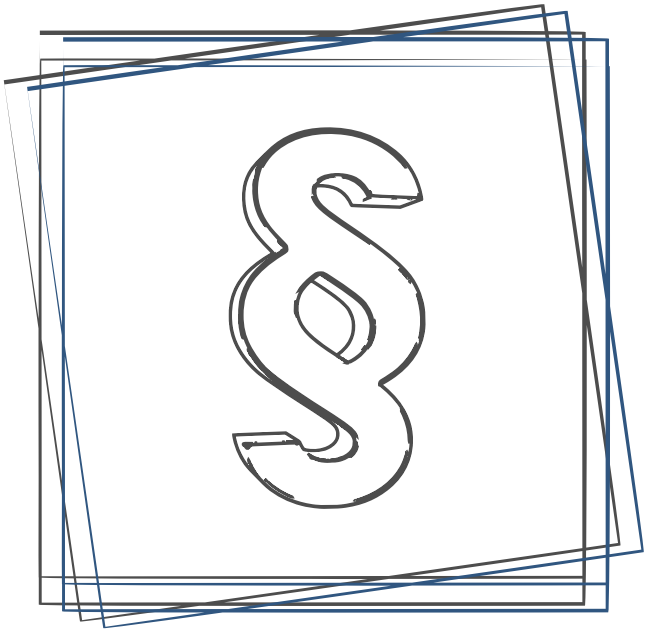
CYBER PRZEMOC

JAK SIĘ PRZED NIĄ BRONIĆ?



Dane aktualne na dzień 19.06.2024 r.

NIEZBĘDNIK PRAWNY

NIEODPŁATNE USŁUGI
-POMOC PRAWNA
-PORADY OBYWATELSKIE
-MEDIACJA

Ministerstwo Sprawiedliwości

KATOWICE dla odmiany

Zadanie publiczne współfinansowane ze środków budżetu Państwa otrzymanych z Miasta Katowice

Spis treści

Spis treści 2

1. Wstęp 4

2. Phishing – zagrożenie w każdym miejscu: "Kliknij w ten link" ..4

3. Malware – złośliwe oprogramowanie 5

4. Ransomware – blokada urządzenia 6

5. Zagrożenia dla prywatności 6

6. Kradzież danych – cenny łup dla cyberprzestępców 8

7. Cyberprzemoc – nękanie w sieci 9

8. Niebezpieczne reklamy (malvertising) – reklama jako narzędzie ataku 9

9. Spoofing – kiedy oszust udaje kogoś innego 10

10. Oszustwa internetowe – uważaj, na kogo trafisz w sieci 10

11. Wiadomości e-mail od nieznanego i „znanego” nadawcy 11

12. Nietypowe formy płatności - kryptowaluty 13

13. Oszustwa randkowe – porywy serca 13

14. Fałszywa pomoc techniczna - fachowiec mile widziany 14

15. Oszustwo „na wnuczka” 14

16. Oszustwa inwestycyjne – pieniądze same się mnożą 15

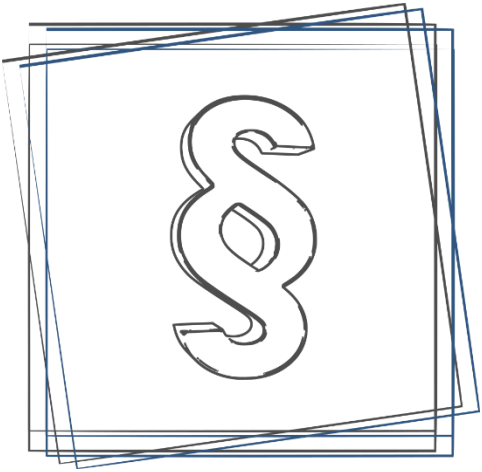
17. Fałszywe zbiórki charytatywne – wspomóż nas 16

18. Przekręty dotyczące leków, czyli maść na wszystko.....16

19. Fałszywe sklepy internetowe – sklep widmo.....17

20. Fałszywe sklepy internetowe – sklep widmo.....17

Stowarzyszenie Na rzecz Poradnictwa Obywatelskiego DOGMA - informacje.....19



1. Wstęp

Postęp technologiczny ułatwia ludziom podtrzymanie aktywnego uczestnictwa w codziennym życiu. Media społecznościowe ułatwiają kontakt z rodziną, która jest np. za granicą.

