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 kampanii phishingowej wykorzystującej wizerunek Ministerstwa Finansów

2023-01-13 14:11:07

Pełna treść ostrzeżenia dostępna w komunikacie "Kampania phishingowa wykorzystująca wizerunek Ministerstwa Finansów" na stronie CERT.

- **Szczególnie narażeni użytkownicy: Klienci banków**
- **Wektor ataku: Strona internetowa oraz wiadomości SMS**
- **Możliwe skutki: Utrata środków finansowych i kontroli nad kontem bankowym**
- **Atakowane platformy: Różne**

Schemat działania

1. **Podszycie się pod Ministerstwo Finansów**
   Zespół CERT Polska zaobserwował nowy wariant oszustwa, w którym przestępcy wykorzystują wizerunek Ministerstwa Finansów. Oszuści na fałszywej stronie internetowej informują o rzekomym nowym rozporządzeniu. Według dokumentu, bezrobotnym i pracującym obywatelom RP, ze względu rosnące bezrobocie i migracje związane z rosyjską agresją, ma przysługiwać jednorazowa wypłata świadczenia finansowego. Na stronie zamieszczone jest fałszywe rozporządzenie, a poniżej znajduje się formularz do przesłania szczegółowych danych osobowych, danych kontaktowych i informacji o banku potencjalnej ofiary. Po przesłaniu wypełnionego formularza wyświetlany jest komunikat o jego pomyślnym uzupełnieniu oraz prośba o oczekiwanie na dalsze instrukcje, które zostaną dostarczone w wiadomości e-mail lub SMS.
2. **Fałszywy SMS**
   Na kolejnym etapie oszustwa poszkodowany otrzymuje wiadomość SMS. Przestępcy, wykorzystując bramki SMS, podszywają się pod nadawcę wiadomości, którym jest rzekomo bank wybrany podczas uzupełniania formularza. W treści wiadomości oszuści zawierają informację o przyznanej kwocie świadczenia oraz link do strony podszywającej się pod bank potencjalnej ofiary.
3. **Fałszywy panel logowania**
   Po kliknięciu w link użytkownik przenoszony jest do fałszywego panelu logowania banku, w którym przestępcy próbują pozyskać informacje o danych uwierzytelniających i kodzie PIN ofiary. W przypadku podania prawidłowych danych poszkodowany zostaje przeniesiony na stronę, na której proszony jest o podanie kodu autoryzacyjnego, który ofiara otrzyma ze swojego banku w wiadomości SMS.

Skutki oszustwa

Udostępnienie przez ofiarę danych uwierzytelniających oraz kodu autoryzacyjnego umożliwia przestępcom uzyskanie pełnego dostępu do konta bankowego. W dalszych krokach starają się oni wykonać przelewy na jak najwyższe kwoty na zewnętrzne konta bankowe, w wyniku czego poszkodowany może stracić oszczędności życia.

Jak się chronić?

Kluczowym aspektem ochrony jest wyrobienie odpowiednich nawyków: -przed podaniem wrażliwych danych należy sprawdzić domenę odwiedzanej strony, zweryfikować czy zgadza się z adresem prawdziwej usługi -należy zwrócić uwagę na treść wiadomości z kodem autoryzacyjnym, co może uchronić przed nadaniem dostępów do konta przestępcom.

Co zrobić w przypadku, gdy wyłudzono dane logowania do bankowości internetowej?

W przypadku, gdy oszust uzyska dostęp do danych logowania konta bankowości internetowej, zalecamy podjąć następujące kroki:

- **jak najszybciej skontaktować się ze swoim bankiem,**
- **zmienić hasło do bankowości internetowej,**
- **jeżeli doszło do wyłudzenia środków finansowych, zgłosić ten fakt na najbliższym komisariacie Policji.**
- **podejrzane wiadomości SMS, zawierające adres URL, przekazać nam na numer 799-448-084, a wszelkie inne zagrożenia zgłosić za pomocą formularza na stronie Zgłoś incydent CERT.PL.**

Dziękujemy za odwiedziny i zapraszamy ponownie

bezpośredni link do strony www