



RAZEM BEZPIECZNIEJ W CYBERPRZESTRZENI ŁĄCZYMY POKOLENIA MIESZKAŃCÓW MIASTA I GMINY ŁASIN

PATRONAT BURMISTRZ MIASTA I GMINY ŁASIN



PODSTAWOWE ZASADY BEZPIECZEŃSTWA W SIECI

Phishing

Podejrzana wiadomość? Nie daj się złowić!

Phishing to jedna z najpopularniejszych metod działania hakerów! Udają oni Twojego kuriera, bank, ulubione platformy sprzedażowe (Allegro, OLX, Vinted) lub instytucje rządowe tylko po to, aby wyłudzić od Ciebie hasła lub pieniądze.

Oszuści, podszywając się pod zaufane firmy, wysyłają wiadomości, które najczęściej zawierają link przekierowujący do fałszywej strony.

Jak oszuści działają w praktyce:

- Oszustwo na Allegro/OLX/Vinted: kupujący prosi Cię o adres e-mail lub numer telefonu, a następnie wysyła Ci link rzekomo potrzebny do finalizacji transakcji. Link ten prowadzi do fałszywej strony do logowania albo fałszywej bramki płatności, która ma na celu wyłudzić Twoje dane lub pieniądze.
- Wyłudzenie na BLIK-a: Otrzymujesz od znajomego prośbę o kod BLIK, bo zabrakło mu pieniędzy na pilny zakup. W rzeczywistości to wiadomość od hakerów, który przejął konto Twojego znajomego w mediach społecznościowych.

W 2025 roku wykryto w Polsce ok. 80 tysięcy przypadków phishingu*. Liczba ta z roku na rok gwałtownie wzrasta, dlatego miej świadomość i nie klikaj w podejrzane linki!

Dowiedz się, jakie są rodzaje phishingu, jak go rozpoznawać oraz poznaj inne związane z nim zagrożenia:

<https://cyber3.pl/2026/04/30/phishing-analiza-zagrozenia-i-sposoby-zapobiegania/>

* Źródło: Raport roczny 2025 z działalności CERT Polska, https://cert.pl/uploads/docs/Raport_CP_2025.pdf

Spoofing

Idealny cyfrowy kamuflaż. Czy potrafisz przejrzeć spoofing?

Spoofing to technika oszustwa, która polega na podrabianiu danych identyfikacyjnych. Przestępcy używają specjalnych narzędzi, aby zmodyfikować nagłówki wiadomości e-mail, adresy stron internetowych lub sygnał telefoniczny. W efekcie Twoje urządzenia „zostają oszukane” – na ekranie telefonu wyświetla się oficjalny numer Twojego banku, a w skrzynce mailowej widzisz autentyczny adres znanej firmy lub platformy streamingowej.

Oszuści wykorzystują Twoje zaufanie, aby wyrzucić presję czasu i wyłudzić loginy, hasła lub zmusić do szybkiego przelewu! Ofiary spoofingu tracą nie tylko oszczędności swojego życia, ale także ufność w stosunku do drugiego człowieka.

Obecnie oszuści potrafią za pomocą sztucznej inteligencji sklonować czyjś głos w czasie rzeczywistym. Wystarczy im krótki fragment dźwięku wycięty z filmu na TikToku lub Instagramie, aby wygenerować komunikat brzmiący jak głos członka rodziny lub znajomego.

Nie daj się zmanipulować! Dowiedz się więcej o spoofingu: <https://cyber3.pl/2026/04/10/spoofing-czym-jest-i-jak-sie-przed-nim-chronic/>



RAZEM BEZPIECZNIEJ W CYBERPRZESTRZENI ŁĄCZYM Y POKOLENIA MIESZKAŃCÓW MIASTA I GMINY ŁASIN

PATRONAT BURMISTRZ MIASTA I GMINY ŁASIN



Ransomware

Zaszyfrowany komputer i żądanie okupu: poznaj ransomware

Ransomware to jeden z najbardziej złośliwych rodzajów cyberataków, który potrafi w kilka sekund sparaliżować prywatny komputer lub całą firmę. Złośliwy program szyfruje wszystkie zdjęcia, dokumenty i bazy danych na urządzeniu, a hakerzy żądają ogromnych pieniędzy w zamian za klucz do ich odzyskania.

Najczęściej infekcja zaczyna się od otwarcia zainfekowanego załącznika w mailu, pobrania darmowego programu z niesprawdzonej strony lub kliknięcia w fałszywą aktualizację systemu.

Przezorny zawsze zabezpieczony – regularny backup danych to Twoja najlepsza tarcza! Aby czuć się bezpiecznie, wszystkie ważne dla Ciebie dane powinny być zapisane co najmniej na trzech różnych nośnikach danych (w tym jedna kopia offline).

