LUNA EUROPEANĂ A SECURITĂȚII INFORMATICE

CENTRUL NAȚIONAL DE RĂSPUNS LA INCIDENTE DE SECURITATE CIBERNETICĂ
CERT-RO

GHID

Securitatea terminalelor mobile

Ghid realizat de către:

Bitdefender

în cadrul campaniei de conștientizare a riscurilor de securitate cibernetică derulată în Romania sub egida ECSM de către CERT-RO.

BE AWARE, BE SECURE.
www.enisa.europa.eu/cybersecmonth

www.cert-ro.eu/tag/ecsm

Pagină albă

Cuprins

Într-o piață care însumează aproximativ 2 miliarde de telefoane mobile inteligente (smartphones)[1], protejarea datelor salvate în terminalele mobile devine o problemă serioasă, mai ales că acestea nu mai sunt folosite de mult doar pentru a suna sau a trimite mesaje prietenilor. Între timp au devenit niște mini-calculatoare folosite pentru a stoca date, fotografii, pentru a accesa conturi de e-mail, rețele sociale, jocuri, sau multimedia. De cele mai multe ori, telefoanele sunt legate nu numai de viața privată a cuiva, ci și de locul de muncă al posesorului telefonului.

[1] http://www.gartner.com/newsroom/id/2525515

Astfel, o vulnerabilitate sau un atac asupra telefonului mobil poate afecta nu doar individul, prietenii dar și compania pentru care acesta lucrează.

Bitdefender va prezenta câteva dintre cele mai des întâlnite atacuri asupra telefoanelor mobile, posibilele implicații la nivel personal și nu numai cât și o serie de metode de protejare împotriva escrocilor care folosesc dispozitivele mobile pentru a înșela oamenii, a le fura banii și chiar pentru a pătrunde în organizațiile și firmele unde aceștia au acces.

1. TIPURI DE AMENINȚĂRI CARE VIZEAZĂ TERMINALELE MOBILE

În mai puțin de 10 ani, telefoanele mobile și-au schimbat total înfățișarea și funcționalitatea. Interesul crescut al producătorilor și al utilizatorilor a atras atenția atacatorilor care au văzut în telefoane și tablete un nou domeniu de exploatat.

Una dintre cele mai răspândite metode de atac asupra terminalelor mobile sunt amenințările care apelează sau trimit SMS-uri pe ascuns la numere cu supra-taxă. Utilizatorul va înțelege că ceva nu este în regulă cu telefonul sau tableta sa abia la prima factură, când va trebui să plătească mult mai mult decât anticipase sau dacă este pe cartelă, va termina creditul mult mai repede.

Dacă vă întrebați cum ajung aceste aplicații malițioase pe dispozitivele utilizatorilor, răspunsul este simplu: atacatorii iau o aplicație legitimă, o modifică adăugând cod periculos și o deghizează într-o aplicație populară. Apoi, folosind diferite tehnici de inginerie socială conving utilizatorii să descarce și să instaleze aplicația pe telefon sau pe tabletă.

Aceste aplicații periculoase pot de asemenea fura și alte informații din telefon, cum ar fi datele de identificare ale dispozitivului, coordonate GPS, lista de contacte, adrese de e-mail sau e-mailuri.

Foarte multe aplicații periculoase (exemplu: Android.Trojan.FakeInst) pretind că instalează browsere, antiviruși și aplicații de chat pe mobile când de fapt păcălesc utilizatorul și trimit SMS-uri la numere cu supra-taxă. Unele au nevoie ca utilizatorul să le configureze manual, pe când altele se instalează singure odată ajunse în dispozitivele mobile, și eventual își schimbă iconița la un interval de timp pentru ca utilizatorii să nu le detecteze prezența.

O altă categorie generoasă de aplicații periculoase pretind că țin în viață bateria dispozitivului pentru mai mult timp. În schimb, ele spionează în fundal tot ce face utilizatorul cu telefonul sau tableta, culeg date și le trimit pe server-ele atacatorilor.

