CYBERPRAWO
JAK NIE ZŁAPAĆ SIĘ W SIEĆ?

#ZAGROŻENIA W SIECI

PORADNIK DLA MIESZKAŃCÓW
POWIATU WROCŁAWSKIEGO

Autor:

Krzysztof Pławecki

Hubert Plichta

Skład i opracowanie graficzne:

Katarzyna Winkler

Wydawca:

Fundacja LexCultura
ul. Fiołkowa 18/2
53-239 Wrocław
tel. 730336909

fundacja@lexcultura.pl

www.lexcultura.pl

@LexCultura

fundacja_lexcultura

POWIAT WROCŁAWSKI

Poradnik przygotowany w ramach realizacji zadania publicznego pt.:

„Cyberprawo dla młodzieży – jak nie złapać się w sieć”

realizowanego dzięki finansowaniu ze środków Powiatu Wrocławskiego

Wrocław
maj 2023

WSTĘP

Drodzy mieszkańcy powiatu wrocławskiego!

Przedstawiamy Wam pierwszą publikację edukacyjną dotyczącą bezpieczeństwa prawnego w sieci, wydaną w ramach projektu Fundacji LexCultura finansowanego ze środków Powiatu Wrocławskiego.

W kompletnym zbiorze 3 publikacji omówimy najważniejsze zagadnienia związane z bezpieczeństwem w sieci.

Od wybuchu pandemii w 2020 roku aktywność społeczna w Internecie znacząco wzrosła, niestety dotyczy to także osób nieuczciwych, chcących nas oszukać lub obrazić. Równolegle rozwija się technologia i pojawiają się nowe treści i zagrożenia, za którymi z trudnością możemy nadążyć.

Definicje słów takich jak scam czy phishing są często nieznane większości z nas, a niestety pojawiają się w sieci coraz częściej. Jako zespół Fundacji LexCultura rozumiemy, że w życiu codziennym nie ma czasu na wyszukiwanie kolejnych nowych zagrożeń i w tej publikacji postaramy się wyjaśnić najważniejsze definicje i zagrożenia w przystępny sposób.

Bardzo istotne pod kątem zapobiegania cyberzagrożeniom jest poznać je i nauczyć się przed nimi bronić.

Pragniemy, aby niniejsza publikacja służyła Wam jako swoisty przewodnik i koło ratunkowe w jednym, dzięki czemu poznacie lepiej cyberprzestrzeń.

Drodzy Czytelnicy, życzymy Wam owocnej lektury i wszystkiego bezpiecznego w sieci!

SPIS TREŚCI

PHISHING

Phishing to jedna z najpopularniejszych metod ataku w cyberprzestrzeni. Polega on na oszustwie, którego celem jest zdobycie naszych poufnych informacji, takich jak hasła, numery kart kredytowych czy dane personalne. Atakujący udają w tym celu instytucje finansowe, sklepy internetowe, firmy kurierskie i wiele innych, zachęcając nas do podania swoich danych na fałszywej stronie internetowej.

Przykłady phishingu są różne. Może to być fałszywa wiadomość e-mail, która wygląda jak oficjalna wiadomość od banku, prosząca o podanie naszych danych. Może to być fałszywa strona internetowa, która wygląda identycznie jak prawdziwa strona banku, ale w rzeczywistości jest to tylko fałszywa strona stworzona przez oszustów. Innym przykładem phishingu jest fałszywe ogłoszenie, które prosi nas o podanie naszych danych osobowych w zamian za obietnicę nagrody.

Jak się bronić przed phishingiem? Oto kilka podstawowych zasad, które powinniśmy zawsze pamiętać:

1. Nie otwieraj podejrzanych wiadomości e-mail - fałszywe wiadomości e-mail to jedna z najpopularniejszych metod phishingu. Podejrzliwe wiadomości, zwłaszcza te od nieznanych nadawców, należy traktować z dużą ostrożnością.

2. Uważaj na podejrzane strony internetowe - fałszywe strony internetowe wyglądają często bardzo podobnie do prawdziwych stron, dlatego trzeba uważać na adresy URL, sprawdzać certyfikaty SSL i zwracać uwagę na wszelkie nieprawidłowości.

