

Oszustwa „na powodzian”

Data publikacji: 18.09.2024 14:40

Oszuści nie mają litości. Dramat powodzian jest dla nich kolejnym sposobem na wyciągnięcie od nas danych czy pieniędzy. Uważajcie! Policjanci ostrzegają!

Mat. informacyjne Policji

Fałszywe wiadomości rzekomo od RCB, przejęcia kont na social mediach i fałszywe zbiórki - to tylko niektóre z możliwych oszustw w związku z występującą sytuacją powodziową. Zapoznajcie się z zaleceniami przygotowanymi przez Centralne Biuro Zwalczania Cyberprzestępczości, aby uniknąć tych zagrożeń.

Fałszywe SMSy podszywające się pod Alert RCB

UWAGA na fałszywe wiadomości SMS, które oszuści rozsyłają podszywając się pod Alert RCB!

W wiadomościach tych umieszczone są linki, w które nie należy klikać!

Przypominamy, że prawdziwe Alerty RCB NIE ZAWIERAJĄ LINKÓW!

Aby upewnić się, że otrzymany Alert RCB jest autentyczny, możesz to zweryfikować poprzez:

- oficjalną stronę internetową Rządowego Centrum Bezpieczeństwa: <https://www.gov.pl/web/rcb>
- profile w mediach społecznościowych Rządowego Centrum Bezpieczeństwa.

Jeśli otrzymasz wiadomość, która wygląda jak Alert RCB, ale zawiera link lub budzi Twoje wątpliwości, prosimy, abyś nie klikał w odnośnik i nie odpowiadał na wiadomość.

Fałszywe zbiórki

W związku z pojawiającymi się informacjami o fałszywych zbiórkach, dotyczących pomocy powodzianom, apelujemy o szczególną ostrożność. Oszuści coraz częściej wykorzystują dramatyczne wydarzenia, aby wyłudzać pieniądze pod pozorem działań charytatywnych.

Ostrzegając przed fikcyjnymi ziórkami dla powodzian, przypominamy o kilku podstawowych zasadach:

- wspierajmy przede wszystkim znane i zaufane fundacje lub organizacje pomocowe, które działają od lat mają doświadczenie oraz są transparentne zarówno w działaniu, jak i w późniejszym rozliczaniu zebranych środków;
- sprawdźmy, czy przeprowadzana zbiórka jest organizowana na sprawdzonej platformie - uważajmy na podejrzane linki;
- zwróćmy uwagę na szczegóły - uczciwe zbiórki mają informację na temat tego, kto dokładnie jest beneficjentem, jak środki będą rozdysponowane oraz jakiego wsparcia potrzeba;
- uważajmy na nagłe apele o pomoc - oszuści często działają impulsywnie i mogą prosić o natychmiastowe wpłaty, często stosując presję czasu;
- odradzamy wpłacania pieniędzy mało znanym lub nieznanym firmom czy instytucjom charytatywnym, które wcześniej nie pomagały;
- nie polecamy wspierania także osób fizycznych, chyba że są to nasi bliscy lub zaufani znajomi;
- nie przekazujemy środków rzeczowych ani pieniężnych domokrężcom, nie wpuszczamy pod żadnym pretekstem do domów osób obcych;
- zachowajmy czujność podczas rozmów telefonicznych – nie dajmy się zmanipulować popularnym metodom oszustów;

- pod żadnym pozorem nie wypłacajmy w pośpiechu gotówki z banku – informacja o zajęciu konta bądź awarii systemów bankowych, nadal jest powszechną metodą działania oszustów.

Pomagajmy, ale rozsądniej!

Przejęcia kont na mediach społecznościowych

Oszuści żerując na ludzkiej tragedii, w związku z sytuacją powodziową, próbują przejąć konta na profilach społecznościowych.

W tym celu przygotowują krzykliwy nagłówek ze zdjęciem, np. dziecka lub zwierzęcia w sytuacji zagrożenia. Do wpisu dołączony jest link, w który należy kliknąć i zalogować się podając swoje wrażliwe dane. Podanie tych danych na podstawionej stronie powoduje przejęcie naszych danych do logowania.

Pamiętaj! Jeśli jesteś już zalogowany na swoim koncie, nie ma konieczności ponownego logowania!

Nie podawaj loginu i hasła. Nie panikuj. Po prostu zamknij podejrzaną stronę.

Możesz też zgłosić ją do nas tutaj: <https://incydent.cert.pl/>

NG/mat.pras.