PORADNIK DLA SZKÓŁ OGÓLNOPOLSKIEJ SIECI EDUKACYJNEJ

BEZPIECZEŃSTWO ONLINE W SZKOŁACH OGÓLNOPOLSKIEJ SIECI EDUKACYJNEJ

CZĘŚĆ 2

Warszawa 2020

OGÓLNOPOLSKA SIEĆ EDUKACYJNA
NASK
Ministerstwo Cyfryzacji

SPIS ZAGADNIEŃ

Redakcja
Marek Sowala, dr Agnieszka Wrońska

Autorzy
Kinga Kaczmarek, Katarzyna Kujawa, Michał Łuciuk, Anna Pudłowska, Marek Sowala, Agnieszka Wrońska

Redakcja językowa, korekta
Katarzyna Gańko, Diana Kania

Opracowanie graficzne, skład
Agnieszka Staręga

Warszawa 2020

ISBN: 978-83-65448-23-1

NASK Państwowy Instytut Badawczy
ul. Kolska 12
01-045 Warszawa

WSTĘP

Oddajemy w Państwa ręce drugą część poradnika „Bezpieczeństwo online w szkołach Ogólnopolskiej Sieci Edukacyjnej”. Znalazły się tutaj informacje o kolejnych internetowych zagrożeniach dzieci i młodzieży. Mamy nadzieję, że poradnik pomoże właściwie reagować w ryzykownych sytuacjach, a także podpowie, jak unikać niebezpieczeństw online.

Zgodnie z zapisami Ustawy z dnia 27 października 2017 r. o Ogólnopolskiej Sieci Edukacyjnej (OSE) w ciągu najbliższych lat do wszystkich placówek oświatowych w Polsce doprowadzony zostanie światłowodowy symetryczny internet o przepływności 100 Mb/s. Zarówno cele programu OSE, jak i zadania jego operatora zdefiniowane w powyższej Ustawie kładą duży nacisk na zagadnienie cyberbezpieczeństwa. Do zadań operatora sieci OSE należy m.in. świadczenie szkole usług bezpieczeństwa teleinformatycznego, obejmujących ochronę przed szkodliwym oprogramowaniem, monitorowanie zagrożeń i bezpieczeństwa sieciowego oraz promowanie zasad bezpiecznego korzystania z technologii cyfrowych. Jednocześnie art. 27 Ustawy Prawo oświatowe z dnia 14 grudnia 2016 r. nakłada na szkoły i placówki zapewniające dostęp do internetu obowiązek podejmowania działań zabezpieczających uczniów przed dostępem do treści, które mogą stanowić zagrożenie dla ich prawidłowego rozwoju. W szczególności szkoły obowiązane są zainstalować i aktualizować oprogramowanie zabezpieczające.

Korzystanie przez młodych użytkowników z sieci oraz coraz większa obecność internetu w edukacji i w procesach komunikowania w szkole i poza nią powinny iść w parze zarówno z edukacją dotyczącą bezpiecznego korzystania z sieci, jak i tworzeniem i wdrażaniem zasad profilaktyki oraz procedur reagowania na zagrożenia cyberprzestrzeni. Najważniejsze znaczenie dla zapewnienia podstaw bezpieczeństwa cyfrowego w szkole mają działania edukacyjne i profilaktyczne. Istotne jest także posiadanie przez szkołę opracowanych modeli reagowania w sytuacjach kryzysowych.

W poradniku zaprezentowane zostały informacje o zagrożeniach online oraz propozycje procedur postępowania w przypadku ich wystąpienia. Zachęcamy szkoły do włączenia ich do szkolnej polityki bezpieczeństwa cyfrowego. W materiale poruszono następujące zagadnienia: hejt i mowa nienawiści, grooming, cyberstalking, patostreaming, flaming, skimming, kradzież tożsamości, ochrona wizerunku w sieci, prawo do zapomnienia w internecie, Business E-mail Compromise, a także bezpieczne użytkowanie urządzeń mobilnych.

Układ treści kolejnych rozdziałów obejmuje: krótki opis zagrożenia, odwołanie do wyników badań i przepisów prawa oraz porady.

Dodatkowo piktogramy ułatwiają określenie, czy dane zagrożenie podlega ochronie w ramach usług bezpieczeństwa OSE, a także wskazują, które zagadnienia wymagają podjęcia działań edukacyjnych czy interwencyjnych.

Wyjaśniaj, edukuj, ostrzegaj, korzystaj z porad ekspertów

Usługi bezpieczeństwa OSE

Zgłoś do Dyżurnetu (dyzurnet.pl)

Planowane usługi bezpieczeństwa OSE

Gdzie uzyskać pomoc?

- Centrum Kontaktu OSE – informacja o usługach bezpieczeństwa OSE: **+48 22 182 55 55**
- Dyżurnet.pl **www.dyzurnet.pl** – anonimowe zgłaszanie nielegalnych bądź szkodliwych treści w internecie
- **800 100 100** – Telefon dla rodziców i nauczycieli
- **116 111** – Telefon zaufania dla dzieci i młodzieży
- **Administratorzy serwisów internetowych**

PATOSTREAMING

Anna Pudłowska

Opis zjawiska

Patostreaming jest najczęściej określany jako transmisja internetowa na żywo, prowadzona w serwisach internetowych udostępniających wideo strumieniowe, w trakcie której prezentowane są liczne zachowania powszechnie uznawane za będące dewiacjami społecznymi, w tym zwłaszcza libacje alkoholowe, przemoc domowa lub wulgaryzmy. Patotreści to także filmy zamieszczane w mediach społecznościowych, zachęcające do zachowań szkodliwych dla zdrowia, np. upijania się do nieprzytomności czy samookaleczania.

Patostreaming w Polsce ma swoje źródło w środowisku tzw. letsplejerów (od ang. let's play – „zagrajmy"), którzy nagrywają przebieg gry komputerowej razem z komentarzem. Kiedy okazało się, że wiele osób streamuje swoją grę i niełatwo jest zdobyć satysfakcjonujące zasięgi, letsplejerzy do relacji włączyli kontrowersyjne zachowania. Obecnie nowe patostreamingi powstają na fali popularności istniejących już treści. Dużym zainteresowaniem cieszą się tzw. shoty, które są archiwizowanymi i publikowanymi w mediach społecznościowych fragmentami patostreamów. Widzowie najczęściej poszukują tzw. dymów – najbardziej spektakularnych sytuacji, takich jak np. bójki czy demolowanie domów.

Innym niepokojącym przejawem agresji, w tym przypadku już nie tylko elektronicznej, jest happy slapping (od ang. „radosne okładanie"). To forma przemocy, która polega na fizycznym zaatakowaniu przypadkowej osoby i nagraniu całego wydarzenia, a następnie umieszczeniu filmiku w sieci. Happy slapping możemy zakwalifikować jako jedną z form cyberstalkingu.

Skala zjawiska

- 84% nastolatków w wieku 13–15 lat słyszało o patotreściach (częściej byli to chłopcy niż dziewczęta), a 37% z nich deklaruje, że oglądało tego typu nagrania.
- 53% respondentów jako źródło wiedzy o istnieniu patotreści wskazuje osobę znajomą, 27% otrzymało link do takich materiałów, natomiast 30% trafiło na nie przypadkiem.
- Trzy czwarte ankietowanych jako powód oglądania patotreści wskazało ciekawość, 29% – nudę, 24% – chęć rozrywki, a 10% – chęć bycia na czasie (wszystkie dane za: FDDS, 2019).

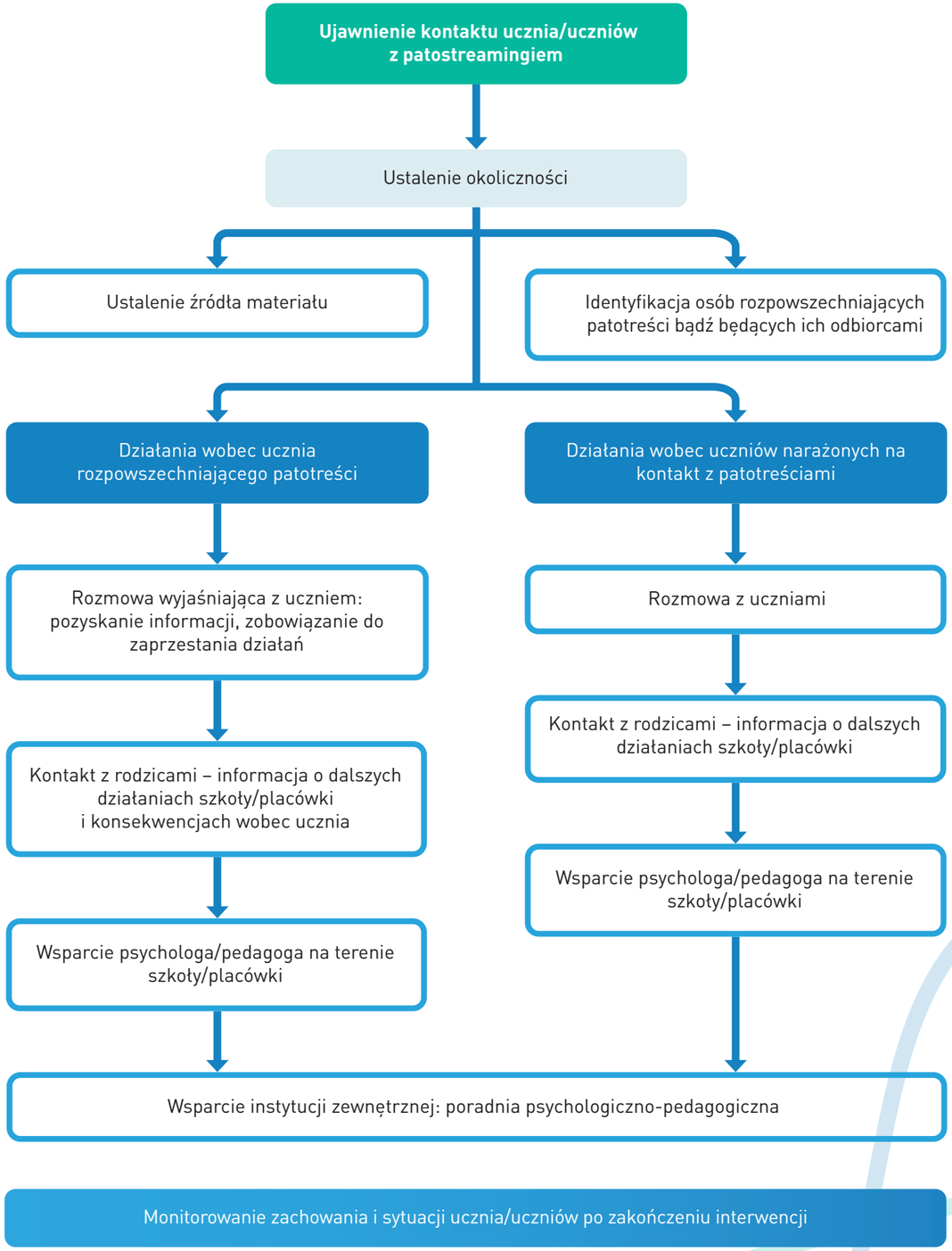
Przepisy prawa

Zjawisko patostreamingu i happy slappingu może wiązać się z łamaniem prawa. Patostreaming podlega odpowiedzialności karnej (przestępstwo), cywilnej (naruszenie dóbr osobistych lub czyn niedozwolony), porządkowej (naruszenie regulaminu serwisu internetowego).

