

# POLICJA PODKARPACKA

<https://podkarpacka.policja.gov.pl/rze/komendy-policji/kpp-lezajsk/wydarzenia/97310,Zamien-swoj-dom-w-bezpieczna-cybertwierdze.html>

2021-01-26, 23:29

## ZAMIEŃ SWÓJ DOM W BEZPIECZNAŁ CYBERTWIERDZĘ

Data publikacji 27.03.2020

**Biuro do Walki z Cyberprzestępczością KGP we współpracy z NASK (Naukową i Akademicką Siecią Komputerową) oraz Europolem przypominają o najważniejszych zasadach cyberbezpieczeństwa. #zostanwdomu to czas aktywnego korzystania z Internetu. Wiążą się z tym możliwości zdalnych zakupów czy kontaktu z bliskimi i znajomymi, ale to także przestrzeń aktywności oszustów. Warto zadbać o swoje bezpieczeństwo w sieci.**

Najważniejsza jest zasada ograniczonego zaufania. Tylko ostrożność i dokładne weryfikowanie tego, co się w Internecie czy skrzynce poczty elektronicznej znajdzie, pozwoli uniknąć przykrych konsekwencji.

# ZAMIEŃ SWÓJ DOM W BEZPIECZNĄ CYBERTWIERDZĘ



- Wi-Fi: zawsze zmieniaj domyślne hasło routera
- Zainstaluj program antywirusowy na wszystkich urządzeniach podłączonych do Internetu
- Sprawdź uprawnienia swoich aplikacji i usuń te, których nie używasz
- Wybierz silne i unikalne hasła dla adresów e-mail i kont w mediach społecznościowych
- Twórz kopie zapasowe danych i regularnie je aktualizuj
- Zabezpiecz urządzenia elektroniczne hasłem, numerem PIN lub danymi biometrycznymi
- Sprawdź ustawienia prywatności swoich kont w mediach społecznościowych

## Bezpieczne zakupy online

- Kupuj w **sprawdzonych** sklepach internetowych i sprawdzaj opinie o nich
- Pomyśl **dwa razy**: jeśli oferta brzmi zbyt dobrze, by była prawdziwa, to prawdopodobnie ktoś chce Cię oszukać
- Używaj **kart płatniczych** podczas zakupów online dla większego bezpieczeństwa
- Sprawdź często swoje konto bankowe, by wychwycić **podrzaną aktywność** na koncie



## Zachowaj czujność w czasie pandemii

- ⊗ Nie odpowiadaj na podejrzane wiadomości lub telefony
- ⊗ Nie otwieraj linków i załączników z podejrzanych maili i wiadomości sms
- ⊗ Nie kupuj przez Internet rzeczy, których nigdzie indziej nie można dostać
- ⊗ Nie wysyłaj pieniędzy z góry do kogoś, kogo nie znasz
- ⊗ Nie udostępniaj danych swojej karty płatniczej czy informacji o swoich finansach
- ⊗ Nie udostępniaj wiadomości, które nie pochodzą z oficjalnych źródeł
- ⊗ Nie przekazuj darowizn na cele charytatywne bez dokładnego sprawdzenia wiarygodności organizacji

## Zadbaj o cyberbezpieczeństwo swoich dzieci



Sprawdź **bezpieczeństwo** i ustawienia **prywatności** interaktywnych zabawek

Korzystaj z programów do **kontroli rodzicielskiej**, by zabezpieczyć aktywność internetową swojego dziecka

Zmień fabryczne **hasło** i pamiętaj o aktualizowaniu oprogramowania

Rozmawiaj ze swoim dzieckiem o bezpieczeństwie w sieci. **Słuchaj** o jego internetowych doświadczeniach i **wyjaśnij** mu, jak ważne jest bycie bezpiecznym online i offline

### PAMIĘTAJ

Korzystaj z wiarygodnych źródeł informacji. Jeżeli padłeś ofiarą cyberprzestępstwa, zawsze powiadom o tym policję.



## Czujność w czasie pandemii

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 (np. na leczenie osoby zarażonej COVID-19), zawsze weryfikuj wiarygodność organizacji,

nie odpowiadaj na podejrzane wiadomości (szczególnie oferty „cudownych” leków, szczepionek itp.),

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).

### Zadbaj o cyberbezpieczeństwo swoich dzieci

#zostanwdomu to czas, kiedy dzieci szczególnie dużo czasu spędzą przed komputerem, nadzoruj to, co robią i ograniczaj czas korzystania z Internetu,

korzystaj z programów do kontroli rodzicielskiej,

zmień hasło fabryczne routera,

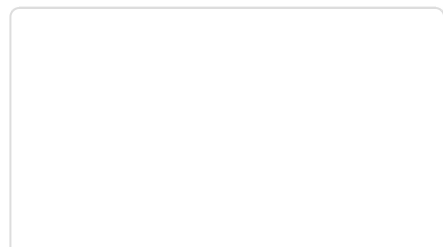
aktualizuj oprogramowanie systemowe i antywirusowe,

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 (link): [Zgłoszenia do CSIRT NASK](#).

**Sprawdź listę ostrzeżeń NASK** przed niebezpiecznymi stronami, które służą do wyludzania danych i środków finansowych użytkowników internetu (link): [Lista ostrzeżeń przed niebezpiecznymi stronami](#).

Więcej informacji i przydatne linki na temat bezpieczeństwa w sieci znajdziesz na stronie Policja.pl w materiale (link): [Żyj bezpiecznie](#).



# ZAMIEŃ SWÓJ DOM W BEZPIECZNĄ CYBERTWIERDZĘ

NASK

EURPOL

CC3

Wi-Fi: zawsze używaj bezpiecznego hasła routera

Zaktualizuj program antywirusowy na wszystkich urządzeniach podłączonych do Internetu

Sprawdź ograniczenia swoich aplikacji i usług, których nie używasz

Wybierz silny i unikalny hasło dla adresu e-mail i kont w mediach społecznościowych



Twórz kopie zapasowe danych i regularnie je aktualizuj

Sprawdź ustawienia prywatności swoich kont w mediach społecznościowych

Zaktualizuj urządzenia osobiste i komercyjne hasłem, numerem PIN lub danymi biometrycznymi

Sprawdź ustawienia prywatności swoich kont w mediach społecznościowych