Wykorzystanie tych nowych możliwości daje wiele korzyści, trzeba jednak pamiętać o zasadach bezpieczeństwa.

Internet to niesamowite narzędzie, które ułatwia nam codzienne życie, ale niesie ze sobą również liczne niebezpieczeństwa. Rozpoznanie tych zagrożeń to klucz do bezpiecznego poruszania się po sieci. Jeżeli coś wydaje Ci się podejrzane to prawdopodobnie takie jest.

Co więc nam grozi podczas aktywności online?

2. Phishing – zagrożenie w każdym miejscu: "Kliknij w ten link"

Phishing - wyłudzenie informacji - polega on na wyłudzeniu danych wrażliwych takich jak: hasła, numery kart kredytowych, dane kont bankowych, numer PESEL. Te zaś pozwalają na dostęp do konta bankowego i opróżnienie go z pieniędzy. Większość tego typu kradzieży odbywa się poprzez portale społecznościowe lub pocztę elektroniczną. Nieświadomy niczego człowiek otwiera link, który przekierowuje go do witryny imitującej oryginalną stronę danej organizacji (banku, sklepu internetowego, portalu aukcyjnego), więc nie podejrzewając zagrożenia wpisuje swoje dane (login, numer klienta, hasło itp.), które następnie zostają przesłane do oszusta.

Przestępca może podszyć się pod… każdego z nas, aby wysłać mnie, tobie link, który zawiera złośliwe oprogramowanie lub przekieruje ją na fałszywą stronę, a następnie poprosi ją o podanie poufnych danych, takich jak dane karty kredytowej.

Jak się bronić?

Najlepszą obroną przed phishingiem jest weryfikacja osoby lub firmy, która wysłała wiadomość e-mail lub inną przed kliknięciem czegokolwiek. Pamiętaj, aby zawsze sprawdzać, czy strona, na której wpisujesz swoje dane, jest prawdziwą stroną instytucji, a nie fałszywym serwisem stworzonym przez przestępców.

Pamiętaj!

Banki czy platformy umożliwiające płatności w Internecie nigdy nie proszą o aktualizację danych w wiadomościach. Wszelkie zmiany należy wprowadzać logując się na stronie banku po samodzielnym wpisaniu adresu lub sprawdzeniu czy strona jest zabezpieczona certyfikatem.

3. Malware – złośliwe oprogramowanie

Malware czyli złośliwe oprogramowanie, to jedno z najbardziej powszechnych zagrożeń w Internecie. Jego celem jest zazwyczaj zdobycie dostępu do Twojego komputera lub informacji i danych, które na nim przechowujesz. Złośliwe oprogramowanie może przybierać różne formy – od wirusów, przez trojany, po oprogramowanie szpiegujące. Często infekuje komputer poprzez załączniki w e-mailach, zainfekowane strony internetowe lub poprzez pobranie i zainstalowanie zainfekowanego oprogramowania nieświadomie przez użytkownika.

Jak się bronić?

Na naszych komputerach powinno być zainstalowane i aktualne oprogramowanie antywirusowe(antywirus) i zaktualizowany system.

4. Ransomware – blokada urządzenia

Ransomware to specyficzny rodzaj malware, który blokuje dostęp do komputera lub plików do momentu zapłacenia okupu. Cyberprzestępcy wykorzystują go do szyfrowania danych na dysku, co uniemożliwia dostęp do nich.

W ostatnich latach ransomware stał się jednym z największych zagrożeń dla użytkowników sieci. Co jakiś czas słychać o masowych atakach na firmy lub zwykłych użytkowników sieci.

Jak się bronić?

