



## WIFI-BASED IMSI CATCHER

The main focus of the work of Oxford University in 5G-ENSURE is the provision of privacy in mobile communications. Oxford is developing mechanisms for providing privacy enhanced operation for devices connecting to 5G networks to ensure that we minimise the potential for illicit tracking of past and present locations of mobile users. Major research findings were presented and demonstrated by Piers O’Hanlon and Ravishankar Borgaonk at the Black Hat Europe security conference in early November 2016: **WiFi-based IMSI Catcher**, with considerable press coverage, which will help to flag privacy issues at the highest levels and ensure they are swiftly addressed.

Here we provide a short report on the press coverage, totalling 20 articles in IT and security media channels in 7 languages:

- The Register
- Network World
- PC World
- SC Magazine
- International Business Times
- Best Security Search
- The Intercept
- The Hacker News
- Bitshacker
- Naked Security
- 01 Net.com (FR)
- Computer World (HU)
- Version (DK)
- Intelligence Online
- Techworm
- Xakep (Russian)
- SecNews (Greek)
- The TechNews
- Univers Free Box (French)
- Autobild (Spanish)

Press clippings follow.



Online media channel: The Register

Link: [http://www.theregister.co.uk/2016/11/03/wifi\\_imsi\\_catcher/](http://www.theregister.co.uk/2016/11/03/wifi_imsi_catcher/)

The screenshot shows the top of a news article on The Register website. The header is red with the 'The Register' logo and the tagline 'Biting the hand that feeds IT'. Below the header is a navigation bar with links for DATA CENTRE, SOFTWARE, SECURITY, TRANSFORMATION, DEVOPS, BUSINESS, PERSONAL TECH, SCIENCE, EMERGENT TECH, and BOONOTES. The article is categorized under 'Security' and has the title 'Build your own IMSI slurping, phone-stalking Stingray-lite box – using bog-standard Wi-Fi'. The sub-headline reads 'Uni eggheads discuss track-and-trace threat'. The article features a photograph of a blue and white Stingray aircraft flying over a rocky landscape. Below the photo is the date '3 Nov 2016 at 18:27' and the author 'John Leyden'. The article text discusses how Wi-Fi networks can be used to track and monitor people by their handsets' fingerprints, mentioning that this involves special hardware and that it's possible to harvest IMSI details via Wi-Fi authentication protocols. It also notes that Android and iOS smartphones and tablets can be tracked this way.



Online media channel: Network World

Link: <http://www.networkworld.com/article/3138468/security/mobile-subscriber-identity-numbers-can-be-exposed-over-wi-fi.html>

TRENDING: China may retaliate against Apple · CEO to stand for social injustice · Cities using Cisco's smart service · Cool Yule Tools 2016 · Resources/White Papers

**NETWORKWORLD**  
FROM IDG

Technology CyberSecurity Apple Google

### The great smartphone security scare: Your mobile can be hijacked and tracked without you knowing

Attack discovered by Oxford University can only be fixed with help from all parties in the mobile industry.

By Mary-Ann Russell  
November 3, 2016 14:30 GMT



Oxford University security researchers have uncovered an attack that allows rogue Wi-Fi hotspots to steal a user's unique IMSI identifying number from their smartphone. (iStock)

Cybersecurity researchers Piers O'Hanlon and Ravishankar Borgeankar from Oxford University have demonstrated a new attack at Black Hat Europe 2016 that enables hackers to capture a smartphone's unique 15-digit IMSI number within a second as they walk past, and then use that number to spy on the user's movements.

**Phone makers, mobile OS creators and operators must work together**

Clearly this is a big privacy issue, and since government law enforcement agencies have access to databases of IMSI numbers, this attack could easily be used for mass surveillance. Unfortunately, solving the issue isn't simple and the researchers say it hasn't been fixed, so if an attacker were to set up a rogue wireless access point today, they could start collecting IMSI numbers in droves.

"I reported this to the OS manufacturers, handset manufacturers and the GSMA over six months ago. They all suffer from the same problem and ultimately a solution needs to be deployed to suit them all," O'Hanlon told **IBTimes UK**.

"It's not an overnight fix. It's not a vulnerability you can just patch, it requires work from the standards body level, the operator level, the handset level and the vendor level so they have support from the hardware, meaning the boxes the operators stick in their data centres."