Dowiedz się więcej o ransomware i jak zapobiegać atakom: <https://cyber3.pl/2026/04/30/ransomware-analiza-zagrozen-i-sposoby-zapobiegania/>

Sharenting

Rodzicu, pomyśl, zanim opublikujesz zdjęcia swoich dzieci!

Sharenting, czyli regularne publikowanie przez rodziców zdjęć, nagrań i informacji o swoich dzieciach w mediach społecznościowych oraz innych platformach, to dziś codzienność. Wbrew pozorom takie działanie może wiązać się z poważnymi konsekwencjami dla Twojego dziecka w przyszłości!

Pamiętaj, że **każde dziecko ma prawo do prywatności**. Dopóki nie będzie mogło samo wyrazić zgody na publikację jego wizerunku, Ty jako opiekun musisz dbać o jego bezpieczeństwo. Zdjęcia z wakacji czy zabawne filmiki z placu zabaw tworzą trwały, cyfrowy ślad, z którym młody człowiek będzie musiał żyć, gdy dorośnie. Dodatkowo dziecko zostaje narażone na hejt ze strony rówieśników oraz obcych ludzi!

Dowiedz się więcej o niebezpieczeństwach związanych z sharentingiem: <https://cyber3.pl/2026/03/17/sharenting-a-rodo-jak-chronic-prywatnosc-dzieci-w-internecie/>

OSINT

OSINT – czy wiesz, co to oznacza?

Czy wiesz, że obca osoba potrzebuje tylko kilku minut na Twoich social mediach, aby poznać całe Twoje życie? Pozwala na to **OSINT** (ang. Open Source Intelligence), czyli legalny, biały wywiad.

Z Twoich postów przestępcy mogą dowiedzieć się: kim jest Twoja rodzina, gdzie i kiedy spędzasz czas, jak masz na imię Ty i Twoje dzieci. W efekcie dostosowują oni ataki idealnie pod Ciebie! Stąd biorą się wiadomości: „Cześć mamo, zepsuł mi się telefon...”, w których oszust posługuje się imieniem Twojego dziecka oraz zna szczegóły z jego życia. Internet nie zapomina, a cyfrowy ślad trudno wymazać. Korzystaj z sieci rozważnie, bo to Ty jesteś głównym źródłem wiedzy dla atakującego!

Dowiedz się więcej o tym, czym jest OSINT: <https://cyber3.pl/2026/05/29/osint-czyli-cyfrowe-slady-ktore-zostawiamy-w-internecie/>



RAZEM BEZPIECZNIEJ W CYBERPRZESTRZENI ŁĄCZYMY POKOLENIA MIESZKAŃCÓW MIASTA I GMINY ŁASIN

PATRONAT BURMISTRZ MIASTA I GMINY ŁASIN



Ochrona dziecka przed zagrożeniami w sieci

Czy wiesz, co Twoje dziecko robi w sieci, gdy gasną światła?

Rodzice uważnie pilnują, aby dziecko nie rozmawiało z obcymi na ulicy. Jednak w Internecie często wpuszczamy tych obcych prosto do ich pokoi. Zagrożenia takie jak cyberbullying, grooming czy uzależnienie od ekranów to niestety codzienność.

Jak realnie chronić dziecko w cyfrowym świecie? Na początek postaraj się przestrzegać dwóch zasad:

- Rozmawiaj, nie tylko kontroluj! Zaufanie chroni lepiej niż jakakolwiek blokada rodzicielska.
- Ustal jasne zasady dotyczące czasu przed ekranem i stref bez telefonu (np. sypialnia, stół).

Blokady rodzicielskie i aplikacje kontrolne są pomocne, ale to tylko wsparcie, a nie gotowe rozwiązania. Najważniejsze to nauczyć dzieci, jak bezpiecznie i rozważnie korzystać z Internetu samodzielnie. Żaden algorytm nie zastąpi mądrego rodzica, a świadomość dziecka jest jego najlepszą tarczą obronną.

Dowiedz się więcej o ochronie Twoich dzieci przed zagrożeniami w sieci: <https://www.doering-partnerzy.pl/jak-chronic-dziecko-przed-zagrozeniami-w-sieci-przewodnik-dla-swiadomych-rodzicow/>

Dezinformacja w Polsce

Jakie formy przybiera dezinformacja w 2026 roku?

Od lat zwraca się szczególną uwagę na to, że Internet kłamie i nie można wierzyć we wszystko, co zobaczy się w sieci. Dezinformacja zaczęła przybierać jednak zupełnie nowe formy. Przez rozwój sztucznej inteligencji uderza ona w renomowane instytucje i obszary, które dotąd kojarzyły się nam z bezpieczeństwem.

Z raportów NASK wynika, że najczęstsze kampanie oszustów w Polsce dotyczą m.in. fałszywych aplikacji mObywatel oraz podszywania się pod osoby publiczne, np. znanych dziennikarzy, prezydenta lub premiera.

Dezinformacja uderza również w sektor medyczny, gdzie oszuści wykorzystują wizerunek znanych lekarzy, aby reklamować niesprawdzone i często niebezpieczne metody leczenia lub suplementy.

