

**Portal Bezpieczny Olsztyn** to miejsce w sieci związane z bezpieczeństwem, zagrożeniami i sposobami zapobiegania ich skutkom w Olsztynie. Na [www.bezpieczny.olsztyn.eu](http://www.bezpieczny.olsztyn.eu) znajdziemy:

- ✓ informacje o utrudnieniach w ruchu oraz robotach prowadzonych na olsztyńskich drogach,
- ✓ informacje o zdarzeniach na terenie miasta i powiatu (pożary, wypadki drogowe),
- ✓ informacje o imprezach w Olsztynie i związanych z nimi utrudnieniach,
- ✓ telefony służb, szpitali, urzędów i instytucji,
- ✓ ważne komunikaty, np. o nadciągającej wicherze lub fali upałów,
- ✓ poradniki ABC w sytuacjach zagrożeń itp.
- ✓ linki do stron informacyjnych służb,
- ✓ aktualną prognozę pogody.

**Aplikacja Bezpieczny Olsztyn** jest mobilną wersją portalu [www.bezpieczny.olsztyn.eu](http://www.bezpieczny.olsztyn.eu), można ją pobrać bezpłatnie ze sklepu Google Play, Windows Store, App Store.

- ✚ Pogotowie Ratunkowe: **999**
- 🔥 Straż Pożarna: **998**
- 🚓 Policja: **997**
- 👮 Straż Miejska: **986**
- 📞 Telefon alarmowy: **112**
- 📍 Dyżurny Miasta Olsztyna: **+48 89 522 81 12**

⚠ **Czy niepokoi Cię ilość czasu, jaki Twoje dziecko spędza przed komputerem?**

⚠ **Czy znasz świat wirtualny swojego dziecka, tak jak świat realny?**

⚠ **Czy wiesz co zrobić gdy Twoje dziecko doświadczy jednej z poniżej wymienionych form przemocy?**

- 👤 **Podszywanie się w sieci pod inną osobę i działanie na jej niekorzyść.**
- 👤 **Robienie niechcianych zdjęć lub kręcenie niechcianych filmów.**
- 👤 **Wyzywanie, straszenie, obrażanie w sieci.**
- 👤 **Wysyłanie wulgarnych, ośmieszających smsów.**
- 👤 **Publikowanie ośmieszających materiałów (zdjęć, filmów, tekstów, żartów).**
- 👤 **Grożenie komuś w internecie lub przez telefon.**

Jeżeli nurtują Cię te i inne pytania związane z bezpieczeństwem Twojego dziecka czy wnuka w internecie lub z czasem jaki spędza przed komputerem skontaktuj się ze specjalistami:

**Miejski Zespół Profilaktyki i Terapii  
Uzależnień w Olsztynie**



al. Wojska Polskiego 8  
tel. 89 535 77 78

[www.mzptu.pl](http://www.mzptu.pl)



**Bezpieczny**  **Bezpieczny  
Olsztyn**

# E-OLSZTYN

**CO ROBIĆ, A CZEGO NIE, ABY NIE STAĆ SIĘ  
OFIARĄ CYBERPRZESTĘPSTWA.**





## KORZYSTASZ Z KART PŁATNICZYCH? PAMIĘTAJ!

⚠ Podczas transakcji **nie należy tracić karty** z pola widzenia. Po transakcji należy ją odebrać bez zbędnej zwłoki.

⚠ **Należy zachować rozwagę** przy przekazywaniu numeru karty. Nie należy udostępniać numeru karty nikomu, kto do nas dzwoni, również w sytuacji, gdy osoba dzwoniąca informuje, że są problemy z komputerem i proszą o weryfikację informacji. Nie ma zwyczaju by firmy dzwoniły prosząc przez telefon o numer karty kredytowej. Jeżeli to my inicjujemy połączenie, również nie należy udostępniać numeru karty przez telefon, gdy nie mamy pewności, że rozmówca zasługuje na zaufanie.

⚠ **Nigdy nie odpowiadaj** na pocztę elektroniczną, z której wynika konieczność podania informacji o karcie. Nigdy też nie odpowiadaj na maile które zapraszają do odwiedzenia strony internetowej w celu weryfikacji danych, w tym o kartach. Ten rodzaj oszustwa jest nazywanych „phishingiem”.

