150 fałszywych zbiórek dla powodzian. Hakerzy żerują na ludzkiej tragedii – czy wiesz jak się przed tym uchronić?

Kategoria: Aktualności
Opublikowano: czwartek, 03, październik 2024 08:45
Alicja Cisowska

Kiedy tysiące Polaków próbuje stanąć na nogi po dramatycznej powodzi, cyberprzestępcy nie śpią. Próbują wykorzystać dobre serca darczyńców chcących pomóc poszkodowanym. Do dziś policja wykryła 150 incydentów związanych z fałszywymi zbiórkami pieniężnymi dla powodzian – wynika z danych przekazanych przez Centralne Biuro Zwalczania Cyberprzestępczości. Jednak to może być tylko wierzchołek góry lodowej, ponieważ służby codziennie informują o kolejnych przypadkach oszustw.

Metody hakerów są coraz bardziej wyrafinowane. To już nie tylko fałszywe strony internetowe, które łudząco przypominają prawdziwe witryny organizacji charytatywnych i fundacji. Cyberprzestępcy również coraz częściej po przejęciu kontroli nad profilem w mediach społecznościowych, wysyłają wiadomości od „znajomych" rzekomo potrzebujących pomocy. Niestety wiele osób w dobrej wierze wpłaca pieniądze, nie zdając sobie sprawy, że nie trafią do potrzebujących powodzian, a kieszeni oszustów.

Fałszywe alerty RCB

Oszuści wyjątkowo sprytnie wykorzystują stan zagrożenia powodzią w południowo-zachodniej Polsce. Wysyłają fałszywe wiadomości SMS, podszywając się pod alert RCB. Znajdują się w nich linki przekierowujące na zainfekowane strony internetowe. Pod żadnym pozorem nie wolno w nie klikać lub odpisywać nadawcy. Przejście na podejrzaną witrynę może skutkować przejęciem kontroli nad telefonem, czy zdobyciem danych osobowych przechowywanych na urządzeniu, które następnie oszuści mogą użyć do wyłudzenia lub kradzieży pieniędzy z konta bankowego.

Co ważne, prawdziwe alerty RCB nie zawierają żadnych linków. Aby zweryfikować, czy otrzymana wiadomość jest autentyczna, należy wejść na oficjalną stronę Rządowego Centrum Bezpieczeństwa lub profile tej instytucji w mediach społecznościowych.

Fikcyjne zbiórki napychają kieszenie oszustów

Jednak hakerzy mają w swoim arsenale o wiele więcej nikczemnych sztuczek. Centralne Biuro Zwalczania Cyberprzestępczości wykryło ponad 100 fałszywych zbiórek pieniężnych dotyczących pomocy powodzianom. Wielka woda dociera do kolejnych miejscowości, więc z pewnością ich liczba jeszcze wzrośnie.

Inną metodą oszustów są próby przejęcia profili w mediach społecznościowych. W tym celu cyberprzestępcy przygotowują krzykliwy nagłówek ze zdjęciem, np. dziecka lub zwierzęcia w sytuacji zagrożenia. Do wpisu podany jest link, w który należy kliknąć i zalogować się podając wrażliwe dane, co skutkuje przejęciem loginów do konta w serwisie. Następnie cyberprzestępcy mogą się pod nas podszywać, wyłudzając pieniądze od członków rodziny czy znajomych.

– Phishing, czyli technika polegająca na próbie spowodowania, aby odbiorca wiadomości e-mail czy SMS podjął działanie zgodnie z zamierzeniami cyberprzestępców, jak kliknięcie w link przekierowujący na zainfekowaną witrynę to jedna z najpopularniejszych metod stosowanych przez oszustów. W tym celu często podszywają się pod instytucje zaufania publicznego, jak urzędy, banki, czy obecnie fundacje i organizacje charytatywne. W 2023 roku Zespół Szybkiego Reagowania na Incydenty Komputerowe (CERT Polska) otrzymał 95,7 tys. zgłoszeń phishingu w polskim Internecie, a na jego listę ostrzeżeń trafiło 79,3 tys. domen stosujących tę formę oszustwa – ostrzega Bartłomiej Drozd, ekspert serwisu ChronPESEL.pl.

Kategoria: Aktualności
Opublikowano: czwartek, 03, październik 2024 08:45
Alicja Cisowska

Cyberprzestępcy kolejny raz wykorzystują poczucie zagrożenia Polaków

Podczas kryzysowych sytuacji, jak ostatnia powódź rośnie aktywność oszustów. Tak było m.in. w czasie pandemii koronawirusa. Wówczas oszuści wykorzystywali naszą nieostrożność oraz poczucie niepewności i panujący chaos komunikacyjny. Podszywali się pod instytucje zaangażowane w walkę z epidemią, czyli sanepid, ministerstwa, policję czy pocztę, a także rachmistrzów zaangażowanych w przeprowadzenie Narodowego Spisu Powszechnego Ludności i Mieszkań. Natomiast obecnie są to zwykle fundacje i organizacje charytatywne. Aby więc uniknąć zagrożenia, należy przestrzegać kilku podstawowych zasad cyberbezpieczeństwa.

– *Najbezpieczniej wspierać akcje charytatywne prowadzone przez znane i zaufane organizacje. Najlepiej samodzielnie wpisać adres fundacji lub rządowej instytucji w przeglądarce i wejść bezpośrednio na jej stronę, gdzie podano numery specjalnych rachunków bankowych na rzecz powodzian. Jednak jeśli zdecydujemy się wpłacić środki na prywatną zbiórkę, to upewnijmy się, czy ta osoba rzeczywiście potrzebuje wsparcia. Warto również weryfikować witryny i profile w mediach społecznościowych, na których publikowane są apele o pomoc. Pod żadnym pozorem nie klikajmy również w podejrzane linki otrzymywane w wiadomościach e-mail, SMS-ach lub Facebooku i innych serwisach* – mówi Bartłomiej Drozd.

Źródło: IP