Porady

- Dyrektorze: zadbaj o rozwój kompetencji cyfrowych nauczycieli, których wiedza dotycząca bezpieczeństwa w internecie powinna być stale pogłębiana i aktualizowana.
  Nauczycielu: zdobywaj aktualne informacje i pogłębiaj swoją wiedzę.
- Ustal zasady korzystania z internetu, edukuj dzieci w tym zakresie.
- Ze starszymi dziećmi rozmawiaj o ich aktywności w sieci, z kolei u młodszych – miej pod kontrolą ich aktywność w sieci.

Procedura reagowania na incydenty związane z kontaktem ucznia z patostreamingiem



FLAMING

Michał Łuciuk

Opis zjawiska

Flaming lub utrwalony w społeczności polskich internautów flejm to termin określający kłótnie w internecie. Jest to zjawisko charakterystyczne dla mediów społecznościowych, forów tematycznych czy sekcji komentarzy w serwisach internetowych.

Zjawisko polega na umieszczeniu prowokacyjnego wpisu-przynęty, tzw. flamebaitu, nierzadko w kontrze do publikowanej treści. Powoduje on negatywną reakcję współrozmówców lub skutkuje ostrą polemiką uczestników dyskusji. W konsekwencji prowadzi to do eskalacji internetowego konfliktu, opartego na agresji i złośliwości, określanego mianem flame war.

Najczęściej flaming pozbawiony jest merytorycznego sensu. Nie jest to również umiejętne balansowanie na emocjach, przekonaniach i opiniach konkretnej grupy odbiorców, a często bezpardonowy atak oparty na stereotypach. Jego pojawienie się w danym miejscu nie przechodzi więc bez echa. Dodatkowo charakter zamieszczanych treści sprawia, że zazwyczaj o celowe działanie podejrzewa się internetowych trolli. Niejednokrotnie są oni autorami pierwszego wpisu albo uczestniczą w początkowej wymianie zdań, ożywiając dyskusję i rozniecając konflikt.

Bezpośrednio flaming może wpływać na samopoczucie rozmówców. Pośrednio może także skutkować próbą przeniesienia niezdrowej dyskusji do życia codziennego i prowadzić choćby do wzrostu uprzedzeń względem wybranej grupy społecznej.

Przepisy prawa

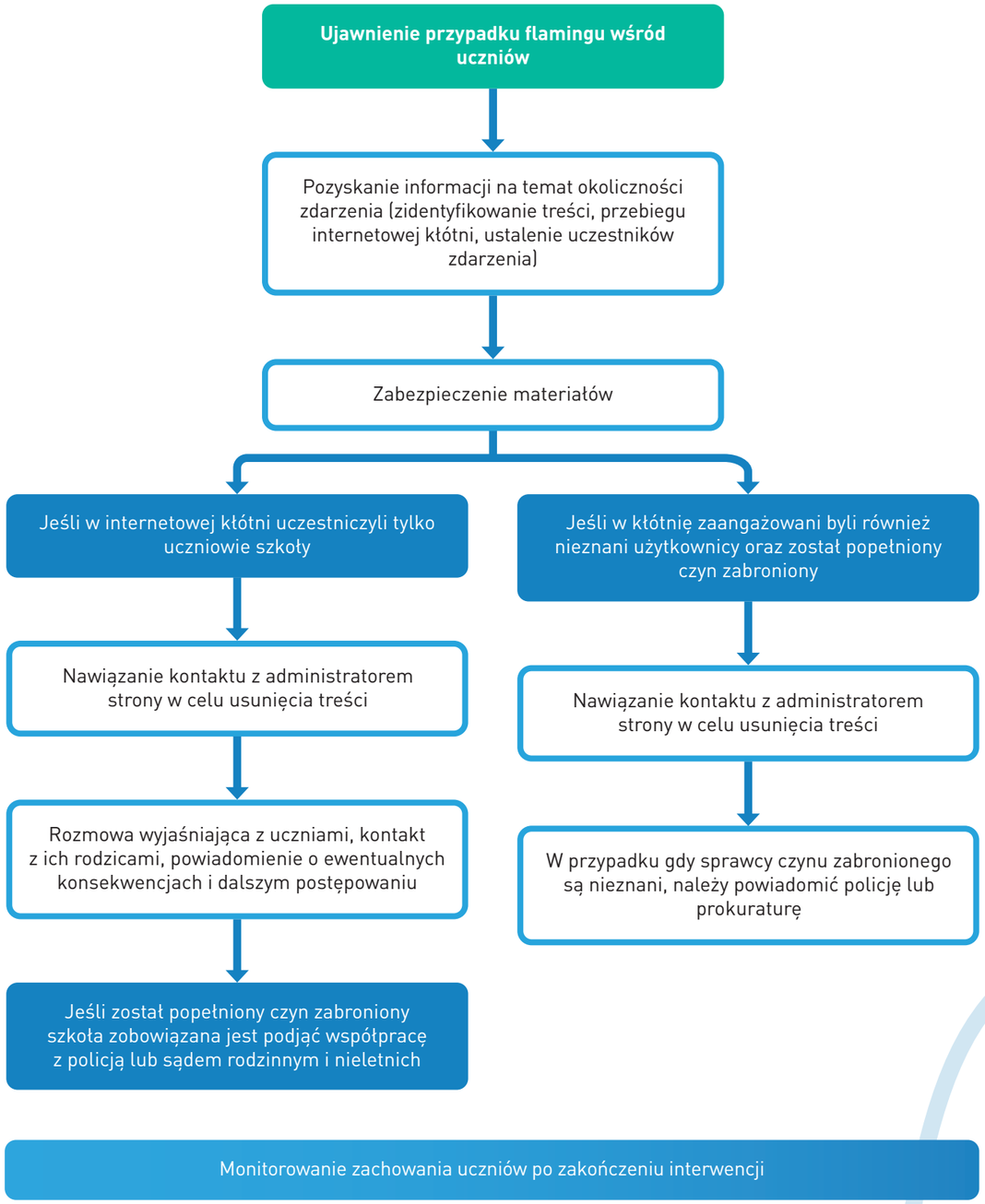
Samo zjawisko flamingu nie jest usankcjonowane prawnie, jednak w czasie ostrej wymiany zdań może dojść do sytuacji, w której zostanie popełniony czyn zabroniony, jakim jest zniesławienie (art. 212 Kodeksu karnego). Ściganie przestępstwa odbywa się na wniosek pokrzywdzonego. Dopuszczenie się flamingu w środkach masowego przekazu, w tym w internecie, zagrożone jest karą grzywny, ograniczenia wolności lub pozbawienia wolności do roku.

Innym przestępstwem, do którego może doprowadzić flaming, jest nawoływanie do nienawiści, za które art. 256 Kodeksu karnego przewiduje karę grzywny, ograniczenia wolności lub pozbawienia wolności do lat dwóch. Nawoływanie do nienawiści ma charakter publicznoskargowy i ścigane jest z urzędu.

Porady

- Pierwszym sygnałem do potraktowania danego wpisu jako próby rozpoczęcia internetowej kłótni są charakterystyczne dla flamingu uogólnienia i powielane schematy oraz promowanie utrwalonych w społeczeństwie stereotypów. Zignoruj taką treść, aby zminimalizować ryzyko eskalacji, ale pamiętaj, że powinieneś monitorować rozwój sytuacji.
- O ile to możliwe, wszelkie treści przeczące zaleceniom netykiety zgłaszaj administratorom strony, na której się znalazły. Dodatkowo część stron umożliwia ukrywanie lub blokowanie treści autorstwa danego użytkownika. Wykorzystaj tę funkcję, by uniknąć niekomfortowych sytuacji w przyszłości.

Procedura reagowania w przypadku flamingu



KRADZIEŻ TOŻSAMOŚCI

Kinga Kaczmarek, Katarzyna Kujawa

Opis zjawiska

Tożsamość to wszelkie informacje na temat danej osoby, które pozwalają ją zidentyfikować, tj. dane personalne, cechy wyglądu, fakty na jej temat.

Kradzież tożsamości polega na podszyciu się pod inną osobę poprzez wykorzystanie jej wizerunku czy innych danych osobowych. Celem takiego działania może być m.in. próba wyłudzenia kredytu lub przywłaszczenie sprzętu wypożyczonego wcześniej na czyjeś nazwisko. Bywa, że kradzież tożsamości wiąże się z cyberstalkingiem: sprawca, publikując w imieniu wybranej osoby niedozwolone czy ośmieszające treści, dąży do jej kompromitacji (np. na profilu społecznościowym).

Kradzież tożsamości to przestępstwo przeciwko wolności scharakteryzowane w art. 190a § 2 Kodeksu karnego. Zachowanie sprawcy przestępstwa jest ukierunkowane na wyrządzenie danej osobie szkody majątkowej lub osobistej, np. poprzez dokonywanie wyłudzeń za pośrednictwem bankowości internetowej i konta osoby pokrzywdzonej. Kradzież tożsamości jest też bardzo często powiązana ze zjawiskiem stalkingu, czyli uporczywego nękania.

Kradzież tożsamości może być dokonywana na dwa sposoby. Pierwszy polega na wybraniu osoby, której poufne dane (imię, nazwisko, PESEL, hasła do kont mailowych, bankowych i profili społecznościowych) łatwo zdobyć lub której sprawca kradzieży nie darzy sympatią i dąży do uprzykrzenia jej życia.

W drugim przypadku sprawca przypadkowo wchodzi w posiadanie wrażliwych danych, np. poprzez znalezienie czyjegoś dowodu osobistego. Zamiast zgłosić ten fakt na policję, niejako korzysta z okazji i wykorzystuje dokument do niewłaściwych celów.

W dzisiejszych czasach kradzież tożsamości jest znacznie łatwiejsza niż dawniej. Szczególnie w internecie można w łatwy sposób uzyskać czyjeś dane osobowe, dlatego warto zwracać uwagę, jakie informacje na swój temat umieszczamy w sieci.

Skala zjawiska

- 15% nastolatków podszywało się pod inną osobę, zakładając w jej imieniu ośmieszający profil na portalu społecznościowym (Pyżalski, 2010).
- 40,5% nastolatków doświadczyło podszywania się przez inne osoby pod ich znajomych („Nastolatki 3.0", 2016).

