**Dziś Światowy Dzień Mediów Społecznościowych. Oto najczęściej popełniane błędy bezpieczeństwa.**

**Udostępnianie danych osobowych, odpowiadanie na złośliwe wiadomości e-mail dotyczące resetowania hasła czy bezmyślne klikanie łączy – to błędy, które mogą prowadzić do włamania na nasze konta w mediach społecznościowych. W Światowy Dzień Mediów Społecznościowych firma Check Point Software przedstawiła najczęstsze błędy zagrażające bezpieczeństwu naszych danych**

[Na początku 2022 roku ponad połowa świata korzystała z mediów społecznościowych](https://www.smartinsights.com/social-media-marketing/social-media-strategy/new-global-social-media-research/#:~:text=More%20than%20half%20of%20the,social%20media%20is%202h%2027m). Innymi słowy, mówimy o ponad 4,6 miliarda ludzi, dla których social media są częścią ich codziennego życia i często zajmują im więcej czasu, niż by chcieli. Choć platformy te sprawiają nam często wiele radości i są świetnym sposobem na dzielenie się doświadczeniami z przyjaciółmi, stanowią również potencjalnie niebezpieczne zagrożenie dla bezpieczeństwa cybernetycznego.

*- Sieci społecznościowe, co oczywiste, odgrywają ważną rolę w naszym codziennym życiu. Musimy jednak musimy mieć się na baczności, bowiem media społecznościowe są jednym z głównych celów cyberprzestępców, a znajomość ich technik jest jedynym sposobem, aby móc się odpowiednio bronić. Dziś, w Dniu Mediów Społecznościowych, chcielibyśmy ostrzec użytkowników o istniejących zagrożeniach, aby byli bezpieczni przed najpowszechniejszymi atakami dokonywanymi za pośrednictwem tych platform* - mówi Wojciech Głażewski, Country Manager firmy Check Point Software.

Firma Check Point Software Technologies wskazuje na cztery najważniejsze czynniki ryzyka, o których należy pamiętać, zachowując bezpieczeństwo podczas korzystania z mediów społecznościowych

**1. Udostępnianie swoich danych osobowych:** to częsty i niebezpieczny błąd, który zdarza się praktycznie codziennie w sieciach społecznościowych. Cyberprzestępcy chcą przede wszystkim przejąć nasze dane. Uzbrojeni w nie, mogą następnie uruchomić kampanie phishingowych, a nawet ukraść nasze pieniądze z konta. Jeśli dodamy do tego fakt, że większość ludzi używa tych samych danych logowania do różnych platform społecznościowych, to kradzież loginów i haseł z jednego serwisu daje hakerom potencjalny dostęp do wszystkich innych. Stąd tak ważne jest, aby nie dzielić się danymi oraz loginami, a także używać różnych haseł, aby zminimalizować potencjalne szkody.

**2. Odpowiadanie na niechciane wiadomości e-mail z prośbą o zresetowanie hasła:** Jeśli otrzymamy wiadomość e-mail z prośbą o zmianę hasła, nawet jeśli o to nie prosiliśmy, to pierwszym naszym odruchem zwykle jest kliknięcie na link i zresetowanie hasła. Niestety, przy pewnej dozie pecha cyberprzestępca może uzyskać dostęp do całego naszego konta. Aby tego uniknąć, należy przejść bezpośrednio na platformę mediów społecznościowych (nie klikać linku w wiadomości e-mail) i dokonać zmiany hasła na stronie (a następnie zrobić to samo dla innych kont, do których mamy to samo hasło).

**3. Klikanie w nieznane łącza:** Cyberprzestępcy często wykorzystują linki do przekierowania użytkowników na złośliwe strony. Linki te mogą przyjść w formie niewinnie wyglądającego e-maila lub SMS-a. Jeżeli otrzymamy taki nieoczekiwany odnośnik, najlepszym sposobem na zabezpieczenie się jest wejście na daną stronę za pomocą zwykłej przeglądarki i upewnienie się czy znajdziemy tam istotne dla nas informacje. Kliknięcie bezpośrednio w link z wiadomości może wiązać się z narażeniem na poważne zagrożenia.

**4. Niesprawdzanie adresów URL:** Inną sztuczką, którą atakujący wykorzystują do kradzieży danych użytkownika, jest zmiana adresu URL, aby wyglądał on jak prawdziwy. Stosując tę technikę, hakerzy mogą nakłonić użytkownika do odwiedzenia strony, którą uważa za godną zaufania (np. strony na Facebooku, gdzie są proszeni o zmianę hasła, aby następnie zostać przekierowanym na sklonowaną stronę, z której hakerzy mogą ukraść tyle informacji, ile tylko zechcą). Ostatnio LinkedIn po raz pierwszy zdominował raport *Brand Phishing* firmy Check Point, wg którego marka odpowiadała za ponad połowę (52%) wszystkich prób phishingu w pierwszym kwartale tego roku. Aby nie dać się nabrać na tego typu oszustwa, ważne jest, aby sprawdzać adresy URL, na które wchodzimy, **upewniając się, że strona posiada certyfikat bezpieczeństwa SSL.** Jeśli ma certyfikat bezpieczeństwa, zobaczysz literę "s" w pasku adresu. Powinien on więc brzmieć: https://. Dzięki tej technologii wszelkie poufne informacje przesyłane między dwoma systemami są chronione, co uniemożliwia cyberprzestępcom uzyskanie dostępu do przesyłanych danych, w tym informacji, które mogą być uznane za osobiste.