

# OUCH!

## NË KËTË EDICION..

- Kontrolli paraprak
- Pajisjet e humbura/vjedhura
- Qasja Wi-Fi
- Kompjuterët publikë

## Si të rrini të sigurt gjatë udhëtimit

### Përmbledhje

Ky buletin flet si të lidhemi në mënyrë të sigurt me internetin dhe të mbarojmë punë gjatë udhëtimeve.

### Kontrolli paraprak

Edhe pse rrjeti i internetit që keni në shtëpi apo në punë mund të jetë i sigurt, kur udhëtoni duhet të mendoni gjithmonë që rrjeti me të cilin lidheni nuk është i besueshëm. Ju nuk mund ta dini se kush tjetër po e përdor këtë rrjet dhe çfarë rreziku përbën. Disa masa të thjeshta që mund të merrni para se të udhëtoni mund t'ju ndihmojnë të mbronin të dhënat tuaja gjatë udhëtimeve. Një ose dy javë përpara udhëtimit tuaj:

### Botuesi i ftuar

Steve Armstrong është drejtor teknik i CyberCPR në Logically Secure, është instruktor i certifikuar nga SANS dhe ish autor i një kursi në SANS. Ai është aktiv në Twitter si [@Nebulator](#) dhe Google plus: [+SteveArmstrongSecurity](#).

- Identifikoni të dhënat që nuk ju duhen në pajisjet elektronike që do të merrni me vete dhe fshini çdo informacion të panevojshëm. Kjo ndihmon në reduktimin e dëmit në rast se pajisjet vidhen, humbasin apo konfiskohen nga dogana apo personeli i sigurisë së kufirit. Nëse po udhëtoni për qëllime pune, pyesni eprorin tuaj nëse organizata ofron pajisje elektronike që mund t'i përdorni për qëllime pune ndërsa udhëtoni.
- Në rast udhëtimesh ndërkombëtare, kontrolloni çfarë lloj prizash përdoren në vendin ku po shkoni sepse mund t'ju duhet të përdorni një adaptor për mbushjen e baterive të pajisjeve. Kontrolloni planin e shërbimit telefonik që ofrohet nga kompania e shërbimeve celulare. Shpesh herë ofruesit e shërbimeve përdorin tarifa të larta për përdorim ndërkombëtar të të dhënave, kështu që mund të dëshironi të çaktivizoni të dhënat celulare (ang. mobile data) ndërsa udhëtoni ose të ndryshoni planin tarifor gjatë udhëtimeve ndërkombëtare.
- Instaloni aplikacione në pajisjen tuaj për të gjurmuar nga distanca se ku ndodhet pajisja juaj dhe për të fshirë të dhënat nga distanca në rast vjedhjeje apo nëse humb. Shumë pajisje elektronike e kanë këtë funksion të instaluar, ju thjesht duhet ta aktivizoni (mos harroni se për këtë veprim ju duhet të keni internet).

Një ose dy ditë para udhëtimit:

- Përditësoni pajisjet, aplikacionet dhe software-ët anti-virus në mënyrë që të jeni duke përdorur versionet më të fundit.
- Aktivizoni të gjithë veprimet e duhura në lidhje me sigurinë në pajisjen tuaj, si për shembull firewalls.

## Si të rrini të sigurt gjatë udhëtimit

- Vendosni nga një fjalëkalim të sigurt për secilën pajisje. Në këtë mënyrë, edhe nëse e humbisni pajisjen apo dikush e vjedh, nuk do të mund të shohin informacionin që përmban pajisja.
- Enkriptoni të gjitha pajisjet, në mënyrë që të dhënat të mos gjenden në rast se humbet apo vidhet pajisja. Disa pajisje si iPhone e bëjnë automatikisht enkriptimin nëse ju vendosni një fjalëkalim për pajisjen.
- Ruani të gjithë informacionin diku tjetër (ang. backup). Në këtë mënyrë, edhe nëse ndodh diçka gjatë udhëtimit, ju i keni të ruajtura të dhënat tuaja në një vend të sigurt.

### Pajisjet e humbura/vjedhura

Siguroni që pajisjet tuaja të jenë të sigurta kur filloni udhëtimin. Për shembull, mos i lini asnjëherë në makinë ku mund t'i shohin njerëzit, sepse kriminelët do të thyejnë xhamin e makinës për të marrë çdo gjë me vlerë që duket nga jashtë. Një ide është të përdorni një kablo sigurie që shërben si kyç fizik për pajisjet, si për shembull për laptopin, kur e lini diku. Edhe pse krimi përbën një nga rreziqet, ka shumë më shumë gjasa që ju ta humbisni një pajisje sesa t'ua vjedhin. Kjo do të thotë që të kontrolloni shpesh gjatë udhëtimeve nëse i keni pajisjet elektronike me vete, si për shembull gjatë kontrollit të sigurisë në aeroport, kur dilni nga taksia apo restoranti, kur largoheni nga hoteli apo përpara se të zbrisni nga avioni.

