WYŁUDZANIE INFORMACJI SMSEM

Smishing (kombinacja słów SMS i Phishing) to próba wyłudzenia informacji poufnych, firmowych lub dotyczących bezpieczeństwa za pośrednictwem SMS.

JAK TO DZIAŁA?

Otrzymujesz SMS, w którym nadawca prosi Cię o kliknięcie linku lub telefon pod wskazany numer, aby "zweryfikować", "zaktualizować" lub "ponownie aktywować" konto. Odnośniki prowadzą do fałszywej strony/telefonu oszusta, który podaje się za usługodawcę.

CO MOŻESZ ZROBIĆ?

- **Nie klikaj linków, załączników ani obrazów** otrzymywanych w SMS niewiadomego pochodzenia, bez wcześniejszego sprawdzenia nadawcy.
- **Nie spiesz się.** Sprawdź źródło wiadomości zanim udzielisz odpowiedzi.
- **Nigdy nie odpowiadaj na SMS,** który prosi o podanie Twojego numeru PIN, hasła do konta bankowego lub innych poufnych informacji.
- Jeśli podałeś swoje dane w odpowiedzi na SMS, który mógł być wyłudzeniem, **niezwłocznie skontaktuj się z bankiem.**

EUROPOL EC3 European Cybercrime Centre · EBF · POLICJA · NASK

#CyberScams