Članak

27-01-2022 - 22:40
20200327STO76003

Europski parlament

Kako se zaštititi od kibernetičkog kriminala

©Vitalii Vodolazskyi/AdobeStock

Od početka pandemije Covid-19 kibernetički kriminal je u porastu jer zlonamjerni pojedinci žele iskoristiti situaciju i prisutan strah. Pročitajte kako se zaštititi.

Uvođenje mjera za ograničavanje širenja koronavirusa dovelo je do toga da više vremena provodimo na internetu, bilo radeći od kuće ili u pretraživanju vijesti. Zbog zabrinutosti prouzročene krizom, često nismo dovoljno oprezni, a kiberkriminalci iskorištavaju te slabosti.

Uz pomoć internetske krađe podataka (phishing), instalacije štetnog softvera (malware) i drugih štetnih praksi uzimaju podatke i pristupaju uređajima kako bi došli do bankovnih računa ili baza podataka organizacija.

Saznajte više o glavnim i rastućim prijetnjama kibersigurnosti

Najčešći oblici Covid-19 kibernetičkih napada

- Lažne poruke ili poveznice (vijesti o čudotvornim lijekovima, lažne karte o širenju virusa, zahtjevi za donacijama, poruke u ime organizacija zdravstvene skrbi) koje iskorištavaju zabrinutost i vode do štetnih internetskih stranica ili softvera
- Lažne poruke ili pozivi u ime Microsofta, Googlea Drivea itd. kojima se pokušava doći do korisničkog imena i lozinke, uz lažno nuđenje „pomoći" ili poruke o ugrožavanju vašeg računa.
- Lažne poruke o nepostojećim isporukama paketa

Kako se zaštititi na internetu?

EU zajedno s telekomunikacijskim operaterima radi na zaštiti mreža od kibernapada, no unatoč tome, primijenite sljedeće savjete i zaštitite se kod korištenja interneta i rada na daljinu.

- **Budite oprezni oko e-pošte, SMS poruka i telefonskih poziva za koje ne znate,** posebno ako koriste krizu i stvaraju pritisak kako biste zaobišli uobičajene sigurnosne postupke. Napadači znaju da je često lakše prevariti ljude nego „provaliti" u složeni sustav. Zapamtite, banke i drugi pravni subjekti nikad neće tražiti otkrivanje vaše lozinke.
- **Osigurajte svoju mrežu.** Promijenite inicijalno dobivenu lozinku za bežičnu mrežu i pritom izaberite „jaku" lozinku. Ograničite broj uređaja spojenih na vašu bežičnu mrežu i dopustite spajanje samo pouzdanim uređajima.
- **Jačanje lozinki.** Upotrijebite duge i kompleksne lozinke koje sadrže brojeve, slova i posebne znakove.
- **Zaštitite svoju opremu.** Provjerite sve svoje sustave i aplikacije i instalirajte softver za suzbijanje virusa.
- **Obitelj i gosti.** Vaša djeca i drugi članovi obitelji mogu slučajno izbrisati ili izmijeniti podatke, ili još gore, postati žrtve kibernetičkog napada, pa im ne dozvolite korištenje uređaja koji vam služe za posao.

Dodatni savjeti o tome kako zaštititi sebe i svoje poduzeće

Europske mjere za internetsku sigurnost

Europski parlament već dugo podupire mjere EU-a za internetsku sigurnost jer pouzdanost i sigurnost mrežnih i informacijskih sustava i usluga imaju ključnu ulogu u društvu.

Institucije EU-a, kao što su Europska komisija, Agencija Europske unije za kibersigurnost, CERT-EU i Europol, prate zlonamjerne aktivnosti, podižu svijest i štite građane i poduzeća te će to i dalje činiti.

Daljnje informacije

Suzbijanje dezinformacija na internetu
CERT-EU: Najnovije vijesti o COVID-19 kiberprijetnjama
Podizanje svijesti o kibersigurnosti: Europski mjesec kibersigurnosti