Najlepszą obroną przed ransomware jest regularne tworzenie kopii zapasowych swoich danych.

5. Zagrożenia dla prywatności

Zagrożenia dla prywatności polegają na zbieraniu i wykorzystywaniu danych użytkowników, często bez ich świadomej zgody. Wykorzystuje się je do różnych celów – od marketingu, przez politykę, aż po oszustwa internetowe. Często nie zdajemy sobie sprawy, jak wiele informacji o nas jest dostępnych w sieci i jak łatwo można je wykorzystać.

Jak się bronić?

Nie udzielać zbędnych informacji na każdym portalu, gdzie się znajdujemy.

Przykład e-maila:

Drogi właścicielu poczty e-mail.

Europejska Komisja ds. Zwalczania Nadużyć Finansowych, zatwierdziła wypłatę odszkodowania w wysokości 950,000.00 (EURO) do Ciebie. Ta rekompensata jest wypłacana za straty/szkody powstałe w wyniku oszustwa lub spraw związanych z Oszustwem. Uprzejmie prosimy o przesłanie nam swoich informacji wymienionych poniżej.

Twoje imię i nazwisko:

Kraj:

Adres domowy:

Numer:

Wiek:

Zawód:

Najbliżsi krewni (imiona):

Wszystkie informacje zostaną przekazane Europejskiej Komisji ds. Zwalczania Nadużyć Finansowych, "EAFC" (organizationeu@gmail.com). Dziękujemy za zrozumienie i współpracę, ponieważ czekamy na jak najszybsze przeczytanie od Ciebie.

Dział Monitoringu European Anti-Fraud Commission, "EAFC"

organizationeu@gmail.com

6. Kradzież danych – cenny łup dla cyberprzestępców

Kradzież danych jest jednym z najczęstszych rodzajów przestępstw w sieci. Cyberprzestępcy włamują się do baz danych firm czy instytucji, by wykradzionymi danymi użytkowników później manipulować. Takie naruszenia danych mogą prowadzić do wielu negatywnych scenariuszy, takich jak kradzież tożsamości, oszustwa finansowe czy utrata prywatności. Cyberprzestępcy korzystają z różnych technik, aby włamać się do sieci i systemów komputerowych. Mogą wykorzystywać luki w zabezpieczeniach komputerów i serwerów.

Kradzież tożsamości – to poważne zagrożenie w sieci, łączy się z kradzieżą danych. Cyberprzestępcy mogą wykorzystać wykradzione lub zdobyte w inny sposób informacje takie jak numer PESEL, skan dowodu osobistego, adres czy data urodzenia do kradzieży Twojej tożsamości. Takie działanie może prowadzić do wielu negatywnych konsekwencji, na przykład zaciągania pożyczek na Twoje dane.

Jak się bronić?

Nigdy nie należy udostępniać swoich danych osobowych nieznanej stronie internetowej, a wszystkie wiadomości e-mail, które proponują podanie danych osobowych, należy traktować jako potencjalnie niebezpieczne.

7. Cyberprzemoc – nękanie w sieci

Cyberprzemoc to zjawisko polegające na wykorzystywaniu technologii do nękania, zastraszania lub ośmieszania innych. Może to obejmować takie działania jak doxxing (udostępnianie prywatnych informacji o osobie w sieci), hejt, wysyłanie obraźliwych wiadomości, nękanie psychiczne przez internet, publikowanie fałszywych informacji o innych osobach w sieci czy groźby przemocy fizycznej. Cyberprzemoc jest szczególnie niebezpieczna, ponieważ może prowadzić do poważnych problemów emocjonalnych i psychicznych u ofiar.

Jak się bronić?

Ważne jest szybkie reagowanie i zgłaszanie ich odpowiednim służbom (policja).

8. Niebezpieczne reklamy (malvertising) – reklama jako narzędzie ataku

Malvertising to metoda, która polega na wykorzystywaniu reklam do dystrybucji złośliwego kodu. Reklama na pierwszy rzut oka może wydawać się niewinna, ale po kliknięciu w nią może dojść do uruchomienia złośliwego kodu, który doprowadzi do infekcji urządzenia. Najczęściej wykorzystywane są do tego luki bezpieczeństwa w przeglądarkach internetowych.

