AUTORITATEA DE SUPRAVEGHERE FINANCIARĂ

Malware-ul este un program malițios, un software creat cu scopul de a distruge sau strica funcționarea unui computer sau telefon. Cel mai adesea, malware-ul este distribuit prin email-uri cu atașamente sau link-uri sau prin accesarea diferitelor ferestre pop-up apărute în timpul navigării pe internet sau a folosirii unor aplicații. Scopul malware este ca fraudatorii să preia controlul asupra dispozitivului, pentru a șterge sau infecta fișiere (virus), a obține informații (worms), a fura date personale (trojans), a înregistra ce face utilizatorul pe dispozitiv (spyware), a bloca accesul la fișiere și informații sub amenințarea ștergerii lor dacă nu este plătită o recompense (ransomware), a folosi dispozitivul fără voia proprietarilor (botnets), a afișa publicitate agresivă și cu un conținut malware (adware), a urmări tastele apăsate (keylogging), a prelua controlul dispozitivului (SQL injection), a schimba fișierele unui sistem de operare (fileless malware), a permite controlul de la depărtare (rootkits), a șterge definitive date (wiper malware) etc.

AUTORITATEA
DE SUPRAVEGHERE
FINANCIARĂ

Phishing-ul este o tehnică a fraudatorilor prin care într-un email sau mesaj (SMS, mesaj social media etc.) aceștia pretind că reprezintă entitatea financiară cu care ai o relație (bancă, intermediar, asigurător etc.) și că verifică informațiile tale individuale, pentru o mai bună „securitate". Este important să știi că nicio entitate financiară autorizată nu va solicita în acest mod actualizarea sau verificarea datelor personale sau de cont. Astfel de operațiuni se fac personal sau prin intermediul aplicației proprii a entității. Aceste mesaje pot avea greșeli de scriere sau de gramatică sau numele adresantului redat incorect sau incomplet (în orice corespondență sau dialog cu o entitate reglementată, numele trebuie să apară exact așa cum este în contractul cu aceasta). Mesajele pot conține link-uri către site-uri aproape identice cu cele ale entității reale. Pentru a te proteja, nu accesa link-ul, accesează site-ul separat de mesaj, prin calea URL pe care o cunoști. Poți lua contact cu entitatea pentru a verifica dacă mesajul transmis este chiar de la aceasta.

Smishing-ul este o formă de phishing prin SMS, prin care se primesc facturi false, link-uri care „trebuie" accesate pentru a revendica un premiu câștigat, link-uri care „trebuie" accesate pentru actualizarea de date la un cont financiar sau la un curier, link-uri în care se solicită actualizarea de date personale pentru o aplicație financiară sau a unei instituții, link-uri care te conduc spre platforme false sau frauduloase de tranzacționare ș.a.

AUTORITATEA DE SUPRAVEGHERE FINANCIARĂ

Vishing sau voice phishing este o abordare ilegală în care fraudatorii apelează telefonic posibila victimă, pretinzând că sună din partea unei entități financiare sau a unei autorități. De regulă, ei încearcă să convingă posibila victimă să acceseze imediat un cont financiar (pentru verificare, plată etc.), făcând-o astfel să dezvăluie informații importante (nume, cont, detalii de logare etc.).

Spoofing-ul este o activitate online frauduloasă prin care este falsificat un email, o identitate telefonică sau un profil de whatsapp, un site etc., expeditorul real fiind ascuns sub o identitate falsă, de regulă a unei instituții sau entități de încredere. Astfel sunt distribuite malware-urile sau phishing-ul, destinatarul încrezându-se în falsa identitate și devenind victimă. Number spoofing este o tehnică a fraudatorilor prin care numărul de telefon afișat este similar cu cel al entității financiare.

Baiting-ul este un atac în care victimele sunt păcălite să dea informații în schimbul promisiunii că vor primi recompense (ex. anunțuri pop-up care oferă gratuit o aplicație, joc etc.) și odată accesat acest link dispozitivul este infectat cu un malware. Similar este și Scareware, care apare sub forma unui pop-up în browser care anunță că dispozitivul a fost infectat și victima trebuie să facă click pe un buton care înlătură virusul sau asigură un antivirus gratuit.

Watering hole este o infectare a unui site pe care îl vizitezi des, iar atunci când îl accesezi este automat descărcat un malware (drive-by-download) sau ești direcționat către o versiune clonă (cu scopul de a-ți fura datele personale sau de cont).

Și lista de mai sus se diversifică constant.