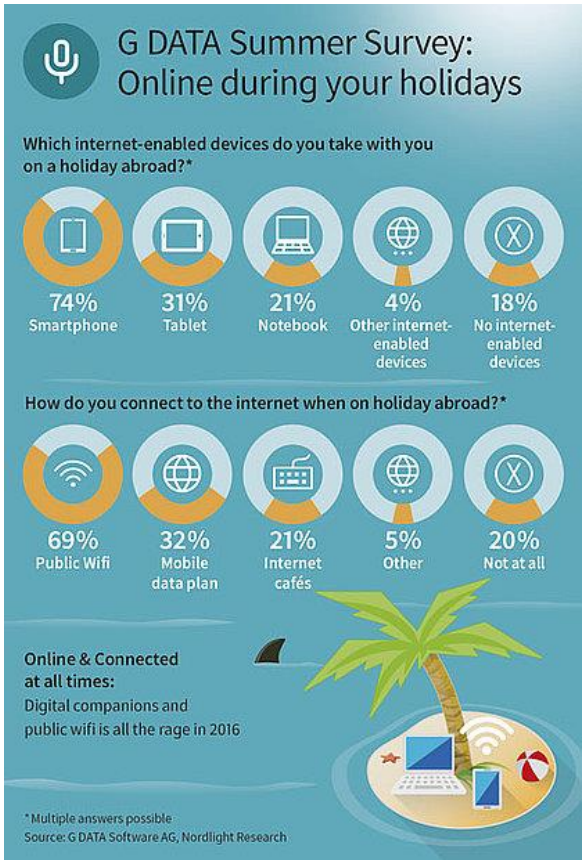
G Data press release 2016

Sondaj de vacanta G DATA: 80% dintre turisti sunt online in vacanta

Dispozitivele mobile sunt cei mai populari insotitorii intr-o calatorie, insa securitatea acestora pica, de cele mai multe ori, testul.

Bucuresti (Romania) 12.07.2016

Vara, soare, securitate - indiferent daca se afla pe plaja sau la munte, turistii doresc acces online atunci cand calatoresc. Din acest motiv, 74% isi iau cu ei un smartphone in vacanta, iar 31% prefera o tableta si doar unul din cinci turisti isi impacheteaza in bagaje un notebook. Acesta a fost rezultatul unui studiu pe timpul verii efectuat de G DATA pe 1000 de utilizatori de Internet. Care este modalitatea prin care se poate obtine o conexiune online? 69% din turisti se conecteaza la retele WiFi publice, insuficient protejate, din hoteluri, aeroporturi sau restaurante, iar 21% folosesc Internet Cafe-uri sau computere situate in spatii dedicate. Aceasta este o invitatie la furtul de date si nu doar parolele sunt in pericol, ci si toate datele personale. G Data recomanda securizarea in mod corespunzator a companionilor digitali inainte de a porni la drum si ofera sfaturi importante de calatorie pentru a va bucura de vacanta.



Trimiterea unui selfie de pe plaja, fotografierea unei mese imbelsugate sau verificarea rapida a conditiilor meteo locale sunt mai simplu de facut online, decat offline, in cea mai asteptata perioada a anului. WiFi-ul este adesea o facilitate standard in hoteluri, pensiuni sau alte forme de cazare. Numeroase cafenele, baruri si restaurante ofera acces gratuit la Internet pentru a atrage clientii. Acest lucru permite oamenilor sa ramana in contact cu prietenii si familia atunci cand calatoresc. Din nefericire, multe dispozitive mobile sunt insuficient protejate, ceea ce le face sa devina o tinta usoara pentru infractorii cibernetici.

“Hotspot-urile gratuite din aeroporturi sau hoteluri sunt tinte obisnuite, pentru ca astfel de puncte de acces sunt rareori asigurate in mod corespunzator, astfel incat infractorii pot citi cu usurinta traficul de date si pot spiona informatii de pe cardurile de credit, parole si alte date personale. Acestea sunt transformate in bani lichizi pe forumuri speciale de pe piata neagra sau utilizate in mod abuziv pentru alte activităati infractionale. Din acest motiv, turistii ar trebui sa evite platile de online banking si cumparaturile online," spune Tim Berghoff, G DATA security evangelist. Expertul G Data oferă si un sfat pentru rețelele sociale. “ Fotografiile din vacanta nu ar trebui sa fie postate in mod public pe Facebook sau pe alte portaluri in timp real, ci la o data ulterioara, astfel incat spargatorii sa nu afle ca nu este nimeni la domiciliu.”

Turistii trebuie sa respecte urmatoarele reguli inainte de a pleca departe de casa:

- Rezervari: Se recomanda precautie atunci cand planificati o excursie, portalurile de rezervari online sunt o tinta populara pentru atacuri de phishing. Puteti rezerva numai de pe portaluri de rezervari recunoscute si este recomandat sa folositi o solutie de securitate care ofera protectie web.
- Software: O solutie software de securitate este, in general, o optiune buna pentru a pune obstacole in calea infractorilor cibernetici. In vacanta, poate ajuta chiar la localizarea unui dispozitiv pierdut sau furat si poate preveni activitatile infractorilor. Datele sensibile pot fi sterse cu usurinta, de la distanta, de pe o tableta sau smartphone, in caz de furt sau pierdere, folosind functii speciale integrate in solutiile de securitate.
- Actualizari: Actualizarea programelor de pe dispozitive este la fel de importanta ca si bagajele. Brese potentiale de securitate sunt inchise de actualizari si pregatesc dispozitivele pentru vacanta.
- Backup: Este mai sigur daca datele importante nu sunt luate in vacanta. Backup-urile periodice sunt importante - fie ca este vorba la un mediu de stocare extern sau de date salvate automat in Cloud de software-ul de securitate.

Atunci cand sunteti in vacanta, e bine sa tineti cont de urmatoarele:

- Hotspot-uri Wifi: Tot mai multe hoteluri si cafenele ofera Wi-Fi gratuit. Acest lucru este util, dar poate fi si riscant. Prin intermediul unor astfel de retele, infractorii pot citi

cu usurinta e-mailuri sau pot spiona datele confidentiale ale altor persoane, cum ar fi detaliile cardului de credit sau parolele. Sfat important: Efectuati tranzactii bancare online si faceti cumparaturi online, fie inainte, fie dupa calatorie.

- Internet cafe-uri: Nu puteti obtine o imagine clara a setarilor de securitate sau ale unei posibile infectii malware pe computerele pe care le utilizati. Nu ar trebui sa va conectati la conturile sensibile de pe PC-uri situate in Internet Cafe-uri, in receptia sau pe holurile hotelurilor si, daca este posibil, navigati in browser privat sau in modul incognito, cazuri in care datele nu sunt stocate. Dupa sesiune, iesiti din toate conturile si stergeti istoricul de navigare.
- Retelele de socializare: Publicati cu atentie anunturi publice despre vacante, pe retelele sociale. Infractorii folosesc astfel de date pentru a crea harti pe care sunt marcate proprietatile temporar nelocuite. Din acest motiv, cele mai bune amintiri din vacanta ar trebui sa fie incarcate pe Facebook sau pe alte retele doar la intoarcere sau trimise in mod privat prietenilor si familiei.
- Dezactivati retelele wireless: Functiile Bluetooth si WiFi ar trebui sa fie dezactivate atunci cand nu sunt necesare, pentru a proteja dispozitivul de potentiale atacuri.

-###-