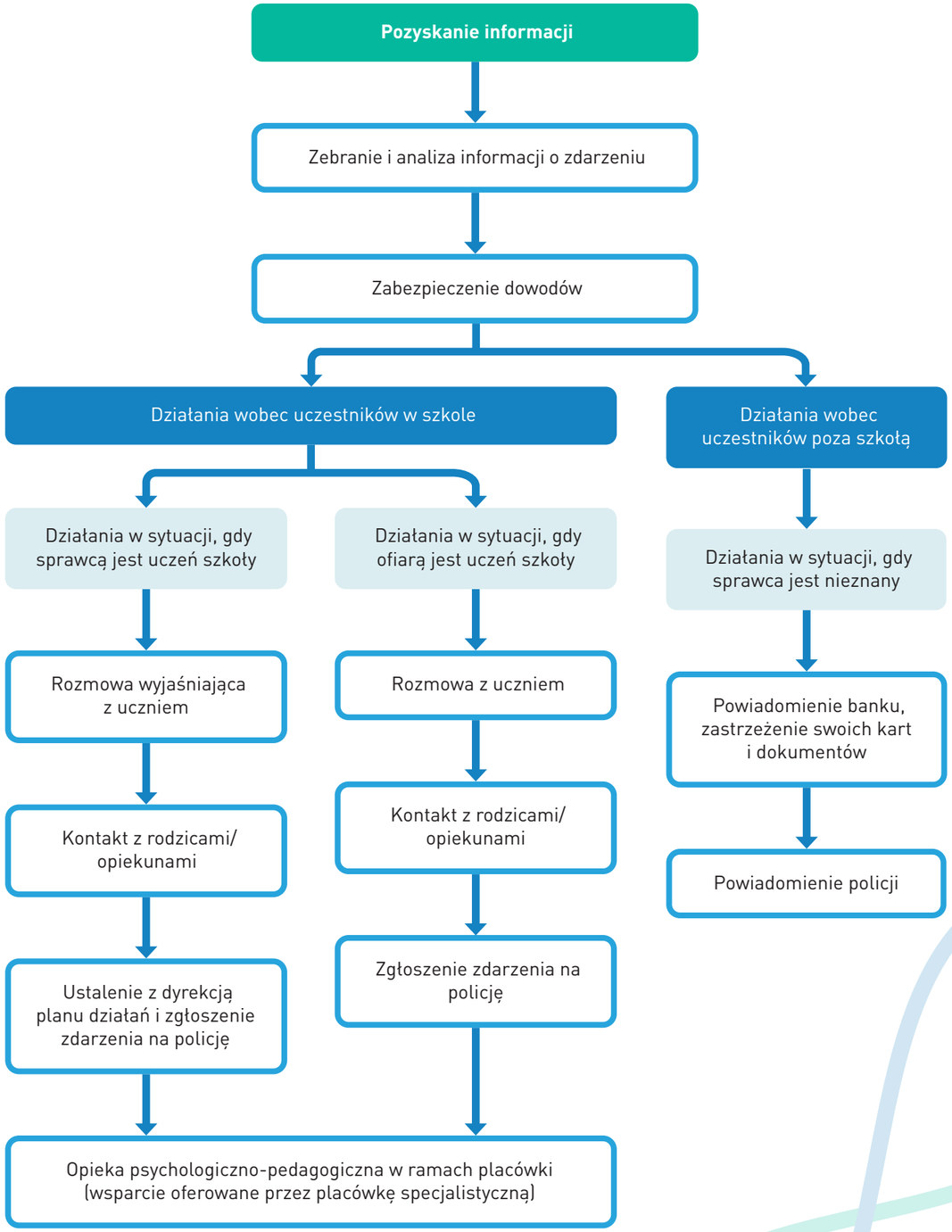
Przepisy prawa

Art. 190a § 2 Kodeksu karnego

Porady

- W przypadku wątpliwości, czy twoje prawa zostały naruszone, skontaktuj się z adwokatem lub radcą prawnym.
- Nie ignoruj naruszania swoich praw. Działaj, gdy dochodzi do ich naruszenia.
- Nie podawaj swoich danych osobowych w internecie lub osobom trzecim.
- Kontroluj swoje konta bankowe i ustal limity na transakcje.
- Osoby pełnoletnie mogą skorzystać z usługi informacyjnej dotyczącej powiadamiania o zaciągniętych zobowiązaniach finansowych (uwaga: usługa płatna, oferowana przez Biuro Informacji Kredytowej).

Procedura reagowania w przypadku kradzieży tożsamości



WIZERUNEK W SIECI

Katarzyna Kujawa

Opis zjawiska

Żyjemy w czasach, w których rozwój technologiczny postępuje w bardzo szybkim tempie. Jeszcze 20 lat temu nie dokumentowaliśmy wszystkich wydarzeń za pomocą aparatów fotograficznych wbudowanych w naszych telefonach. Obecnie każdego dnia miliony ludzi udostępniają swoje zdjęcia na portalach społecznościowych, takich jak Facebook, Instagram czy Snapchat. Jak możemy chronić własny wizerunek w sieci?

Wizerunek jest jednym z dóbr osobistych wymienionych w art. 23 Kodeksu cywilnego – obok zdrowia, wolności, czci, swobody sumienia, nazwiska lub pseudonimu, tajemnicy korespondencji, nietykalności mieszkania, twórczości naukowej, artystycznej, wynalazczej i racjonalizatorskiej. Wizerunek ma cechy prawa niezbywalnego, co znaczy, że nie można go komuś sprzedać czy pożyczyć. Podobnie jak inne dobra osobiste pozostaje pod ochroną prawa cywilnego, niezależnie od ochrony przewidzianej w innych przepisach.

Pojęcie wizerunku nie znalazło do tej pory swojej legalnej definicji w przepisach polskiego prawa. Przyjmuje się, że wizerunek to wytwór niematerialny, który za pomocą środków plastycznych przedstawia rozpoznawalną podobiznę danej osoby.

W praktyce wizerunek interpretuje się jako pewne dostrzegalne cechy człowieka tworzące jego wygląd i pozwalające na identyfikację osoby wśród ludzi; to obraz fizyczny, portret czy rozpoznawalna podobizna. Za wizerunek należy uznać także maskę artystyczną i karykaturę, o ile umożliwiają one odbiorcom identyfikację danej osoby.

Prawo do wizerunku odnosi się zarówno do osób fizycznych, jak i prawnych. W przypadku osób prawnych wizerunek pojmujemy jako symbolizujący ją znak.

Bezprawne działania mogą doprowadzić do naruszenia wizerunku, co będzie miało szczególnie dotkliwe skutki, jeżeli nastąpi ono za pośrednictwem internetu. W przypadku naruszenia dobra osobistego można korzystać z katalogu praw opisanych w art. 24 i 448 Kodeksu cywilnego, tj. żądać zaniechania działania naruszającego dobra poszkodowanego oraz podjęcia czynności potrzebnych do usunięcia skutków naruszenia (np. złożenia oświadczenia o odpowiedniej treści). Można domagać się również zapłaty zadośćuczynienia pieniężnego.

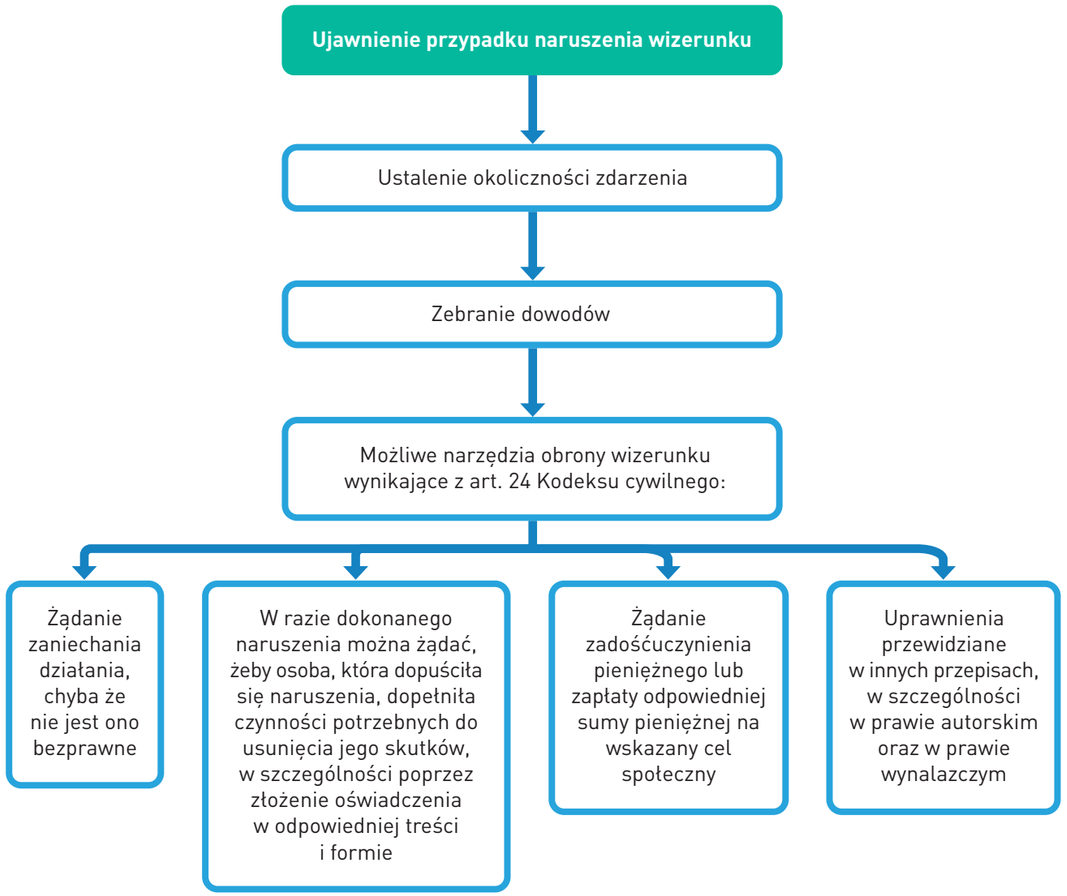
Przepisy prawa

Art. 23, 24 i 448 Kodeksu cywilnego

Porady

- W przypadku wątpliwości, czy twoje prawa zostały naruszone, skontaktuj się z adwokatem lub radcą prawnym.
- Nie ignoruj naruszania swoich praw. Działaj, gdy dochodzi do ich naruszenia.
- Pamiętaj, że nierozważne udostępnianie swojego wizerunku może spowodować problemy zarówno w życiu zawodowym, jak i osobistym.

Procedura reagowania na naruszenie wizerunku



PRAWO DO BYCIA ZAPOMNIANYM

Katarzyna Kujawa

Opis zjawiska

W internecie bardzo często podajemy nasze dane osobowe: czy to rejestrując swój udział w konferencji, czy robiąc zakupy w e-sklepie, czy zakładając konto na portalu społecznościowym. A co w sytuacji, kiedy chcemy, żeby internet o nas zapomniał? Czy to w ogóle możliwe?

Prawo do zapomnienia to jedna z gwarancji prawa do prywatności. Powodem jego wprowadzenia jest zapewnienie użytkownikom sieci skutecznego prawa do bycia zapomnianym w internecie. Osoby fizyczne mają prawo do usunięcia swoich danych, jeśli wycofają zgodę i nie ma innych zasadnych podstaw do zachowania tych danych.

Z prawem do bycia zapomnianym wiąże się wyrok w sprawie Google'a z maja 2014 r. Trybunał Sprawiedliwości Unii Europejskiej stanął w tej sprawie na stanowisku, że osoba, której dane dotyczą, jest uprawniona do żądania od operatora wyszukiwarki internetowej, aby ten zablokował możliwość wyszukiwania określonych informacji dotyczących tej osoby.

Prawo do bycia zapomnianym składa się z dwóch uprawnień:

- możliwości żądania usunięcia danych osobowych przez administratora danych;
- możliwości żądania, aby administrator danych poinformował innych administratorów danych, którym upublicznił dane osobowe, że osoba, której dane dotyczą, żąda, by administratorzy ci usunęli wszelkie łącza do tych danych osobowych, a także ich kopie lub replikacje.

W ramach prawa do usuwania danych osoba, której dane dotyczą, może żądać usunięcia swoich danych osobowych, jeżeli nie są one już niezbędne do celów, w których zostały zebrane, lub nie muszą być przetwarzane w inny sposób. Dodatkowo jeżeli osoba, której dane dotyczą, wycofała zgodę na przetwarzanie danych osobowych i nie istnieje inna podstawa ich przetwarzania – tzn. zgoda stanowiła jedyną podstawę przetwarzania danych – może ona żądać usunięcia swoich danych osobowych.

