Kielce, 2020-05-05

Jak oszuści wykorzystują COVID – 19

Oszustwo na darowiznę

Pojawiła się nowa kampania phishingowa, której celem jest wyłudzenie wrażliwych danych osobowych. Oszuści rozsyłają e-maile informując o rzekomej darowiźnie od Unii Europejskiej. Wiadomości rozsyłają z adresu mailowego dyrektor włoskiej kliniki medycznej.

Wiadomość brzmi tak:

"Z przyjemnoscia informujemy, ze zostales wybrany do rekompensaty pienieznej w wysokosci 3 000 000,00 EUR (trzy miliony euro) z Komisji Europejskiej ds. Wynagrodzen za ofiare oszustwa internetowego, za posrednictwem Sekretarza Generalnego Unii Europejskiej (Pani Ilze Juhansome). Odpowiedz po wiecej szczegółów" .

Jego autorzy chcą nawiązać kontakt i od razu proszą ofiarę o całą serię danych osobowych, a nawet o zdjęcie dowodu osobistego lub paszportu. Napisano to dokładnie tak:

1.Pelne nazwy:
2.Adres zamieszkania:
3.Numer telefonu:
4.Numer faksu (jesli istnieje):
5.Zawód:
6.Wiek:
7.Narodowosc:
8.Zeskanowana kopia dokumentu tozsamosci (prawo jazdy,paszport miedzynarodowy lub dowód osobisty).

Następie proszą o przesłanie danych na konkretny adres e-mail, zarejestrowany w domenie gmail.

Będzie szczepienie. Zapłać

Oszuści rozsyłali SMS-y o rzekomym obowiązkowym szczepieniu za 70 zł. Treść wiadomości wyglądała tak:

Zgodnie z specustawa dt koronawirusa wszyscy obywatele RP beda szczepieni. Z refundacja koszt wynosi 70 PLN. Oplac aby uniknac kolejek https://…

Link kierował do strony **dpdoplata[.]org/1**, a z kolei ta strona kierowała do **fałszywej bramki PayU**. Sam adres dpdoplata[.]org sugeruje, że pierwotnie fałszywa bramka została przygotowana do oszustw na dopłatę do przesyłki.

Rząd zabierze ci pieniądze do walki z epidemią!

Do strony dpdoplata[.]org kierował również inny SMS, którzy przekonywał, iż środki zgromadzone na naszych rachunkach mogą zostać przesunięte do rezerw NBP.

Informujemy, iz zgodnie z specustawa dt koronawirusa Panstwa srodki na rachunku zostaja przekazane do rezerw krajowych NBP. Zaloguj sie aby zatrzymac 1000 PLN.

Przed tym SMS-em ostrzegał m.in. PKO BP. Należy zapoznać się z prawem dotyczącym nieautoryzowanych płatności.

Wsparcie żywnościowe

Kolejnym sposobem nielegalnego pozyskania danych była próba skierowania ludzi na stronę, która miała podszywać się pod Ministerstwo Zdrowia. W pierwszej kolejności otrzymywaliśmy wiadomość SMS:

“Ministerstwo Zdrowia”: Dla kazdego obywatela przysluguje wsparcie zywieniowe w zwiazku z epidemia Koronawirusa. Zapisz sie na https://mzgov.net…

W tym przypadku link kierował do strony internetowej, która przekonywała o potrzebie zalogowania się do Profilu Zaufanego. Do tego Profilu można się logować przez bank więc strona kierowała do wykazu banków, a następnie do fałszywych stron wyłudzających dane logowania.


Ministerstwo Zdrowia | Serwis Rzeczypospolitej Polskiej

Login | Profil Zaufany

Wsparcie żywieniowe - Koronawirus

Zgodnie z rozporządzeniem Ministerstwa Zdrowia dla każdego obywatela przysługuje wsparcie żywieniowe w związku z epidemią Koronawirusa.

Na jedną osobę przysługuje:
- 20 l wody
- 3,5 kg zbóż, produktów zbożowych, chleba, ziemniaków, makaronu i ryżu.
- 2,5 kg owoców w puszkach lub słoikach i orzechów
- 4 kg suchych roślin strączkowych i warzyw w puszkach lub słoikach
- 2,6 kg mleka i produktów mlecznych
- 1,5 kg mięsa, ryb i jajek, ewentualnie jajek w proszku (świeże

Wyłudzanie haseł do Facebooka

Pamiętajmy, że przestępcy mogą kraść nie tylko pieniądze. Cenne mogą być dla nich nasze dane logowania do Facebooka, których następnie można użyć np. do okradania naszych znajomych, także oszustwem na BLIKA (jak również innych rzeczy np. dalszego propagowania fałszywych wiadomości).

