

Informujemy, iż w celu optymalizacji treści dostępnych w naszym serwisie i dostosowania ich do Państwa indywidualnych potrzeb korzystamy z informacji zapisanych za pomocą plików cookies na urządzeniach końcowych użytkowników. Pliki cookies użytkownik może kontrolować za pomocą ustawień swojej przeglądarki internetowej. Dalsze korzystanie z naszego serwisu internetowego bez zmiany ustawień przeglądarki internetowej oznacza, iż użytkownik akceptuje stosowanie plików cookies.

[Akceptuję pliki cookies](#)

MENU

[Instrukcja korzystania z BIP](#)

[Nabór](#)

[Zamówienia publiczne](#)

[Organizacja przyjmowania i załatwiania skarg i wniosków](#)

[Podstawa prawna powstania Centrum Usług Informatycznych w Białymstoku](#)

[Plan zamówień publicznych](#)

[Sprawozdania finansowe](#)

[Dostęp do informacji publicznej nieudostępnionej w BIP](#)

[Ochrona danych osobowych](#)

[Cyberbezpieczeństwo](#)

[Zarządzenia](#)

[Petycje](#)

[Sygnałista](#)

[Raport o stanie zapewnienia dostępności podmiotu publicznego
zgłoszeń naruszeń prawa](#)

Komunikat Pełnomocnika Rządu do spraw Cyberbezpieczeństwa o kampanii phishingowej

Jednostki samorządu terytorialnego są celem nowej kampanii phishingowej, w której oszuści podszywają się pod Ministerstwo Cyfryzacji i wiceministra Pawła Olszewskiego. Próbują wyłudzić wrażliwe dane lub zainfekować urządzenia złośliwym oprogramowaniem. Przed zagrożeniem ostrzega Pełnomocnik Rządu do spraw Cyberbezpieczeństwa, Krzysztof Gawkowski.

Komunikat Pełnomocnika Rządu do spraw Cyberbezpieczeństwa o kampanii phishingowej
O kampanii

Kampania skierowana jest przede wszystkim do podmiotów samorządowych i może naruszyć ich cyberbezpieczeństwo oraz doprowadzić do wyłudzenia danych.

Zaobserwowano dwa warianty działań oszustów:

1. Dystrybucja złośliwego oprogramowania: wiadomości zawierają załączniki, których uruchomienie skutkuje instalacją złośliwego oprogramowania (malware) na urządzeniach ofiar.
2. Wyłudzenie Danych Kontaktowych: wiadomości mają pozyskać dane kontaktowe (np. imiona, nazwiska, numery telefonów, adresy e-mail) osób odpowiedzialnych za cyberbezpieczeństwo w poszczególnych urzędach.

Wiadomości te są dystrybuowane z fałszywej domeny govministry[.]pl, która nie ma żadnego związku z administracją rządową.

Zrzuty ekranu przykładowych wiadomości, które ułatwią ich identyfikację, są załączone poniżej.

W związku z tym Pełnomocnik Rządu do spraw Cyberbezpieczeństwa zaleca wykonanie poniższych działań, aby się chronić:

1. Należy weryfikować adres nadawcy – Ministerstwo Cyfryzacji wysyła wiadomości z oficjalnej domeny cyfra.gov.pl.
2. Nie wolno uruchamiać plików oraz klikać w linki z niezaufanych źródeł.

3. Należy rozdyskrybuować niniejszy komunikat wśród pracowników urzędów aby zwiększyć świadomość.
4. Należy weryfikować czy przedmiotowe wiadomości wpłynęły do jednostki i zgłosić wykryty incydent niezwłocznie do właściwego zespołu CSIRT (dla podmiotów samorządowych jest to CSIRT NASK)

Incydent można zgłosić do CSIRT NASK pod adresem:

<https://incydent.cert.pl>.

METRYKA STRONY

REJESTR ZMIAN