1. Cele mai întâlnite tipuri de amenințări informatice • Viruși: virușii informatici sunt programe care se autocopiază pe sistemul compromis, fără știrea utilizatorului. Virusul va infecta astfel componente ale sistemului de operare sau alte programe informatice. • Viermi: programe care se pot auto-replica. Acestea folosesc rețeaua de calculatoare pentru a-și trimite propriile copii ȋn alte noduri (calculatoare din rețea), reușind să facă acest lucru fără intervenția vreunui utilizator. Spre deosebire de un virus informatic, un vierme informatic nu are nevoie să fie atașat la un program existent. Viermii provoacă daune rețelei, chiar și prin simplul fapt că ocupă bandă, ȋn timp ce virușii corup sau modifică aproape ȋntotdeauna fișiere de pe computerul țintă. • Troieni: aceste programe se prezintă sub forma unor programe legitime, care, în realitate, sunt create cu scopul de a fura date confidențiale, sau de a permite unor utilizatori sau programe neautorizate accesul la sistemul infectat. • Spyware: o categorie de software malițios, ataşate de obicei la programe gratuite (jocuri, programe de schimbat fișiere, programe de video chat etc.), care captează pe ascuns date de marketing (prin analiza site-urilor pe care le vizitează utilizatorul, de exemplu de modă, pantofi, cluburi de tenis, ș.a.m.d.) și le folosesc apoi pentru a transmite utilizatorului reclame corespunzătoare dar nesolicitate. • Adware: orice program care afișează reclame la rularea acestuia, reclame care pot fi afișate ca bannere în fereastra programului, sau de tip pop-up (care deschide ferestre noi cu reclame, deasupra tuturor ferestrelor). Unele programe adware pot fi considerate o formă de spyware care nu colectează date de marketing, ci doar transmit reclame. • Rootkit: un rootkit este o colecţie de utilitare proiectate să menţină controlul sau accesul la calculator. Dupa instalare, rootkit-ul utilizează funcţii ale sistemului de operare pentru a se “ascunde” astfel încât să rămână nedetectat. Rootkit-urile au fost Pagină 5 din 15 utilizate mai întâi în Unix, dar sunt folosite în prezent şi în Linux, Windows şi alte sisteme de operare. Acestea pot fi folosite în scopuri legale, dar sunt cunoscute în general pentru utilizarea lor în scopuri maliţioase. • Spam: mesaje electronice nesolicitate, de cele mai multe ori cu caracter comercial, de publicitate pentru produse și servicii dubioase, folosite de industria emarketingului și de proprietarii de site-uri cu un conținut indecent. Mesajele spam sunt trimise cu ajutorul unor calculatoare infectate cu troieni, care fac parte dintrun botnet (o rețea de calculatoare compromise utilizate pentru trimiterea de spam sau atacuri asupra unor site-uri de internet, fără știrea posesorilor calculatoarelor respective). Mesajele spam, deși nu sunt un program malițios în sine, pot include atașamente care conțin astfel de programe, sau trimit utilizatorii către pagini de internet periculoase pentru siguranța sistemului. • Hacker: o persoană care pătrunde în calculatoare (fără acordul proprietarului), de obicei prin accesarea controalelor administrative. Auxiliar amenințărilor reprezentate de programe create cu scopul compromiterii siguranței sistemului, dorim să atragem atenția asupra tehnicilor de manipulare socială, cele mai des utilizate fiind practicile de phishing și scam, ce urmăresc manipularea utilizatorilor astfel încât aceștia să furnizeze de bunăvoie informații importante, precum sunt datele bancare.

2. Reguli generale de securitate Pentru a asigura integritatea calculatorului și a datelor personale, vă recomandăm respectarea următoarelor reguli: • Instalați o soluție de securitate ce oferă cel puțin protecție la nivel antimalware, antispam și antiphishing • Aveți în vedere ca soluția de securitate instalată să fie permanent actualizată • Nu deschideți atașamente și nu accesați link-urile ce vin din partea unor expeditori necunoscuți. Dacă este absolut necesară deschiderea unui atașament, se recomandă ca acesta să fie descărcat și scanat cu soluția antivirus instalată pe calculator • Nu deschideți atașamentele și nu dați click pe link-urile din mesajele spam • Nu folosiți niciodată calculatoare publice pentru a efectua tranzacții bancare, sau pentru alte tipuri de achiziții online. Aceste calculatoare ar putea conține programe care înregistrează datele personale, precum troienii bancari • Evitați să faceți shopping online atunci când sunteți conectați la un hotspot Wi-Fi public, precum cele din aeroporturi, cafenele sau mall-uri. De obicei, informațiile schimbate între dumneavoastră și magazinul online, nu sunt criptate, și pot fi interceptate ușor de către un atacator • În cazul în care vă conectați la hotspot-uri publice nesecurizate, utilizați o aplicație firewall care să filtreze accesul din exterior • Dezactivați funcția ”Network Share” înainte de a vă conecta la un hotspot public • Atunci când doriți să achiziționați software online, introduceți adresa de internet manual în bara de adresă a browserului. Este de preferat să utilizați calculatorul personal, sau unul care nu este utilizat in mod public de către alți utilizatori, iar conexiunea la internet ar trebui sa fie sigură (rețeaua de acasă sau un modem 3G) Pagină 7 din 15 • Verificați în mod repetat pagina de internet a furnizorului dumneavoastră de internet și instalați toate patch-urile puse de către aceștia la dispoziție • Evitați să accesați link-uri care sunt marcate drept periculoase de către soluția de securitate instalată pe sistem, sau de către browser-ul de internet. Dacă primiți orice mesaj de atenționare în timpul navigării pe o pagină, ieșiți imediat de pe respectiva pagină de internet • Nu instalați software din locații despre care nu sunteți sigur, mai ales software care pare să fie codec. În schimb, accesați pagina producătorului pentru a descărca acest tip de program. • Nu vă lăsați amăgiți de probleme privind cardul de credit, sau invitații diverse care provin din partea unor surse necunoscute. Atunci când găsiți astfel de mesaje în inbox, luați legătura cu banca (sau mergeți personal la bancă) pentru a vă asigura ca totul este în regulă referitor la contul dumneavoastră. • Nu trimiteți niciodată parolele dumneavoastră de cont prin e-mail sau prin atașamente. Nici un furnizor de servicii nu ar trebui să solicite astfel de informații, având în vedere că ar trebui să le aibă deja. • Este greu de imaginat că o agenție guvernamentală v-ar contacta prin internet pentru a colecta o amendă, așadar, tratați astfel de mesaje cu suspiciune și sub nici o forma nu accesați link-urile sau atașamentele conținute de mesajul respectiv. • În această situație, chiar și existența unei soluții de securitate eficiente, factorul uman joacă un rol decisiv. Ingineria socială poate ajuta un hacker sau un program să stabilească o conexiune cu utilizatorul, și convingerea acestuia în a oferi date critice sau bani. Așadar, atunci când doriți să cumpărați online bilete de orice fel, asigurațivă că este un site pe care îl cunoașteți dinainte, și, alternativ, verificați cât mai multe comentarii ale utilizatorilor despre serviciile respectivului website. De asemenea încercați să contactați un reprezentant al companiei, care să vă ofere cât mai multe informații posibil.