3. Zwracaj uwagę na prośby o podanie poufnych informacji - prawdziwe instytucje finansowe nigdy nie proszą o podanie haseł czy numerów kart kredytowych drogą mailową lub telefoniczną.

4. Używaj narzędzi zabezpieczających - dobry program antywirusowy, blokery reklam czy rozszerzenia przeglądarki mogą pomóc w wykrywaniu i blokowaniu podejrzanych stron internetowych.

5. Bądź uważny - zawsze warto być ostrożnym i uważać na wszelkie podejrzane sytuacje.

Podsumowując, phishing to bardzo poważne zagrożenie w świecie cyfrowym. Oszuści stosują różne metody, aby uzyskać nasze poufne informacje, ale zawsze możemy skutecznie się przed nimi bronić. Warto pamiętać o podstawowych zasadach bezpieczeństwa i stosować się do nich w każdej sytuacji.

MALWARE

Malware przyjmuje różne formy, takie jak wirusy, trojany, robaki, ransomware i wiele innych. Wirusy to programy, które zarażają pliki na komputerze i replikują się, szkodząc w ten sposób systemowi operacyjnemu. Trojany są programami, które wydają się być nieszkodliwe, ale faktycznie kradną nasze dane lub umożliwiają atakującemu zdalne sterowanie naszym komputerem. Robaki to oprogramowanie, które rozprzestrzenia się na inne urządzenia poprzez sieć internetową, zagrażając całej sieci. Ransomware to rodzaj malware, który blokuje dostęp do naszych plików i żąda okupu za ich odblokowanie.

Jak chronić się przed malware? Oto kilka podstawowych zasad, które powinniśmy zawsze pamiętać:

1. Zainstaluj i regularnie aktualizuj oprogramowanie antywirusowe - dobry program antywirusowy może wykryć i usunąć większość rodzajów malware.
2. Nie pobieraj podejrzanych plików - pliki pobrane z nieznanych źródeł mogą zawierać malware.
3. Nie otwieraj podejrzanych wiadomości e-mail - atak phishingowy to popularna metoda, której celem jest uzyskanie naszych poufnych informacji.
4. Używaj silnych haseł - słabe hasła to prosta droga do złamania naszej ochrony.
5. Uważaj na podejrzane strony internetowe - strony internetowe, które wyglądają podejrzanie lub proszą o podanie wrażliwych danych, powinny budzić naszą nieufność.

Pamiętajmy, że ochrona przed malware jest niezbędna w dzisiejszych czasach, kiedy większość naszej aktywności odbywa się w świecie cyfrowym. Dbanie o bezpieczeństwo naszych urządzeń i danych to nasza odpowiedzialność, a podstawowe zasady są proste i łatwe do zapamiętania.

RANSOMWARE

Ransomware to złośliwe oprogramowanie, które blokuje dostęp do danych lub całego systemu i żąda okupu za ich odblokowanie. Sposoby, w jakie ransomware może dostać się na komputer lub urządzenie mobilne, to między innymi kliknięcie w podejrzany link, otwarcie załącznika w mailu lub pobranie zainfekowanego pliku z niezaufanych źródeł.

Jeśli komputer lub urządzenie mobilne zostaną zainfekowane ransomwarem, istnieje ryzyko utraty dostępu do ważnych danych, w tym dokumentów, zdjęć, filmów i innych plików. Oszuści żądają zazwyczaj okupu w postaci kryptowaluty, co utrudnia namierzenie ich przez władze.

Aby uchronić się przed ransomware, należy wykonywać regularne kopie zapasowe ważnych plików i przechowywać je w bezpiecznym miejscu, jak np. dysk zewnętrzny. Należy także pamiętać o aktualizacji oprogramowania i systemu operacyjnego, które często zawierają łatki bezpieczeństwa, a także unikać otwierania podejrzanych wiadomości e-mail, linków i pobierania plików z nieznanych źródeł. Korzystanie z antywirusa oraz firewalla może również pomóc w ochronie przed ransomwarem. W przypadku gdy już dojdzie do zainfekowania urządzenia, nie należy płacić żądanej kwoty okupu, ponieważ istnieje ryzyko, że dane nie zostaną odblokowane, a dodatkowo zachęcamy do zgłaszania takich przypadków na policję.