O'Hanlon says that protocols like conservative peer pseudonym support – introduced in iOS 10 by Apple as a result of conversations with the researchers – can help to improve the overall privacy approach, but it's not enough on its own, and a better solution would be to use a security protocol called EAP-TTLS to implement cryptographic certificates on the systems that the smartphone needs to talk to.

"The mobile industry needs to work together to ensure that the users' privacy is sufficiently protected. Some of the organisations don't really see it as much of an issue, but Apple and the GSMA are taking it seriously," he stressed.

"Apple have been very keen to get this problem under control, but no one organisation can fix it, so there's a limit to what Apple can do without operators deploying it."

Online media channel: PC World

Link: <http://www.pcworld.com/article/3138472/security/mobile-subscriber-identity-numbers-can-be-exposed-over-wi-fi.html>


**PCWorld**  
FROM IDG

NEWS REVIEWS HOW-TO VIDEO BUSINESS LAPTOPS TABLETS PHONE  
Privacy Encryption Antivirus

Home / Security

### Mobile subscriber identity numbers can be exposed over Wi-Fi

Wi-Fi Auto Connect and Wi-Fi calling pose privacy risks for mobile device users, researchers show



Credit: Agam Shah

COMMENT 8

Lucian Constantin Nov 3, 2016 12:02 PM  
OS News Service

For a long time, law enforcement agencies and hackers have been able to track the identity and location of mobile users by setting up fake cellular towers and tricking their devices to connect to them. Researchers have now found that the same thing can be done much more cheaply with a simple Wi-Fi hotspot.

The devices that pose as cell towers are known in the industry as IMSI catchers, with the IMSI (International mobile subscriber identity) being a unique number tied to a mobile subscriber and stored on a SIM card. IMSI catchers can be used for tracking and in some cases, for intercepting calls, but commercial solutions, such as the Stingray used by the FBI, are expensive.

5G-ENSURE Press Coverage on WiFi-based IMSI Catcher, November 2016



Online media channel: SC Magazine

Link: <http://www.scmagazineuk.com/blackhat-eu-researchers-remind-that-imsi-catchers-still-a-threat/article/570453/>

The image is a screenshot of a web article from SC Magazine. The page layout includes a top navigation bar with 'SC US' and '&gt; SC UK' links, and a main header with the 'SC MAGAZINE FOR IT SECURITY PROFESSIONALS' logo and 'NEWS', 'EVENTS', and 'VIDEO' categories. The article title is 'BlackHat EU: researchers remind that IMSI catchers still a threat', dated November 03, 2016, by Rai Paraz, Community Manager. The article text discusses a presentation by Piers O'Hanlon and Ravishankar Borgaokar at BlackHat Europe 2016, highlighting a new WiFi-based IMSI catcher. A photo shows the researchers demonstrating their proof-of-concept to an audience. The article concludes with a quote from O'Hanlon about Apple's randomization of MAC addresses in iOS 10.



Online media channel: International Business Times

Link: <http://www.ibtimes.co.uk/great-smartphone-security-scare-your-mobile-can-be-hijacked-tracked-without-you-knowing-1589716>

**International Business Times**

News World Business Fintech Politics Technology Science Sport Entertainment Opinion Video

Technology CyberSecurity Apple Google

### The great smartphone security scare: Your mobile can be hijacked and tracked without you knowing

Attack discovered by Oxford University can only be fixed with help from all parties in the mobile industry.

By Mary-Ann Russon  
November 3, 2016 14:30 GMT

Phone makers, mobile OS creators and operators must work together

Clearly this is a big privacy issue, and since government law enforcement agencies have access to databases of IMSI numbers, this attack could easily be used for mass surveillance. Unfortunately, solving the issue isn't simple and the researchers say it hasn't been fixed, so if an attacker were to set up a rogue wireless access point today, they could start collecting IMSI numbers in droves.

"I reported this to the OS manufacturers, handset manufacturers and the GSMA over six months ago. They all suffer from the same problem and ultimately a solution needs to be deployed to suit them all," O'Hanlon told IBTimes UK.

"It's not an overnight fix, it's not a vulnerability you can just patch, it requires work from the standards body level, the operator level, the handset level and the vendor level so they have support from the hardware, meaning the boxes the operators stick in their data centres."