3. Reguli de securitate în cadrul rețelelor sociale • Alegeți o parolă pentru contul dumneavoastră care să nu fie ușor de ghicit de către un alt utilizator sau program. În acest sens, evitați parolele generice, precum ”123456789” sau ”parola” sau o parolă identică cu numele de utilizator; • Asigurați-vă că știți pe cine urmăriți și pe cine adăugați drept prieten • Evitați să accesați link-urile împărtășite de către alți utilizatori; • Evitați să faceți publice informații personale, precum ziua de naștere, adresa de email sau adresa fizică; • Atunci când împărtășiți poze, asigurați-vă că o faceți doar cu persoanele cunoscute • Nu dezvăluiți niciodată informații referitoare la perioadele în care părăsiți locuința (mesaje precum: ”plec la mare tot weekend-ul; ”sunt singur acasă” trebuie evitate) • Utilizați o soluție de securitate specializată, care să scaneze mesajele și comentariile, și care să verifice nivelul de securitate al informațiilor confidențiale;

4. Reguli de folosire a telefoanelor inteligente (smartphones) Smartphone-urile joacă un rol esențial în felul în care comunicăm și ținem legătura cu cei dragi. Securitatea acestor dispozitive este, de multe ori, trecută în afara priorităților, deoarece utilizatorii percep aceste dispozitive ca pe niște simple telefoane, și nu ca pe minicalculatoare ce sunt. Pagină 11 din 15 • Când folosiți rețelele sociale, asigurați-vă că fotografiile făcute cu smartphone-ul și pe care doriți să le încărcați pentru a le partaja cu prietenii, nu conțin informații legate de poziția dumneavoastră actuală. Partajarea locației e ideala pentru întâlnirile cu amicii în locuri publice, dar în același timp, permit persoanelor răuintenționate să vă monitorizeze obiceiurile și rutina zilnice facilitând tentativele de hărțuire; • Sincronizați-vă telefonul cu un calculator personal. În cazul în care pierdeți smartphone-ul sau acesta este furat, veți avea o copie de siguranță a contactelor, mesajelor, imaginilor și documentelor de pe acesta; • Folosiți o soluție de securitate pentru telefoane mobile care să aibă un modul antifurt, în mod special dacă folosiți un telefon care rulează Android. Din cauza cotei de piață ridicate, telefoanele bazate pe Android au devenit ținta predilectă a infractorilor informatici. O soluție antivirus vă permite să filtrați aplicațiile potențial periculoase și să le blocheze înainte ca acestea să cauzeze modificări asupra sistemului. În cazul în care pierdeți telefonul sau vă este furat, modulul de antifurt vă poate ajuta să identificați și să recuperați telefonul, chiar dacă acesta nu are acces la Internet. În cazul în care recuperarea este imposibilă, puteți bloca definitiv accesul la telefon și la datele acestuia și, întrun final, să ștergeți toate informațiile dumneavoastră de pe acesta printr-un simplu SMS; • Nu uitați că telefonul dumneavoastră este de fapt un mini-calculator personal, care poate fi infectat prin simpla vizitare a unui website sau prin accesarea unui link dintrun mesaj. Înainte de a accesa un link, asigurați-vă că site-ul pe care doriți să-l vizitați e de încredere. Dacă nu aveți informații despre site sau dacă nu recunoașteți link-ul, cel mai bine este să evitați accesarea acestuia; • Aveți mare grijă la ce fotografiați. Puteți fi tentat să fotografiați și să procesați coduri QR (coduri de bare care stochează informații despre diverse produse sau linkuri către website-uri). Dacă fotografierea și procesarea codurilor QR de pe ambalajele produselor nu sunt, de obicei, periculoase, puteți găsi coduri QR lipite în locuri publice sau chiar desenate pe elemente de mobilier stradal, ziduri etc. Aceste coduri pot conține URL-uri către website-uri care să exploateze vulnerabilități din telefonul dumneavoastră care să se finalizeze cu o infecție.