Poważny problem stanowią **materiały typu deepfake**. Wykorzystują one wizerunek konkretnych osób i potrafią idealnie sklonować ich głos. Przez to w Internecie krążą nagrania i zdjęcia z sytuacji, które nigdy nie miały miejsca, oraz wypowiedzi osób, które nigdy takich słów nie wypowiedziały. Wchodzimy w erę, w której nie można już wierzyć własnym oczom i uszom, a wszystkie informacje należy weryfikować.

Dowiedz się więcej o dezinformacji w Polsce i wnioskach płynących z raportu NASK: <https://www.doering-partnerzy.pl/dezinformacja-w-polsce-najwazniejsze-wnioski-z-raportu-nask-za-2025-rok/>



RAZEM BEZPIECZNIEJ W CYBERPRZESTRZENI ŁĄCZYMY POKOLENIA MIESZKAŃCÓW MIASTA I GMINY ŁASIN

PATRONAT BURMISTRZ MIASTA I GMINY ŁASIN



Wyciek Danych

Co dzieje się, gdy pękają zabezpieczenia?

Osoba nieupoważniona uzyskała dostęp do Twoich danych poufnych (np. haseł, adresów e-mail, kart płatniczych)? Jest to tzw. **wyciek danych**, do którego może dojść ze względu na różne przyczyny, np. przez ataki hakerskie, nieprawidłowo zabezpieczone serwery, phishing czy też prosty błąd ludzki.

Tymczasem wyciek Twojego numeru telefonu może ułatwić przestępcom celowane ataki SMS-owe (tzw. smishing). Podszywając się pod bank, mogą oni wyłudzić Twoje dane logowania. Jeśli dodatkowo wejdą w posiadanie Twoich danych osobowych, mogą wyrobić duplikat Twojej karty SIM (tzw. SIM swapping). To pozwala im na przechwycenie SMS-ów autoryzacyjnych i kradzież oszczędności.

Czy wiesz, że możesz łatwo sprawdzić, czy Twój adres e-mail lub telefon padły ofiarą wycieku, za pomocą popularnych darmowych serwisów, np. Have I Been Pwned?

Dowiedz się jakie są najczęstsze błędy prowadzące do wycieku danych: <https://cyber3.pl/2025/06/27/najczestsze-bledy-prowadzace-do-wycieku-danych/>

Przeczytaj również, jak postępować w przypadku wycieku, krok po kroku: <https://cyber3.pl/2025/06/16/wyciek-danych-osobowych-co-robic-krok-po-kroku/>

Hejt

Hejt to nie opinia! Przestańmy go usprawiedliwiać.

Często mylimy konstruktywną krytykę z czystą agresją. **Hejt w Internecie** stał się zjawiskiem na tyle powszechnym, że zaczynamy go ignorować, uznając go za nieodłączny element naszej obecności w sieci. To błąd. Niewinne kliknięcie i złośliwy komentarz nie powinny być tolerowane, bo mogą zostawić realne ślady w psychice drugiego człowieka.

Nie bój się walczyć o własny dobrostan w sieci! Masz prawo stawiać twarde granice. Zablokuj lub zgłoś hejtera, zamiast karmić go swoją reakcją. Pamiętaj też, że nie jesteś sam i zawsze możesz porozmawiać na ten temat z rodzicem, nauczycielem lub inną zaufaną osobą.

Dowiedz się więcej o hejcie: <https://cyber3.pl/2026/07/17/hejt-w-sieci-czym-jest-i-jak-go-zatrzymac/>

Media społecznościowe

730 godzin rocznie. Zobacz, ile naprawdę kosztuje Cię „bezpłatny” TikTok.

Choć przy zakładaniu konta w mediach społecznościowych nie musisz podawać numeru karty kredytowej, giganci technologicznie doskonale wiedzą, jak na Tobie zarabiać. Prawdziwą walutą w sieci nie są bowiem pieniądze, ale Twój czas, uwaga i prywatność.

Przeciętny Polak spędza w social mediach około 2 godziny dziennie. W skali roku daje to aż 730 godzin – czyli cały jeden miesiąc ciągłego patrzenia w ekran non stop, bez przerwy na sen!

Nowy model subskrypcyjny firmy Meta w Europie stawia użytkowników Facebooka i Instagrama przed ultimatum: albo płacisz za prywatność bez reklam, albo wyrażasz zgodę na profilowanie danych w zamian za darmowy dostęp. Wprowadzone zmiany oznaczają koniec darmowego Internetu w dotychczasowej formie. Od tego momentu dane użytkowników są jawnie traktowane jak waluta.

Dowiedz się więcej o tym jak media społecznościowe zarabiają na Twoim życiu: <https://cyber3.pl/2026/09/16/iluzja-darmowosci-jak-media-spoecznościowe-zarabiaja-na-twoim-zyciu/>