are not directional -- they disperse in all directions so that anyone with the right kind of radio receiver can listen in.

- Although the law provides penalties for the interception of cellular telephone calls, it is easily accomplished and impossible to detect.

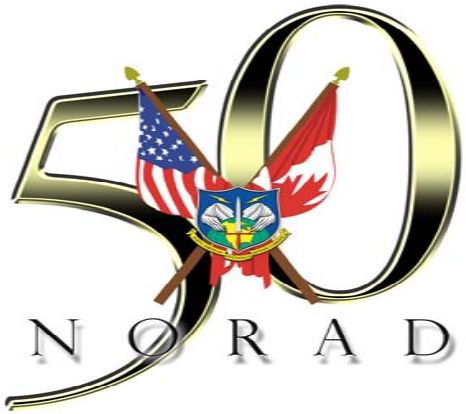


VULNERABILITY TO MONITORING:

- Radio hobbyists have web sites where they exchange cell phone numbers of "interesting" targets (**YOU**). Opportunistic hobbyists sometimes sell their best "finds" (**YOU**).

- Criminal syndicates in several major U.S. metropolitan areas maintain extensive cell phone monitoring operations.

- It is easy for an eavesdropper to determine a target's (**YOU**) cell phone number, because transmissions are going back and forth to the cell site whenever the cell phone has battery power and is able to receive a call.



CAR PHONES

- For a car phone, this generally happens as soon as the ignition is turned on.

- Therefore, the eavesdropper simply waits for the target (**YOU**) to leave his or her home or office and start the car.

- The scanner immediately picks up the initial transmission to the cellular site to register the active system.

- The number can be entered automatically into a file of numbers for continuous monitoring.

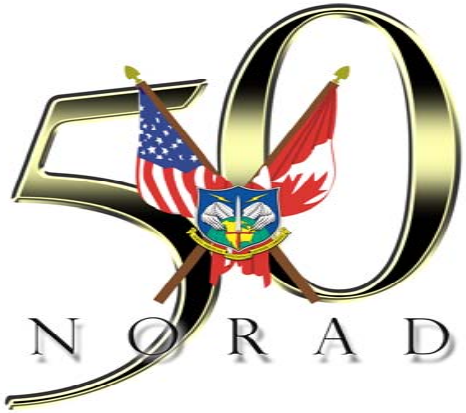
REAL-WORLD EXAMPLE

- One of the most highly publicized cases of cellular phone monitoring concerned former Speaker of the House of Representatives Newt Gingrich.

- A conference call between Gingrich and other Republican leaders was "accidentally" overheard and then taped.

- The conversation concerned Republican strategy for responding to Speaker Gingrich's pending admission of ethics violations being investigated by the House Ethics Committee.

- The intercepted conversation was reported in the New York Times and other newspapers.

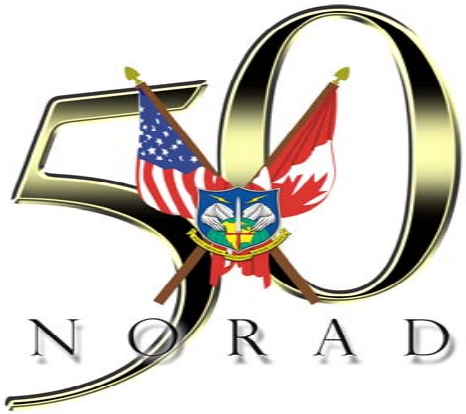


PAGERS

- Pagers have similar vulnerabilities.

- In 1997, police arrested officials of a small New Jersey company, Breaking News Network, that was monitoring pager messages to New York City leaders, police, fire, and court officials, including messages considered too sensitive to send over the police radio.

- They were selling the information to newspaper and television reporters. The offenses carry a penalty of up to five years in prison and fines of $250,000 for each offense.



VULNERABILITY TO BEING USED AS A MICROPHONE:

- A cell telephone can be turned into a microphone and transmitter for the purpose of listening to conversations in the vicinity of the phone.
- This is done by transmitting a maintenance command on the control channel to the cell phone.
- This command places the cell telephone in the "diagnostic mode."
- When this is done, conversations in the immediate area of the telephone can be monitored over the voice channel.

