Newsletter Nacionalnog CERT-a – CERT info

Sadržaj

Tema mjeseca: Sigurnost na društvenim mrežama

Društvene mreže postale su sastavni dio načina na koji komuniciramo, izražavamo se i ostajemo povezani, a osmišljene su kako bi povezivale ljude - bilo dijeljenjem novosti s prijateljima, otkrivanjem novih trendova, izgradnjom profesionalnih odnosa ili jednostavnim praćenjem vijesti. Društvene mreže su digitalna središta društvenih interakcija koje odražavaju stvarni život, često na javniji i trajniji način nego što mislimo.

Među najpopularnijim platformama danas su Facebook, Instagram, X (bivši Twitter), LinkedIn, TikTok, Snapchat i Reddit. Svaka od njih ima svoju svrhu - neke su fokusirane na vizualni sadržaj, druge na kratke videozapise ili profesionalno umrežavanje - ali sve dijele jednu zajedničku značajku: prikupljaju i prikazuju goleme količine korisničkih podataka. Koliko god nam se to činilo korisno, može biti i opasno.

Osim savjeta za sigurnost na društvenim mrežama, donosimo vam i informacije o drugom Hackultet natjecanju na kojem je sudjelovalo čak 80 studenata.

Fear of missing out - FOMO

Jedan od psiholoških pokretača pretjeranog korištenja društvenih mreža svakako je **FOMO - *strah od propuštanja***. To je snažan osjećaj koji korisnike potiče da neprestano provjeravaju objave, uspoređuju se s drugima i osjećaju pritisak da moraju sudjelovati u internetskim trendovima. Potreba za stalnim prisustvom često dovodi do pretjeranog dijeljenja informacija, kada korisnici, u potrazi za potvrdom ili iz straha da će biti zaboravljeni, otkrivaju više nego što su namjeravali. Uz FOMO, često se javljaju i tjeskoba, ovisnost o društvenim mrežama i uspoređivanje s drugima - sve to može zamagliti prosudbu pri dijeljenju osobnih podataka na internetu.

Izvor: pixabay.com

Digitalni trag i socijalni inženjering

Svaka objava, „lajk", komentar ili prijava lokacije doprinosi vašem digitalnom tragu. To je trag podataka koji ostavljate korištenjem interneta, često i bez vlastite svijesti o tome. Čak i sadržaj koji izbrišete može ostati pohranjen na poslužiteljima, indeksiran od strane tražilica ili sačuvan putem snimki zaslona. Npr., takve zapise stvara *wayback machine*, te pomoću njega možete provjeriti kako je određena stranica izgledala u prošlosti. Naizgled bezazlene aktivnosti poput komentiranja objava, dijeljenja lokacije ili sudjelovanja u izazovima mogu drugima pružiti zapanjujuće točnu sliku o vašoj osobnosti, navikama i načinu života.

Uz dovoljno podataka, platforme i treće strane mogu doznati mnogo o vama: vaša zanimanja, političke stavove, krug prijatelja, pa čak i dnevnu rutinu. I nisu samo oglašivači ti koji se zanimaju za te informacije. Kibernetički kriminalci i zlonamjerni akteri često koriste te osobne podatke kako bi osmislili uvjerljive prijevare ili *phishing* napade. Ta metoda, poznata kao socijalni inženjering, manipulira ljudskim ponašanjem kako bi zaobišla sigurnosne sustave. Na primjer, napadač se može predstaviti kao prijatelj ili kolega, poslati poruku koja izgleda poznato i hitno, i tako navesti žrtvu da klikne na zlonamjerni link ili otkrije povjerljive podatke. U drugim slučajevima, haker može prikupiti dovoljno tragova s vašeg profila da pogodi vašu lozinku ili prevari drugu osobu predstavljajući se kao vi.

Kibernetička higijena i postavke privatnosti

Zbog toga je **dobra kibernetička higijena** na društvenim mrežama od ključne važnosti. Koristite jake i jedinstvene lozinke za svaku platformu i omogućite višestruku autentifikaciju gdje god je to moguće. Redovito provjeravajte postavke privatnosti. Provjerite postavke kao što su ograničavanje pristupa vašim objavama, označavanju i zahtjevima za prijateljstvo jer tako značajno smanjuje izloženost. Također, izbjegavajte objavljivanje osjetljivih informacija poput kućne adrese, planova putovanja ili osobnih identifikatora poput datuma rođenja ili broja mobitela.

