# Article information:

» Twitter wyłącza kody 2FA przez SMS-y, bo tracił na tym 60 milionów dolarów rocznie... -- Niebezpiecznik.pl --  
<https://niebezpiecznik.pl/post/twitter-wylacza-kody-2fa-przez-sms-y-powodem-sa-nieuczciwi-operatorzy-ktorzy-go-okradali/>

# Article summary:

1. Twitter wyłącza możliwość korzystania z najsłabszej formy dwuskładnikowego uwierzytelnienia, czyli kodów SMS, ponieważ tracił na tym 60 milionów dolarów rocznie.

2. Za darmo i dla każdego nadal dostępne będą bezpieczniejsze warianty dwuskładnikowego uwierzytelnienia: przez aplikację lub przy pomocy kluczy U2F.

3. Nie jest do końca jasne, co się stanie 19 marca 2023 dla osób, które nie zmienią swojego dwuskładnikowego uwierzytelnienia z kodów SMS na inny rodzaj.

# Article rating:

Appears moderately imbalanced: The article provides some useful information, but is missing several important points or pieces of evidence that would be required to present the discussed topics in a balanced and reliable way. You are encouraged to seek a more balanced perspective on the presented issues by exploring the provided research topics and looking at different information sources.

# Article analysis:

Analiza artykułu "Twitter wyłącza kody 2FA przez SMS-y, bo tracił na tym 60 milionów dolarów rocznie... -- Niebezpiecznik.pl --"

Artykuł omawia decyzję Twittera o wyłączeniu najsłabszej formy dwuskładnikowego uwierzytelnienia, czyli kodów wysyłanych SMS-em. Autorzy artykułu sugerują, że ta decyzja nie wynika z troski o bezpieczeństwo użytkowników, ale z faktu, że Twitter tracił na tym 60 milionów dolarów rocznie. Według Elona Muska, operatorzy telekomunikacyjni zakładali konta na Twitterze i konfigurowali na nich 2FA przez SMS na numery telefonów ze swojej puli, sztucznie wymuszając ich wysyłkę i zarabiając na tym pieniądze.

Artykuł zawiera kilka punktów do rozważenia. Po pierwsze, autorzy sugerują, że wyłączenie najsłabszej formy dwuskładnikowego uwierzytelnienia nie wynika z troski o bezpieczeństwo użytkowników. Jednakże, w świetle coraz częstszych ataków hakerskich i naruszeń prywatności online, decyzja ta może być uzasadniona potrzebą zapewnienia większego bezpieczeństwa dla użytkowników.

Po drugie, autorzy artykułu rekomendują korzystanie z klucza U2F jako drugiego składnika dwuskładnikowego uwierzytelnienia. Wskazują oni na to jako najbezpieczniejszą formę dwuskładnikowego uwierzytelnienia. Jednakże, warto pamiętać o kosztach zakupu takiego klucza oraz o konieczności jego przechowywania w bezpiecznym miejscu.

Po trzecie, autorzy artykułu sugerują możliwe zagrożenia związane z korzystaniem z aplikacji typu Authenticator jako drugiego składnika dwuskładnikowego uwierzytelnienia. Wskazują oni na ryzyko utraty telefonu lub braku kopii zapasowej seed'ów generowanych przez aplikację. Jednakże istnieją sposoby minimalizowania tych zagrożeń poprzez regularne tworzenie kopii zapasowych seed'ów oraz przechowywanie ich w bezpiecznym miejscu.

Podsumowując, artykuł zawiera wiele cennych informacji dotyczących zmian w systemie dwuskładnikowego uwierzytelnienia Twittera oraz rekomendacji dotyczących korzystania z bardziej zaawansowanych metod uwierzytelniania. Jednakże warto zachować ostrożność wobec sugestii autorów dotyczących potencjalnych zagrożeń i jednostronnych doniesień.

# Topics for further research:

* Bezpieczeństwo dwuskładnikowego uwierzytelnienia
* Klucz U2F jako drugi składnik uwierzytelnienia
* Koszty zakupu klucza U2F
* Przechowywanie klucza U2F w bezpiecznym miejscu
* Zagrożenia związane z aplikacją Authenticator
* Tworzenie kopii zapasowych seed'ów aplikacji Authenticator

# Report location:

<https://www.fullpicture.app/item/46fbc5e668d2a8399134ccd89d60809d>