Unele aplicații de mobil procedează într-un mod similar cu programele false de securitate de pe PC. Odată ce utilizatorul instalează o astfel de aplicație, aceasta îi spune că dispozitivul are probleme cu durata de viață a bateriei, care se descarcă mult prea repede. Îi sugerează să acceseze un website de unde să descarce un utilitar. Dar pe site utilizatorul va gasi un instrument care spionează de fapt activitățile utilizatorului.

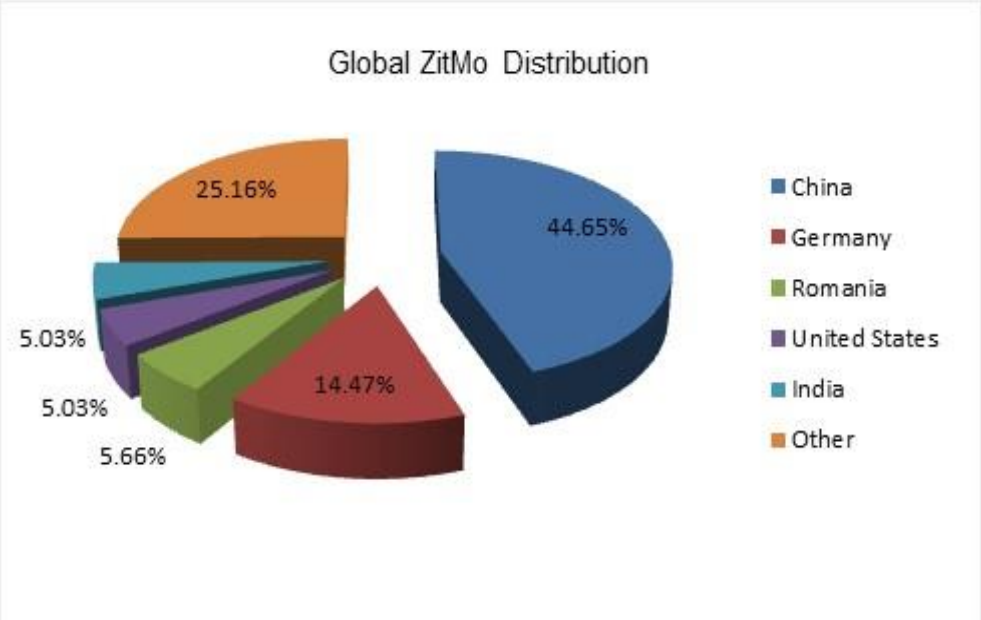
Utilizatorii trebuie să se ferească și de aplicațiile false de video player, care odată instalate trimit mesaje la un număr cu supra-taxă care ajung să coste până la 5 dolari SMS-ul. Android.Trojan.FakePlayer, de exemplu, păcălește utilizatorul să-i dea permisiunea să modifice sau să șteargă cardul de memorie al telefonului, să acceseze informații de pe telefon fără a cere alte permisiuni.

Odată cu creșterea constantă a numărului de aplicații din piețele oficiale Google Play și AppStore, dezvoltatorii au început să adauge tot mai multe funcții în aplicațiile făcute de ei pentru un plus de competitivitate. Dacă ne uitam atent la sutele de mii de aplicații care stau la dispoziția utilizatorilor de telefoane mobile și tablete, vedem că unele dintre aceste aplicații pot pune probleme de securitate posesorilor de dispozitive mobile atunci când transferă date din telefon – nume de utilizator și parole folosind rețele nesecurizate, în timp ce altele activează fără permisiunea posesorului de mobil funcția de GPS pe lângă furtul de contacte, adrese de email.

2. PEISAJUL ACTUAL AL AMENINȚĂRILOR CARE VIZEAZĂ TERMINALELE MOBILE

Amenințările care vizează terminalele mobile sunt tot mai răspândite și se modifică foarte repede în contextul dezvoltării foarte rapide a pieței de mobile. Astfel, amenințările informatice care vizează furtul datelor personale și al detaliilor de autentificare în conturile bancare câștigă din ce în ce mai mult teren în peisajul virușilor pentru terminale mobile cu Android. Dacă virușii care trimit SMS-uri la numere premium sunt în continuare în top din punct de vedere al numărului de atacuri, noile amenințări, mai complexe, de tip ransomware – ce blochează terminalul și solicită plata unei amenzi – și virușii bancari înregistrează creșteri susținute.

