Oszustwa na PIT- jak się przed nimi uchronić w czasie rozliczeń podatkowych?

Okres rozliczeń podatkowych to czas, kiedy intensywnie działają nie tylko Urzędy Skarbowe, ale również cyberprzestępcy. Co roku wymyślają oni nowe sposoby, aby wyłudzić dane lub pieniądze. Często podszywają się pod instytucje państwowe i wykorzystują to, że wiele osób chce szybko zdążyć z rozliczeniem PIT.

Na czym polega oszustwo na PIT?

Oszuści podszywają się pod urzędy skarbowe, Ministerstwo Finansów lub inne instytucje publiczne, rozsyłając fałszywe e-maile, wiadomości SMS, a nawet kontaktują się telefonicznie z potencjalnymi ofiarami. W swoich komunikatach najczęściej informują o:

- rzekomej niedopłacie podatku i potrzebie potwierdzenia danych, aby otrzymać zwrot,
- błędach w deklaracji PIT, które wymagają natychmiastowej korekty,
- grożących karach finansowych za brak rozliczenia
- konieczności szybkiej dopłaty podatku poprzez przelew

W rzeczywistości takie działania mają jeden cel - wyłudzenie poufnych danych, takich jak dane osobowe, loginy i hasła do bankowości elektronicznej, a często także bezpośrednio pieniędzy.

Najczęstsze metody stosowane przez oszustów

1. **Fałszywe e-maile** (phishing) - wiadomości są przygotowane tak, aby wyglądały jak oficjalna korespondencja - zawierają logotypy instytucji, podpisy urzędników oraz poprawny, formalny język. Zazwyczaj umieszczony jest w nich link prowadzący do strony do złudzenia przypominającej prawdziwy serwis podatkowy.

2. **SMS-y z linkiem** (smishing) - krótka wiadomość informuje np. o przysługującym zwrocie podatku i zachęca do kliknięcia w podany link. Po wejściu w link użytkownik trafia na fałszywą stronę, której celem jest przejęcie jego danych.

3. **Fałszywe strony internetowe** - strony te wyglądają niemal identycznie jak oficjalne portale rządowe. Wprowadzenie na nich danych logowania skutkuje przekazaniem ich bezpośrednio w ręce przestępców.

4. **Telefony od „urzędników”**- przestępcy kontaktują się telefonicznie, podszywając się pod pracowników urzędów. W trakcie rozmowy próbują zdobyć dane osobowe lub wywrzeć presję, aby skłonić rozmówcę do wykonania przelewu.

Jak rozpoznać próbę oszustwa?

Zwróć uwagę na charakterystyczne sygnały ostrzegawcze, takie jak:

- wywieranie presji czasu (np. komunikaty typu „działaj natychmiast, inaczej poniesiesz karę”)
- podejrzane adresy e-mail lub linki (np. zawierające literówki w nazwie domeny)
- prośby o przekazanie poufnych danych (takich jak PESEL, hasła czy dane karty płatniczej)
- brak odniesienia do odbiorcy (wiadomość bez personalizacji)
- błędy językowe lub nienaturalna konstrukcja zdań

Jak się zabezpieczyć?

- unikaj klikania w podejrzane linki - szczególnie jeśli pochodzą od nieznanych nadawców

- dokładne sprawdzaj adresy stron internetowych - korzystaj tylko z oficjalnych i zaufanych serwisów
- nie udostępniaj danych poprzez e-mail ani SMS - instytucje publiczne nie proszą o takie informacje w ten sposób
- korzystaj z zaufanych narzędzi i oficjalnych platform do rozliczeń podatkowych
- zadbaj o bezpieczeństwo urządzenia - używaj programu antywirusowego i regularnie aktualizuj system
- potwierdzaj informacje u źródła - jeśli coś budzi wątpliwości, skontaktuj się bezpośrednio z odpowiednim urzędem.

Co zrobić jeśli doszło do oszustwa?

- jak najszybciej skontaktuj się z bankiem i zablokuj dostęp do swojego konta
- zgłoś incydent na policję
- powiadom odpowiednie instytucje (np. CERT Polska), aby ograniczy skutki oszustwa i ostrzec innych
- natychmiast zmień hasła do wszystkich istotnych usług

Podsumowanie

Okres rozliczeń PIT to moment, kiedy trzeba być szczególnie ostrożnym. Oszuści często wykorzystują pośpiech oraz niewiedzę, aby wyłudzić dane i pieniądze. Dlatego tak ważne jest, aby znać potencjalne zagrożenia i stosować podstawowe zasady bezpieczeństwa. Bezpieczne rozliczenie podatku to nie tylko obowiązek, ale też dbanie o swoje dane.