VULNERABILITY TO BEING USED AS A MICROPHONE:

- The user doesn't know the telephone is in the diagnostic mode and transmitting all nearby sounds until he or she tries to place a call.

- Then, before the cell telephone can be used to place calls, the unit has to be cycled off and then back on again.

This threat is the reason why cell telephones are prohibited in areas where classified or sensitive discussions are held!

VULNERABILITY TO CLONING

- Cell phone thieves don't steal cell phones in the usual sense of breaking into a car and taking the telephone hardware.

- Instead, they monitor the radio frequency spectrum and steal the cell phone pair as it is being anonymously registered with a cell site.

- Cloning is the process whereby a thief intercepts the electronic serial number (ESN) and mobile identification number (MIN) and programs those numbers into another telephone to make it identical to yours.

VULNERABILITY TO CLONING Cont.

- Once cloned, the thief can place calls on the reprogrammed telephone as though he were the legitimate subscriber.

- Cloning resulted in approximately $650 million dollars worth of fraudulent phone calls in 1996.

- Police made 800 arrests that year for this offense.

VULNERABILITY TO CLONING Cont.

- Each day, more unsuspecting people are being victimized by cell phone thieves.

- In one case, more than 1,500 telephone calls were placed in a single day by cell phone thieves using the number of a single unsuspecting owner.

- The ESN and MIN can be obtained easily by an ESN reader, which is like a cellular telephone receiver designed to monitor the control channel.

- The ESN reader captures the pair as it is being broadcast from a cell telephone to a cell site and stores the information into its memory.

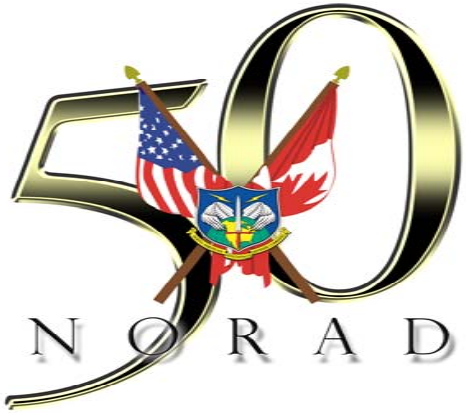
VULNERABILITY TO CLONING Cont.

What makes this possible is the fact that each time your cell phone is turned on or used, it transmits the pair to the local cellular site and establishes a talk channel.

It also transmits the pair when it is relocated from one cell site to another.

Cloning occurs most frequently in areas of high cell phone usage -- valet parking lots, airports, shopping malls, concert halls, sports stadiums, and high-congestion traffic areas in metropolitan cities.

No one is immune to cloning, but you can take steps to reduce the likelihood of being the next victim.



CELL PHONE SECURITY MEASURES:

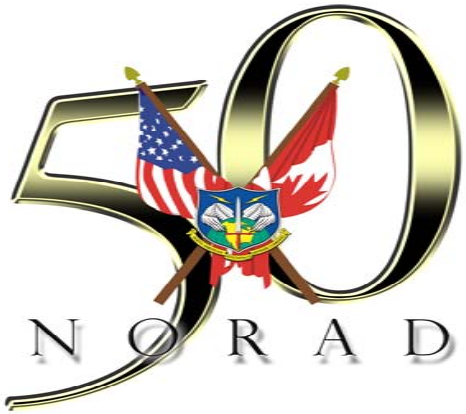
The best defense against these three major vulnerabilities of cell phones is very simple:

- Do not use a cell phone.
- If you must use a cell phone, you can reduce the risk by following these guidelines:

- **Because a cell phone can be turned into a microphone without your knowledge, do not carry a cell phone into any classified area or other area where sensitive discussions are held.**

- **Turn your cell phone on only when you need to place a call.**

- **Turn it off after placing the call.**



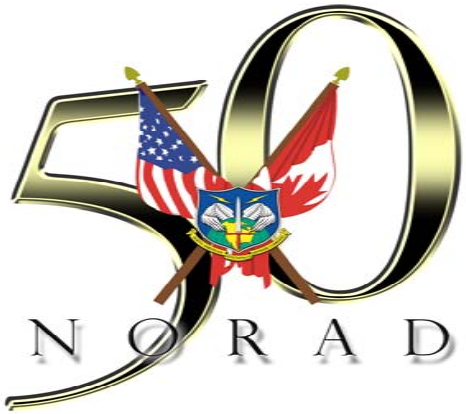
CELL PHONE SECURITY MEASURES:

- Ask your friends and associates to page you if they need to talk with you.

