

## EKSPERCI OSTRZEGAJĄ PRZED OSZUSTWAMI W TRAKCIE CYBER MONDAY

---

Cyber Monday oznacza w USA zwiększony ruch w sieci w poszukiwaniu oferowanych tradycyjnie w ten dzień zniżek na zakupy online. Eksperci ostrzegają przed internetowymi oszustwami i obawiają się, że z powodu stresów związanych z epidemią klienci będą na nie szczególnie podatni.

Koniec listopada - tradycyjnie w USA czas rabatów - z powodu epidemii przeniósł się w znacznym stopniu do Internetu, ruch w sklepach jest mniejszy niż w poprzednich latach. Rekordowa liczba transakcji online przewidywana jest na "cybernetyczny poniedziałek".

Okres Cyber Monday to czas, gdy cyberprzestępcy wykazują się szczególną aktywnością - ostrzega Steven Merrill, szef zajmującej się przestępstwami finansowymi sekcji w FBI.

Merrill obawia się, że wielu Amerykanów jest w tym roku w tak trudnej sytuacji finansowej lub jest tak przygniecionych psychicznie epidemią, że stanowi łatwiejszy cel dla oszustów. "Ludzie tracą ostrożność (...) Okoliczności są inne i podejmują decyzje, których normalnie by nie podjęli" - twierdzi.

Przed oszustwami w Internecie ostrzeżenie wydała także amerykańska Agencja Cyberbezpieczeństwa i Bezpieczeństwa Infrastruktury (CISA). W opublikowanym dokumencie opisującym podstawy bezpieczeństwa podczas zakupów online podkreśliła, że internauci przed przesłaniem pieniędzy powinni "upewnić się, że kontaktują się z renomowanym dostawcą".

O to czasem w sieci trudno, gdyż oszustwa często polegają na tworzeniu fałszywych stron internetowych, które naśladują witryny prawdziwych sklepów. "Zachowaj szczególną ostrożność w przypadku fałszywych stron podszywających się pod renomowane firmy czy niechcianych e-maili rzekomo pochodzących od organizacji charytatywnych" - apeluje CISA.

Według zajmującej się oszustwami firmy MyChargeBack sygnałem ostrzegawczym powinny w przypadku stron internetowych być błędy w pisowni i gramatyce oraz brak danych kontaktowych czy brak adresu fizycznego lub numeru telefonu. Wtedy przestrzega się przed wpisywaniem danych karty kredytowej w formularzu internetowym. Jeśli transakcja "wygląda zbyt dobrze, by była prawdziwa, prawdopodobnie tak jest" - zauważa także Michael B. Cohen, wiceprezes MyChargeBack.

Gdy już padnie się ofiarą internetowego oszustwa, należy to zgłosić odpowiednim służbom. W USA skontaktować się można z FBI czy organizacją Cybercrime Support Network. Jeśli sprawa dotyczy danych z karty kredytowej, to konieczna może okazać się jej blokada za pośrednictwem banku.