Cyberprzestępcy wykorzystują polityków do opróżniania kont Polaków z pieniędzy

Kategoria: Styl życia
Opublikowano: wtorek, 20, maj 2025 12:59
Katarzyna Sekuła

Gorączka kampanii prezydenckiej trwa w najlepsze i rozgrzewa emocje wielu wyborców do czerwoności. Niestety, cyberprzestępcy doskonale o tym wiedzą i bez skrupułów to wykorzystują. Nie tylko publikują w Internecie fake newsy i sieją dezinformację, ale także często ich celem są pieniądze Polaków. W ubiegłym roku aż 26 proc. oszustw inwestycyjnych dotyczyło fałszywych reklam z wizerunkami polityków. To dwukrotnie więcej niż w przypadku celebrytów (14 proc.) – wynika z raportu rocznego CSIRT KNF.

Cyberprzestępcy doskonale wiedzą, kogo atakować. Na ich celowniku znajdują się przede wszystkim młode osoby, bo to one najczęściej przesiadują w mediach społecznościowych. Właśnie tam oszuści zamieszczają fałszywe reklamy, podszywając się pod kandydatów na prezydenta i innych znanych polityków. Aż 35-37 proc. Polaków w wieku 18-44 lata przyznało, że padło ofiarą kradzieży lub próby wyłudzenia danych osobowych. Dla porównania – w grupie wiekowej 45-64 lata ten odsetek jest zdecydowanie niższy i wynosi 26 proc., a wśród seniorów powyżej 65. roku życia jedynie 20 proc. – wynika z badania serwisu ChronPESEL.pl i Krajowego Rejestru Długów.

Starsi ufają oficjalnym komunikatom, a młodzi mediom społecznościowym

Przestępcy bezlitośnie wykorzystują nasz brak wiedzy dotyczący cyberbezpieczeństwa. Co prawda, aż 57 proc. Polaków przyznaje, że szuka informacji na ten temat w oficjalnych komunikatach, ale w tej grupie zdecydowanie dominują seniorzy (76 proc.). Z kolei młodsi (25-34 lata) korzystają z tego źródła najrzadziej (36 proc.). Z drugiej strony, prawie połowa Polaków (47 proc.) na pierwszym miejscu stawia media społecznościowe, a wśród osób w wieku 18-24 lata ten wskaźnik wynosi aż 62 proc.

Młodzi ludzie traktują media społecznościowe jako główne źródło informacji – zauważa Bartłomiej Drozd, ekspert ChronPESEL.pl. Jak podkreśla, cyberprzestępcy doskonale zdają sobie z tego sprawę i skutecznie to wykorzystują. Od lat stosują jedną z najpopularniejszych metod oszustwa – phishing, polegający na podszywaniu się pod znane osoby lub instytucje. Kliknięcie w fałszywą reklamę z wizerunkiem polityka może prowadzić do poważnych konsekwencji, takich jak zdalne przejęcie urządzenia i opróżnienie konta bankowego. To jednak dopiero początek, ponieważ skradzione dane osobowe mogą zostać wykorzystane do zaciągania kolejnych zobowiązań finansowych.

Fałszywe inwestycje w polityczne emocje

Zwłaszcza że cyberprzestępcy coraz częściej stosują złożone, wieloetapowe schematy działań, wykorzystując media społecznościowe do publikowania fałszywych treści. Podszywają się pod polityków, tworząc reklamy wyglądające jak artykuły znanych serwisów prasowych lub oficjalne komunikaty instytucji rządowych. W takich materiałach często rozpowszechniają nieprawdziwe informacje, na przykład o rzekomej śmierci lub skandalach z udziałem osób publicznych.

Ale na tym sztuczki cyberprzestępców się nie kończą. Coraz większą popularność wśród oszustów zdobywa technologia deepfake, umożliwiająca tworzenie realistycznych, lecz całkowicie fałszywych nagrań wideo z udziałem znanych osobistości. Celem takich działań jest nakłonienie odbiorców do pozornie atrakcyjnych inwestycji i wyłudzenie środków finansowych. Według danych CERT Polska, w 2024 roku odnotowano aż 139 przypadków nielegalnego wykorzystania wizerunku osób publicznych, w tym polityków, celebrytów, dziennikarzy, sportowców oraz lekarzy.

Walka z cyberprzestępcami jak z wiatrakami

Skuteczna walka z fałszywymi reklamami wykorzystującymi wizerunek polityków stanowi duże wyzwanie. Niestety, często sami ułatwiamy zadanie cyberprzestępcom. Zaledwie 11 proc. Polaków,

którzy mieli do czynienia z wyłudzeniem danych osobowych, zgłosiło ten incydent do CERT Polska. W efekcie większość niebezpiecznych stron w ogóle może nie trafić na listę ostrzeżeń tej organizacji.

Nie pomaga też podejście największych platform społecznościowych. CERT Polska w ubiegłym roku apelował do Mety o większe bezpieczeństwo reklam, w tym automatyczne blokowanie stron umieszczonych na liście ostrzeżeń. Niestety, bez skutku, ponieważ Facebook i Instagram nie przyjęły tych postulatów.

– Musimy być czujni na każdym kroku w mediach społecznościowych. Nie klikajmy w podejrzane newsy z szokującymi nagłówkami, ani w reklamy wyjątkowo atrakcyjnych inwestycji, nawet jeśli promują je znani politycy. Podstawą cyberbezpieczeństwa jest również dbanie o regularne aktualizacje programów antywirusowych i monitorowanie swojego numeru PESEL w sieci – dodaje ekspert.

Źródło: IP