

KPP W OTWOCKU

<https://otwock.policja.gov.pl/po/aktualnosci/113222,Zadbaj-o-bezpieczenstwo-w-sieci.html>
2022-12-02, 03:37

Informacja

Strona znajduje się w archiwum.

ZADBAJ O BEZPIECZEŃSTWO W SIECI

Data publikacji 10.08.2022

Policjanci przypominają, jak bezpiecznie korzystać z Internetu, aby nie paść ofiarą przestępców. Coraz częściej oszuści próbują uśpić naszą czujność i nakłonić do przelania środków pieniężnych lub przekazania danych do logowania w bankowości elektronicznej. Najważniejsza jest zasada ograniczonego zaufania. Tylko ostrożność i dokładne weryfikowanie tego, co się znajdzie w Internecie, skrzynce poczty elektronicznej czy wiadomościach sms, pozwoli uniknąć przykrych konsekwencji.

Czujność

- nie udostępniaj i nie powielaj wiadomości, które nie pochodzą z oficjalnych źródeł (gov.pl, policja.pl itp.). W ten sposób zatrzymasz rozprzestrzenianie się fake newsów,
- nie przekazuj spontanicznie darowizn na cele charytatywne i apele o pomoc zawsze weryfikuj wiarygodność organizacji,
- nie odpowiadaj na podejrzane wiadomości,
- nie otwieraj linków i załączników od adresatów, których nie znasz lub budzą twoje wątpliwości (dotyczy to i skrzynki poczty elektronicznej i wiadomości SMS).

Zdalne zakupy

- kupuj tylko od sprawdzonych dostawców i weryfikuj ich wiarygodność,
- używaj kart płatniczych (pozwalają ograniczyć ew. straty, ponadto transakcje dokonywane kartami kredytowymi są ubezpieczone),
- nie daj się ponieść emocjom, jeśli jakaś oferta brzmi zbyt pięknie, to prawdopodobnie nie jest prawdziwa,
- regularnie sprawdzaj stan swojego konta, pozwoli ci to szybko wychwycić wszelkie nieprawidłowości i podejrzane operacje (jeśli masz jakiegokolwiek wątpliwości, niezwłocznie skontaktuj się ze swoim bankiem).

Ochrona przed oszustwami telefonicznymi

- Sprawdź tożsamość dzwoniącego.
- Nie sprawdzaj dzwoniącego za pomocą numeru telefonu, który ci podał - to może być fałszywy numer.

- Wyszukaj w Internecie numer telefonu instytucji/organizacji/firmy i zadzwoń bezpośrednio.
- Nie działaj pod presją czasu. Uważaj na wszystkie wiadomości, które skłaniają do natychmiastowego działania.
- Nie podawaj żadnych poufnych danych przez telefon (hasła, loginów, danych karty kredytowej, itp.).
- Nie ufaj komuś, kto podaje się za urzędnika państwowego lub funkcjonariusza organów ścigania i żąda zapłaty lub poufnych informacji. Od razu skontaktuj się z lokalną Policją, aby to sprawdzić.

Zadbaj o cyberbezpieczeństwo swoich dzieci

- nadzoruj to, co robią i ograniczaj czas korzystania z Internetu przez dzieci,
- korzystaj z programów do kontroli rodzicielskiej,
- zmień hasło fabryczne routera,
- aktualizuj oprogramowanie systemowe i antywirusowe,
- rozmawiaj z dzieckiem o niebezpieczeństwach grożących w sieci.

Zgłaszaj naruszenia w sieci – cyberataki i wszelkie naruszenia w sieci zgłaszaj do CERT Polska – ochronisz siebie i innych przed cyberprzestępcami.

Sprawdzaj listę ostrzeżeń NASK przed niebezpiecznymi stronami, które służą do wyłudzenia danych i środków finansowych użytkowników internetu.