⚠ **Nie zapisuj kodu PIN** na karcie, ani nie przechowuj go razem z kartą (na wypadek kradzieży portfela czy portmonetki).

⚠ **Chroń swój numer karty** i inne poufne kody umożliwiające dokonane transakcji (np. numer PIN, numer CVV2, numer CVC2), by obcy nie mogli wejść w jego posiadanie, rejestrując obraz karty np. przy użyciu telefonu komórkowego z aparatem fotograficznym, kamerą video lub w inny sposób.

⚠ Przed wyrzuceniem **niszcz wszystkie dokumenty**, które zawierają pełen numer karty.

⚠ Jeśli się przeprowadzasz, **nie zapomnij** jak najszybciej poinformować banku, który wydał karty, o zmianie adresu.

⚠ Jeżeli byłeś w sytuacji, która sprzyja kradzieży **sprawdź czy masz karty** (np. w przedziale pociągu, gdy rozpoczynasz podróż).

⚠ **Nigdy nie należy podawać informacji o karcie** na stronach, które nie są bezpieczne (np. strony ze zdjęciami pornograficznymi lub strony nieznanych szerzej firm oferujące markowy towar po rewelacyjnych cenach).

*Oprac. na podstawie:*

[http://zbp.pl/public/repozytorium/dla\\_konsumentow/poradnik\\_zbp/24rady.pdf](http://zbp.pl/public/repozytorium/dla_konsumentow/poradnik_zbp/24rady.pdf)



## JAK ZABEZPIECZYĆ KOMPUTER?

**Aby nie stać się ofiarą cyberprzestępstwa pamiętaj zabezpieczyć swój komputer!**

🔒 Surfując po Internecie **zachowaj daleko posuniętą czujność i ostrożność**. Na niektórych stronach, zwłaszcza pornograficznych i hakerskich, bardzo często znajdują się złośliwe programy, które możemy nieświadomie zainstalować na komputerze. Mogą sparaliżować pracę komputera bądź wyciągnąć z niego poufne dane.

🔒 **Korzystaj tylko z legalnego systemu operacyjnego**. Pirackie oprogramowania są nielegalne, ale mogą również zawierać programy szpiegujące, które bez naszej wiedzy zainstalują się w komputerze. Będą podglądały wszystko, co wpisujemy na klawiaturze i przekazywały tę wiedzę niepożądanym osobom. W ten sposób możemy utracić kody dostępu do naszych kont internetowych, poczty i autoryzowanych stron.

🔒 **Zainstaluj oprogramowanie antywirusowe i antyszpiegowskie** – darmowe wersje takich programów można znaleźć w internecie i legalnie je pobrać. Programy te uchronią nasz komputer przed wirusami i programami hakerskimi.



**Zainstaluj tzw. firewall** (dosł. ścianę ogniową), który zablokuje próby włamania się z sieci do komputera. Z internetu możemy pobrać darmowe oprogramowanie tego typu.



**Regularnie aktualizuj:** system operacyjny, oprogramowanie antywirusowe, antyszpiegowskie i inne programy, których używamy podczas łączenia się internetem. Luki w oprogramowaniu mogą posłużyć do włamania się do komputera.



**Nie otwieraj** e-maili od nieznanych adresatów i linków rozsyłanych w niechcianej poczcie (tzw. spamie) oraz przez komunikatory. Mogą prowadzić do niebezpiecznych stron lub programów. Użycie oprogramowania antyspamowego znacznie ogranicza ilość niechcianej poczty.



Komunikatory internetowe (np. Skype) są bezpieczne pod warunkiem, że **rozmawiamy tylko ze znanymi nam osobami i nie korzystamy** z linków oraz plików przesyłanych przez niewiadomych nadawców.



W przeglądarkach internetowych można ustawić opcję filtru rodzinnego lub zainstalować na komputerze oprogramowanie, które **uniemożliwi młodszym członkom rodziny korzystanie z niepożądanych stron**.