Jak się bronić?

Zainstalować program antywirusowy (płatny lub darmowy), który będzie skanował wszystkie pliki przed ich otwarciem. Równie ważne jest

regularne aktualizowanie oprogramowania, aby zminimalizować ryzyko wykorzystania luk w zabezpieczeniach.

9. Spoofing – kiedy oszust udaje kogoś innego

Spoofing to atak, który polega na podszywaniu się pod inną osobę lub organizację w sieci. Przestępca może na przykład udawać bank lub inną instytucję państwową, aby skłonić Cię do podania danych do zainstalowania na swoim urządzeniu złośliwego oprogramowania lub do podania swoich danych do logowania lub innych ważnych informacji.

Jak się bronić?

Zawsze weryfikować, czy strona, z którą mamy do czynienia jest prawdziwa i nigdy nie podawać swoich danych na podejrzanych stronach.

10. Oszustwa internetowe – uważaj, na kogo trafisz w sieci

Oszustwa internetowe to szeroka kategoria zagrożeń na portalach aukcyjnych takich jak OLX, Vinted, Facebook, oszustwa przy pomocy BLIKA, wyłudzanie pieniędzy, fałszywe wiadomości email i SMS. Użytkownicy Internetu powinni być świadomi, że nie wszystko, co widzą w sieci, jest prawdziwe.

Jak się bronić?

Należy zachować szczególną ostrożność przy dokonywaniu transakcji online, podawaniu swoich danych osobowych i klikaniu w linki otrzymywane w wiadomościach e-mail czy SMS.

11. Wiadomości e-mail od nieznanego i „znanego" nadawcy

Wiadomość od nieznanego nadawcy, zwłaszcza jeśli zawiera ona linki lub załączniki, to potencjalne zagrożenie. Oszuści często udają osoby, które znasz lub firmy, z którymi współpracujesz, aby skłonić cię do kliknięcia na link lub otwarcia zainfekowanego załącznika.

- **Natychmiastowe działanie** – oszuści często używają strachu, twierdząc, że Twoje konto zostało zaatakowane i musisz natychmiast podjąć działania. Ma to skłonić Cię do szybkiego podania swoich danych, bez możliwości spokojnego przeanalizowania sytuacji. Pamiętaj, że prawdziwe instytucje zwykle nigdy nie zmuszają użytkownika do natychmiastowych działań.
- **Błędy gramatyczne i ortograficzne** – wiele oszustw internetowych wywodzi się z innych państw niż Polska. Przestępcy nie znają dobrze języka polskiego lub wykorzystują translatory internetowe do tworzenia reklam, wiadomości lub oszukujących stron internetowych.
- **Podszywanie się pod znajomych** – jeżeli otrzymasz wiadomość od kogoś znajomego, ale styl pisania lub szczegóły wydają się podejrzane, to może to być to sygnał, że konto Twojego

znajomego zostało zhakowane i podszywa się pod niego oszust. Dobrze wtedy skontaktować się ze znajomym np. telefonicznie i dopytać, czy coś wysyłał.

- **Podszywanie się pod służby** - napastnicy mogą używać również podszywać się pod policję lub inne służby w celu zastraszenia ofiary. Możemy otrzymać maila z informacją, że na komputerze zostały znalezione nielegalne materiały, że odtworzyliśmy albo pobraliśmy nielegalny film. Jeśli ofiara da się nabrać i uwierzy przestępcom, zapłaci karę, aby uniknąć aresztowania lub innej kary.
- **Fałszywe nagrody** - schemat tego ataku jest prosty – ofiara otrzymuje informację, że wygrała nagrodę rzeczową, wycieczkę lub dużą kwotę, ale z powodu biurokracji musi uiścić stosunkowo niewielką opłatę, aby ją odebrać.
- **„Paczka do odebrania”** – dostajemy informacje o zatrzymanej paczce z powodu niedopłaty. By ja otrzymać musimy uiścić opłatę na spreparowanej stronie, na której musimy podać dane karty kredytowej, lub wpłacić na nieznane konto niewielka kwotę.