- You can then return the page by using your cell phone.

- **Do not discuss sensitive information on a cell phone.**

- When you call someone from your cell phone, consider advising them that you are calling from a cell phone that is vulnerable to monitoring, and that you will be speaking generally and not get into sensitive matters.



CELL PHONE SECURITY MEASURES:

- Do not leave your cell phone unattended.

- If your cell phone is vehicle-mounted, turn it off before permitting valet parking attendants to park the car, even if the telephone automatically locks when the car's ignition is turned off.

- Avoid using your cell phone within several miles of the airport, stadium, mall, or other heavy traffic locations.

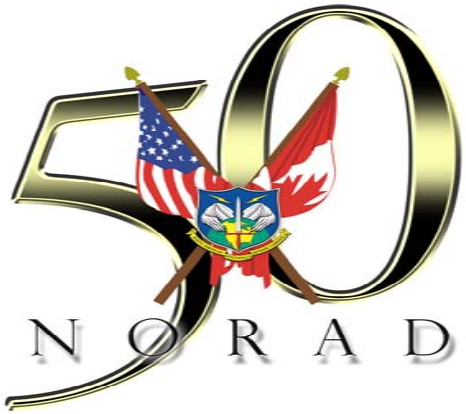
- These are areas where radio hobbyists use scanners for random monitoring.

CELL PHONE SECURITY MEASURES:

- If they come across an interesting conversation, your number may be marked for regular selective monitoring.

- If your cell service company offers personal identification numbers (PIN), consider using one.

- Although cell PIN services are cumbersome and require that you input your PIN for every call, they are an effective means of preventing cloning.



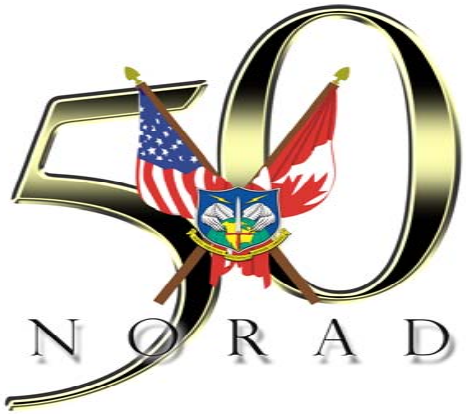
$26,000 Cell Phone Bill

- A recent CBS 5 ConsumerWatch report by Jeanette Pavini profiles the plights of three consumers in California -- all of whom had their cell phones stolen and were left stuck with a huge bill for unauthorized charges.

- The report told the story of San Francisco resident Wendy Nguyen, who was shocked to receive a bill for $26,000 after her cell phone was unknowingly stolen before she left for an overseas vacation. Cingular held her responsible for charges incurred after the phone was taken, up until the time Wendy discovered the theft and called the carrier.

- She was able to prove via airline and passport documents that she was out of the country and couldn't possibly have made the unauthorized calls from San Francisco during that time, but Cingular still held Wendy accountable for all charges.

- Not only that, they advised Wendy that if she couldn't pay the bill she should consider filing for bankruptcy!



Adding Insult to Injury

- Eileen Perrera's story revealed what happened after her phone was stolen while she was on vacation. She filed a police report and contacted Sprint immediately, but then received a bill totaling almost $16,000. Sprint claimed to have never received the call from her reporting the stolen cell phone.

- Eileen was able to submit proof from landline phone records that she had indeed called Sprint customer service. As her late fees piled up, the situation remained unresolved for months.

