Tapping your cell phone

-
-
- Share on facebook
- Share on twitter
- Share on gmail
- Share on email
- Share on print
- More Sharing Services
- 183

Posted: Nov 13, 2008 4:39 PM MDT Updated: Jun 29, 2009 8:58 AM MST

Bob Segall/13 Investigates

Imagine someone watching your every move, hearing everything you say and knowing where you are at every moment. If you have a cell phone, it could happen to you. 13 Investigates explains how your cell phone can be secretly hijacked and used against you - and how to protect yourself.

After four months of harassing phone calls, Courtney Kuykendall was afraid to answer her cell phone.

The Tacoma, Washington, teenager was receiving graphic, violent threats at all hours.

And when she and her family changed their cell phone numbers and got new phones, the calls continued.

Using deep scratchy voices, anonymous stalkers literally took control of the Kuykendall's cell phones, repeatedly threatened Courtney with murder and rape, and began following the family's every move.

"They're listening to us and recording us," Courtney's mother, Heather Kuykendall, told NBC's Today Show. "We know that because they will record us and play it back as a voicemail." How is something like this possible?

Just take a look on the internet. That's where you'll find the latest spy technology for cell phones.

"Anywhere, anytime"

Spyware marketers claim you can tap into someone's calls, read their text messages and track their movements "anywhere, anytime." They say you can "catch a cheating spouse", protect your children from an evil babysitter and "hear what your boss is saying about you." And while you're spying on others, the Spyware companies say "no one will ever know" because it's supposed to

be "completely invisible" with "absolutely no trace."

Security experts say it's no internet hoax.

"It's real, and it is pretty creepy," said Rick Mislan, a former military intelligence officer who now teaches cyber forensics at Purdue University's Department of Computer and Information Technology.

Mislan has examined thousands of cell phones inside Purdue's Cyber Forensics Lab, and he says spy software can now make even the most high-tech cell phone vulnerable.

"I think a lot of people think their cell phone calls are very secure but our privacy isn't always what we think it is."

Is your privacy truly at risk?

13 Investigates tested some cell phone Spyware to find out.

With the permission of WTHR producer Cyndee Hebert, 13 Investigates purchased and downloaded Spyware on her personal cell phone.

Hebert agreed to be spied on - if the spy software lived up to its bold claims.

WTHR's Spy Test

The process of downloading the software took several attempts and a great deal of patience. But once the spy program was installed, Hebert's phone could indeed be tapped into at any time - just as its distributor promised.

While Hebert was at home making phone calls to her family, investigative reporter Bob Segall was outside her house, listening to the conversations on his cell phone.

And there's more - much more.

Every time Hebert made or received a phone call, Segall received an instant text message, telling him that Hebert was talking on her cell phone so that Segall could call in and listen.

On his computer, Segall also got a copy of Hebert's text messages and a list of phone numbers detailing each incoming and outgoing call to Hebert's cell phone.

And no matter where Hebert went with her phone, Segall received constant satellite updates on her location. He could literally track Hebert anywhere she went.

"It's hard to believe you can do all that," Hebert said when she saw the spy software in action. "I think that's really scary."

It gets even scarier.

When spy software was installed onto Hebert's phone, that phone became an instant spy device - even when the phone was not being used.

As Hebert's cell phone was simply sitting on a table or attached to her purse, Segall could activate the speaker on the phone and secretly listen in to the phone's surroundings. While Hebert was in a meeting on the 36th floor of a downtown Indianapolis building, Segall heard her conversations, even though he was four miles away.

13 Investigates found more than a dozen companies willing to sell this type of cell phone spy software, which ranges in price from $60 to $3,000. The majority of the companies are located in foreign countries such as Thailand, Taiwan and the United Kingdom - and for good reason.

Most of the advertised applications for the spy software are illegal in the United States, and the existence of the software angers CTIA-The Wireless Association, an industry organization representing the nation's major cell phone manufacturers.

"These are gross violations of federal and state laws," said association spokesman Joe Farren. "It's very clear, without their express permission, you can't listen in to someone's phone calls, you cannot read their text messages, you can't track their movements. You can't do any of those things and there are numerous laws being broken."

Farren said his organization was not familiar with cell phone Spyware prior to WTHR's investigation, adding "I can tell you our lawyers and engineers are now looking into this."

Government spying

The United States government is familiar with spy software for cell phones.

In 2003 and 2004, the FBI used cell phone spy software to eavesdrop on the conversations of organized crime families in New York, and it used those conversations in its federal prosecutions.

Private investigator Tim Wilcox says several federal agencies rely on cell phone spying technology to monitor suspected criminals, and he says private citizens are now using the technology, too.

"The technology is there. It's been there a long time. It's accessible, and it's done all the time," Wilcox said.

As founder of Indianapolis-based International Investigators Inc., Wilcox says he receives daily letters and e-mails from people wanting help with "cell phone bugging," the ability to download spy software onto a cell phone, turning it into a secret listening device.

"There's only two kinds of people," Wilcox said, holding a large stack of e-mails. "One wants to

bug somebody and the other has been bugged and wants to know how it's being done and how to find out and how to stop it.... it's a federal crime, but it's still happening."

The harassment eventually did stop for the Kuykendalls, but only after they brought in police and the FBI. While authorities never figured out who hijacked the family's cell phones, security experts say the case serves as a powerful lesson for others.

"Your privacy is not your privacy. It is exposed and it is exploited," Mislan said. "The key is being vigilant and knowing how to protect yourself.

How to protect yourself

Mislan suggests keeping a close eye on your cell phone so that others never get an opportunity to download information such as spy software when you're not looking. He also says it's important to install a security password on your phone to restrict anyone else from using it.

And while some Spyware marketers claim their products can be used on any make and model of cell phone, Mislan says high-end cell phones that include internet access and online capability are particularly vulnerable to Spyware tapping. To limit the ability of others to download certain types of spyware onto your phone, choose a cell phone that is not internet-accessible.

Wilcox recommends removing the battery from your cell phone when it's not being used and, for sensitive phone calls, he suggests making them on a newly-purchased cell phone that comes with a pre-paid month-to-month service plan.

Based on WTHR's test, here are some subtle signs that could suggest your cell phone is being secretly tapped:

- Cell phone battery is warm even when your phone has not been used
- Cell phone lights up at unexpected times, including occasions when phone is not in use
- Unexpected beep or click during phone conversation