Jak rozpoznać szkodliwe maile i co z nimi zrobić.

2025-12-06 06:27:46

Drukuj informację FAQ

Kategoria:	Informacje ogólnofirmowe	**Głosy:**	15
Stan:	publiczne (wszyscy)	**Wynik:**	100.00 %
Język:	pl	**Last update:**	Cz 2025-06-12 09:14:55

Słowa kluczowe

Mail, phising, szkodliwe, podejrzane, spam, atak, podszywanie

Objaw (publiczny)

Podejrzany mail

Problem (publiczny)

Podejrzany mail

Rozwiązanie (publiczny)

Pamiętaj! przestępcy w taki sposób przygotowują szkodliwe maile by udawały zwykłą wiadomość. Nie zawsze jednak im się to udaje. Im większa Twoja czujność i podejrzliwość tym mają mniejsze szanse na zainfekowanie Twojego komputera bądź dokonania wyłudzenia. Najważniejsze jest to by zanim się upewnisz, że jest to prawidłowy mail nie klikaj w jego treść lub w widoczne linki oraz nie otwieraj załączników. Pamiętaj że każdy może być celem ataku typu phising czy próba wyłudzenia - jest to bardzo prawdopodobne. Nie ukrywaj takiego zdarzenia. Właściwą reakcją, jest powiadamianie o potencjalnym zagrożeniu. Poniżej kilka wskazówek jak rozpoznać szkodliwą przesyłkę.
Wskazówka 1

Najczęstszym sposobem zarażenia komputera ofiary jest skłonienie jej do kliknięcia w link w treści maila lub otwarcie załącznika. Jeżeli wiadomość podsiada linki lub załącznik, Twoja czujność powinna być wzmocniona. Nie klikaj w linki i nie otwieraj załączników jeżeli masz jakiekolwiek wątpliwości.

Wskazówka 2

Zwracaj uwagę na błędy w pisowni lub brak „ogonków”. Przestępcy często nie znają języka ofiary i liczą na jego ciekawość, nieświadomość i łatwowierność. Nawet ci posługujący się językiem polskim popełniają błędy szczególnie gdy funkcjonują w atmosferze zagrożenia i pośpiechu.

Wskazówka 3

Uważaj na tematy w stylu „Twoje konto zostało zablokowane”, „Nieautoryzowana próba logowania”, „Pilne zlecenie”, „Twoja usługa właśnie się kończy dokonaj opłaty”, „Proszę opłacić zaległą fakturę” itp. Przestępcy chcą wzbudzić w Tobie poczucie zagrożenia licząc na to, że chcąc mu przeciwdziałać podejmiesz działania w pośpiechu i bez zastanowienia.

Wskazówka 4

Zwróć uwagę na początek i zakończenie maila. Jeżeli nie są one spersonalizowane lub posiadają formę bezosobową, może to oznaczać, że są to wiadomości zawierające szkodliwe treści.

Wskazówka 5

Najczęściej jest tak, że nie znasz adresata wiadomości szkodliwej. Przestępcy posługują się jednak różnymi trikami by wywołać przekonanie, że znasz nadawcę i możesz mu zaufać. Nazwa wyświetlana w polu adresata nie zawsze odzwierciedla rzeczywistego nadawcę. Trzeba zwracać uwagę na kontekst wiadomości. Jeżeli Twój znajomy lub współpracownik nigdy wcześniej nie prosił Ciebie o jakieś działanie lub nie pisał w danej sprawie, to zapewne nie jest to wiadomości od niego. Jeśli masz wątpliwości po prostu nie klikaj w linki i nie otwieraj załączników. Skontaktuj się z Twoim znajomym lub współpracownikiem nie używając podejrzanej wiadomości np. telefonicznie i sprawdź.

np. nazwa wyświetlana „My Bank” adres rzeczywisty „accounts@secure.com”

Pamiętaj! Celem ataku nie zawsze jest komputer i dane na nim zgromadzone. Coraz częściej celem przestępców są informacje które posiadasz lub te do jakich możesz mieć dostęp w wyniku Twoich uprawnień w systemach informatycznych np. możliwość pobrania danych, zlecenie przelewu czy zamówienia usługi.

Wskazówka 6

Nie ufaj zewnętrznym wiadomościom pocztowym odsyłającym do wewnętrznych systemów informatycznych. Stosuj własne linki zgromadzone w ramach przeglądarki internetowej lub znane Tobie ikony na pulpicie. Strony do których prowadzi odwołanie mogą być osadzone poza organizacją i łudząco przypominać witryny prawdziwych wewnętrznych systemów informatycznych. Podając w nich swoje parametry logowania (użytkownika i hasło) w praktyce ujawniasz je przestępcom, którzy wykorzystają je do pozyskania informacji, które najczęściej stanowią tajemnicę przedsiębiorstwa lub co ważniejsze chronione są

przepisami prawa.

Wskazówka 7

Nie udostępniaj innym osobom swoich haseł. Żaden pracownik IT nigdy nie będzie o to prosił.

Co zrobić, gdy rozpoznasz szkodliwą wiadomość?

- Nie klikaj w linki i nie otwieraj załączników.

- Jeśli otwarłeś wiadomość i przeczytałeś treść i dopiero wówczas nabrałeś co do niej podejrzeń, nic się jeszcze nie stało. Zamknij ją.

- Nie przesyłaj jej dalej, nie odpowiadaj na nią.

- Otwórz nową wiadomość pocztową. Zaadresują ją [1]helpdesk@komputronik.pl dodaj temat np. „podejrzana wiadomość”, „phishing” lub dowolnie inaczej ostrzegając adresata o niepokojącej zawartości.

- Załącz podejrzaną wiadomość do treści nowo utworzonej wiadomości jako załącznik i wyślij. (wybierz ze wstążki „Dołącz element” -> „Element programu Outlook” -> wskaż podejrzaną wiadomość -> wyślij).

- Usuń podejrzaną wiadomość z poczty.

Zachowaj czujność. Nie ulegaj sugestii. Lepiej sprawdzić swoje podejrzenia niż być ofiarą ataku. Zgłaszaj swoje obawy. Każde Twoje zgłoszenie będzie zweryfikowane.

[1] mailto:helpdesk@komputronik.pl