O'Hanlon says that protocols like conservative peer pseudonym support - introduced in iOS 10 by Apple as a result of conversations with the researchers - can help to improve the overall privacy approach, but it's not enough on its own, and a better solution would be to use a security protocol called EAP-TTLS to implement cryptographic certificates on the systems that the smartphone needs to talk to.

"The mobile industry needs to work together to ensure that the users' privacy is sufficiently protected. Some of the organisations don't really see it as much of an issue, but Apple and the GSMA are taking it seriously," he stressed.

"Apple have been very keen to get this problem under control, but no one organisation can fix it, so there's a limit to what Apple can do without operators deploying it."

Oxford University security researchers have uncovered an attack that allows rogue WiFi hotspots to steal a user's unique IMSI (Identifying number from their smartphone).

Cybersecurity researchers Piers O'Hanlon and Ravishankar Borgaonkar from Oxford University have demonstrated a new attack at Black Hat Europe 2016 that enables hackers to capture a smartphone's unique 15-digit IMSI number within a second as they walk past, and then use that number to spy on the user's movements.

Online media channel: Best Security Search

Link: <http://bestsecuritysearch.com/cell-phones-can-easily-traced-via-wifi/>

**Best Security Search**  
Security Search For How to remove PC viruses

BROWSER HIJACKERS TROJANS SUSPICIOUS SOFTWARE SECURITY NEWS

### CELL PHONES CAN EASILY BE TRACED VIA WIFI

SECURITY NEWS | NOVEMBER 8, 2016 | BY MARTIN BELTOV

It appears that the WiFi connectivity that is bundled in virtually every cell phone sold today can be used to track the owners easily.

#### Cell Phones can Be Traced Via WiFi

As it appears most cell phones used today can be used to actively track their owners just by using the WiFi connectivity option. A well-established option that has been used to date was the use of a tool called IMSI catcher. This has been used by law enforcement agencies to track suspects and find missing people. The way things is that the device mimics a cellphone tower which tricks the devices in range to connect to it. The IMSI catcher has the capability to intercept internet traffic, calls, send and receive fake texts and install malicious programs (spyware) on the victim device. By definition this is considered a man-in-the-middle attack. Nowadays it is quite easy for anyone to obtain such a device. Last year security experts reported that customers can easily purchase and order a low-cost IMSI catcher that has the ability to work with most modern connectivity standards, including 4G. One such device can be purchased for 1400 US dollars and works in a 20 meters radius.

Now a new danger has arose. During the international hacker conference BlackHat Europe a research team from Oxford University demonstrated a new type of IMSI catcher attack that used the WiFi protocol. The demonstrated attack allowed the capture of the cell phone's IMSI number within seconds as soon as the user came in range of the network.

The consequences include the active tracking in real time of the victims and this affects both Android and iOS device owners. This can be fixed by disabling the WiFi calling feature on the device and the network auto connect feature.

The summary of the findings are given on the conference's web site:

WIFI-BASED IMSI CATCHER

Piers O'Hanlon | Researcher, University of Oxford

5G-ENSURE Press Coverage on WiFi-based IMSI Catcher, November 2016



Online media channel: The Intercept

Link: <https://theintercept.com/2016/11/07/hackers-and-law-enforcement-could-hijack-wifi-connections-to-track-cellphones/>

**The Intercept**  
UNOFFICIAL SOURCES

**Hackers and Law Enforcement Could Hijack Wi-Fi Connections to Track Cellphones**

Jenna McLaughlin  
November 7 2016, 9:30 p.m.

**ONE MORNING** on the underground in London, Piers O'Hanlon, a privacy and security researcher at Oxford University, noticed something strange about his phone: it kept automatically connecting to Wi-Fi networks from his provider without asking for a password – displaying a small lock icon.

What started off as another morning on the tube prompted O'Hanlon's next research project. He began digging into the widely available public, automatic Wi-Fi provided by the phone companies, and looking at the ways it could be exploited and spied on. It turns out, those initial connections, which largely happen without consent, are insecure and unencrypted – and can be easily intercepted by malicious hackers or law enforcement.

What O'Hanlon and his Oxford research associate, Ravishanker Borgsonkar, looked into was a previously known – but unaddressed – flaw in the automatic Wi-Fi protocols that would allow someone to track the location of phones that connect to these networks. While tech experts are aware of the flaw, it's so deeply engrained in the system that it would require a large overhaul to fix – something companies aren't eager to invest in.

