

Uważajcie na przelewy internetowe

Data publikacji: 25.05.2019 15:00

Ostatnio w sieci pojawia się coraz więcej informacji, na temat coraz bardziej popularnej metody wyłudzenia pieniędzy przez oszustów internetowych. Tym razem „hakerzy” zdecydowali się na podrabianie stron, kierujących do szybkich płatności internetowych. Chociaż w regionie nie było jeszcze tego typu zgłoszeń, należy uważać.



fot. pixabay.com

Metody przestępstw internetowych, w szczególności te, nastawione na wyłudzenie pieniędzy, wciąż ewoluują. Hakerzy stają się coraz bardziej pomysłowi, a przeciętny użytkownik sieci nie zawsze jest w stanie wyłapać, kiedy ma styczność z oszustwem. Aktualnie w sieci głośno zrobiło się o metodach oszustwa, polegających na tworzeniu stron, łudząco podobnych do stron pośredników płatności.

O zgłoszenia dotyczące tego typu przestępstw w regionie, postanowiliśmy zapytać asp. Krzysztofa Pawlika – Oficera Prasowego KPP w Cieszynie. Zgodnie z informacjami, jakie udało nam się uzyskać, Wydział Przestępstw Gospodarczych KPP Cieszyn obecnie nie prowadzi spraw tego typu, jak podkreśla jednak policja, zawsze należy zachować ostrożność — **Jeżeli ktoś kupuje przez internet, a takich osób jest oraz więcej, powinien uważać na strony łudząco podobne do stron pośredników płatności. Jeśli tej ostrożności nie zachowa może, stracić swoje oszczędności. Logując się poprzez otrzymany link, możemy (nie zwracając na to uwagi), przekazać swoje dane nie, jak myślimy, bankowi, ale przestępcom. Jeśli ujawnimy w ten sposób swoją tożsamość, to mogą oni wykorzystać nasze dane do zawarcia umów — np. zaciągnięcia kredytu, zakupów internetowych czy innych zobowiązań finansowych. Przestępcy na ogół podszywają się pod serwisy oferujące szybkie przelewy. Podstawione przez nich strony wyłudzają loginy i hasła do bankowości internetowej oraz kody autoryzacyjne zatwierdzające przelewy** – ostrzega Pawlik.

W przypadku tego typu oszustwa ciężko jest wymienić jedną, dominującą metodę, dzięki której możemy zorientować się, że nasze pieniądze są zagrożone. Powinniśmy uważać jednak na linki wysyłane w wiadomościach SMS, komunikatorach internetowych, czy na wiadomości wysyłane przez fałszywe sklepy internetowe — **Aby nie zostać ofiarą przestępców, trzeba zwrócić uwagę na to, w jaki sposób się logujemy. Nie róbmy tego za pośrednictwem otrzymanego linku tylko bezpośrednio na stronie internetowej banku. Weryfikujemy dostawcę wiadomości. Jeśli na stronie pojawi się prośba o login i hasło do bankowości internetowej, należy sprawdzić, czy w pasku przeglądarki widnieje właściwy adres banku oraz, czy strona jest bezpieczna (https — czyli czy mamy znaczek kłódki przy nazwie strony). Jeśli adres jest inny, nie loguj się — nie podawaj tam swoich danych oraz powiadom o tym bank. W sytuacji, gdy zorientujemy się, że na naszym koncie zaistniały nieautoryzowane przez nas transakcje należy zgłosić ten problem w formie reklamacji do banku, który podejmie dalsze kroki w tej sprawie** – wyjaśnia Pawlik.

Na oszustwa tego typu szczególnie narażeni są seniorzy i osoby rzadko korzystające z Internetu. W związku z tym dobrze jest zwrócić uwagę na działania bankowe, podejmowane w sieci przez starszych członków naszej rodziny. W przypadku wątpliwości należy odstąpić od podejmowania działań bankowych i spróbować ponownie, bezpośrednio przez stronę banku.