Jak się bronić?

Czujność i kasowanie niepotrzebnych i nieznanych maili, zabezpieczenie komputera.

Przykład emaila:

Dobry dzień. Mam z Tobą do omówienia coś bardzo ważnego, na czym skorzystasz. Będę czekać na Twoją szybką odpowiedź, ale musisz ją wysłać od razu. Inaczej spadek, który odziedziczyłeś przepadnie. Pani María Rodríguez.

12. Nietypowe formy płatności - kryptowaluty

Oszuści w internecie często proszą o nietypowe formy płatności, takie jak karty podarunkowe czy płatności przy pomocy kryptowaluty. Większość prawdziwych firm nie będzie wymagać od Ciebie płatności wyłącznie w taki sposób.

13. Oszustwa randkowe – porywy serca

Mają miejsce, gdy oszust tworzy atrakcyjny, fałszywy profil w Internecie, aby nawiązywać miłosne relacje, mające na celu wyłudzenie pieniędzy. Często wszystko wygląda bardzo wiarygodnie. Gdy fałszywy randkowicz wyczuje, że zdobył zaufanie lub nawet miłość ofiary, zaczyna prosić o poufne informacje lub o pomoc finansową, np. na pokrycie kosztów podróży lub leczenia.

Jak się bronić?

Nigdy nie przelewajmy pieniędzy osobie, której nie znamy osobiście. Nie wysyłajmy zbyt sugestywnych zdjęć, które oszust może później wykorzystać do szantażu. Nie zamieszczajmy takich które mogą naprowadzić oszusta na miejsce, gdzie mieszkamy i pracujemy.

14. Fałszywa pomoc techniczna - fachowiec mile widziany

Oszuści zajmujący się pomocą techniczną dzwonią lub wysyłają wiadomości udając, że są legalnie działającą firmą. Mogą nawet podszywać się pod dużą organizację, jak Microsoft czy Apple. Podają jakiś nieistniejący problem, który rzekomo istnieje na komputerze ofiary i przekonują do wykonania kroków, które pozwolą przestępcom na uzyskanie zdalnego dostępu do komputera lub wykradzenie danych osobowych czy finansowych.

Jak się bronić?

Korzystajmy z pomocy pewnych techników i informatyków.

15. Oszustwo „na wnuczka”

To jedno z najgroźniejszych, a równocześnie najpopularniejszych oszustw na tej liście. Polega na podszywaniu się pod krewnego (najczęściej wnuka) i wyłudzaniu informacji lub pieniędzy od starszej osoby. Oszustwo może przebiegać zarówno telefonicznie, jak i przez internet. Przestępcy często działają w sposób bardzo przemyślany. Przykładowo, tworzą w mediach społecznościowych duplikat konta wnuka i za jego pośrednictwem piszą do dziadka lub babci z prośbą o pomoc. Mówią, że mają kłopoty (np. zostali okradzeni na zagranicznych wakacjach itp. historie) i potrzebują pieniędzy, aby wyjść z tej sytuacji. Powiedzą, że to pilne i że wstydzą się iść do rodziców. Zanim sięgniemy do portfela sprawdźmy innym kanałem komunikacji czy wnuczek jest w opałach…

Przykład:

70-letnia kobieta odebrała telefon od nieznajomego mężczyzny, który podawał się za policjanta. Rozmówca poinformował, że jej wnuczka spowodowała wypadek i potrzebuje pieniędzy, aby wykupić się z aresztu. Zapytał, ile ma oszczędności, a ta szybko przeliczyła gotówkę, którą miała w domu. Zebrało się tego 15 tysięcy. Oszust poprosił o podanie adresu, a do rozmowy włączyła się kobieta, podszywająca się za jej wnuczkę, dziękując babci za pomoc. Seniorka przekazała pieniądze nieznajomemu mężczyźnie, który przyszedł pod wskazany oszustom adres babci. W ten sposób 86-latka straciła całe swoje oszczędności. Po dwóch dniach kobieta w rozmowie z prawdziwą wnuczką dowiedziała się, że została oszukana.