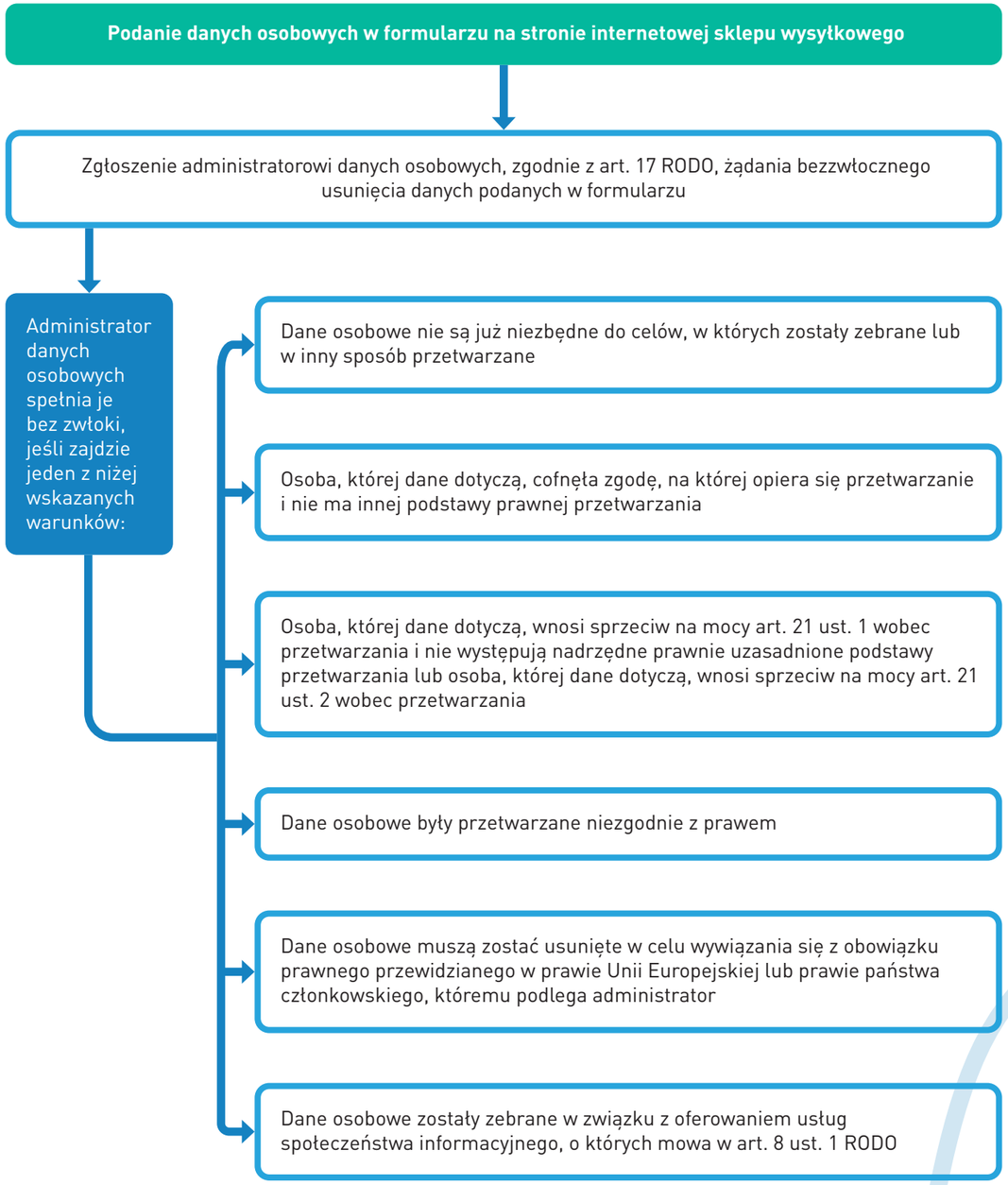
Przepisy prawa

Art. 17 ogólnego rozporządzenia o ochronie danych osobowych (RODO)

Porady

- Rozważnie udostępniaj swoje dane osobowe w internecie. Zarówno w świecie realnym, jak i wirtualnym są oszuści, którzy mogą je wykorzystać.
- W przypadku wątpliwości, czy twoje prawa zostały naruszone, skontaktuj się z adwokatem lub radcą prawnym.
- Nie ignoruj naruszania swoich praw. Działaj, gdy dochodzi do ich naruszenia.

Procedura realizacji prawa do zapomnienia



HEJT

Agnieszka Wrońska

Opis zjawiska

Określenia hejt i mowa nienawiści pochodzą od angielskich słów „hate" (nienawidzić) i „hate speech". Hejtem określa się negatywne i agresywne komentarze w sieci, oczerniające osobę o odmiennym zdaniu; to także wrogie odnoszenie się do jakichś tematów lub osób oraz obraźliwe memy, grafiki i filmy.

Obiektem ataku może stać się każdy, najczęściej jednak jego ofiarą padają osoby publiczne. Treści publikowane przez hejterów nie mają żadnej wartości – ich celem jest jedynie sprawianie przykrości. Najczęściej nie istnieją relacje osobiste pomiędzy osobą hejtowaną a hejterem oraz innymi hejterami. Przyczynami mowy nienawiści często są przykre doświadczenia sprawcy, zazdrość, a także chęć udowodnienia czegoś sobie i innym. Bywa też, że atakowanie innych sprawia hejterowi przyjemność. Hejt zwiększa moc swojego działania wraz z kolejnymi przyłączającymi się do niego osobami. Młodzi ludzie często ze świadków zamieniają się w sprawców i te właśnie role najczęściej odgrywają w przypadku przemocy w internecie.

Konsekwencje hejtu odczuwa głównie jego ofiara. Takie napiętnowanie skutecznie obniża jej poczucie wartości, a czasami może prowadzić do problemów zdrowotnych. Ofiara żyje w stresie, może cierpieć na bezsenność, nerwicę, depresję, a nawet podejmować próby samobójcze.

Skala zjawiska

- 14% badanych twierdzi, że często sugeruje się internetowymi opiniami, a ponad 60% młodych Polaków przyznaje, że zmieniło swoje zdanie pod wpływem negatywnych komentarzy w internecie.
- Dla 10% respondentów pisanie obraźliwych komentarzy jest formą rozrywki.
- Według 66% badanych hejt jest sposobem na wyrażenie własnej opinii (Global Dignity, 2016).

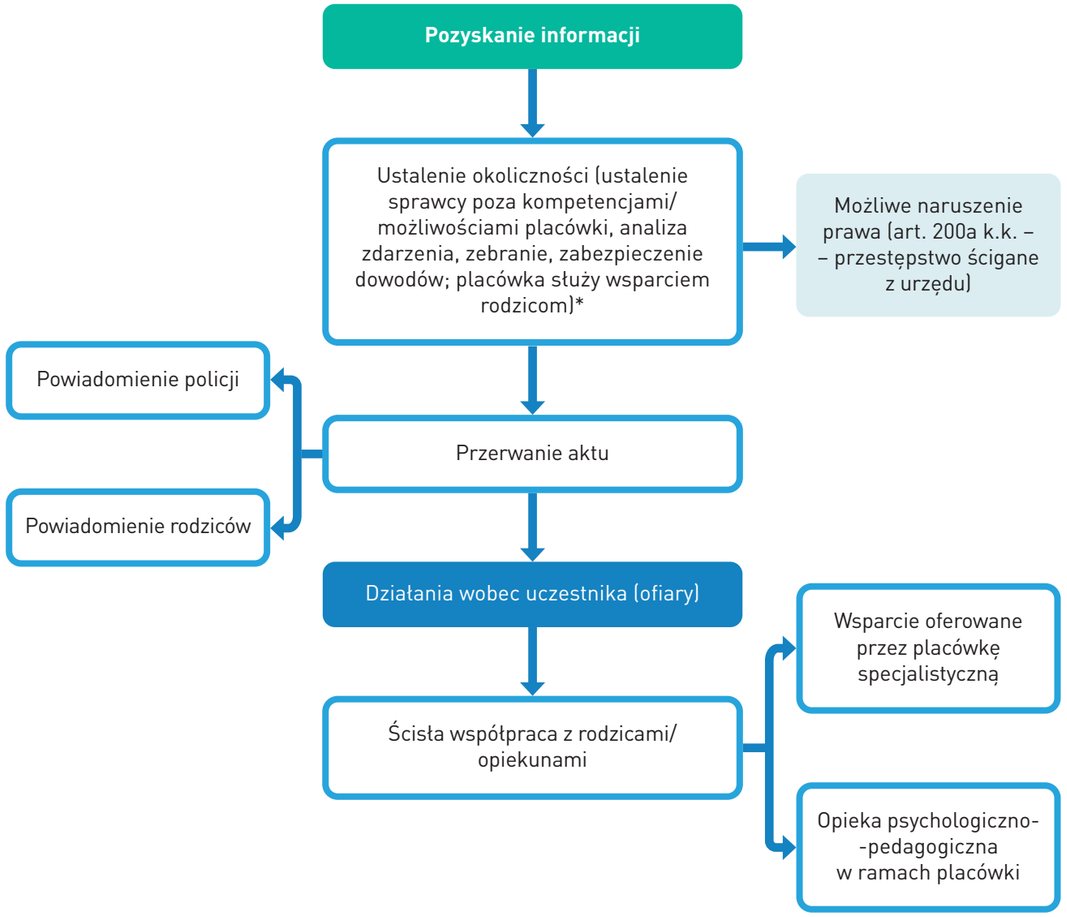
Przepisy prawa

Hejterzy nie są bezkarni. Penalizacji podlega naruszenie czci, dóbr osobistych w sieci: znieważenie, zniesławienie, naruszenie wizerunku (art. 23 i 24 Kodeksu cywilnego oraz art. 212 i 216 Kodeksu karnego), używanie wulgaryzmów w celu lekceważenia bądź obrażenia drugiej osoby albo grupy ludzi (art. 141 Kodeksu wykroczeń) oraz uporczywe, złośliwe nękanie kogoś przy użyciu m.in. narzędzi dostępnych w internecie (art. 190a Kodeksu karnego i art. 107 Kodeksu wykroczeń).

Porady

- Rozmawiaj o zjawisku hejtu – tłumacz, jak się przejawia, jakie są jego konsekwencje. Podpowiadaj, co można zrobić, jeżeli jest się ofiarą lub świadkiem mowy nienawiści w internecie.
- Obserwuj zachowanie dziecka – ofiary hejtu, otocz je specjalistyczną opieką psychologiczną.
- Zabezpiecz dowody (zapisy rozmów na portalach społecznościowych, SMS-y, MMS-y, zrzuty ekranów, zdjęcia, e-maile).
- Zgłoś problem do administratora strony internetowej w celu usunięcia lub zablokowania obraźliwych wpisów.
- Złóż wniosek o popełnienie wykroczenia, wniosek o ściganie na policję lub do prokuratury. Możesz złożyć pozew cywilny o odszkodowanie.

Procedura reagowania wobec hejtu



* W całym procesie bardzo ważna jest współpraca z policją, sądem rodzinnym, rodzicami, opiekunami prawnymi.

CYBERSTALKING

Kinga Kaczmarek

Opis zjawiska

Cyberstalking jest odmianą tradycyjnego stalkingu polegającą na nękaniu drugiej osoby w internecie. Termin powstał z połączenia słów „cyberprzemoc" i „stalking". Cyberstalking może mieć swoje źródło zarówno w wirtualnym, jak i rzeczywistym życiu.

Cyberstalkingiem określamy zachowania takie jak: cyberdręczenie, śledzenie, kradzież tożsamości, nielegalny monitoring, elektroniczne inwigilowanie wybranej osoby, rozpowszechnianie jej danych wrażliwych (np. numeru telefonu, adresu zamieszkania czy prywatnych zdjęć – ang. outing), rozsyłanie w jej imieniu – ale wbrew woli – wiadomości do innych osób, wysyłanie do niej prezentów czy też zbieranie informacji dotyczących jej życia. Często sytuacjom tym towarzyszą fałszywe oskarżenia (ang. denigration), agresywne zachowanie, groźby i szantaż. Nękanie może dotyczyć jednej lub wielu osób, mniejszości, instytucji bądź przedstawicieli organizacji.

W wielu przypadkach stalkerem zostaje były partner ofiary, jednak może to być również osoba nieznajoma. Stalker w swoich działaniach używa m.in. serwisów społecznościowych i komunikatorów. Jego zachowania wywołują u ofiary nieprzyjemne uczucia: strach, panikę, wstyd i poczucie winy.