Adding Insult to Injury

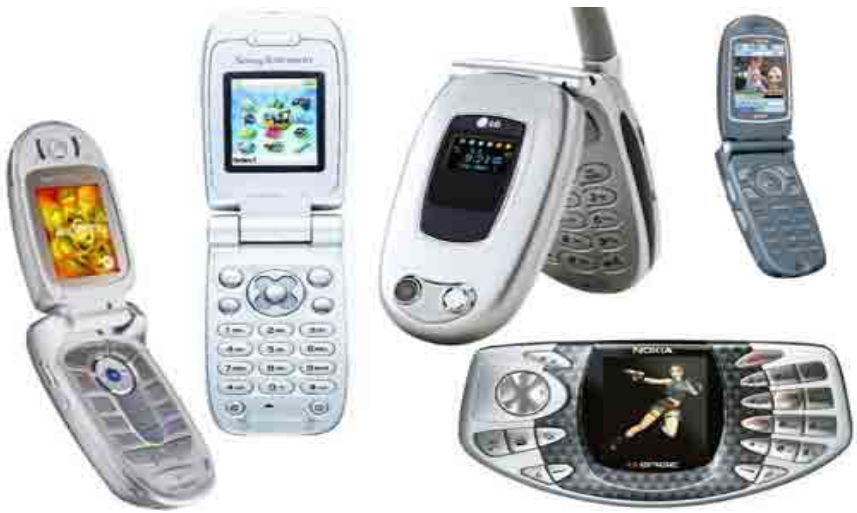
- Then there's Pamela Woodson's story. As revealed in the CBS 5 Consumer Watch report, when Pamela's cell phone was stolen she reported it the next day.

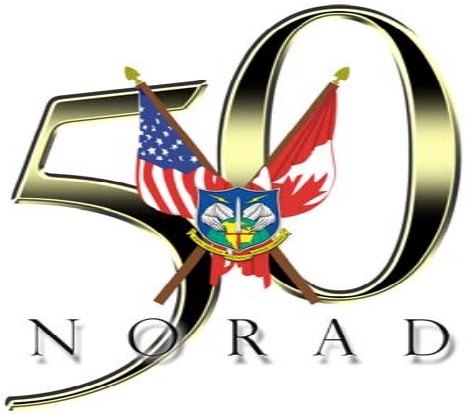
- However, by that time her account had already incurred over $1,800 in unauthorized charges. Due to the suspicious nature of the fraudulent charges, she was actually interviewed by the FBI -- and cleared of all responsibility.

- Nevertheless, T-Mobile pressed on, insisting she pay the outstanding charges in addition to late fees and interest.

- This year, an estimated 600,000 cell phones will be reported lost or stolen. Here are the 10 things you need to know to protect yourself from cell phone theft and fraudulent charges:

CELL PHONE SECURITY TIPS



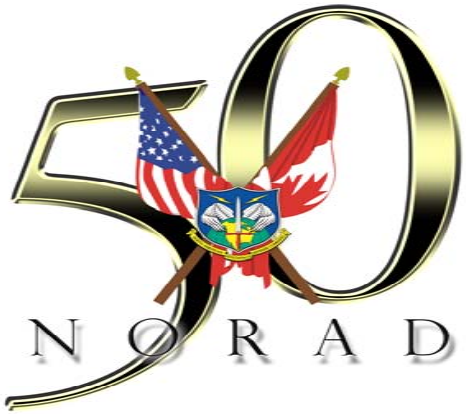


1. Guard your cell phone like you would your wallet.

The best way to *not* get stuck with fraudulent charges is to do what you can to prevent unauthorized calls in the first place. Think twice about what information you store on your device. A stolen cell phone will not only lead to a huge bill, but to identity theft as well.

2. Password-protect your device

Check the user guide that came with your phone and start using the "lock" or "password" feature to potentially prevent a thief from making unauthorized calls. There are ways to override passwords, you might be buying yourself some time until you discover the loss and call your provider.



3. Don't be fooled by cell phone insurance.

Purchasing cell phone insurance will provide coverage for the device itself, but it won't protect you against charges for unauthorized calls.