This flaw would allow someone to hijack a user's Wi-Fi connection the way law enforcement currently does with wireless communications using Stingrays, or IMSI Catchers, the handheld devices that imitate cell phone towers. Stingrays and similar devices trick nearby phones to connect and dump information about the phone, like its location, and sometimes also the content of calls, onto the tracker. (Stingrays are a specific brand sold by Harris Corporation in Florida.)

Online media channels: The Hacker News and BitsHacker

Links: <http://thehackernews.com/2016/11/imsi-track-cellphone.html>

<http://bitshacker.com/2016/11/04/wi-fi-can-turn-imsi-catcher-track-cell-phone-users/>

**The Hacker News**  
Security in a serious way

Home Hacking Tech Deals Cyber Attacks Vulnerabilities Malware Spying

Wi-Fi can be turned into IMSI Catcher to Track Cell Phone Users Everywhere

Thursday, November 03, 2016 & David Thordarson

Here's a new danger to your smartphone security: Your mobile device can be hijacked and tracked without your knowledge.

Remember *Stingray*?

The controversial cell phone spying tool, also known as "IMSI catchers," has long been used by law enforcement to track and monitor mobile users by mimicking a cellphone tower and tricking their devices to connect to them. Sometimes it even intercepts calls and Internet traffic, sends fake texts, and installs spyware on a victim's phone.

Setting up such *Stingray*-type surveillance devices, of course, is expensive and needs a lot of effort, but researchers have now found a new, cheaper way to do the same thing with a simple Wi-Fi hotspot.

**BITSHACKER**  
HACKING, CYBER SECURITY, TECHNOLOGY

HOME HACKING TECHNOLOGY SECURITY BUGS MALWARE RES

ABOUT US

Wi-Fi can turn into IMSI Catcher to Track Cell Phone Users

November 4, 2016 sunny mishra Hacking

Your mobile device can be hacked or hijacked without your knowledge. Mobile connected to Wi-Fi which control by hackers can give your IMSI number to hacker.

IMSI (international mobile subscriber identity) is a unique 15-digit number used for authentication of a person when moving network to network. The number is stored in the read-only section of a SIM card and with the mobile operator.

IMSI number is tied to a user, while IMEI number is tied to a device.



Online media channel: Naked Security

Link: <https://nakedsecurity.sophos.com/2016/11/08/who-needs-a-stingray-when-wi-fi-can-do-the-job/>

The screenshot shows the article page on the Naked Security website. The article title is "Who needs a Stingray when Wi-Fi can do the job?" by Bill Camarda, dated 08 NOV 2016. The article discusses how Wi-Fi-based IMSI catchers can be used to track mobile phones, a technology previously associated with Stingray devices. It mentions that these devices can be used to track phones in a specific area, and that they can be used to track phones in a specific area. The article also mentions that these devices can be used to track phones in a specific area.

Online media channel: O1 Net.com (FR)

Link: <http://www.O1net.com/actualites/comment-le-wi-fi-des-operateurs-mobiles-permet-de-pister-les-abonnes-1055430.html>

The screenshot shows the article page on the O1net.com website. The article title is "Comment le Wi-Fi des opérateurs mobiles permet de pister les abonnés". The article discusses how Wi-Fi-based IMSI catchers can be used to track mobile phones, a technology previously associated with Stingray devices. It mentions that these devices can be used to track phones in a specific area, and that they can be used to track phones in a specific area. The article also mentions that these devices can be used to track phones in a specific area.



Online media channel: Computer World (HU)

Link: <http://computerworld.hu/computerworld/ellophatok-a-mobil-elofizetok-azonositoi-wifin-keresztul.html>

Online media channel: Version (DK)

Link: <https://www.version2.dk/artikel/forskere-forvandler-almindeligt-wifi-prisvenlig-imsi-catcher-1020909>





Online media channel: Intelligence Online

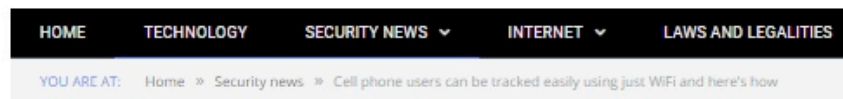
Link: [https://www.intelligenceonline.com/corporate-intelligence\\_terabytes/2016/11/09/fake-wi-fi-hotspot-replaces-imsi-catcher,108188976-ART](https://www.intelligenceonline.com/corporate-intelligence_terabytes/2016/11/09/fake-wi-fi-hotspot-replaces-imsi-catcher,108188976-ART)