SCAM

Scam, zwany również oszustwem internetowym, to kolejna forma przestępczości, która jest bardzo popularna w sieci. Osoby stosujące scam próbują oszukać ludzi, na przykład poprzez wyłudzenie pieniędzy lub wrażliwych danych, takich jak hasła, numery kart kredytowych czy dane osobowe. Warto wiedzieć, jak rozpoznać scam i jak się przed nim uchronić.

Jak rozpoznać scam w sieci? Oto kilka sygnałów, na które warto zwrócić uwagę:

1. Obietnice zbyt piękne, by były prawdziwe - osoby stosujące scam często obiecują szybkie bogactwo, np. w zamian za inwestycję lub uczestnictwo w jakimś projekcie.

2. Prośby o wpłaty lub udostępnianie danych osobowych - osoby stosujące scam często proszą o udostępnienie swoich danych osobowych lub wpłaty pieniędzy w zamian za korzyści, które nie są warte takiego ryzyka.

3. Fałszywe strony internetowe - osoby stosujące scam często tworzą fałszywe strony internetowe, które wyglądają jak oficjalne strony znanych firm lub instytucji.

Jak nie dać się oszukać scamowi w sieci? Oto kilka podstawowych zasad, które warto pamiętać:

1. Zachowaj ostrożność - jeśli oferta wydaje się zbyt dobra, aby była prawdziwa, być może to jest scam. Zawsze warto zachować zdrowy rozsądek i zastanowić się, czy oferta jest realna.

2. Sprawdź źródło informacji - przed podjęciem jakiejkolwiek decyzji warto sprawdzić źródło informacji. W przypadku podejrzanych ofert lub próśb o udostępnienie wrażliwych danych, warto skontaktować się z firmą lub instytucją, z której to ma pochodzić.

3. Nie udostępniaj wrażliwych danych - nigdy nie powinno się udostępniać swoich wrażliwych danych, takich jak hasła, numery kart kredytowych czy dane osobowe, w przypadku podejrzanych ofert czy próśb.

4. Używaj zabezpieczeń - warto korzystać z zabezpieczeń, takich jak programy antywirusowe czy firewall. Te narzędzia pomagają wychwycić podejrzane aktywności w sieci i chronią przed atakami.

5. Edukuj się - warto się edukować na temat scamu i innych form oszustw w sieci. Dzięki temu będzie się łatwiej rozpoznawać podejrzane oferty i prośby oraz unikać ryzyka oszustwa.

Podsumowując, scam w sieci to poważny problem, z którym coraz częściej spotykają się użytkownicy Internetu. Oszustwa tego typu mają na celu wyłudzenie pieniędzy lub wrażliwych danych, takich jak hasła, numery kart kredytowych czy dane osobowe. Aby nie dać się oszukać scamowi, warto zachować ostrożność, sprawdzić źródło informacji, nie udostępniać wrażliwych danych, używać zabezpieczeń i edukować się na temat tej formy przestępczości. Pamiętajmy, że zdrowy rozsądek jest najlepszą bronią w walce z oszustami w sieci.

NIGERIA SCAM

Nigeria scam, znane również jako „nigeryjski przekręt" lub „przekręt 419", jest jednym z najstarszych i najbardziej powszechnych oszustw internetowych. Nazwa pochodzi od sekcji kodeksu karnego Nigerii, która dotyczy oszustw.

Ten rodzaj oszustwa zwykle zaczyna się od otrzymania e-maila lub wiadomości na platformie społecznościowej od osoby, która twierdzi, że jest wysokiej rangi urzędnikiem lub przedstawicielem rządu, korporacji lub organizacji charytatywnej z Afryki lub innej części świata. Wiadomość ta informuje o możliwości zysku dużych pieniędzy w zamian za pomoc w przeniesieniu lub odzyskaniu funduszy.