Virușii bancari de Android pretind a fi actualizări ale certificatelor digitale și păcălesc astfel utilizatorii să îi descarce și să îi instaleze. Așa cum Zeus este vedeta virușilor bancari pentru PCuri, ZitMo este corespondentul acestuia pe Android și este la fel de periculos. Acesta primește comenzi de la un server de comandă și control către care poate trimite toate SMS-urile pe care le primește utilizatorul pe mobil. În acest fel, hackerii pot intercepta numărul de autentificare al tranzacțiilor (mTAN) imediat ce utilizatorii le inițiază.

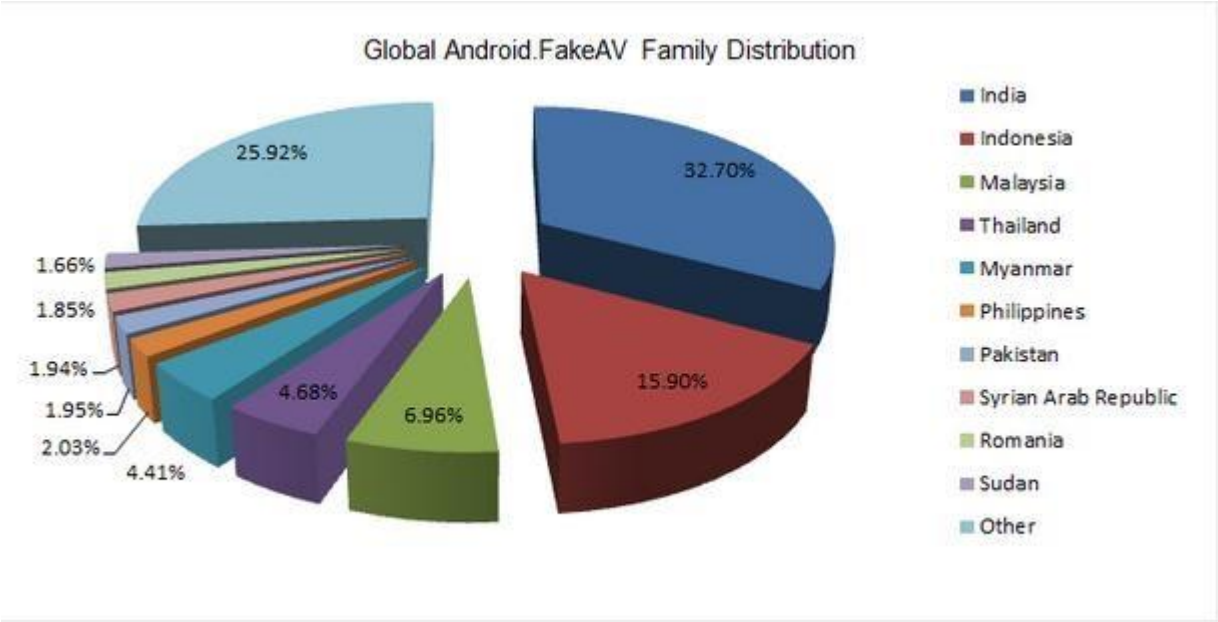


	Distribuția globală ZitMo	
1	China	44.65%
2	Germania	14.47%
3	România	5.66%
4	Statele Unite	5.03%
5	India	5.03%
	Altele	25.16%

Acționând prin intermediul unui PC infectat cu Zeus și al unui terminal mobil de pe care ZitMo interceptează SMS-urile, atacatorii câștigă controlul complet asupra tranzacțiilor bancare online ale unei persoane. Cele mai multe raportări ale lui ZitMo, în primul semestru al acestui an, vin din China și mai bine de 5% dintre detecții din România.

