Panic button movie 2007

It has long been an urban legend that if you're in trouble at an ATM, you can dial in your PIN backwards to call the police. Unfortunately, however, this is not the case for the victims of ATM robberies and the violence that goes with them. It seems likely that such a system may have helped police intervene in the recent kidnapping and murder of a young woman in Boston who was driven to five ATMs in the area and forced to make withdrawals before she was stabbed. According to the Boston Herald: Amy E. Lord spent 47 minutes driving between five banks in Boston early Tuesday after being kidnapped by at least one assailant in her South Boston neighborhood, a kidnapping that ended with the woman's murder and her body dumped at the Stony Brook Reservation in Hyde Park, officials said. Boston police said Lord was taken in her jeep between 6 a.m. and 6:47 a.m. to banks at the following locations: East Boston Savings Bank, 501 Southampton St.; Metro Credit Union, 1071 Massachusetts Ave. Bank of America, 555 Columbia Road. Sovereign Bank, 585 Columbia Road, and Citizens Bank, 217 Adams St.The technology that may have helped Lord warn police that something was wrong has been around since at least 1994, when inventor Joseph Zingher patented a reverse PIN warning system called SafetyPIN. However, Zingher was unsuccessful in marketing the technology to banks, according to a 2010 Federal Trade Commission report. State laws requiring the use of the technology were considered in Illinois, Georgia, and Kansas, but were rejected or watered down in all areas. The same report found that ATM offences are relatively rare compared to the number of trouble-free transactions, with only one crime per 3.5 million transactions. But the sheer volume of ATM transactions – 11.8 billion transactions a year in 2008 alone, according to the American Bankers Association – means that there are thousands of ATM-related crimes every year, like the one that ultimately took Amy Lord's life. Of course, like any security technology, there are a variety of potential drawbacks. Critics point to the possibility of fat-fingered errors by ATM users, which causes a lack of alarms for law enforcement. And it's unclear whether police in many areas would be able to respond quickly enough to make a difference, according to the FTC report. Then there's the cost: an estimated 10 million dollars to add the technology to every ATM in the nation, according to the report. But when you consider how much price Americans pay for using an ATM, it's constantly rising – according to Bankcouncil's latest audit, it's up to an average of up to 2.50 dollars, according to Bankcouncil's latest audit. Bank customers deserve a little more security and peace of mind for their money. What do you think? Should ATMs have some kind of panic button to warn the authorities that a crime is taking place? Or are ATMs okay as they are? Follow me on Twitter: @ClaesBell.Senior Bank reporter Claes Bell is co-author of Future Millionaires' Guidebook, an e-book e-book bank rate editors and reporters. It is available from all major e-book retailers. Websites such as Twitter, Netflix and PayPal have become the essential building blocks of digital life. Last week, when service in these and other popular places was temporarily suspended, life came to a standstill for many, the virtual equivalent of the Mississippi River froze. It wasn't long before the company at the center of the attack solved the problems, but the fact that botnet executives gained access through connected home devices triggered a new round of alarms about Internet of Things security. Massive cyberattack turned ordinary devices into weapons, a CNN headline shouted. My first inclination is to direct my best Ronald Reagan -- There you go again -- to the press that jumped on the Connected-Home-as-Pandora's-box car. For tech writers, IoT security is a virtual job security blanket that's all soft and convenient, as it guarantees stories that securely attract clicks. People need to know if their lives could one day imitate art, with their devices that oppose them like an episode from Futurama. But I will not select them this time, because it is the job of the media to make the public aware of potential dangers in the simplest and most alarmist way. Likewise, it is the prerogay of ankle heads who tend to imagine the worst: that there are people who try to read their thoughts and infiltrate their kitchen cupboards, and that all the information obtained from connected devices ends up in the underground lair of an evildoer to be used against them. But despite the fear-mongering quality of most news on this subject and the irrational fears of an irrational subset, security in the connected home is a very real concern, and it is one that our company takes very seriously. Last week's hack reached the scale it did because manufacturers had not put in the necessary security measures, essentially leaving the back door open for bad guys to walk in. And without any real requirements that the supply chain must meet, it is up to the companies that manufacture and sell products to ensure that these products are safe. Even the best password generated by the customer does not help if the back door has a password that no customer could change. But consumers also have a certain responsibility. They need to be smart about the products they buy and the companies behind them. At Big Ass Solutions, we do our best to ensure that our products are not hacked. We require that each product be fitted with a safe connected. It annoys some people who prefer an unsecured network, but it's important. We also keep an eye on our vendors -- and of course our products work well without the Internet. But we realize that it is essentially an arms race between well-intentioned manufacturers and mayhem-minded hackers, 400 lbs. and otherwise. If connected devices part part more people are living, hackers will find new ways to thwart security measures, and companies will adapt. Following the recent infringements, there has been renewed call for some form of government regulation in the industry, and we would welcome all sensible efforts in this direction and want to be involved. Among the many things that have shown us this election season -- and I'm almost misty about the thought that it's about to be over -- is that everything can be hacked. As someone crouching under a school table while the Cuban Missile Crisis raged, this thought certainly gives me a break. But the dangers associated with the Internet of Things are no different, and probably even less than many other threats that we accept every day and with which we live. People need to be diligent to ensure home security, but certainly not paranoid, and companies in the connected home business need to take all possible measures to ensure the safety of customers or otherwise get out of the house. Photograph: Thomas Trutschel/Photothek via Getty Images Tinder, the erotic digital aneam that makes your personal data look like a small child consuming a yoo-hoo, ventures a few new features in the name of user security. The Wall Street Journal reports that the popular dating app will soon give users who want additional security measures the ability to press a panic button and get check-ins. Tinder's parent company, Match Group, Inc., is working with an app called Noonlight to provide this service. Noonlight tracks the user's location and sends notifications to the police when security issues occur. The feature will be free for US Tinder users by the end of January and will appear on other dating apps in the coming months. Tinder users can add a badge to their dating profiles that shows they are protected by the new tracking feature; Match Group hopes this will work as a deterrent. The company's chief executive, Mandy Ginsberg, told the Journal: 'You should run a dating business as if you were a mother. I think a lot about security, especially on our platforms, and what we can do to curb bad behavior. There are a lot of things we tell users to do. But if we can also provide instruments beyond that, we should do so. Of course, there is an obvious privacy compromise for users who choose to have their data tracked by a tech company. As the Journal notes, the investment in Noonlight marks the first step Tinder takes to monitor the real-time security of its users after they connect on the platform and meet for coffee or drinks. Tinder's security efforts focused on monitoring users' communications with each other. Ginsberg told the Journal that location data is not used for marketing purposes, but Tinder and other dating apps have reportedly been involved in such systems before. Another problem with the feature: What if users accidentally raise the alarm and the cops crash their date? Ginsberg isn't too worried about this, The wrong positives, believe me, we have taken them into account ... In the worst case, someone turns up and knocks on the door. It's not the worst thing in the world. Maybe not in the world, but on a date? Almost. Tinder adds a 'Panic Button' button'