16. Oszustwa inwestycyjne – pieniądze same się mnożą

To przekręt skierowany do emerytów z oszczędnościami, którzy potrzebują pomocy w zarządzaniu nimi. Obiecują dobry zwrot z inwestycji, jednak po przekazaniu pieniędzy senior już nigdy więcej ich nie zobaczy.

Jak się bronić?

Unikajmy ofert wywierających presję na szybkie kupowanie lub mocno ograniczonych czasowo.

17. Fałszywe zbiórki charytatywne – wspomóż nas

Chęć niesienia pomocy i ufność każdego z nas bywa brzydko wykorzystywana przez cyberprzestępców. Podszywają się oni pod zaufane organizacje charytatywne i zbierają od ofiar darowizny, które trafiają prosto do ich kieszeni.

Jak się bronić?

Upewnijmy się, czy zbiórka jest prawdziwa i warta wsparcia.

18. Przekręty dotyczące leków, czyli maść na wszystko

Internet niesie to ryzyko trafienia na oszustów, którzy sprzedają podróbki leków (niekiedy bardzo groźne dla zdrowia) lub wyłudzają pieniądze za produkty, których nigdy nie wysyłają.

Jak się bronić?

Kupujmy nasze leki w sprawdzonych sklepach i aptekach i konsultujmy ich użycie z lekarzem.

19. Fałszywe sklepy internetowe – sklep widmo

Fałszywe strony internetowe to żadna nowość, jednak aktualnie wyglądają bardziej wiarygodnie niż kiedykolwiek wcześniej. Wykorzystują one zdjęcia od prawdziwych sprzedawców i naśladują wygląd i styl prawdziwych sklepów.

Często wabikiem są tu atrakcyjne ceny. Niestety, po zapłaceniu zwykle kontakt urywa się lub – w najlepszym przypadku – wysłany zostaje przedmiot o niższej jakości, będący podróbką tego, co oferował sprzedawca.

Jak się bronić?

Nie kupujmy produktów z niezaufanych witryn, które kuszą podejrzanie niskimi cenami. Zanim dokonamy zakupu, sprawdźmy dane sklepu – nazwę firmy, adres jej siedziby, dane kontaktowe, numer KRS, porównując je z internetowymi bazami przedsiębiorców – Centralną Ewidencją i Informacji o Działalności Gospodarczej (CEIDG) i Systemem EKRS.

20. Fałszywe sklepy internetowe – sklep widmo

Jeżeli padłeś ofiarą cyberprzemocy mobbingu, nękania lub prześladowania w sieci skorzystaj z porady i dowiedz się, jakie przysługują Ci prawa.

Osoba, która stała się ofiarą oszustwa internetowego (cyberprzestępstwa) ma prawo je zgłosić:

- w najbliższej jednostce policji lub prokuraturze. Tego typu przestępstwa są ścigane na wniosek osoby poszkodowanej.
- online: https://www.gov.pl/web/gov/zglos-przestepstwo
- do CSIRT NASK: https://incydent.cert.pl/ - dostępny jest interaktywny formularz umożliwiający wysłanie zgłoszenia o potencjalnym niebezpiecznym incydencie, w którego treści należy zapisać otrzymaną wiadomość w całości, wraz z załącznikiem i nagłówkami w osobnym pliku i przesłać do analizy.

Doświadczyłeś cyberprzemocy, potrzebujesz porady i pomocy - skontaktuj się z nami!

Spotkanie z jest możliwe w każdym z punktów nieodpłatnej pomocy prawnej i punktów nieodpłatnego poradnictwa obywatelskiego, zlokalizowanych na terenie Powiatu Gliwickiego, po uprzednim umówieniu. Szczegółowe informacje na ostatniej stronie poradnika.