### Qasja Wi-Fi

Përdorimi i internetit gjatë udhëtimeve do të thotë shpesh përdorim i pikave publike të internetit Wi-Fi në hotel, kafene, apo në aeroport. Problemi me pikat publike ku ka Wi-Fi është se jo vetëm që nuk e dini kush i ka krijuar, por as nuk dini se kush tjetër është lidhur me internetin. Për këtë arsye, duhen konsideruar si të pabesueshme; sepse kjo është arsyeja pse morët të gjitha hapat për të siguruar pajisjet përpara se të niseshit për udhëtim. Për më tepër, Wi-Fi përdor valë radioje për të komunikuar nga pajisja juaj me Pikën e Aksesit Wireless (ang. Wireless Access Point) . Kjo do të thotë që kushdo që ndodhet afër jush mund të përgjojë dhe monitorojë këtë komunikim.

Ndaj, nëse përdorni pika publike Wi-Fi, duhet të siguroheni që aktiviteti juaj online është i enkriptuar. Për shembull, kur lidheni me internetin përmes browser-it tuaj, sigurohuni që faqet e internetit që përdorni të jenë të enkriptuara ('https://' në URL dhe një figurë kyçi të mbyllur). Mund të keni gjithashtu atë që quhet llogari VPN (ang. Virtual Private Network) e cila enkripton të gjithë aktivitetin tuaj online. Kjo mund t'ju sigurohet nga punëdhënësi ose mund ta blini



*Çelësi i sigurisë gjatë udhëtimeve është të siguroni pajisjet përpara se të niseni, t'i mbani të sigurt fizikisht duke ditur gjatë gjithë kohës se ku ndodhen, dhe të enkriptoni të gjithë aktivitetin tuaj online.*

## Si të rrini të sigurt gjatë udhëtimit

për përdorim vetjak. Nëse mendoni se nuk ka pika Wi-Fi të cilave mund t'u besoni, mund të lidheni me smartphone-in tuaj (Kujdes: Siç e përmendëm më lart, kjo mund të jetë e kushtueshme kur udhëtoni në një vend të huaj, prandaj pyesni më parë ofruesin e shërbimit).

### Burimet publike

Mos përdorni kompjuter publikë si për shembull kompjuterin në lobin e hotelit, bibliotekë apo internet-kafe. Ju nuk e dini se kush e ka përdorur më parë, ndaj kompjuterit mund të jetë infektuar qëllimisht apo aksidentalisht. Nëse është e mundur, përdorni vetëm pajisjet që mund t'i kontrolloni dhe besoni për aktivitete online. Nëse jeni të detyruar të përdorni një kompjuter publik, mos përdorni shërbime që ju kërkojnë të logoheni apo të përdorni një fjalëkalim.

### Mëso më shumë

Regjistrohuni në buletin tonë mujor për vetëdijësimin mbi sigurinë OUCH!, qasuni në arkivat e OUCH!, dhe mësoni më shumë mbi zgjidhjet për ngritjen e vetëdijes mbi sigurinë të ofruara nga SANS duke na vizituar në faqen <http://www.securingthehuman.org>.

### Edicioni në shqip

Edicioni në shqip i OUCH! është përkthyer nga gjuha angleze nga Ilir Bytyçi dhe Jorida Nano. Iliri është magjistër i shkencave në administrimin e rrjetave dhe sistemeve kompjuterike, është ligjërues në universitet për lëndë të ndryshme nga fusha e TI, dhe është përgjegjës për sigurinë e teknologjise informative në bankë. Jorida është përkthyes e profesioniste e gjuhës angleze në OSBE.

### Burimet

Fjalëkalime:	<a href="http://www.securingthehuman.org/ouch/2013#may2013">http://www.securingthehuman.org/ouch/2013#may2013</a>
Verifikimi me dy nivele:	<a href="http://www.securingthehuman.org/ouch/2013#august2013">http://www.securingthehuman.org/ouch/2013#august2013</a>
Enkriptimi:	<a href="http://www.securingthehuman.org/ouch/2014#august2014">http://www.securingthehuman.org/ouch/2014#august2014</a>
Sigurimi i tabletës tuaj të re:	<a href="http://www.securingthehuman.org/ouch/2013#december2013">http://www.securingthehuman.org/ouch/2013#december2013</a>
Verizon DBIR 2014:	<a href="http://www.verizonenterprise.com/DBIR/2014/">http://www.verizonenterprise.com/DBIR/2014/</a>

OUCH! botohet nga SANS Securing The Human dhe shpërndahe nën licencën [Creative Commons BY-NC-ND 4.0](http://creativecommons.org/licenses/by-nc-nd/4.0/). Lejohet ta shpërndani këtë buletin ose ta përdorni për programet tuaja vetëdijësuese, për sa kohë nuk e modifikoni përmbajtjen e buletinit. Për përkthimet apo më shumë informata, ju lutemi na kontaktoni në [ouch@securingthehuman.org](mailto:ouch@securingthehuman.org).

Bordi editorial: Bill Wyman, Walt Scrivens, Phil Hoffman, Bob Rudis  
Përkthyer nga: Ilir Bytyçi dhe Jorida Nano



[securingthehuman.org/blog](http://securingthehuman.org/blog)



[/secrethehuman](https://www.facebook.com/secrethehuman)



[@secrethehuman](https://twitter.com/secrethehuman)



[securingthehuman.org/gpl](https://www.securingthehuman.org/gpl)