Warto zastanowić się, jakie dane udostępniamy w sieci. Szczególną ostrożność należy zachować przy wysyłaniu innym swoich zdjęć, które mogą być podstawą do tworzenia różnego typu przeróbek graficznych i memów. Niejednokrotnie publikacja prywatnego zdjęcia ma przykre i długotrwałe konsekwencje dla ofiary. Wykluczenie czy wyśmiewanie spowodowane działaniami stalkera mogą odcisnąć w psychice poszkodowanego piętno na całe życie.

Skala zjawiska

- 39,5% uczniów spotkało się ze zjawiskiem cyberprzemocy (NIK, 2017).
- 33% nastolatków zadeklarowało, że było zaangażowanych w cyberprzemoc jako sprawca lub ofiara (Pyżalski, 2012).
- 48,8% uczniów nie zwróciłoby się do nikogo o pomoc w sytuacji cyberprzemocy – jedynie 13,3% z nich zgłosiłoby się do nauczyciela (NIK, 2017).
- 33,3% nastolatków zadeklarowało rozpowszechnianie kompromitujących informacji o swoich znajomych, a 24,4% przyznało się do szantażowania za pośrednictwem sieci („Nastolatki 3.0", 2016).

Przepisy prawa

Cyberprzemoc i stalking są w Polsce przestępstwem i zgodnie z art. 190a Kodeksu karnego podlegają karze pozbawienia wolności.

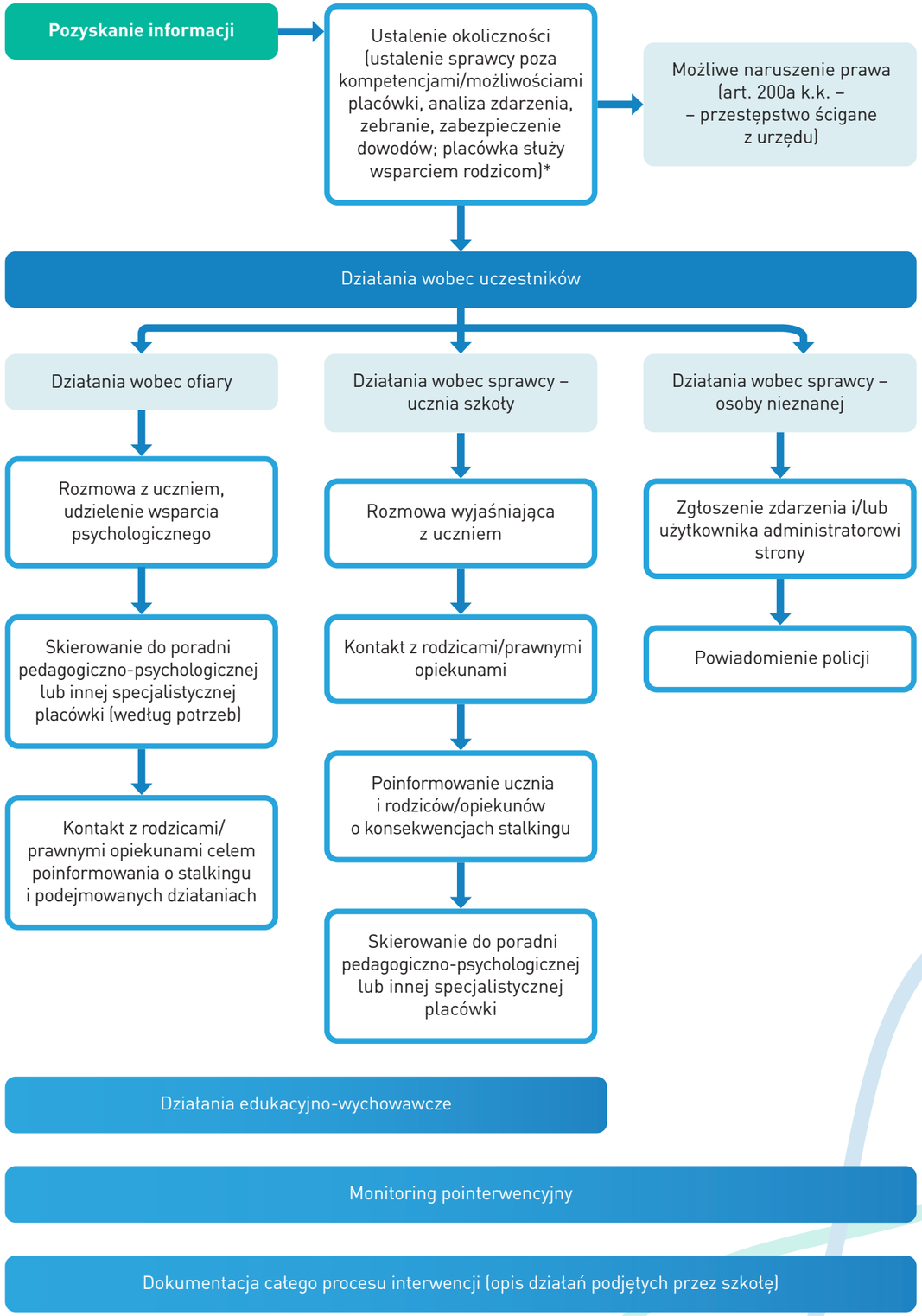
Na wniosek osoby pokrzywdzonej stalker zostaje ścigany i/lub sąd może orzec o zakazie zbliżania się.

Porady

Co zrobić, gdy twój uczeń padnie ofiarą cyberstalkingu?

- Poinformuj ucznia, aby nie utrzymywał kontaktu z cyberstalkerem i nie odpisywał na wiadomości.
- Zapisz i zachowaj wszystkie informacje i wiadomości od stalkera, które mogą stanowić dowód w sprawie.
- Zawiadom policję i przedstaw zebrane dowody.

Procedura reagowania wobec cyberstalkingu dzieci



UWODZENIE DZIECI W INTERNECIE (GROOMING)

Agnieszka Wrońska

Opis zjawiska

Uwodzenie dzieci w internecie (ang. child grooming) polega na wytworzeniu niebezpiecznej relacji między osobą dorosłą a małoletnią (poniżej 15 r.ż.). Działania podejmowane przez sprawcę są nastawione na zaprzyjaźnienie się i nawiązanie więzi emocjonalnej z dzieckiem w celu zdobycia jego zaufania, zmniejszenia oporu, nakłonienia do czynności o charakterze seksualnym.

Osoby o pedofilskich skłonnościach najchętniej wybierają dzieci samotne, z niskim poczuciem własnej wartości. Sprawcy podejmują różnego typu działania izolujące ofiary od najbliższego otoczenia, stosują manipulacje, szantaż czy naciski emocjonalne. Uwiedzenie ułatwia również brak odpowiedniej opieki ze strony dorosłych opiekunów.

Uwodzenie w internecie może przybierać różne formy: od szybkiej i jednorazowej seksualizującej reakcji na opublikowane zdjęcie małoletniego, do długotrwałego procesu, prowadzącego do wykorzystania seksualnego w świecie realnym. Wszystkie są szkodliwe i prowadzą do nadużyć wobec dziecka.

Skala zjawiska

- Co dwudzieste dziecko (5%) było namawiane do zachowań o charakterze seksualnym przez osobę poznaną w internecie (FDDS, 2017).
- 12% chłopców i 9% dziewcząt w wieku 13–15 lat oraz 24% chłopców i 23% dziewcząt w wieku 15–17 lat otrzymało przez internet wiadomości związane z seksem.
- Jedna czwarta nastolatków przyznaje, że zdarzyło im się spotkać z dorosłym poznanym w sieci: 39% z nich poinformowało o tym rodziców, a 29% – nikogo („Nastolatki 3.0", 2016).
- Z uwagi na specyficzną materię większości przestępstw na tle uwodzenia nieletnich nie udaje się ujawnić. Statystyki policyjne wskazują, że rocznie wszczyna się blisko 600 postępowań w takich sprawach, co prawdopodobnie stanowi wycinek realnej skali problemu.

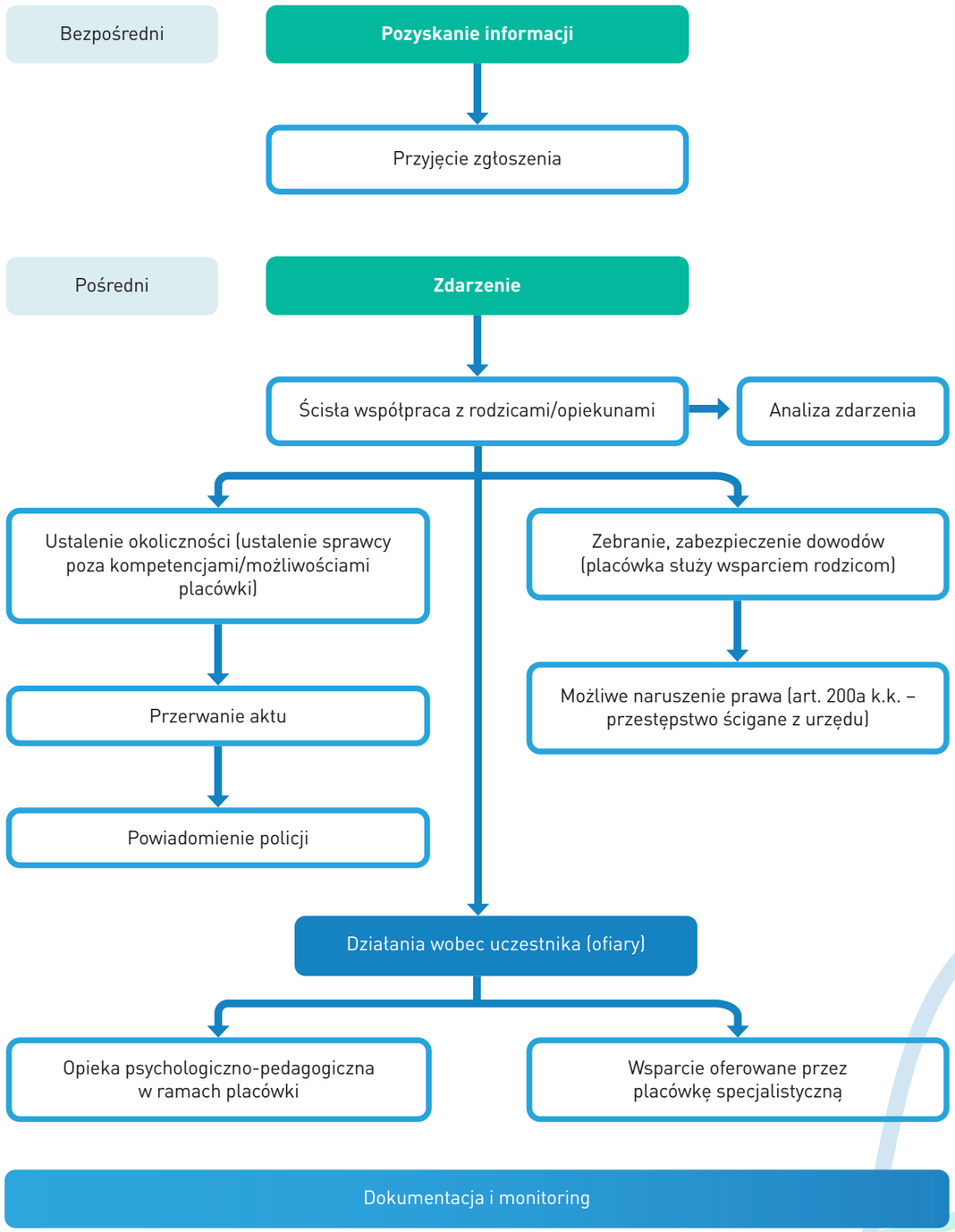
Przepisy prawa

Uwodzenie dzieci w internecie jest przestępstwem uregulowanym w Kodeksie karnym (art. 200, 200a § 1 i 2, art. 286 § 1). Chroni on osoby małoletnie przed nawiązywaniem kontaktu z osobami, które mają na celu obcowanie płciowe lub poddanie się innej czynności seksualnej. Ponadto prawnie zabronione jest produkowanie i utrwalanie treści pornograficznych, a także samo składanie propozycji seksualnych.

