# CYBEROSZUŚCI NACIĄGAJĄ NA WIRTUALNY WĘGIEL - ZACHOWAJCIE OSTROŻNOŚĆ

Data publikacji 12.08.2022

**Internet stał się nieodłączną częścią naszego codziennego życia. Wykorzystujemy go w pracy, do nauki, wymiany informacji lub jako formę zabawy, czy relaksu. Niestety niektóre osoby wykorzystują Internet do popełniania różnego rodzaju przestępstw. Jednak nie wszyscy zdają sobie sprawę z tego, jak łatwo można stać się ofiarą cyberprzestępczości.**

Niemal każdego dnia kędzierzyńsko-kozielscy policjanci otrzymują zgłoszenia od mieszkańców, którzy padli ofiarą oszustwa internetowego i stracili pieniądze. Wachlarz metod, jakimi posługują się przestępcy działający w sieci jest szeroki. Przesyłają linki do fałszywych stron wyłudzających dane dostępowe do konta bankowego. Nakłaniają do instalowania aplikacji umożliwiających im dostęp do naszych kont i kradzież pieniędzy. Podszywają się pod klientów, którzy chcą od nas kupić towar wystawiony na portalu aukcyjnym i wyłudzają dane, żeby nas okraść. Na portalach aukcyjnych zamieszczają fałszywe oferty sprzedaży różnego rodzaju towarów, które po opłaceniu nie docierają do kupującego. Oferują możliwość szybkiego i dużego zysku poprzez inwestowanie w krypto waluty, czy zakup akcji.

W ostatnim czasie na celowniku przestępców znalazł się także węgiel. Oszuści tworzą kopie stron internetowych spółek górniczych działających w Polsce. Uwaga, posiadają nawet logotypy tych spółek, a strony mogą byc łudząco podobne. Potencjalni klienci otrzymują wiadomość SMS z linkiem, który rzekomo ma odsyłać ich do strony sprzedawcy. Odebranie takiej wiadomości powinno być sygnałem dla klienta, że znajduje się na fałszywej stronie, ponieważ, jak podaje np. Polska Grupa Górnicza, podczas transakcji w prawdziwym sklepie, klient nie otrzymuje żadnej wiadomości SMS. Pojawia się także coraz więcej ofert zakupu tego surowca w „okazyjnej" cenie, która jest mocno zaniżona w porównaniu do ceny regularnej. Od potencjalnego kupca oszuści oczekują wpłaty zaliczki, pokrycia kosztów transportu lub uiszczenia całej opłaty za pomocą kodu BLIK. Jednak po wpłaceniu pieniędzy kontakt ze sprzedającym się urywa.

Aby nie stać się ofiarą oszustów powinniśmy pamiętać o kilku ważnych zasadach:

- kierujmy się zawsze zasadą ograniczonego zaufania;
- korzystajmy tylko ze sprawdzonych portali aukcyjnych;
- unikajmy łączenia się z internetem za pośrednictwem publicznych sieci WiFi;
- przed zakupem zasięgnijmy opinii o sprzedawcy i sprawdźmy jego rzetelność. Zwróćmy uwagę, czy podaje swój adres i numer telefonu, żebyśmy mogli się z nim skontaktować w razie jakichkolwiek wątpliwości;
- przeczytajmy komentarze o sprzedającym. Brak komentarzy pozytywnych lub ich niewielka liczba powinny wzbudzić naszą czujność;

- otrzymując ofertę e-mailem, nie klikajmy w linki - mogą one zawierać złośliwe oprogramowanie lub przekierować nas na fałszywą stronę banku. Wpiszmy samodzielnie adres w oknie przeglądarki, w ten sposób unikniemy stron podszywających się pod legalnie działające sklepy;
- nie udostępniajmy swoich danych osobowych oraz danych konta bankowego;
- przy płaceniu kartą kredytową zwracajmy uwagę, czy połączenie internetowe jest bezpieczne. Na początku adresu powinien pojawić się ciąg liter „https”, a na końcu symbol zamkniętej kłódki. Zazwyczaj jednak można zamówić towar z opcją płatności przy odbiorze;
- uważajmy na super oferty, mocno zaniżone lub wręcz niewiarygodnie niskie ceny - powinny wzbudzić naszą czujność;
- zachowujmy całą korespondencję ze sprzedającym - w przypadku oszustwa może ona stać się dowodem w sprawie.

Oszuści cały czas modyfikują swoje metody i wykorzystają każdą okazję, aby wzbogacić się cudzym kosztem. Liczą na naszą łatwowierność, chęć szybkiego wzbogacenia się, czy pośpiech. Pamiętajmy, że bezpieczeństwo w wirtualnej przestrzeni zależy od nas samych. Nie pomogą żadne zabezpieczenia systemowe jeśli sami nie zachowamy należytej ostrożności i zdrowego rozsądku.

(KWP w Opolu /sc)