Un alt tip de malware de Android, detectat cu precădere în Asia, este varianta pentru mobile a foarte răspânditului virus de PC - **ransomware**. Această amenințare pretinde a fi o soluție antivirus. Îi spune utilizatorului că are dispozitivul mobil plin de viruși și încearcă să-l convingă să descarce un utilitar de dezinfecție. Odată descărcat, virusul blochează terminalul și apoi solicită bani pentru a-l debloca.

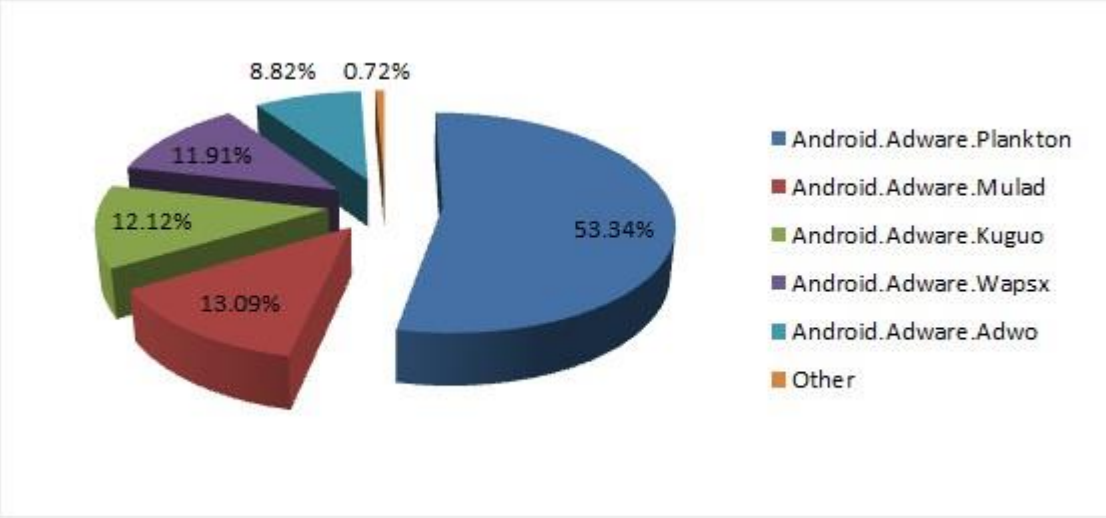
Familia de viruși Android.FakeAV se regăsește mai frecvent în țările unde utilizatorii descarcă aplicații din magazine neoficiale, fiind tentați cu promisiunea unei soluții antivirus eficiente.



Distribuția globală a familiei FakeAV

1	India	32.70%	5	Myanmar	4.41%	9	România	1.85%	
2	Indonezia	15.90%	6	Filipine	2.03%	10	Sudan	1.66%	
3	Malaiezia	6.96%	7	Pakistan	1.95%		Altele	25.92%	
4	Thailanda	4.68%	8	Siria	1.94%				