Wyświetlona na Facebooku sensacyjna informacja prowadzi do rzekomej strony z materiałem informacyjnym. Aby zobaczyć materiał wideo należy się zalogować niby przez Facebooka, ale kliknięcie w link do logowania skieruje nas na stronę tylko podobną do strony logowania Facebooka


FAKT24.PL

NOWE FAKTY NA TEMAT KORONAWIRUSA [WIDEO]

Koronawirus nadal rozprzestrzenia się na świecie. Liczba zachorowań w Polsce wzrosła do 17(prawdopodobnie liczba ta jest mocno zaniżona). Kolejna zakażona osoba to kobieta, która przebywa w szpitalu w Poznaniu. Rząd postanowił wprowadzić kontrole sanitarne na granicach z Czechami i Niemcami, a od jutra na pozostałych przejściach granicznych. Tymczasem pierwsze dwa przypadki zakażenia koronawirusem odnotowano na Cyprze co oznacza, że Covid-19 pojawił się już we wszystkich 27 krajach Unii Europejskiej. Z punktu widzenia zagrożenia epidemiologicznego, Główny Inspektor Sanitarny nie zaleca podróżowania do Chin, Hongkongu oraz Korei Południowej, Włoch, Iranu, Japonii, Tajlandii, Wietnamu, Singapuru i Tajwanu. Ciężki przebieg choroby obserwuje się u ok.15-20% osób. Do zgonów dochodzi u 2-3% osób chorych.


WYPOWIEDŹ DOKTORA Z JEDNEGO Z WARSZAWSKICH SZPITALI NA TEMAT NAMNAŻAJĄCEJ SIĘ LICZBY ZARAŻONYCH W POLSCE.

Ze względu na wytyczne Ministerstwa Zdrowia materiał dostępny dla osób powyżej 18 roku życia
Zweryfikuj swój wiek przez facebooka

Zaloguj się

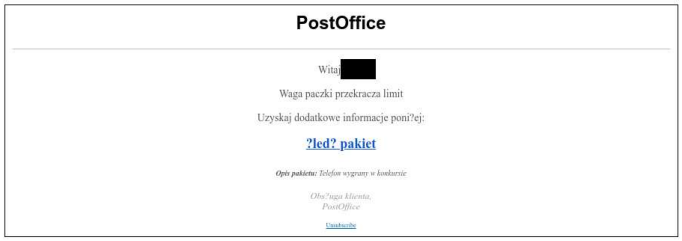
Przed tymi oszustwami przestrzegał m.in. NASK. Informował on, że domeny używane do takich oszustw to m.in. koronawirusnews[.]com.pl, e-koronawirusnews[.]pl, koronawirusnews[.]net.pl oraz ikoronawirusnews[.]pl.

Wyłudzenie danych "na paczkę"

Kolejna wiadomość, która ma za zadanie oszukać odbiorcę ma temat:

*"**Aktualizacja Covid-19: Twoja paczka przekracza limit wagi**"*.

Tekst "covid-19" wstawiono jakby na siłę, aby wiadomość zwróciła na siebie uwagę. W samej treści wiadomości nie ma odniesień do wirusa, a jakość tłumaczenia sugeruje oszustwo dokonywane przez osoby nieznające języka polskiego. Imię użyte w treści wiadomości sugeruje, że adres pozyskano z pewnego wycieku danych ze sklepu sprzedającego m.in. elektronikę.


PostOffice

Wita [redacted]

Waga paczki przekracza limit

Uzyskaj dodatkowe informacje poni?ej:

?led? pakiet

Opis pakietu: Telefon wygrany w konkursie

Obs?uga klienta,
PostOffice

Unsubscribe

Link prowadził do strony **parceltracking1[.]com**, która nie prowadziła do bramki płatności, ale do strony wyłudzającej dane osobowe pod pretekstem wygrania iPhone'a i dane karty płatniczej pod pretekstem niewielkiej opłaty (która w rzeczywistości jest regularną, dużą opłatą).

Leki na koronawirusa

Warto ostrożnie interpretować treść wiadomości. Zdarza się, że tego typu wiadomości są rozsyłane masowo przez osobę, która chce zrobić na złość posiadaczowi danego adresu e-mail.

Jeśli faktycznie ktoś oszukuje i sprzedaje leki, może być to podwójnie niebezpieczne.

Podstawowe zasady bezpieczeństwa:

1. wszelkie informacje przesłane mailem lub sms-em należy traktować z dystansem;
2. **nie należy klikać w linki w mailach lub SMS-ach, a mówiąc ściślej nigdy nie należy logować się na stronę, do której link przyszedł przez e-mail lub SMS.** Nawet jeśli ktoś musi zalogować się do banku by coś sprawdzić, może wprowadzić adres ręcznie lub skorzystać z wcześniej utworzonego skrótu w przeglądarce.
3. Najbardziej sensacyjne informacje trzeba sprawdzać w kilku źródłach, a w przypadku informacji o epidemii najlepiej będzie sprawdzać wszystko u źródeł, a więc np. na stronie Ministerstwa Zdrowia, Kancelarii Premiera lub Głównego Inspektora Sanitarnego.

Ponadto:

1. warto ograniczyć instalowanie nowych aplikacji związanych z koronawirusem (można się już teraz spodziewać, że wiele takich produktów powstanie w celu infekowania urządzeń).
2. Trzeba pamiętać, że oszuści działają nie tylko w internecie. Policja spodziewa się też wizyt fałszywych sanitariuszy i policjantów, bo w obecnej sytuacji nietrudno będzie oszustom wpaść na takie pomysły.
3. Zagrożenie epidemią nie może być powodem obniżania jakichkolwiek norm bezpieczeństwa.

Z poważaniem

INSPEKTOR OCHRONY DANYCH
Sylwester Cieśla

CENTRUM ZABEZPIECZENIA INFORMACJI
Sylwester Cieśla
ul. Wapiennikowa 2 lok. 4, 25-112 Kielce
NIP 662-171-24-15, REGON 260124539
tel. (41) 300 55 99, kom. 512 666 944
www.czi24.pl, email: biuro@czi24.pl