Nie Daj Się OSZUKAĆ

1 uwaga na LINKI

http.....

2 chroń HASŁA

xxxxxxxxxxxx

3 sprawdź TOŻSAMOŚĆ - zadzwoń!

4 chroń PIN do aplikacji bankowej

5 weryfikuj KOMU podajesz kod BLIK

blik

KAMPANIA EDUKACYJNA ZORGANIZOWANA PRZEZ
KOMENDĘ POWIATOWĄ POLICJI W GNIEŹNIE, POWIAT GNIEŹNIEŃSKI, BANK SPÓŁDZIELCZY W GNIEŹNIE

Nie Daj Się OSZUKAĆ

OSZUŚCI KORZYSTAJĄ Z PSYCHOLOGICZNYCH TECHNIK MANIPULACJI, aby wyłudzić nasze dane osobowe. Zrozumienie tych technik oraz wdrożenie środków obrony może znacząco zwiększyć bezpieczeństwo. Kluczowym elementem socjotechniki jest wykorzystanie naturalnych skłonności ludzkich, takich jak ufność, strach czy chęć pomocy. Oszuści zamiast atakować systemy komputerowe, koncentrują się na ludzkiej psychice, wykorzystując nasze skłonności i emocje. Należy być świadomym, że nawet najbardziej zaawansowane systemy bezpieczeństwa mogą zostać pokonane przez prostą, ale skuteczną manipulację psychologiczną. BĄDŹ CZUJNY! ZAPOZNAJ SIĘ Z KILKOMA ZASADAMI BEZPIECZEŃSTWA.

1 uwaga na LINKI

Oszuści podszywają się pod znane internetowe serwisy aukcyjne. Wysyłają SMS-y z informacją o rzekomym odebraniu pieniędzy za sprzedany towar oraz konieczności wejścia w podany link. Wiadomości te wyglądają bardzo wiarygodnie - znajduje się w nich link, który rzekomo prowadzi do strony znanego serwisu. Kliknięcie PRZEKIEROWUJE NA FAŁSZYWĄ STRONĘ. Wprowadzenie swoich danych na takiej stronie może skutkować kradzieżą informacji osobistych oraz danych finansowych. Aby się chronić, NIGDY NIE KLIKAJ W LINKI ZAWARTE W SMS-ach!

2 chroń HASŁA

Oszuści włamują się na pocztę internetową, a następnie na konta użytkowników portali społecznościowych i wyłudzają pieniądze od naszych znajomych. Oszust ZMIENIA HASŁA i uniemożliwia nam szybką reakcję na to, co się dzieje chwilę później. Po przechwyceniu profili zamieszczają w naszym imieniu sprzęty na sprzedaż w atrakcyjnych cenach. ZADBAJ O BEZPIECZEŃSTWO SWOICH HASEŁ I ZMIENIAJ JE REGULARNIE. Silne hasło to co najmniej 12 znaków, kombinacja wielkich liter, małych liter, cyfr i symboli. Nie udostępniaj nikomu danych do logowania i pamiętaj o wylogowaniu się z aplikacji.

3 sprawdź TOŻSAMOŚĆ - zadzwoń!

JEŚLI ZNAJOMY PROSI O POŻYCZKĘ lub kusi kupnem sprzętu w atrakcyjnej cenie - SPRAWDŹMY CZY TO FAKTYCZNIE ON! Oszust podszywa się pod kogoś, komu ufasz. Przykładem może być fałszywy pracownik banku, który dzwoni i prosi o potwierdzenie danych osobowych. W rzeczywistości celem oszusta jest ich zdobycie i umożliwienie mu dostępu do konta bankowego ofiary. PAMIĘTAJ O WERYFIKOWANIU TOŻSAMOŚCI kontaktującej się z nami osoby w sprawach wymagających podania danych osobowych. SAMODZIELNIE SKONTAKTUJ SIĘ Z INSTYTUCJĄ, KORZYSTAJĄC Z OFICJALNYCH KANAŁÓW.

4 chroń PIN do aplikacji bankowej

Chroń swój telefon a szczególnie swój PIN do aplikacji mobilnej banku. Pamiętaj, że UWIERZYTELNIANIE DWUSKŁADNIKOWE STANOWI DODATKOWĄ WARSTWĘ OCHRONY, UTRUDNIAJĄC PRZESTĘPCOM DOSTĘP DO TWOJEGO KONTA, nawet jeśli zdobędą dane logowania. Ważne jest także korzystanie z filtrów antyspamowych oraz programów antywirusowych, które mogą wykrywać podejrzane wiadomości za pomocą których możesz nieświadomie udostępnić dane oszustom. Jeśli zorientujemy się, że ktoś przejął Twój pin do aplikacji bankowej, zgłośmy sprawę w banku i na Policję.

5 weryfikuj KOMU podajesz kod BLIK

ZANIM PRZEKAŻEMY KOMUKOLWIEK KOD BLIK, upewnijmy się, że za prośbą o pomoc finansową nie kryje się próba oszustwa! Prośby oszustów są różne - na leki, zagubiona torebka, zagubiony portfel, brak pieniędzy na powrót do domu, brak pieniędzy na jedzenie. Przestępcy tłumaczą, że teraz brakuje im środków, ale oddadzą je wieczorem, gdy tylko otrzymają przelew. Dlatego WARTO OSOBIŚCIE SIĘ SPOTKAĆ ZE ZNAJOMYM LUB ZADZWONIĆ I POROZMAWIAĆ, CZY NAPRAWDĘ POTRZEBNE MU SĄ PIENIĄDZE.