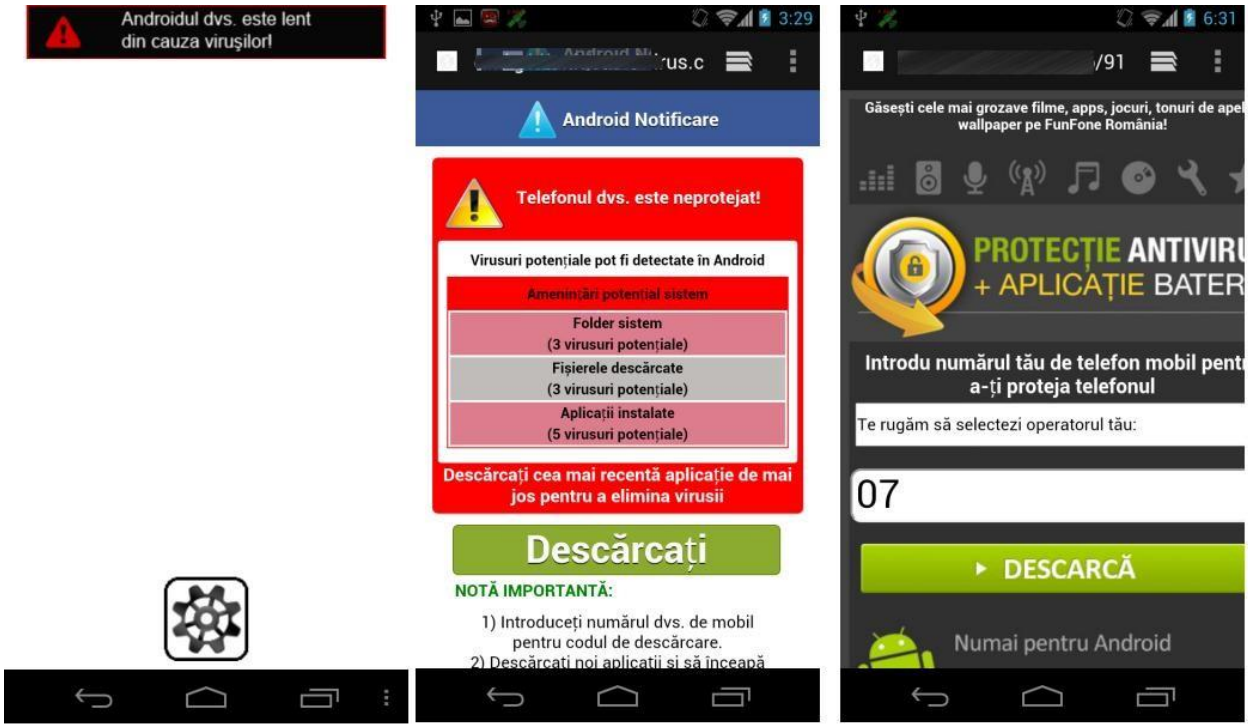
Reclamele agresive afișate utilizatorilor de aplicații gratuite sunt cunoscute pentru faptul că adună date personale pentru a adapta conținutul în funcție de utilizator. Agențiile de marketing apreciază drept foarte valoros acest tip de informație care face campaniile promoționale mai eficiente și mai profitabile.



	Familii de Adware la nivel global	
1	Android.Adware.Plankton	53.34%
2	Android.Adware.Mulad	13.09%
3	Android.Adware.Kuguo	12.12%
4	Android.Adware.Wapsx	11.91%
5	Android.Adware.Adwo	8.82%
	Altele	0.72%

Una dintre cele mai recente amenințări mobile analizate în laboratoarele Bitdefender vizează **reclamele periculoase care promit soluții de antivirus**, dar creează în schimb abonamente la servicii cu supra-taxă care livrează imagini pentru ecran și screensaver-e.

Specialiștii Bitdefender au identificat bannere de reclamă în diverse aplicații legitime de Android, care lansează atacuri menite să păcălească utilizatorii să cumpere un produs fals de securitate. Printre reclamele livrate de platforma InMobi s-a strecurat un banner care afișează pe ecranul smartphone-ului mesajul precum că dispozitivul este infectat cu viruși. Ca să-l dezinfecteze, utilizatorul trebuie să acceseze un link ca să descarce soluția de AV. De fapt, în loc de soluția AV, utilizatorul este păcălit să-și facă un abonament de 3 sau 4 euro pe săptămână prin care pot avea acces la tonuri de apel premium și wallpaper-e. Abonamentul poate fi întrerupt doar manual.



Dacă nu aveți nicio soluție de securitate instalată pe smartphone sau tabletă, nu ar trebui să vi se afișeze niciun mesaj de tip pop-up care să vă informeze cu privire la diverse infecții. Nu vă grabiți

să urmați instrucțiunile din aplicație. Dacă însă folosiți o soluție antivirus dedicată, trebuie să știți că nicio aplicație legitimă nu vă cere bani în plus pentru a curăța sistemul de viruși.

În acest caz particular, dezabonați-vă imediat trimițând un SMS la numărul menționat în secțiunea Termeni și Condiții. Trebuie doar să mergeți în josul paginii unde v-ați abonat inițial. Dezinstalați aplicațiile pe care le-ați descărcat recent. O soluție AV care să blocheze paginile este de asemenea foarte utilă. Bitdefender recomandă folosirea software-ului Clueful, care vă informează la ce tip de informații au acces aplicațiile pe care le instalați și care sunt riscurile pe care vi le asumați instalându-le.

