Nie daj się złowić - nie klikaj bez zastanowienia!

Sensacyjne i szokujące nagłówki bardzo często przykuwają naszą uwagę. Jednak należy pamiętać, że kontrowersyjne treści, przypominające nagłówki artykułów prasowych, zamieszczane zwłaszcza na portalach społecznościowych, bardzo często są w rzeczywistości stronami phishingowymi, mającymi na celu przejęcie profili społecznościowych i wykorzystanie ich do przestępczego procederu.

Fake newsy i dezinformacja, czyli fałszywe informacje, których głównym celem jest zmanipulowanie odbiorcy, mogą negatywnie wpływać na nasze poglądy i zachowania, kreują nieprawdziwy obraz rzeczywistości, ośmieszają polityków i inne znane osoby, a także wywołują różne, często negatywne i trudne emocje.

Uważaj na to, co klikasz

Eksperci zajmujący się cyberbezpieczeństwem przestrzegają, że fałszywe strony internetowe i posty zamieszczane na portalach społecznościowych, którym przeważnie towarzyszą sensacyjne nagłówki, wykorzystywane są przez oszustów w celu przeprowadzania kampanii phishingowych.

Ogłoszenia i posty wykorzystywane przez oszustów skłaniające użytkownika do kliknięcia w link, mają przeważnie podobną strukturę. Bardzo często są nacechowane emocjonalnie (co pozwala im przyciągnąć uwagę czytelnika), zawierają prośbę o pomoc (np. w zidentyfikowaniu sprawcy lub pomoc finansową) lub w inny sposób manipulują odbiorcą, aby kliknął w zawarty w nich link. Czasami widnieje na nich informacja o drastycznych i brutalnych scenach, które dostępne są po ponownym zalogowaniu się do swojego profilu na portalu społecznościowym. Następnie przekierowują użytkownika na fałszywą stronę logowania (np. do portalu społecznościowego), gdzie należy wpisać dane. Dzięki temu, przestępcy mogą przejąć konto osoby, która próbowała się zalogować i wykorzystać je w różnych celach. Jednym z przykładów, to włamanie i podszywanie się pod właściciela konta i w jego imieniu rozsyłanie wiadomości do niczego nieświadomych znajomych, np. w celu wyłudzenia płatności lub przelewu z wykorzystaniem kodu BLIK.

Posty i ogłoszenia, które mogą prowadzić do fałszywych stron i paneli logowania publikowane są w różnych miejscach. Według raportu CERT Polska za rok 2021, najczęściej fałszywe linki zamieszczano w otwartych grupach, posiadających dużą liczbą członków (przeważnie lokalne, gminne grupy mieszkańców) oraz grupach o charakterze handlowym (kupię/sprzedam/wymienię). Co ciekawe, dzięki specjalnym algorytmom, wykorzystywanym przez oszustów wiadomości są dostosowywane do grup odbiorców – wyświetlany artykuł zawiera nazwę np. konkretnej miejscowości. Dzięki temu, linki przyciągają uwagę zainteresowanych, którzy zaciekawieni wydarzeniami ze swojej okolicy, klikają w linki.

W jaki sposób możemy się chronić?

Przede wszystkim pamiętajmy o zasadzie ograniczonego zaufania – nie klikajmy w linki, wiadomości i załączniki, jeśli nie mamy pewności co zawierają lub od kogo pochodzą. Zanim zdecydujesz się otworzyć link i sprawdzić jego zawartość, zachowaj spokój i zdrowy rozsądek. Jeśli jednak otworzysz stronę i zostaniesz poproszony o wprowadzenie danych logowania, wycofaj się. Pamiętaj, że prawdopodobnie ktoś próbuje wyłudzić Twoje dane.

Przed atakami phishingowymi i innymi zagrożeniami online mogą nas uchronić podstawowe zasady cyberhigieny. Pamiętaj o ich stosowaniu, a Twoje dane, sprzęt a także środki finansowe będą bardziej bezpieczne.