**INFORMACJA PRASOWA**

Katowice, 21.04.2020 r.

**Aż 80% internautów dzieli się swoimi hasłami ze znajomymi – ta praktyka może mieć dla nich poważne konsekwencje**

**Według ankiety przeprowadzonej wśród amerykańskich konsumentów, blisko 80% użytkowników dzieli się ze znajomymi hasłami do różnych serwisów internetowych. Jak ostrzega Kamil Sadkowski, starszy analityk zagrożeń w ESET, takie zachowanie jest niebezpieczne i może stanowić doskonałą pożywkę dla cyberprzestępców.**

W ankiecie przeprowadzonej przez firmę ubezpieczeniową Zebra Insurance na grupie 1500 Amerykanów, aż 79% respondentów przyznało się, że dzieli się swoimi hasłami ze znajomymi. Najczęściej udostępniane są hasła do usług streamingu wideo, takich jak Netflix. Jednocześnie aż 39% ankietowanych przyznało się, że wykorzystuje to samo hasło we wszystkich usługach, z których korzystają.

Jak zwraca uwagę **Kamil Sadkowski, starszy analityk zagrożeń w ESET**, choć dane dotyczą rynku amerykańskiego, to obrazują zjawisko, które występuje także w Polsce.

*- Korzystanie z jednego konta stało się popularnym sposobem dzielenia kosztów, szczególnie kiedy chodzi o dobra cyfrowe – muzykę, filmy, gry komputerowe. Niestety trend ten wiąże się z poważnym ryzykiem – wraz z rosnącą liczbą osób, które znają dane hasło, rośnie ryzyko, że od którejś z nich ono wycieknie lub zostanie przypadkiem ujawnione komuś o niezbyt szlachetnych intencjach* – wyjaśnia **Kamil Sadkowski z ESET**.

Konsekwencje takiego wycieku mogą być bardzo dotkliwe. Przestępcy mogą wykorzystać skradzione dane logowania, próbując logować się do innych popularnych usług. Biorąc pod uwagę duży odsetek użytkowników, którzy wszędzie korzystają z tych samych danych logowania, takie próby mają niemałe szanse powodzenia. Potwierdza to również praktyka – opisywana technika (tzw. „credential stuffing”) jest wykorzystywana m.in. do przejmowania kont na platformie Zoom, oferowanych później na sprzedaż przez hakerów.

Jak jednak uspokaja ekspert, jeśli zależy nam na współdzieleniu jednego konta, można zrobić to bezpiecznie. W takie sytuacji należy wykorzystać przy jego tworzeniu unikalne i niemożliwe do odgadnięcia hasło, wymyślone lub wygenerowane dokładnie w tym jednym celu.