Un studiu recent Bitdefender a dezvăluit că multe jocuri și aplicații pentru copii monitorizează locația copiilor în ciuda reglementărilor COPA (Children's Online Privacy Protection Act), care prevede ca dezvoltatorii de soft să nu acceseze date cu caracter personal fără acordul prealabil și explicit al părinților.

În ciuda acestor prevederi, există însă jocuțe și soft educațional, precum Kids ABC Games şi Educational Puzzles care monitorizează locația copiilor și accesează funcția de geolocație. Dat fiind faptul că profilul aplicațiilor nu justifică o astfel de funcție, cel mai probabil dezvoltatorii colectează aceste date pentru a le trimite unor terțe-părți care folosesc aceste informații în scopuri publicitare.

Alte aplicații pentru copii încearcă deasemenea să acceseze istoricul căutarilor pe net sau ID-ul unic al dispozitivului.

3. FENOMENUL BYOD IN COMPANII

BYOD face referire la obiceiul angajaților de a aduce la locul de muncă și de a folosi atât în interes de serviciu cât și în interes personal dispozitivele mobile proprii, precum telefonul, tableta sau laptopul. Această practică poate pune în pericol siguranța informațiilor unei companii dacă angajații și firma nu iau măsuri de protecție serioase care să le apere datele.

In primul rând, toate dispozitivele mobile personale trebuiesc înregistrate atunci când accesează rețeaua companiei. Punctele de access (Hot spots) neautorizate trebuie interzise cu desăvârșire în cadrul rețelei companiei iar un dispozitiv care se conectează la WI-FI-ul autorizat de companie trebuie să permită doar autentificarea bazată pe datele de conectare din domeniu sau cu certificate digitale. Angajații trebuie să înțeleagă responsabilitatea pe care o poartă atunci când manavrează date sensibile ce țin de companie pe dispozitive personale în afara spațiului firmei.

Dacă pierd, rătăcesc sau li se fură un telefon mobil sincronizat cu e-mailul de serviciu, multe informații aparent inofensive pot ajunge pe mâini necunoscute și pot constitui un prim pas întrun atac de lungă durată care întotdeauna începe cu colectarea de date.

4. METODE DE ÎMBUNĂTĂȚIRE A SECURITĂȚII TERMINALELOR MOBILE[2]

În afara casei, telefoanele mobile și tabletele devin cele mai utilizate dispozitive electronice, iar provocările și amenințările asociate acestora sunt diferite și necesită o abordare specială. Principalele probleme care pot apărea sunt furtul sau pierderea dispozitivelor, descărcarea de aplicații ce conțin viruși, fură informații sensibile și direcționează utilizatorii către site-uri și documente compromise.

4.1 Fiți atenți ce aplicații descărcați și de unde

Descărcați aplicații numai din magazinele oficiale ale operatorilor și producătorilor precum Google Play și Apple App Store. Soft-urile provenite de la distribuitorii neoficiali vă pot infecta telefonul sau tableta și pot trimite mai departe, unor terțe părți informații private.

În zone necunoscute, ați putea fi tentați să descărcați aplicații care să vă ajute să găsiți diferite locații precum restaurante, hoteluri sau muzee. Aveți însă încredere doar în cele care provin din surse autorizate. Pentru a evita descărcarea aplicațiilor nesigure din greșeală, verificați configurația terminalului accesând SETĂRI, SECURITATE și asigurându-vă că opțiunea SURSE NECUNOSCUTE este NEbifată.

4.2 Accesați doar hot-spot-uri sigure

Hotspot-urile wireless publice sunt vulnerabile interceptărilor de trafic și răspândirii virușilor, întrucât nu sunt protejate de parole și pot fi accesate de oricine. Imaginați-vă că cineva aflat în apropiere vă interceptează pachetele de date și vede tot ce faceți pe internet. Asigurați-vă că opțiunile de infraroșu, Wi-Fi și Bluetooth-ul sunt oprite atunci când nu le utilizați. Acestea vor consuma bateria și pot facilita accesul neautorizat la datele de pe dispozitivul mobil.

