



Gmina Mielec

ul. Głowackiego 5, 39-300 Mielec

Godziny pracy Urzędu: pon.: 7:30 - 17:00, Wt. - Czw.: 7:30 - 15:30, Pt.: 7:30 - 14:00

Telefon: 17 773 05 90 Fax: 17 773 05 91 Email: sekretariat@ug.mielec.pl

Ostrzeżenie CERT Polska o wakacyjnym oszustwie

2023-08-16 08:23:29

Pełna treść ostrzeżenia dostępna [w komunikacie "Wakacyjne oszustwo - nowa metoda cyberprzestępców" na stronie CERT.](#)

Wakacje to czas wyjazdów, przede wszystkim dla dzieci i młodzieży. Poza domem nietrudno o pechowe przygody z telefonem, takie jak zagubienie czy zniszczenie smartfona. Jeśli dziecko znajdzie się w takiej sytuacji, dość prawdopodobne jest, że będzie się kontaktować z rodzicami z innego numeru i na tym właśnie opiera się schemat opisywanego przez nas oszustwa.

Część z tych wiadomości może trafić do rodziców, których dzieci przebywają na obozach, koloniach, czy innego rodzaju wyjazdach. Zaintrygowany lub jedynie spełniający prośbę "dziecka", rodzic może od razu wysłać wiadomość w komunikatorze pod podany numer. Może też najpierw spróbować zadzwonić do syna lub córki pod dotychczasowy numer, aby dowiedzieć się, co się stało. Jeśli dziecko odbierze, to wszystko się wyjaśni. Jeśli jednak dziecko nie odbierze telefonu, będzie miało wyłączone urządzenie albo akurat będzie poza zasięgiem, to dla rodzica, opisana w otrzymanej wiadomości sytuacja stanie się prawdopodobna.

Zaniepokojony rodzic pisze wówczas wiadomość w komunikatorze na podany numer. Podczas konwersacji oszust wyjaśnia dlaczego komunikuje się z innego telefonu. Z kolei wiadomości od rodzica pozwalają mu uzyskać pewne informacje o dziecku, takie jak imię lub przynajmniej płeć, co ułatwi mu to dalsze podszywanie się. W końcu "dziecko" prosi o zrobienie przelewu na wskazany numer rachunku bankowego, aby zapłacić za nowy telefon.

Jeśli oszust dowie się, że rodzic nie ma bankowości elektronicznej, to poprosi o dane z karty kredytowej i kod SMS autoryzujący operację, aby w ten sposób uzyskać dostęp do pieniędzy rodzica. Kiedy natomiast okaże się, że rodzic nie ma takiej kwoty na swoim koncie, to oszust proponuje zakup tańszego telefonu.

Jak należy się zachować w sytuacji, gdy otrzymamy podobną wiadomość? Przede wszystkim trzeba spróbować skontaktować się z dzieckiem w inny sposób, szczególnie wtedy, gdy pojawia się prośba o przesłanie pieniędzy.

Zawsze, gdy otrzymujemy takie nieoczekiwane prośby należy skontaktować się z nadawcą wiadomości za pomocą innego kanału komunikacji. W szczególności jeśli wiadomości te pochodzą z nieznanymi nam dotąd numerów, adresów email, kont w mediach społecznościowych lub komunikatorach.

Nawet jeśli konto w komunikatorze jest nam znane, to należy mieć na uwadze fakt, że oszuści za pomocą fałszywych paneli logowania mogą przejąć dane uwierzytelniające do kont w mediach społecznościowych. Przejęte konta mogą być następnie wykorzystane do wysyłania do znajomych próśb o przekazanie pieniędzy w powiązanych komunikatorach.

Najłatwiej jest taką prośbę zweryfikować po prostu dzwoniąc do znajomego, dziecka, lub innego członka rodziny, który prosi o przesłanie pieniędzy. Może się jednak zdarzyć tak, że ta osoba nie będzie mogła akurat wtedy odebrać albo będzie miała wyłączony telefon.

Warto wiedzieć, że wiele komunikatorów oferuje także możliwość wykonywania połączeń głosowych. Bardzo trudno jest podrobić czyjś głos na żywo, zwłaszcza jeśli nie ma się nagrań/próbek głosu. Można więc spróbować zweryfikować tożsamość naszego rozmówcy też w taki sposób. Oszust będzie jednak próbował jakoś wytłumaczyć to, że nie może rozmawiać.

Przestępcy mogą wywoływać poczucie presji czasu, aby uniknąć niewygodnych pytań, ponieważ ich wiedza o osobie, pod którą się podszywają, jest bardzo ograniczona. Zawsze istnieje przecież "ryzyko", że początkowe zaskoczenie minie i potencjalna ofiara zorientuje się, że ma do czynienia z oszustem. Może też się zdarzyć, że osoba pod którą się podszywają, w końcu albo odpowie na próby kontaktu ze strony rodzica, albo sama napisze z jakiegoś innego powodu. Nie należy jednak tej presji czasu ulegać i warto zapytać dziecko o wiek lub imię, jeśli nie zdradziliśmy go wcześniej. Nawet takie z pozoru proste pytania mogą okazać się bardzo trudne dla oszusta.

Pamiętajmy, że gra na emocjach to wciąż bardzo skuteczny środek do osiągnięcia celów przez cyberprzestępców.

Dziękujemy za odwiedzin i zapraszamy ponownie

[bezpośredni link do strony www](#)