Porady

- Rozmawiaj o problemie uwodzenia w sieci, wyjaśniaj metody działania osób o złych zamiarach.
- Obserwuj zachowanie dziecka, w przypadku uwiedzenia bądź próby uwiedzenia otocz je specjalistyczną opieką psychologiczną.
- Zabezpiecz dowody uwiedzenia (zapisy rozmów na portalach społecznościowych, SMS-y, MMS-y, zrzuty ekranów, zdjęcia, e-maile).
- Zgłoś problem, skonsultuj się z ekspertem. Gdy dochodzi do naruszenia prawa – szczególnie w przypadku uwiedzenia dziecka do lat 15 – obowiązkiem szkoły jest powiadomienie policji lub sądu rodzinnego.

Procedura reagowania na uwodzenie dzieci w internecie



BUSINESS E-MAIL COMPROMISE – OSZUSTWO „NA PREZESA”

Marek Sowala

Opis zjawiska

Oszustwo „na prezesa”, czyli Business E-mail Compromise (BEC), jest rodzajem ataku opartego na phishingu (szczegółowo phishing został opisany w poprzedniej części poradnika). To ukierunkowany atak, którego sprawcy wysyłają wiadomości podobne do typowych komunikatów biznesowych. Celem BEC są zwykle środki finansowe lub informacje będące tajemnicą organizacji. Poszkodowanymi bywają najczęściej małe i średnie przedsiębiorstwa, organizacje rządowe i samorządowe, ale znane są przypadki, gdy ofiarą oszustwa padały bardzo duże organizacje.

Od zwykłego phishingu BEC różni się przede wszystkim tym, że przestępcy nie kierują spreparowanych wiadomości do wielu adresatów, lecz do ściśle wytypowanej ofiary. Wcześniej starają się zebrać o niej możliwie wiele informacji, aby stworzyć jak najbardziej wiarygodny komunikat. Wykrycie oszustwa jest bardzo trudne ze względu na brak szkodliwego oprogramowania w załączniku wiadomości czy podejrzanych linków w treści. Wiadomość wysyłana jest z adresu bardzo podobnego do znanego osobie atakowanej, czasami wręcz zdarza się, że e-mail wychodzi z prawdziwej skrzynki mailowej, do której udało się włamać przestępcom.

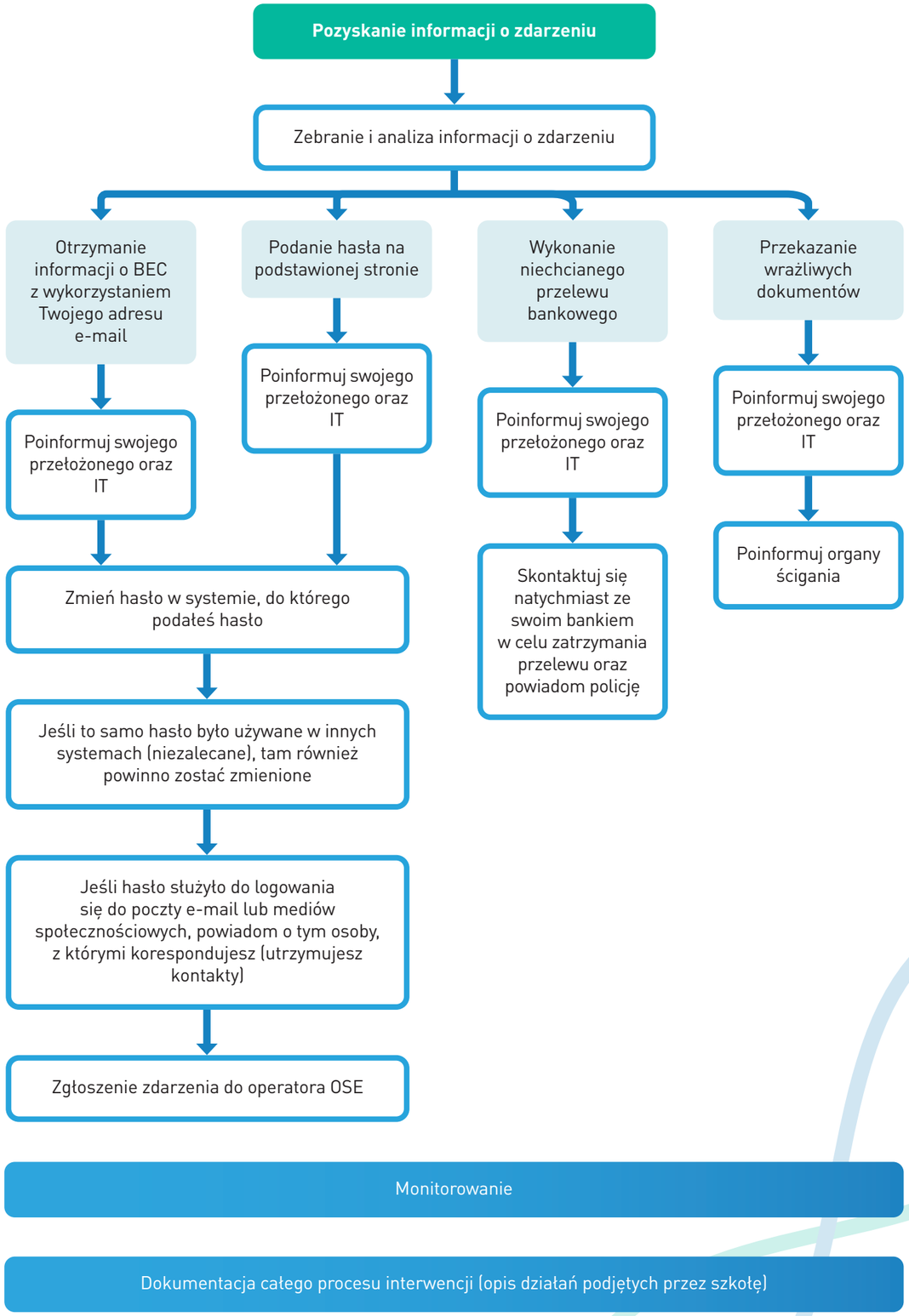
Atak BEC przebiega według scenariusza o kilku charakterystycznych cechach. Cyberprzestępca na podstawie informacji dostępnych w internecie wyszukuje ofiarę oraz osoby, z którymi ta komunikuje się w pracy. Na podstawie tych danych sprawca tworzy wiadomość mailową naśladującą korespondencję, która mogłaby w rzeczywistości pojawić się podczas komunikacji ze współpracownikami. Zazwyczaj e-mail ma nakłonić ofiarę ataku do podjęcia natychmiastowych działań, takich jak dokonanie płatności za fakturę, zmiana danych odbiorcy przelewu czy przesłanie wrażliwych dokumentów.

Porady

Tak jak w przypadku phishingu, zdrowy rozsądek jest podstawową linią obrony. Jeśli e-mail wydaje się podejrzany lub jego treść wskazuje na coś nieprawdopodobnego – może to być próba oszustwa.

- Upewnij się, że pracownicy są świadomi istnienia tego rodzaju oszustw, jeśli nie – przeprowadź szkolenie.
- Jeśli zamierzasz odpowiedzieć na prośbę otrzymaną w e-mailu, pamiętaj:
  - nie odpowiadaj bezpośrednio na otrzymaną wiadomość;
  - nie korzystaj z numerów telefonów ani innych danych kontaktowych podanych w wiadomości, sprawdź te dane w umowie lub zamówieniu.
- Sprawdzaj dokładnie adresy e-mail, w razie wątpliwości skonsultuj się z pracownikiem IT.
- Wprowadź dwuetapowy proces weryfikacji, obejmujący sprawdzenie płatności inną drogą niż e-mail.
- Sprawdź numer rachunku na białej liście podatników VAT w celu potwierdzenia, czy rachunek rzeczywiście należy do Twojego kontrahenta.

Procedura reagowania na incydenty związane z BEC



SKIMMING

Michał Łuciuk

Opis zjawiska

Skimming to przestępstwo polegające na kradzieży danych z paska magnetycznego karty płatniczej w celu wykonania jej nielegalnej kopii. Docelowo takie działanie służyć ma realizowaniu płatności lub wypłatom gotówki z bankomatów bez wiedzy posiadacza karty. Jest to jedno z najpopularniejszych przestępstw dotyczących bankowości elektronicznej. Sprawcy przy pomocy tzw. skimmera – specjalnego urządzenia kopiującego umieszczanego w bankomacie – są w stanie przechwycić informacje zawarte na karcie. Towarzysząca urządzeniu kopiującemu mikrokamera lub specjalna nakładka na klawiaturę pozwalają ponadto rejestrować PIN wprowadzany przez użytkownika.

Rzadszy jest skimming podczas bezpośredniego kontaktu, polegający na skopiowaniu danych z karty przez osobę, która chwilowo weszła w jej posiadanie. Ofiarą można zostać np. w placówce handlowej lub usługowej, restauracji, kinie czy teatrze. W tym przypadku barierą zmniejszającą popularność tej metody wśród przestępców jest konieczność zdobycia PIN-u, który wpisywany jest na klawiaturze terminalu przez użytkownika.

Przyjęto, że skimming dotyczy najczęściej kart z paskiem magnetycznym. Te wyposażone w chip powszechnie uchodzą za bezpieczniejsze. Jednak od kilku lat co jakiś czas do mediów przedostają się informacje o próbie obejścia również tego zabezpieczenia. Urządzenie mające służyć do kopiowania danych z kart wyposażonych w chip zostało określone jako shimmer.

