



INSPECTORATUL DE POLIȚIE JUDEȚEAN BRAȘOV BIROUL ANALIZA ȘI PREVENIREA CRIMINALITĂȚII

VIGILENȚA FACE DIFERENȚA !

Polițiștii Inspectoratului de Poliție Județean Brașov continuă activitățile de informare în cadrul Campaniei naționale ”*Vigilența face diferența*”, subscrise Programului național privind siguranța digitală. Aceasta își propune să ofere cele mai bune practici de securitate cibernetică, pentru a evita victimizarea în mediul online.

Obținerea frauduloasă (ilegală) a accesului la dispozitivele sau conturile tale de e-mail sau de pe rețelele de socializare nu este chiar atât de dificilă pe cât pare. Când auzim de hackeri, ne imaginăm că ne atacă niște genii, cu niște tehnici și instrumente demne de filmele SF.

ATENȚIE! Absolut orice poate fi furat de la tine, în materie de informații și date personale, poate fi vândut și refolosit într-o mulțime de moduri periculoase despre care tu nici nu ai habar.

Ce este furtul de identitate?

Infractorul cibernetic îți trimite un e-mail, de pe o adresă care pare în regulă, prin care te anunță că ai nu știu ce problemă cu contul bancar personal, cu adresa de e-mail sau cu contul de socializare și trebuie să o rezolvi urgent, altfel pierzi contul, banii, adresa de e-mail etc. Pentru asta, ți se cere să dai click pe un link și să completezi acolo datele care ți se cer. Din momentul în care ai dat click pe acel link, ai devenit victima criminalului cibernetic. Poți fi păcălit și prin telefon, de o persoană care pretinde că sună din partea unei surse de încredere (banca ta, un membru al familiei, o autoritate oarecare, cineva de la școală) care îți solicită informații confidențiale, cum sunt: adresa, nume complet, datele părinților etc.

Cum te afectează?

- Pierzi date personale generale și date sensibile;
- Pierzi accesul la conturi (e.g. e-mail, rețele de socializare etc.);
- Pierzi date financiare;
- Instalezi malware (virusi) și alte amenințări informatice;
- Poți infecta și alte dispozitive din rețea;
- Devii sursa atacurilor care vizează prieteni, instituții, organizații etc.

Cum îți dai seama că poți fi victima unui atac de tip phishing?

- Ți se atrage atenția și ești îndemnat să faci ceva URGENT!, cum ar fi să schimbi parole, să pui o adresă de e-mail alternativă pentru recuperarea celei de bază, și ți se dă o adresă care ți se cere să o folosești, să actualizezi datele personale etc. Trebuie să fii conștient însă că NIMIC nu este atât de urgent.

- Se solicită introducerea de date confidențiale folosind un link către un site indicat în textul mesajului sau deschiderea unui fișier atașat, care este infectat și tu nu știi.

NICIODATĂ banca nu-ți va cere, spre exemplu, să faci asemenea lucruri! Cum îți poți da seama?

- **Mesajele conțin erori gramaticale** (atacatorii nu sunt întotdeauna români și folosesc, spre exemplu, *Google translate* sau alte instrumente pentru a traduce text în limba română, ceea ce generează destule erori de exprimare, dezacorduri gramaticale etc.)

- **Ofertele sunt prea bune pentru a fi adevărate.** Chiar te crezi atât de norocos încât să primești gratuit un telefon ultimul răcnet, dacă tot ce trebuie să faci este să dai click pe un link și, eventual, să dai ceva date, dar nu trebuie să plătești nimic, sau o sumă derizorie?;

Cum te poți proteja? Poliția Brașov îți recomandă să fii vigilent în mediul online și să adopți un comportament preventiv pentru a evita victimizarea:

- **Nu deschide email-uri nesolicitate, care provin de la persoane necunoscute.** Nu le deschide nici dacă-ți vin de la prieteni, dar sunt reclame cu oferte prea frumoase să fie adevărate. Email-ul prietenului ar putea fi infectat și el să nu aibă habar că ai primit un asemenea mesaj de la el/ea. Te costă mai puțin să-l suni și să-l întrebi dacă mesajul primit este real și este ok. Nu-ți răspunde prietenul imediat? Nu intra în panică și nu te grăbi, crezând că pierzi marea ofertă sau marele cadou, dacă nu dai click pe linkul respectiv în următoarele 5 minute sau în următoarea oră. Nu uita că acestea intră în categoria „*E prea frumos să fie adevărat!*” și „*Nicio superofertă nu ține doar câteva minute/ore!*”.

- **Nu deschide fișiere atașate și nu accesa linkurile din mesaje nesolicitate.** Poți trăi și fără să vezi pozele sau filmulețele din atașamentul e-mailului sau fără să citești nemaipomenita poveste din documentul atașat sau de pe pagina unde te va duce linkul din corpul mesajului. Curiozitatea te poate costa foarte scump.

- **Raportează și șterge email-urile nesolicitate.**
- **Folosește o soluție de securitate!**