4.3 Opriți serviciul de date mobile atunci când nu îl utilizați

Dacă sunteți în afara țării, nu uitați că serviciile de internet în roaming sunt foarte scumpe iar o aplicație a unei rețele sociale care încearcă să se actualizeze la fiecare cinci minute va costa mai mult decât întregul plan de date achiziționat.

4.4 Nu publicați pe platformele sociale detalii referitoare la locația în care vă aflați

Dacă vă actualizați regulat conturile de social media și împărtășiți cu toată lumea unde sunteți și ce faceți iar profilul dumneavoastră nu este accesibil exclusiv prietenilor, aţi putea ajunge să spuneți unor persoane complet străine că nu sunteți acasă. Ați fi de acord să puneți afișe mari prin tot orașul prin care să faceți public locul în care vă aflați?

[2] http://www.bitdefender.ro/news/ghid-de-protectie-a-terminalelor-mobile-in-vacanta-2791.html

4.5 Fiți atenți la ofertele prea bune pentru a fi reale

Dacă primiți dintr-o dată oferte incredibil de avantajoase cu hoteluri de lux la prețuri foarte mici, rezervări de apartamente sau oferte de reîncărcare a telefonului mobil, ignorați-le. Un click pe link-urile incluse în emailuri pot infecta telefonul sau tableta sau vă pot atrage să completetați formulare cu informații personale.

4.6 Protejați-vă terminalul cu parole și opțiuni de criptare

În cazul în care cineva vă fură sau vă găsește telefonul mobil, îngreunați-i accesul la informațiile stocate. De asemenea, criptați datele cu ajutorul unui software dedicat sau – dacă dispozitivul o permite – cu ajutorul opțiunii de criptare disponibilă în terminal. Folosiți programe anti-theft pentru a vă găsi telefonul, a-l bloca sau a șterge informațiile de pe el de la distanță.

4.7 Tranzacțiile online folosind hotspot-uri nesecurizate sunt riscante

Autentificarea în orice cont de bancă implică date sensibile. Tastarea datelor sensibile în timpul conexiunilor nesecurizate este riscantă, întrucât traficul poate fi urmărit de persoane neautorizate. Pentru tranzacții bancare sigure puteți folosi un laptop, iar dacă acesta rulează Windows, o soluție dedicată precum Safepay vă ajută să efectuați tranzacții bancare în siguranță.

4.8 Nu accesați linkurile sau documentele atașate în emailuri venite la întâmplare.

La fel ca și pe computer, e-mailurile pot avea documente atașate care conțin viruși pentru terminale mobile, iar un click pe un astfel de link vă poate instala software periculos pe telefon.

4.9 Instalați un program de protecție antivirus

Instalarea unei soluții antivirus și a unei soluții de protecție a datelor personale este imperativă. Alegeți însă o sursă reputată și urmăriți furnizorii care oferă și soluții de securitate pentru PC pentru a evita soluțiile de securitate false.

4.10 Mențineți software-ul actualizat

Menținându-vă sistemul de operare și aplicațiile actualizate, vă asigurați că aveți cele mai recente versiuni de software pentru a face față celor mai recente amenințări. Pentru protecția terminalelor mobile cu Android, Bitdefender recomandă folosirea soluției complete de securitate Bitdefender Mobile Security.

5. **BIBLIOGRAFIE**

1. "*Gartner Says Worldwide PC, Tablet and Mobile Phone Shipments to Grow 5.9 Percent in 2013 as Anytime-Anywhere-Computing Drives Buyer Behavior*", comunicat de presă, 24 iunie 2013

2. *”Ghid de protecție a terminalelor mobile în vacanță. Principalele probleme care pot apărea sunt furtul sau pierderea dispozitivelor sau descărcarea de aplicații ce conțin viruși*”, comunicat de presă Bitdefender, 30 iulie 2013