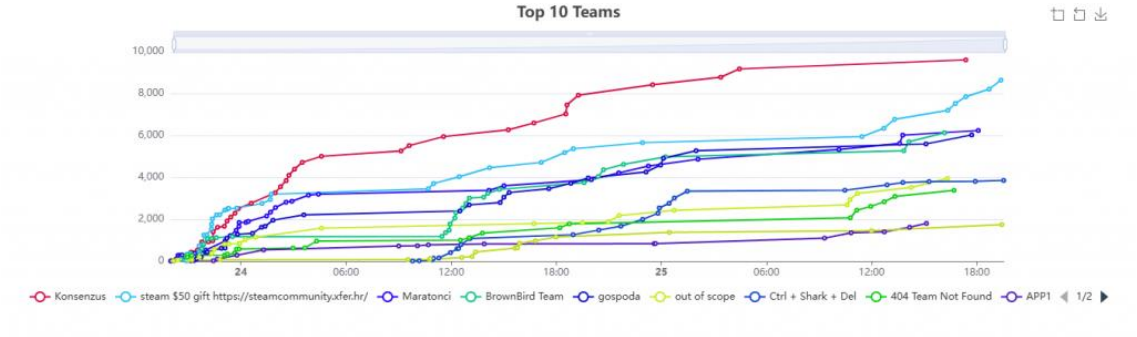
Svijest o prijetnjama i sumnjivim aktivnostima jednako je važna. Budite oprezni s neželjenim porukama, osobito onima koje traže osobne podatke, nude neočekivane prilike ili vas potiču da kliknete na poveznicu. Uvijek provjerite identitet osobe koja vas kontaktira s osjećajem hitnosti, čak i ako izgleda kao netko poznat. Dobra je praksa provjeriti istinitost drugim kanalom komunikacije i ne djelovati u afektu.

U konačnici, ključ sigurnosti na društvenim mrežama je **svjesnost**. Razmislite prije nego što nešto objavite, preispitajte ono što vidite i ne zaboravite da nije sve na internetu onakvo kakvo se čini. Ono što podijelite online može trajati mnogo dulje nego što mislite i koristiti se na načine koje niste mogli predvidjeti.

Društvene mreže nude nevjerojatne prilike za povezivanje i izražavanje, ali zahtijevaju oprez. Ako malo razmislimo o privatnosti i sigurnosti, možemo uživati u prednostima digitalnog svijeta bez ugrožavanja sebe ili svojih podataka.

Hackultet

Proveden je drugi Hackultet, CTF natjecanje iz kibernetičke sigurnosti za studente. Od 23. do 25. svibnja, 80 studenata okupljeni u timove rješavali su zadatke iz različitih područja kibernetičke sigurnosti. Pobjedu je odnio tim Konsenzus sastavljen od petorice studenata s različitih tehničkih fakulteta. Ovo im nije prvo CTF natjecanje te nije ni čudno da su se Antonio Fran, Višen, Lukas, Erik i Leo pokazali kao dobro uigrana ekipa.



Rezultati 10 najboljih timova s Hackulteta

Tim Konsenzus

Digitalni sadržaji o temi mjeseca

Donosimo vam sadržaje koje možete preuzeti i slobodno koristiti za vaše daljnje

Predavanje i prezentacija: Alisa u zemlji TikToka

Brošura „Ne budi i ti hrvatski naivac“

Članak: Lažna Facebook korisnička podrška

Infografika: Digitalni trag

Infografika: Zaštita računa na društvenim mrežama

Dokument: Socijalni inženjering

Predavanje i prezentacija: Socijalni inženjering

Statistika obrađenih incidenata – svibanj 2025.

Prema dostupnim statistikama Nacionalnog CERT-a za svibanj 2025. godine vidljivo je kako je najveći broj prijavljenih i obrađenih incidenata u kategoriji „phishing napad“.

Phishing napad	**61**	**38%**
Neželjene poruke	37	23%
Ostale vrste financijski motiviranih prijevara	28	18%
Pogađanje pristupnih podataka	13	8%
Napadačka infrastruktura	9	6%
Neovlaštena izmjena sadržaja	3	2%
Poslovne prijevare	3	2%
Ispad usluge	2	1%
Krađa pristupnih podataka	2	1%
Pokušaj iskorištavanja ranjivosti	1	1%
Uskraćivanje usluge	1	1%
Ukupno	160	

Prethodni brojevi

Newsletter Nacionalnog CERT-a – CERT info - siječanj 2025.

Newsletter Nacionalnog CERT-a – CERT info – veljača 2025.

Newsletter Nacionalnog CERT-a – CERT info – ožujak 2025.

Newsletter Nacionalnog CERT-a – CERT info – travanj 2025.

Newsletter Nacionalnog CERT-a – CERT info – svibanj 2025.