Uwaga na kampanię cyberataków typu web skimming wymierzoną w wybrane polskie sklepy internetowe!

Ataki te polegają na wyświetlaniu fałszywych formularzy płatności na stronach sklepów, w celu wyłudzenia danych kart płatniczych od nieświadomych klientów. Przestępcy wykorzystują w tym celu szkodliwy kod, który przechwytuje wprowadzone dane.

Jak działa atak?

Przestępcy włamują się do panelu administracyjnego sklepu internetowego i dodają złośliwy kod na stronie płatności, po czym:

1. Na stronie płatności może pojawić się **fałszywy formularz płatności kartą**, który wygląda jak prawdziwa bramka płatnicza (np. Paynow). Pojawi się on nawet jeśli wybierzesz inną metodę płatności np. przelew bankowy.
2. Jeśli wpiszesz dane swojej karty w taki formularz, zostają one **przechwycone przez przestępców**. Przechwycą oni : numer karty, datę ważności, kod CVV/CVC, imię i nazwisko.

Kupujesz online? Przestrzegaj zasad bezpieczeństwa:

- Zachowaj ostrożność podczas dokonywania płatności online i dokładnie weryfikuj adres strony internetowej przed podaniem jakichkolwiek danych karty płatniczej. Fałszywe strony często posiadają błędy w adresie URL

- Sprawdzaj certyfikat SSL: upewnij się, że przed adresem strony widoczna jest zamknięta kłódka oraz prefiks https://

- Zarządzaj limitami do płatności online na swoim koncie bankowym, aby w przypadku kradzieży danych zminimalizować potencjalne straty

- Nie działaj pochopnie: oszuści często wywierają presją czasu, np. strasząc zablokowaniem konta lub anulowaniem zamówienia, aby wymusić szybkie działanie.

W przypadku podejrzenia oszustwa:

1. zablokuj kartę i dostęp do bankowości elektronicznej;
2. skontaktuj się bezpośrednio z placówką Banku.

Więcej informacji o bezpieczeństwie zakupów w sieci znajdziesz na https://cert.pl/falszywe-sklepy/