Protecţia telefoanelor inteligente (smartphone)

Ce puteţi face pentru vă proteja smartphone-ul?

Telefoanele inteligente (smartphone), dispozitive care combină capabilităţile telefonului mobil cu cele ale unui PDA sau chiar ale unui laptop sunt, de asemenea, o ţintă pentru malware. Pentru a utiliza în condiţii de siguranţă aceste dispozitive se recomandă să luaţi măsuri similare cu cele care se aplică computerului personal.

Infectarea cu malware pe telefonul mobil poate:
- "umfla" factura lunară, de exemplu prin trimiterea de mesaje;
- distruge sau fura informaţii personale;
- supraîncărca conexiunea la reţea sau procesorul telefonului.

- **Acces controlat la telefon:** Se recomandă activarea unei forme de acces controlat la aparat, precum un cod PIN (doar cifre), o parolă (orice caractere), un model de blocare sau amprenta unui deget. Codul PIN este un număr care se introduce pentru a accesa dispozitivul. Parola pentru dispozitive mobile funcţionează la fel ca parola pe computer sau pe un cont personal online. O parolă puternică oferă o securitate mai mare decât o parolă de tip PIN. Modelul de blocare este un model grafic stabilit de dumneavoastră care se desenează pe ecranul dispozitivului pentru a-l debloca. Luați serios în considerare permiterea opţiunii de a şterge dispozitivul, în cazul în care mai multe încercări de a debloca dispozitivul nu au reuşit, pentru a vă proteja datele sau în caz de furt al aparatului dumneavoastră. Totuși, dacă selectaţi opţiunea de a şterge conţinutul dispozitivului după mai multe încercări eșuate de autentificare, nu subestimați curiozitatea copiilor. În orice caz, asiguraţi-vă că vă păstraţi un backup al aparatului dumneavoastră.

- **Urmărire și ștergere de la distanţă:** Cele mai multe dispozitive mobile suportă aplicații specifice care pot localiza de la distanţă un dispozitiv care este pierdut şi chiar să şteargă conținutul de la distanţă. Trebuie să instalaţi și să activaţi astfel de aplicații cât timp aveţi aparatul în posesie. Dispozitivele cu sistem de operare IOS (iPhone şi iPad) oferă această funcționalitate din contul iCloud cu aplicaţia, cunoscută ca "Find My iPhone" care este activată dintr-un cont Apple ID. Dispozitivele BlackBerry sau pot fi administrate de la distanță din contul online (conectarea se face cu BlackberryID) după activarea pe dispozitiv a funcției BlackberryProtect. În cazul dispozitivelor cu sistem de operare Android trebuie să vă conectați cu contul personal Google la Android Device Manager online pentru detectarea de la distanţă şi ştergerea datelor. Similar, pentru telefoanele cu sistem de operare Windows Phone, administrarea de la distanță se face de pe pagina Windows Phone după ce vă conectați cu contul personal Microsoft sau Live. Unii producători de telefoane oferă aplicații proprii în acest scop. Indiferent de dispozitiv, această funcționalitate necesită activare. Consultați manualul aparatului și al serviciilor utilizate pentru detalii.

- **Criptare:** Dacă cineva are acces fizic la aparatul dumneavoastră, ar putea folosi, eventual, tehnologii avansate care ocolesc parola și codul PIN pentru a accesa datele. Criptarea dispozitivului vă protejează datele de astfel de atacuri avansate. Unele dispozitive utilizează implicit criptare, în timp ce pentru altele trebuie activată această opțiune sau necesită instalarea unei aplicații de către utilizator.

- **Backup:** Copiile de rezervă ale dispozitivului oferă posibilitatea de a recupera imediat datele în cazul în care aparatul este pierdut sau furat. Copia de rezervă trebuie să fie creată în mod regulat, şi poate fi făcută prin conectarea direct la computer sau prin servicii cloud. Utilizatorul poate să alegă să salveze contacte, e-mail, calendar, imagini, muzică şi alte fișiere.

- **Protejarea dispozitivelor interconectate:** Toate dispozitivele care se conectează la dispozitivul dumneavoastră trebuie protejate prin programe de protecţie împotriva malware-ului. Malware-ul poate fi transferat la un dispozitiv mobil de la computerul dumneavoastră sau viceversa.

- **Utilizarea Bluetooth în condiţii de siguranţă:** Bluetooth este o tehnologie care permite comunicarea şi schimbul de date fără fir între dispozitive care sunt în imediata apropiere. Tehnologia Bluetooth poate fi utilizată și pentru a transmite malware între dispozitive mobile. Utilizați tehnologia Bluetooth astfel incât aparatul să nu fie "vizibil" altora. Dacă telefonul este vizibil, există un risc de a vă infectata cu malware de pe dispozitivele aflate în apropiere. Trebuie să fiți atenţi la instalarea de programe sau fişiere primite prin Bluetooth. Dacă vi se solicită de către aparat să instalați un program necunoscut, evitați acest lucru.

- **Protecţie email / MMS:** Email-urile primite pe dispozitivele mobile (email, MMS), trebuie tratate în acelaşi mod ca atunci când le primiți pe computerul personal. Dacă un mesaj pare suspect sau nu cunoaşteţi expeditorul, nu îl deschideți.

- **Descărcarea fişierelor de pe Internet:** Evitați descărcarea în dispozitiv de conținut de pe Internet dintr-o sursă necunoscută sau care nu prezintă încredere.

- **Instalare antivirus:** Există produse antivirus pentru protecția telefoanelor inteligente împotriva malware-ului. Cele mai multe dispozitive vin cu o aplicație antivirus preinstalata, care are nevoie să fie activată. Dacă nu aveți o soluție antivirus instalată, vă recomandăm să instalați una.

Notă: “malware” este un termen generic prin care se înțelege software care infectează sistemele informatice cu scopul de a sustrage informații, de a provoca daune materiale sau întreruperi ale serviciilor.