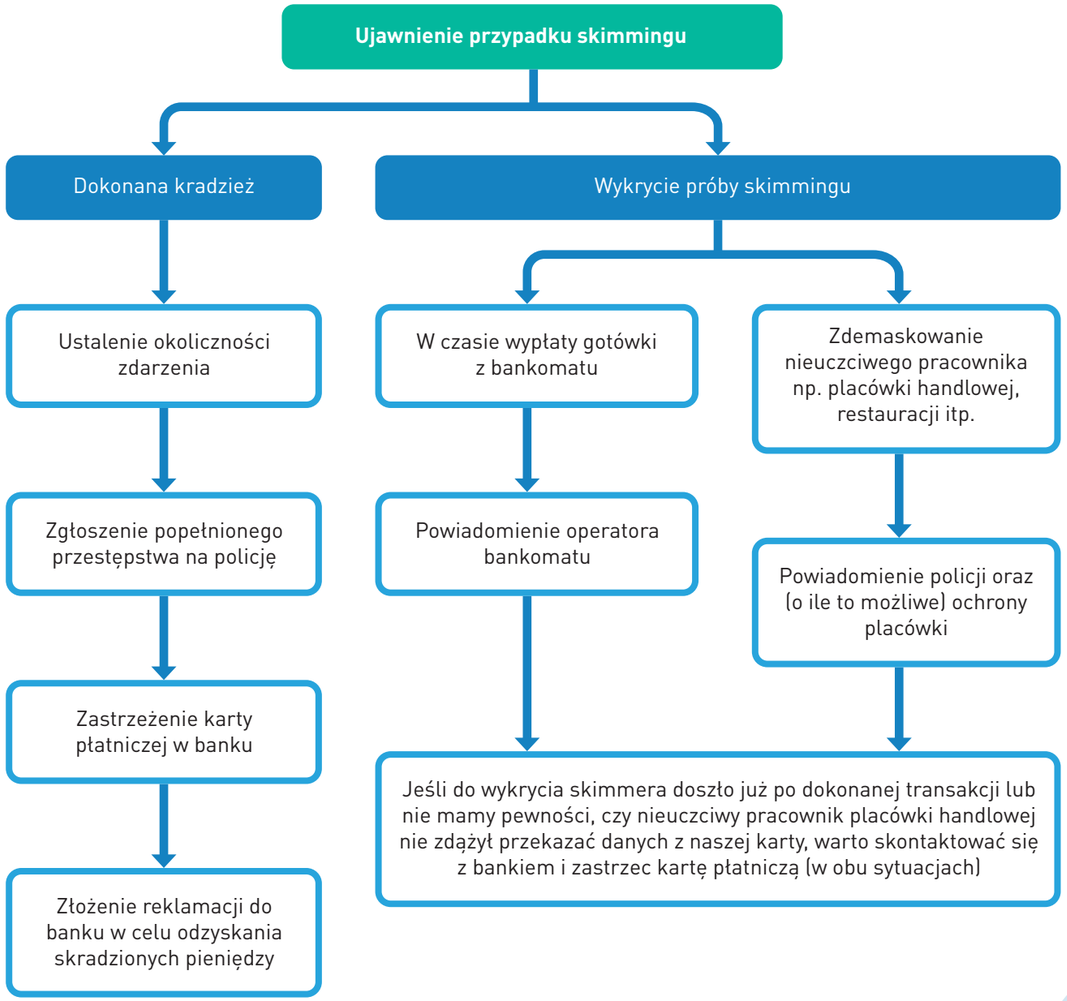
Przepisy prawa

Kara, jaka przewidziana została za podrabianie karty płatniczej, określonej w Kodeksie karnym jako „inny środek płatniczy", to od 5 do 25 lat pozbawienia wolności (art. 310 § 1 Kodeksu karnego).

Porady

- Przed włożeniem karty do bankomatu upewnij się, że żaden z jego elementów nie budzi wątpliwości. Zrezygnuj z wypłaty gotówki z podejrzanego bankomatu, a zaistniałą sytuację zgłoś do operatora sieci bankomatów.
- Obecnie karty płatnicze wyposażone są także w moduł zbliżeniowy, który również pozwala na wypłatę gotówki z bankomatu. Jest to skuteczna alternatywa dla tradycyjnej metody. Banki udostępniają też inne narzędzia umożliwiające wypłaty, jednak powinieneś zwrócić uwagę, czy skorzystanie z nich nie wiąże się z dodatkowymi opłatami.
- Karta przekazana pracownikowi danej placówki, w której dokonujesz płatności, powinna bez przerwy znajdować się w zasięgu twojego wzroku. Powinieneś uczestniczyć w przebiegu transakcji od momentu jej rozpoczęcia, aż do jej zakończenia.
- Wpisywany PIN (zarówno w bankomacie, jak i placówce handlowej) zasłoń, np. drugą ręką, chroniąc go przed ewentualnym zarejestrowaniem przez nieuczciwego pracownika lub kamerę, w którą może być wyposażony bankomatowy skimmer.

Procedura reagowania w przypadku skimmingu



BEZPIECZNE UŻYTKOWANIE URZĄDZEŃ MOBILNYCH

Marek Sowala

Opis zjawiska

Urządzenia mobilne stały się nieodłączną częścią naszego życia. Smartfony i tablety, dzięki powszechnej dostępności niezliczonej wręcz ilości aplikacji, które możemy na nich zainstalować, stają się czymś więcej niż tylko urządzeniami do wykonywania połączeń telefonicznych. Pozwalają nam na nieograniczony dostęp do informacji, umożliwiają kontakty z ludźmi na całym świecie, rozrywkę, zabawę, a także naukę i pracę.

Ponieważ urządzenia mobilne nieodłącznie nam towarzyszą, można powiedzieć, że wiedzą o nas bardzo dużo. W ich pamięci przechowujemy wiele informacji, w tym te najbardziej prywatne – jak zdjęcia, kontakty, SMS-y, e-maile. Często też za ich pomocą wykonujemy operacje finansowe (zakupy, przelewy) czy korzystamy z bardzo wygodnego dostępu do swojego konta w banku. W związku z tym musimy pamiętać, jak ważne jest zadbanie o bezpieczeństwo smartfona i przechowywanych w nim danych.

Porady

- Miej kontrolę nad swoim urządzeniem, nie zostawiaj go bez opieki. Warto rozważyć uruchomienie funkcji typu „znajdź mój telefon". W przypadku utraty sprzętu pozwoli ona go zlokalizować, wyświetlić odpowiedni komunikat dla znalazcy, zablokować urządzenie i ostatecznie usunąć dane z jego pamięci.
- Dostęp do telefonu zabezpiecz co najmniej 6-znakowym PIN-em, a jeśli urządzenie wykorzystuje zabezpieczenia biometryczne (np. skan palca) – zastosuj je. Takie rozwiązanie zapewnia wyższy poziom zabezpieczeń przed nieuprawnionym dostępem niż PIN czy wzór blokady ekranu.
- Dbaj o aktualizacje oprogramowania systemowego. Najlepiej jest włączyć w ustawieniach systemowych funkcję automatycznego sprawdzania dostępnych aktualizacji i powiadamiania o nich.
- Instaluj aplikacje mobilne tylko z zaufanych źródeł (Android – Google Play, Apple – App Store). Unikaj instalowania aplikacji, które są zupełnie nowe i zostały pobrane przez niewiele osób lub mają bardzo mało pozytywnych komentarzy.
- Instaluj tylko te aplikacje, których potrzebujesz i z których naprawdę będziesz korzystać. Kiedy jakaś aplikacja przestanie być potrzebna, odinstaluj ją. Aplikacje mobilne, podobnie jak oprogramowanie systemowe, muszą być na bieżąco aktualizowane.
- Zapewnij dodatkową ochronę dla ważnych danych na urządzeniu w postaci backupu, np. w chmurowej usłudze przechowywania plików.
- Zachowaj rozwagę podczas korzystania z internetu. Pamiętaj o zagrożeniach związanych z phishingiem. twoje dane mogą być cenne nie tylko dla ciebie.

Zasady bezpiecznego korzystania z urządzeń mobilnych

Pilnuj swojego telefonu i nigdy nie zostawiaj go bez opieki

Stosuj kod PIN lub zabezpieczenia biometryczne

Aktualizuj oprogramowanie systemowe

Pobieraj aplikacje tylko z zaufanych źródeł

Instaluj tylko naprawdę potrzebne aplikacje

Zapewnij backup danych

Rozważnie korzystaj z internetu

Stosuj powyższe zasady, a unikniesz trudnych sytuacji

USŁUGI BEZPIECZEŃSTWA OSE

NASK dostarcza usługę bezpieczeństwa, która ma na celu zapewnienie ochrony szerokopasmowego dostępu do internetu przed szkodliwym oprogramowaniem oraz monitorowanie zagrożeń i bezpieczeństwa sieciowego. Ponadto NASK zapewnia wsparcie szkole w podejmowaniu działań zabezpieczających uczniów przed dostępem do treści, które mogą stanowić zagrożenie dla ich prawidłowego rozwoju. NASK, w ramach programu OSE, udostępnia usługę ochrony użytkownika w sieci. Szkoły otrzymują automatyczną ochronę przed treściami nielegalnymi, których prezentacja i dystrybucja jest zabroniona i podlega karze, zgodnie z przepisami Kodeksu karnego i ustaw właściwych, oraz innymi treściami szkodliwymi dla dzieci.

Usługi bezpieczeństwa OSE – korzyści dla szkoły

- Spełnienie wymagań art. 27 ustawy z dnia 14 grudnia 2016 r. – Prawo oświatowe, która nakłada na szkoły i placówki zapewniające dostęp do internetu obowiązek podejmowania działań zabezpieczających uczniów przed dostępem do treści, które mogą stanowić zagrożenie dla ich prawidłowego rozwoju. W szczególności szkoły obowiązane są zainstalować i aktualizować oprogramowanie zabezpieczające.
- Możliwość bezpłatnego korzystania z systemów bezpieczeństwa na najwyższym światowym poziomie, dotychczas dostępnych tylko dla instytucji dysponujących bardzo dużymi budżetami IT.
- Możliwość znaczącego ograniczenia wydatków przez szkoły na oprogramowanie zabezpieczające dostęp szkoły do internetu.
- Całość systemów zlokalizowana jest w centrach przetwarzania danych NASK i zarządzana przez personel operatora OSE, dzięki czemu szkoły nie muszą zatrudniać wykwalifikowanej kadry IT.
- Brak problemów z samodzielną instalacją i aktualizacją oprogramowania zabezpieczającego.

Uruchomienie przez szkołę usług bezpieczeństwa OSE oznacza, że:

- NASK zapewnia ochronę przed szkodliwym oprogramowaniem na poziomie sieci OSE. System mający na celu monitorowanie, wykrywanie i usuwanie znanych wirusów komputerowych działa w następujących procesach: korzystanie z poczty elektronicznej (sprawdzeniu podlegają wyłącznie załączniki), przeglądanie stron internetowych, pobieranie plików z internetu.
- NASK zapewnia ochronę na poziomie sieci przed zaawansowanymi atakami sieciowymi kierowanymi na sieć OSE.
- Usługi bezpieczeństwa OSE nie obejmują działaniem sieci LAN w szkołach, a tylko komunikację sieci LAN z siecią internet.
- Strony zawierające treści nielegalne oraz szkodliwe są zablokowane i nie będą dostępne dla użytkowników sieci OSE.
- NASK udostępnia dyrektorowi szkoły raporty dotyczące monitorowania zagrożeń i przypadków naruszeń bezpieczeństwa użytkowników OSE, zawierające dane o sposobie korzystania z internetu w szkole.
- NASK monitoruje zagrożenia i przypadki naruszeń bezpieczeństwa sieci wykryte przez systemy ochrony przed szkodliwym oprogramowaniem.
- Ze względów związanych z ochroną danych wrażliwych system ochrony przed szkodliwym oprogramowaniem nie będzie obejmować witryn z obszarów: bankowość i finanse, opieka zdrowotna oraz poczta elektroniczna.
- Zaawansowane funkcje bezpieczeństwa OSE wykonywane są na urządzeniach centralnych w sieci OSE. Do ich poprawnego działania wymagana jest inspekcja ruchu szyfrowanego SSL w celu analizy ruchu sieciowego przesyłanego w ramach komunikacji wymienianej z internetem. NASK udostępnia certyfikaty SSL, umożliwiające inspekcję ruchu szyfrowanego, które szkoła korzystająca z usługi bezpieczeństwa jest zobowiązana zainstalować na wszystkich komputerach oraz urządzeniach komputerowych (tablety, smartfony, laptopy).
- Z powodów niezależnych od NASK pewna część aplikacji sieciowych (głównie mobilnych, czyli instalowanych na urządzeniach takich jak tablety i smartfony) może nie działać poprawnie lub nie działać w ogóle.

mLEGITYMACJA SZKOLNA

Czym jest i dla kogo jest przeznaczona?

mLegitymacja to szkolna legitymacja dostępna na telefonie komórkowym. Może ją mieć każdy uczeń, któremu wcześniej została wydana tradycyjna wersja dokumentu oraz który wypełni odpowiedni wniosek i złoży go w swojej szkole (w przypadku ucznia niepełnoletniego wniosek wypełniają jego rodzice).

Korzystanie z tej nowoczesnej, bezpłatnej i w pełni bezpiecznej usługi nie jest trudne. Wystarczy zainstalować na smartfonie aplikację mObywatel, w ramach której dostępna będzie cyfrowa wersja tradycyjnej, papierowej legitymacji.