Stowarzyszenie Na rzecz Poradnictwa Obywatelskiego DOGMA - informacje

Stowarzyszenie „DOGMA” od ponad 20 lat prowadzi działalność poradniczą na rzecz osób zagrożonych wykluczeniem społecznym i będących w trudnej sytuacji życiowej.

Nasza organizacja od 2016 roku realizuje zadania wynikające z ustawy o nieodpłatnej pomocy prawnej oraz edukacji prawnej i posiada Certyfikat dla organizatorów placówek poradniczych dot. Modelu Wsparcia dla Poradnictwa Prawnego i Obywatelskiego, wyd. dnia 12.01.2014 r. przez Fundację Uniwersyteckich Poradni Prawnych.

W Punktach bezpłatnej pomocy prawnej i poradnictwa obywatelskiego powierzonych naszemu Stowarzyszeniu zyskaliśmy zaufanie klientów i opinię, że porady są przez nas prowadzone profesjonalnie, rzetelnie i z dużym wyczuciem.

Każda rozwiązana sprawa to nie tylko kolejny „numer klienta” w statystykach. To przede wszystkim problem, a nierzadko życiowy dramat człowieka, którego nie opuszcza poczucie bezsilności i bezradności; człowieka, któremu próbujemy pomóc w znalezieniu wyjścia z jego trudnej sytuacji. Staramy się pokazać, jak wielka siła drzemie w nim samym i jak wiele od niego zależy.

PUNKTY NIEODPŁATNEJ POMOCY PRAWNEJ PROWADZONE PRZEZ STOWARZYSZENIE "DOGMA"

- **Terenowy Punkt Pomocy Społecznej nr 3 MOPS, ul. Oblatów 24**
- **Terenowy Punkt Pomocy Społecznej nr 5 MOPS, ul. Dębowa 16c**
- **Terenowy Punkt Pomocy Społecznej nr 2 MOPS, ul. Warszawska 42**

Porady są udzielane od poniedziałku do piątku od 16.00 do 20.00

PUNKTY NIEODPŁATNEGO PORADNICTWA OBYWATELSKIEGO PROWADZONE PRZEZ STOWARZYSZENIE "DOGMA"

- **Terenowy Punkt Pomocy Społecznej nr 9 MOPS, ul. Krakowska 138**
- **Terenowy Punkt Pomocy Społecznej nr 8 MOPS, ul. Łętowskiego 6a**
- **Zespół ds. Rodzinnej Pieczy Zastępczej MOPS, ul. Wojewódzka 23**

Porady są udzielane od poniedziałku do piątku od 16.00 do 20.00

PUNKTY NIEODPŁATNEJ POMOCY PRAWNEJ I MEDIACJI

Miejska Izba Wytrzeźwień w Katowicach, ul. Macieja 10
Poniedziałek - piątek 16.00 - 20.00

Przychodnia nr 13 "Moja Przychodnia", ul. Ordona 3
Poniedziałek - piątek 8.00 - 12.00

Przychodnia nr 13 "Moja Przychodnia", ul. Ordona 3
Poniedziałek - piątek 13.00 - 17.00

Miejski Dom Kultury w Katowicach ul. Hallera 28
Poniedziałek - piątek 11.00 - 15.00

Miejski Dom Kultury w Katowicach ul. Markiefki 44a
Poniedziałek - piątek 9.00 - 13.00

ZAPISY NA PORADY

- **telefonicznie** - pod numerem telefonu: **32 259-37-36** w godzinach pracy urzędu
- **elektronicznie** - zapisując się przy pomocy formularza dostępnego na stronie: **https://zapisy-np.ms.gov.pl**
- **osobiście** - stawiając się w urzędzie

NIEODPŁATNE USŁUGI
-POMOC PRAWNA
-PORADY OBYWATELSKIE
-MEDIACJA

Ministerstwo Sprawiedliwości

KATOWICE dla odmiany

Zadanie publiczne współfinansowane ze środków budżetu Państwa otrzymanych z Miasta Katowice