4. Call your cell phone provider as soon as you discover the loss.

Report your missing device. Be sure to keep meticulous records including the date and time you called your carrier, the name and ID number of the representative to whom you spoke, and what you were told. Also note the state or region of their call center, plus their telephone extension number. Finally, ask for confirmation in writing that your device has been disabled. Some companies can even email this to you.

5. File a police report.

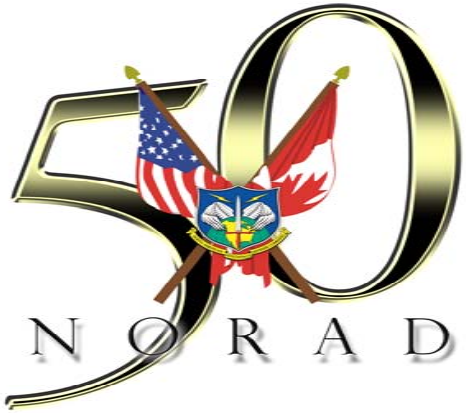
This may not help your chances of getting the stolen phone back, but it still provides an official record of the crime. Your carrier may even require the police report number when you phone in the loss.

6. Open an investigation with your carrier if necessary.

- If you find that you're not getting an immediate resolution by working directly with your cell phone company, don't waste another minute. Call your carrier and request an investigation, then follow up in writing. Requesting an investigation gives you a better chance of preventing any formal collections action to be taken and should also delay reporting to any of the credit bureaus.

- Advise your carrier that you'll be filing a complaint with the Federal Communications Commission (FCC), your state attorney general's office, and your state's public utility commission (PUC). Your carrier is more likely to pay closer attention to you when they know you're an informed consumer.

- 48 percent reported not knowing who to call if their cell phone carrier could not resolve a billing or service problem to their satisfaction. Items 7 through 9 below shed some light.



7. Contact the FCC.

The FCC will forward your complaint to your service provider, requiring a response from them within 30 days. You can contact them via their web site or call them directly at (888) 225-5322.

8. Contact your state attorney general's office.

- According to ConsumersUnion.org, state attorney general offices will handle complaints about cell phone fraud and contract disputes.
- This office has filed lawsuits against wireless companies based on consumer complaints, resulting in refunds to consumers and agreements by some companies to reform certain practices.
- Find the contact information for your state attorney general's office here.

9. Contact your state's PUC.

Each state has a government agency, usually called a public utility commission, that oversees telephone companies. To locate your state's PUC online and to file a complaint, visit the National Association of Regulatory Utility Commissioners web site.

10. When all else fails, contact the media.

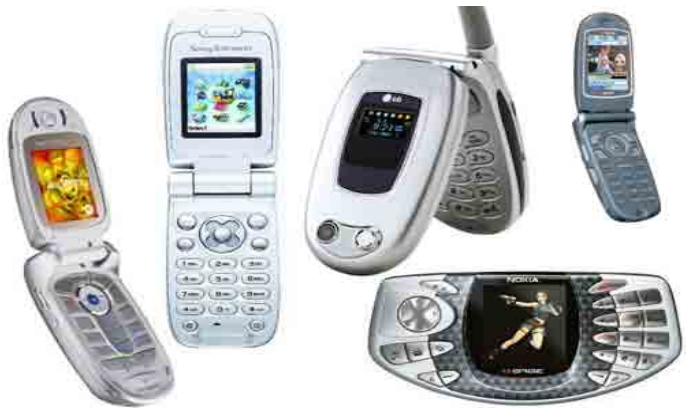
The wireless companies are particularly adverse to negative media attention, so until effective laws are put into place you may have to resort to contacting your local TV station.

- In Wendy, Pamela, and Eileen's cases that's just what they did, and their stories all have happy endings.

- After many months of persistent determination and follow up, all fraudulent charges were dropped. It seems the wireless industry wants to do the right thing after all -- as long as they're forced to by the media.

- But don't be tempted to skip steps 7 through 9. The FCC, state attorney generals offices, and PUCs all need to see how serious a problem this is, so formal complaints DO serve an important purpose.

GUARD YOUR CELL PHONE



TO DETER FRAUD