The screenshot shows the top section of the Intelligence Online website. On the left is the 'Intelligence ONLINE' logo with the tagline 'Global Strategic Intelligence'. In the center is a world map with play button icons over North America, Europe, Middle East, and Asia. On the right is a text block stating: 'Intelligence Online is an exclusive and independent publication supported entirely by readers and published since 1990 by the independent news organisation Indigo Publications.' Below this is a navigation bar with tabs for 'Government Intelligence', 'Corporate Intelligence', 'Europe', 'North America', 'Middle East', and 'Asia'. A red bar below the navigation bar displays 'Issue no. 770 dated 09 november, 2016' and an 'RSS' button. The main article section features a Wi-Fi icon and the text 'UNITED KINGDOM' with social media icons for Twitter, Facebook, and a star. The article title is 'Fake Wi-Fi hotspot replaces IMSI catcher'. The summary reads: 'Researchers have invented a false Wi-Fi hotspot that can extract IMSI numbers from a telephone which can then be intercepted. The method dispenses with the need for an IMSI catcher.(...) [ 311 words ] [€5,2]'. Below the summary is a grey box with the text 'MENTIONED IN THIS ARTICLE : Piers O'Hanlon | Ravishankar Borgaonkar | Circles | Ability | Rayzone'. At the bottom right is a red button with a play icon and the text 'Read this article'.



Online media channel: TechWorm

Link: <http://www.techworm.net/2016/11/cell-phone-users-can-tracked-easily-using-just-wifi-heres.html>



| Cell phone users can be tracked easily using just WiFi and here's how 🗨️

By Muhammad on NOVEMBER 5, 2016

Security news, Technology



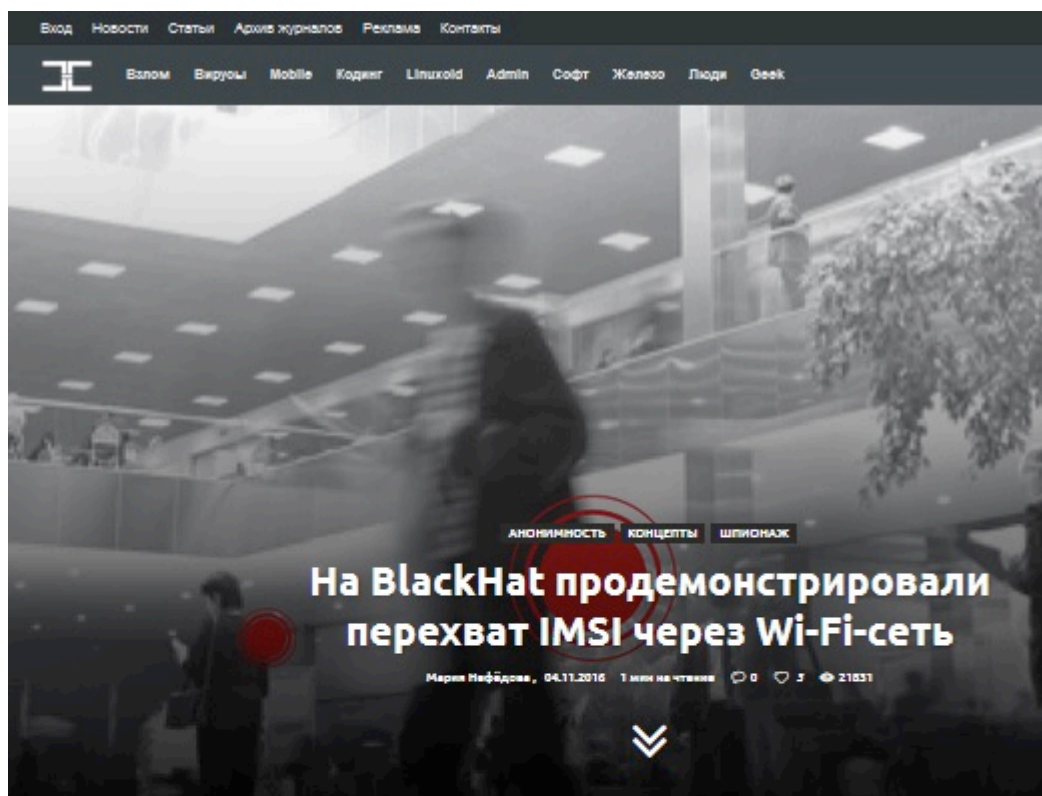
### Next time you see an open WiFi hotspot, you'd best be careful

Another danger of smartphone security is that your device can be traced and hijacked without your knowledge using a very sophisticated spying tool called IMSI catchers. IMSI catches has long been used by law enforcement personnel to track suspects and here is how it works. By mimicking a cellphone tower and tricking their devices to connect to them, it even intercepts calls and internet traffic, sends fake texts, and installs spyware on a victim's phone, all the while the user being unaware of what is going on.



