Bezpieczne zakupy online - jak nie paść ofiarą oszustów?

Internetowe zakupy dają niemal nieograniczone możliwości – za pomocą kilku kliknięć zamawiamy produkty z dobrze znanych nam sklepów, ale również z najodleglejszych zakątków świata. Wiąże się to jednak również z pewnymi zagrożeniami, na które powinniśmy być wyczuleni. Dotyczą one przede wszystkim wiarygodności sprzedawcy i bezpieczeństwa płatności. - Bez zakupów online wielu z nas nie wyobraża sobie już życia. Warto pamiętać o ryzykach związanych z internetowymi transakcjami. Bezpieczeństwo przede wszystkim - mówi Juliusz Brzostek, dyrektor Pionu Centrum Cyberbezpieczeństwa w NASK.

Na co powinniśmy zwrócić uwagę?

Sprawdź, zanim zaufasz

Aby uniknąć sytuacji zagrożenia, zawsze sprawdzajmy wiarygodność sprzedawcy. Pomogą nam w tym opinie na portalach aukcyjnych, forach i w komentarzach. Dane, takie jak e-mail, numer telefonu lub numer skrzynki pocztowej nie wystarczą, aby uznać przedsiębiorcę za zaufanego. Na plus może działać możliwość odbioru osobistego towaru – jeśli sprzedający podaje swój adres to znak, że nie ma nic do ukrycia.

Bądź czujny

Jeśli zdecydujemy się na płatność online, poza sprawdzeniem wiarygodności sprzedawcy, trzeba pamiętać również o tym, aby na bieżąco weryfikować czy strona internetowa, za pośrednictwem której dokonujemy transakcji, jest odpowiednio zabezpieczona. O należytej ochronie świadczy to, że połączenie jest szyfrowane – „https", ma ważny certyfikat, a w pasku adresowym pojawia się symbol kłódki. Zwracajmy również uwagę na to, czy transakcje są realizowane przez znanego operatora płatności. Login i hasło powinniśmy wpisywać dopiero wtedy, gdy jesteśmy pewni, że wszystko jest w porządku. Czujność należy zachować do ostatniej chwili. Przed zatwierdzeniem przelewu jednorazowym kodem, który dostajemy w SMS, należy sprawdzić, czy numer konta odbiorcy zgadza się z tym w wiadomości.

Nie korzystaj wszędzie

Bardzo istotne jest, aby nie dokonywać płatności internetowych z ogólnodostępnych komputerów, znajdujących się w miejscach publicznych. W przypadku urządzeń mobilnych, których używamy do płatności, pamiętajmy - nie należy podłączać ich do otwartych sieci WiFi. Trzeba również upewnić się, że sprzęt, z którego korzystamy ma zainstalowany i na bieżąco aktualizowany program antywirusowy. Po pomyślnie zrealizowanej płatności należy wylogować się z konta bankowego i zamknąć przeglądarkę.

Zgłaszaj nieprawidłowości

Jeżeli zdarzy się, że mimo zachowania ostrożności, zostaniemy oszukani, możemy się zwrócić z prośbą o pomoc do wyspecjalizowanych instytucji. Nieuczciwe praktyki możemy zgłosić w prosty i szybki sposób na stronie www.incydent.cert.pl. Taka reakcja ma bezpośrednie przełożenie na wzrost bezpieczeństwa w sieci dla nas wszystkich.

Stój. Pomyśl. Połącz.

Ministerstwo Cyfryzacji i NASK prowadzą intensywne działania edukacyjne w zakresie zwiększenia świadomości zasad bezpieczeństwa w sieci. Efektem tych prac jest m.in. kompendium porad. Znajdziemy w nich krótkie, przystępne przedstawienie wybranego zagadnienia wraz z listą wskazówek, jak można chronić się przed zagrożeniami.

Polecamy także serwis STÓJ. POMYŚL. POŁĄCZ. To polska wersja międzynarodowej kampanii STOP. THINK. CONNECT.™, mającej na celu zwiększanie poziomu świadomości społecznej i promowanie bezpieczeństwa w cyberprzestrzeni.

- Polecamy korzystanie z tych dedykowanych serwisów. Warto aktualizować swoją wiedzę, aby móc swobodnie i bezpiecznie korzystać z udogodnień, jakie daje Internet – dodaje Juliusz Brzostek, dyrektor Pionu Centrum

Cyberbezpieczeństwa w NASK.