Po utracie ważności elektroniczna legitymacja jest automatycznie unieważniana. Szkoła ma również możliwość jej „ręcznego" unieważnienia lub zastrzeżenia – w przypadku nieprawidłowego działania mLegitymacji, a także uszkodzenia czy zgubienia telefonu, na którym była przechowywana.

mLegitymacje mogą wystawiać szkoły, które uruchomiły taką usługę. Wiąże się z tym podpisanie stosownego porozumienia z Ministerstwem Cyfryzacji. Usługę może uruchomić sam dyrektor lub wyznaczona przez niego osoba za pomocą formularza zgłoszeniowego dostępnego na ose.gov.pl/lista-szkol.

mLegitymacja szkolna – ważne informacje dla szkoły

- mLegitymacja zawiera wszystkie dane, które można znaleźć w jej papierowym odpowiedniku, tj.: imię i nazwisko ucznia, datę urodzenia, PESEL, adres zamieszkania, zdjęcie/wizerunek ucznia, numer legitymacji, datę wydania, termin ważności, nazwę i adres szkoły.
- Autentyczność mLegitymacji można sprawdzić za pomocą aplikacji mWeryfikator.
- mLegitymację można wydawać za pomocą systemu mDokumenty.

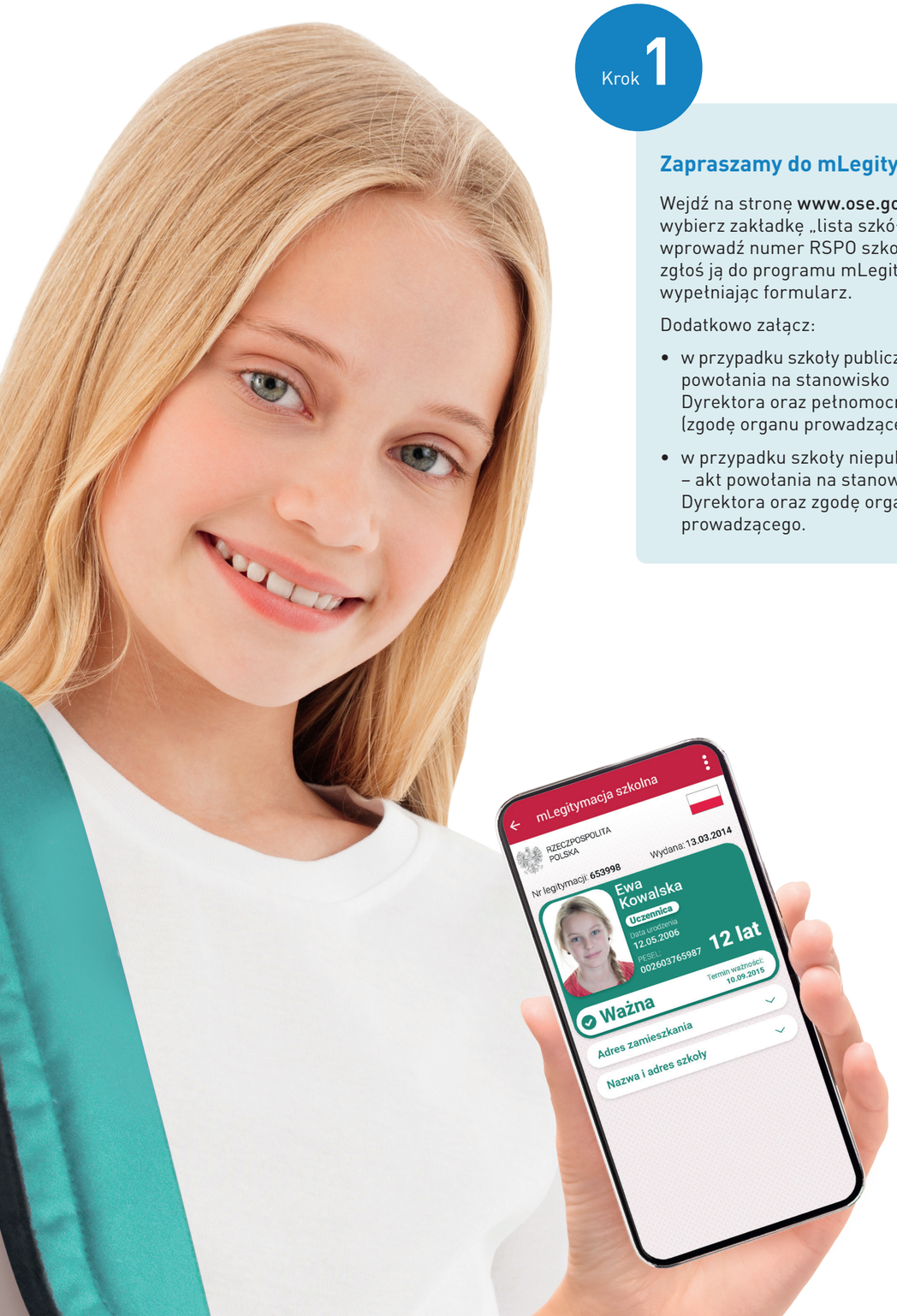
Porady

Co ważne, mLegitymacja ma taką samą moc prawną, jak jej tradycyjna wersja. Pozwala na korzystanie z ulg i zniżek na takich samych zasadach. Jej umocowanie prawne znajduje się w rozporządzeniu Ministra Edukacji Narodowej z dnia 27 sierpnia 2019 r. w sprawie świadectw, dyplomów państwowych i innych druków. Zapisano w nim:

„2. Szkoły, wydając legitymację szkolną albo e-legitymację szkolną, mogą wydać dodatkowo mLegitymację szkolną, stanowiącą dokument elektroniczny przechowywany i prezentowany przy użyciu oprogramowania przeznaczonego dla urządzeń mobilnych, o którym mowa w art. 19e ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz.U. z 2019 r. poz. 700, 730, 848 i 1590).

3. mLegitymacja szkolna jest wydawana na wniosek pełnoletniego ucznia lub rodziców niepełnoletniego ucznia".

Poniżej prezentujemy kroki, jakie należy podjąć, aby otrzymać mLegitymację.



Krok 1

Zapraszamy do mLegitymacji

Wejdź na stronę **www.ose.gov.pl**, wybierz zakładkę „lista szkół", wprowadź numer RSPO szkoły i zgłoś ją do programu mLegitymacji wypełniając formularz.

Dodatkowo załącz:

- w przypadku szkoły publicznej – akt powołania na stanowisko Dyrektora oraz pełnomocnictwo (zgodę organu prowadzącego);
- w przypadku szkoły niepublicznej – akt powołania na stanowisko Dyrektora oraz zgodę organu prowadzącego.

Krok 2

Formularz zgłoszeniowy

W formularzu zgłoszeniowym wskaż osoby niezbędne do efektywnego obsługiwania systemu mLegitymacji:

- **Dyrektor szkoły** – Dyrektor to osoba kluczowa dla mLegitymacji. Pamiętaj, aby podać unikalny adres e-mail Dyrektora szkoły. Na ten adres dostanie on link do założenia konta w portalu Moje OSE, gdzie będzie mógł pobrać porozumienie i formularz.
- **Osoby obsługujące system** – to osoby, które zostaną wyznaczone przez Dyrektora szkoły do obsługi panelu administracyjnego, upoważnione do wprowadzania danych uczniów w celu przygotowania mLegitymacji.

Dyrektor szkoły i osoby obsługujące system muszą posiadać profil zaufany.

Krok 3

Portal Moje OSE

Portal Moje OSE to narzędzie do zarządzania kontem Szkoły. Możliwość pobrania porozumienia i formularza zostanie udostępniona w portalu Moje OSE, na koncie Dyrektora. Po podpisaniu przez profil zaufany pobranych dokumentów należy je załączyć do portalu Moje OSE. Centrum Kontaktu zweryfikuje dokumenty. Następnie otrzymasz link do panelu administracyjnego, w którym wskazane osoby będą mogły przygotować mLegitymacje.

Krok 4

Szkoła w mLegitymacji

Witamy w mLegitymacji!

Centrum Kontaktu pozostaje do Twojej dyspozycji

tel.: **+ 48 42 25 35 484**

e-mail: **mlegitymacja@nask.pl**

BIBLIOGRAFIA

Fundacja Dajemy Dzieciom Siłę, (2019), „Patotreści w internecie – Raport o problemie", Warszawa: Fundacja Dajemy Dzieciom Siłę.

Global Dignity, (2016), „Wilki i owce w internecie, czyli raport na temat hejtu wśród młodzieży", Warszawa: Global Dignity Poland (pod patronatem Rzecznika Praw Dziecka).

Makaruk K., Włodarczyk J., Michalski P., (2017), „Kontakt dzieci i młodzieży z pornografią", Warszawa: Fundacja Dajemy Dzieciom Siłę.

Najwyższa Izba Kontroli, (2017), „Zapobieganie i przeciwdziałanie cyberprzemocy wśród dzieci i młodzieży", Warszawa: Najwyższa Izba Kontroli.

NASK Państwowy Instytut Badawczy, (2016), „Nastolatki 3.0. Wybrane wyniki ogólnopolskiego badania dzieci w szkołach", Warszawa: NASK Państwowy Instytut Badawczy.

Pyżalski J., (2012), „Agresja elektroniczna i cyberbullying jako nowe ryzykowne zachowania młodzieży", Kraków: Oficyna Wydawnicza Impuls.

POLECAMY

ose.gov.pl
Ogólnopolska Sieć Edukacyjna

gov.pl/cyfryzacja
Ministerstwo Cyfryzacji

nask.pl
NASK

osehero.pl
OSEhero

lektury.gov.pl
Portal lektury.gov.pl

oseregio.pl
OSEregio

cert.pl
CERT Polska

dyzurnet.pl
Dyżurnet

akademia.nask.pl
Akademia NASK

Państwowy Instytut Badawczy NASK

Cyberbezpieczeństwo – innowacje – edukacja cyfrowa – OSE

NASK jest Państwowym Instytutem Badawczym nadzorowanym przez Ministerstwo Cyfryzacji. Prowadzi badania naukowe i prace rozwojowe na rzecz bezpieczeństwa systemów sieciowych, a także nad technologiami opartymi na najnowocześniejszych rozwiązaniach, wykorzystujących sztuczną inteligencję i zaawansowaną analizę danych. NASK na mocy ustawy o Krajowym Systemie Cyberbezpieczeństwa pełni zadania jednego z trzech Zespołów Reagowania na Incydenty Komputerowe (CSIRT) poziomu krajowego. Instytut realizuje strategiczne programy z obszaru cyfryzacji Polski, a także prowadzi rejestr domeny .pl, w którym znajduje się ponad 2,6 mln domen. NASK wypełnia misję edukacyjną, ekspercką i popularyzatorską na rzecz podnoszenia poziomu kompetencji cyfrowych oraz świadomości bezpieczeństwa użytkowników sieci.

Państwowy Instytut Badawczy NASK jest operatorem Ogólnopolskiej Sieci Edukacyjnej (OSE) – programu Ministerstwa Cyfryzacji, którego celem jest budowa i podłączenie wszystkich szkół w Polsce do szybkiego, bezpiecznego i bezpłatnego internetu, a także tworzenie Ekosystemu OSE, wspierającego proces kształcenia poprzez dostarczanie nowoczesnych i wartościowych treści oraz narzędzi cyfrowych dla nauczycieli i uczniów.

NASK – współtworzymy rewolucję cyfrową w Polsce!

Kontakt

ul. Kolska 12
01-045 Warszawa

+48 22 182 55 55

ose@nask.pl

ose.gov.pl

ISBN: 978-83-65448-23-1