Bune practici privind siguranța tranzacțiilor online

Tranzacțiile online prezintă un anumit nivel de risc în ceea ce privește subminarea datelor cu caracter personal, dar există unele metode care pot limita acest risc, utilizând mijloace adecvate de prevenire.

Tipuri de atacuri ce vizează tranzacțiile online:

- **E-Skimming**: reprezintă atacuri care vizează comercianții care acceptă plăți online, prin schimbarea codului sursă al paginilor web ce aparțin magazinelor online, cu scopul de a obține în timp real accesul la datele de acces ale clienților.
- **Frauda Card-Not-Present (CNP)**: reprezintă un model de înșelătorie în care atacatorii încearcă să efectueze tranzacții frauduloase fără a deține cardul fizic.

RECOMANDĂRI privind siguranța tranzacțiilor online:

- **Verificați magazinele online -** pentru a vă asigura că acestea sunt legitime. Un site web de comerț dezvoltat recent poate fi un semn legat de o posibilă încercare de fraudă.
- **Verificați siguranța site-ului web** - utilizați site-uri web care beneficiază atât de un certificat digital, cât și de o conexiune de tip HTTPS (în stânga adresei URL ar trebui să puteți vedea semn distinctiv - un lacăt.
- **Evitați introducerea datelor cardului de credit pe site-uri web** - există numeroase site-uri în care sunt necesare datele cardului de credit pentru autentificare și, odată obținute acele credențiale, pot fi utilizate ulterior pentru tranzacții neautorizate.
- **Informați-vă despre drepturile dumneavoastră** - atunci când alegeți să achiziționați bunuri și servicii online și verificați procedura de rambursare.
- **Încercați să efectuați plăți online folosind carduri virtuale** - acestea pot fi reîncărcate doar cu sumele minime de bani de care aveți nevoie pentru tranzacții și care pot fi ușor înlocuite în cazul în care au fost compromise sau încercați să utilizați sisteme alternative, cum ar fi Paypal.
- **Unele magazine online oferă clienților posibilitatea de a păstra datele cardurilor** - pentru a facilita tranzacțiile. Examinați cu atenție aceste situații și riscurile asociate acestor site-uri web și posibilitatea ca acestea să fie compromise.
- Dacă considerați că ați fost victima unei fraude **Anunțați autoritățile competente**.
- **Fiți vigilenți** - dacă o ofertă este prea bună pentru a fi adevărată, luați în considerare că poate fi una falsă.

SERVICIUL TEHNOLOGIA INFORMAȚIEI
și SECURITATE CIBERNETICĂ