Online media channel: Xakep (Russian)

Link: <https://xakep.ru/2016/11/04/wi-fi-imsi-catcher/>



Тема слежки за людьми не иссякнет никогда, а сегодня, когда в кармане у каждого лежит мобильный телефон, следить становится даже проще. Спецслужбы используют для этих целей специальные устройства-перехватчики, известные как Stingray, способные как просто анализировать проходящий через них трафик, так и непосредственно переключать пользовательские устройства на себя, работая как IMSI-ловушка. Напомню, что IMSI-номер уникален для каждой SIM-карты и пользователя, а IMEI-номер привязан к самому устройству.

Конечно, шпионят за пользователями отнюдь не только спецслужбы. К примеру, недавно новозеландский исследователь Джулиан Олливер (Julian Oliver) подробно [рассказал в своем блоге](#) о том, как создать собственную **фемтосоту** на базе RaspberryPi 3 и BladeRF x40 software-defined radio. При этом исследователь спрятал свою поделку внутри корпуса неприметного принтера HP Laserjet 1320, который не вызовет подозрений ни в одном офисе. Настоящая находка для корпоративных шпионов.



Online media channel: SecNews (Greek)

Link:

<https://secnews.gr/150196/%CF%80%CF%8E%CF%82-%CE%BC%CF%80%CE%BF%CF%81%CE%B5%CE%AF%CF%84%CE%B5-%CE%B5%CE%BD%CF%84%CE%BF%CF%80%CE%AF%CF%83%CE%B5%CF%84%CE%B5-wifi/>

The screenshot shows a web page from SecNews with the following content:

- Navigation bar: SecNews /inet /infosec /investigations /hacking /pentesting /rapidalet
- Breadcrumbs: Home / /tweaks / Πώς μπορείτε να εντοπίσετε εύκολα χρήστες κινητών μέσω WiFi
- Article Title: Πώς μπορείτε να εντοπίσετε εύκολα χρήστες κινητών μέσω WiFi
- Author/Date: Absenta Mia /tweaks Νοέμβριος 7, 2016 5:40 μμ
- Actions: Print PDF
- Image: An illustration of a city street with a red dashed circle highlighting a 'WiFi hotspot' area. Inside the circle, several people are shown with their smartphones, and a dog is also present. The background includes buildings labeled 'DEPARTMENT STORE' and 'SHOP'.
- Text: 

*Την επόμενη φορά που θα δείτε ένα ανοικτό WiFi hotspot, καλύτερα να είστε προσεκτικοί!*

Ένας ακόμα κίνδυνος για την ασφάλεια των smartphone είναι ότι η συσκευή σας μπορεί να εντοπιστεί και να χακαριστεί εν αγνοία σας, χρησιμοποιώντας ένα πολύ εξελιγμένο εργαλείο κατασκοπείας που ονομάζεται IMSI. Το IMSI έχει χρησιμοποιηθεί εδώ και καιρό από το προσωπικό επιβολής του νόμου για την παρακολούθηση των υπόπτων και να πώς λειτουργεί. Μιμούμενοι έναν πύργο κινητής τηλεφωνίας, ξεγελούν τις συσκευές τους για να συνδεθούν με αυτούς, παρακολουθώντας έτσι τις κλήσεις και την κυκλοφορία στο διαδίκτυο, στέλνουν πλαστά κείμενα και εγκαθιστούν spyware στο τηλέφωνο του θύματος, ενώ ο χρήστης έχουν άγνοια για το τι συμβαίνει.

Τώρα ανακαλύφθηκε ότι το WiFi είναι ικανό να κάνει ακριβώς το ίδιο πράγμα. Ένα δίκτυο WiFi είναι σε θέση να αιχμαλωτίσει εύκολα τους αριθμούς IMSI, αλλά μπορεί να το κάνει μόνο στα κοντινά smartphones. Οι συσκευές που δεν είναι στην περιοχή του δικτύου θα παραμείνουν ασφαλής, αλλά για πόσο καιρό?



Online media channel: The Tech News

Link: <http://thetechnews.com/2016/11/12/learn-tracking-cell-phones-using-wi-fi-connection/>

≡ The **Technews**

HOME NEWS ▾ TECHNOLOGY ▾ INNOVATION ▾ BUSINESS ▾ TIPS & T

**DEVICES**

## Learn tracking cell phones using a Wi-Fi connection only

 by IRENE ADLER -- NOVEMBER 12, 2016



**3** SHARES     

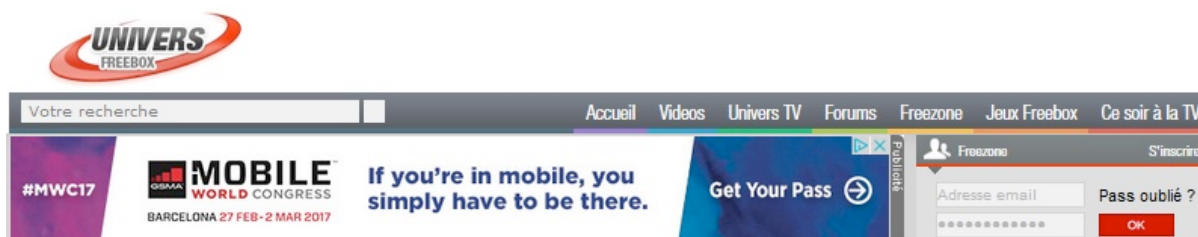
Next time whenever you come across an open WiFi hotspot, avoid connecting your device at all costs. A modern spying device called IMSI catchers is used for tracking cell phone users without their knowledge while violating our rights of privacy.

In the meantime, law enforcers mainly used this tactic for locating suspects. They did it primarily by imitating a cell phone tower for establishing a connection. Even worse, this enabled them to intercept phone calls, transmit false messages and install spyware on their victims' cellphones without approval.



Online media channel: Univers Free Box (French)

Link: <http://www.universfreebox.com/article/37017/Deux-chercheurs-denoncent-le-Wi-Fi-operateur-qui-piste-les-abonnes>



## Deux chercheurs dénoncent le Wi-Fi opérateur qui piste les abonnés



Deux chercheurs de l'université d'Oxford ont montré, lors d'une conférence, qu'il est possible d'utiliser l'accès Wi-Fi des opérateurs afin de pister les abonnés. Ils profitent des failles dans les protocoles télécoms afin d'intercepter les identifiants IMSI des abonnés et révéler leur présence dans une zone donnée, comme le rapporte [01net](#).

Dans la procédure logique, ce sont les agences de renseignements qui interceptent ces données en utilisant un IMSI Catcher, un équipement onéreux simulant une station de base d'opérateur et s'appuyant sur les vulnérabilités dans les protocoles de communications mobiles, surtout ceux de la 2G. Ceci leur permet alors de vérifier la présence d'une personne dans la zone de l'équipement en captant l'IMSI, qui est un identifiant unique de 15 chiffres donné par l'opérateur.

# 5G-Ensure

5G Enablers for Network and System Security and Resilience

Online media channel: Autobild (Spanish)

Link: <http://www.autobild.es/noticias/si-usas-wifi-publico-ten-cuidado-con-esto-304613>



Noticia

## Si usas WIFI público, ten cuidado con esto

Las **redes WiFi** también son capaces de capturar esta numeración. Se desconoce si los **dispositivos** que se encuentren más alejados también estarán en peligro. Si te estás preguntando por el **número IMSI** debes saber que se queda almacenado en un apartado de solo lectura de la **tarjeta SIM**. Además, cabe destacar que la **Universidad de Oxford** ha conseguido desarrollar un **nuevo tipo de ataque al receptor IMSI** a través de una red WiFi pública.

Esto hace que cuando el dispositivo esté expuesto a este tipo de redes, se 'contagie' enseguida. Es importante destacar que todos los dispositivos están expuestos a estas amenazas, ya sean **Android e IOS**. Si tienes un **iPhone** podrás desactivar la **conexión WiFi automática**. ¡Ten mucho cuidado con tu smartphone!

Fuente: **Techworm**