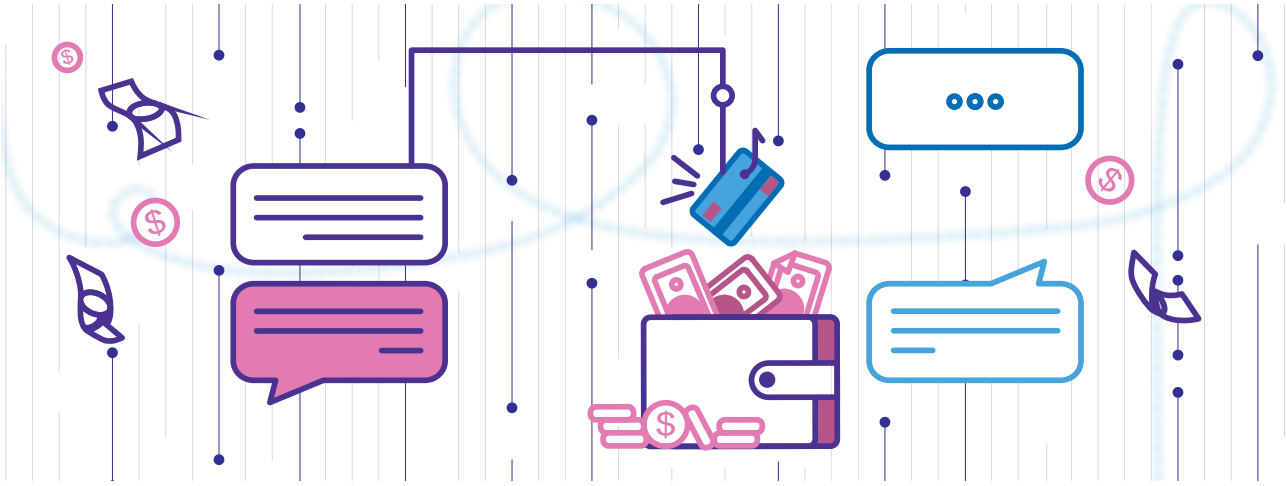
Oszuści często twierdzą, że potrzebują pomocy w przeniesieniu dużej sumy pieniędzy na konto za granicą, a w zamian obiecują hojne wynagrodzenie. Zwykle proszą o informacje na temat konta bankowego, aby mogli dokonać przelewu, lub proszą o przedpłatę kosztów związanych z przeniesieniem pieniędzy, takich jak opłaty administracyjne, cła, podatki itp.

Niektórzy oszuści stosują także różne strategie, aby zachęcić ofiary do udziału w oszustwie, takie jak oferowanie umowy na sprzedaż towarów po bardzo atrakcyjnych cenach lub prośba o pomoc finansową na cele charytatywne.

Wszystkie te prośby są fałszywe, a oszuści mają na celu wyłudzenie pieniędzy ofiar. Nigeria scam jest jednym z najpowszechniejszych i najbardziej znanych oszustw internetowych, a oszuści często zmieniają swoje metody i techniki, aby uniknąć wykrycia.

Aby uniknąć Nigeria scam-u, zawsze należy być ostrożnym wobec wiadomości od nieznanych osób, które obiecują duże zyski lub proponują nietypowe oferty.

Nie udostępniaj swoich danych osobowych, szczególnie numerów kont bankowych, ani nie dokonuj płatności przed dokładnym zweryfikowaniem autentyczności i wiarygodności oferty.



Warto również pamiętać, że instytucje rządowe i korporacje nie będą wysyłać wiadomości e-mailowych z prośbami o udostępnienie informacji finansowych. Jeśli otrzymasz podejrzaną wiadomość, warto skontaktować się z instytucją bezpośrednio i upewnić się, że to oni wysłali wiadomość. W końcu, pamiętaj, że oferty, które brzmią zbyt dobrze, aby były prawdziwe, najprawdopodobniej są oszustwem.

DROPSHIPPING

Zakupy w sieci są tak samo popularne jak zakupy w sklepach stacjonarnych, dlatego przedsiębiorcy szukają nowych sposobów dystrybucji towarów. W ostatnich latach, jednym z takich rozwiązań stał się model sprzedaży dropshippingu, w którym producent lub inny podmiot przesyła towar bezpośrednio do kupującego. Natomiast rola przedsiębiorcy prowadzącego platformę internetową sprowadza się do zbierania zamówień i przesyłania ich do dostawcy.

Problemy z jakimi najczęściej spotykają się konsumenci to m.in.: bardzo długi czas dostawy (zazwyczaj 30-60 dni), konieczność poniesienia dodatkowych opłat, które nie były nigdzie wcześniej uwzględnione w cenie (np. cło, podatek) czy otrzymywanie towaru niekompletnego, uszkodzonego, bez menu w języku polskim, "odnawianego", często nieoryginalnego.

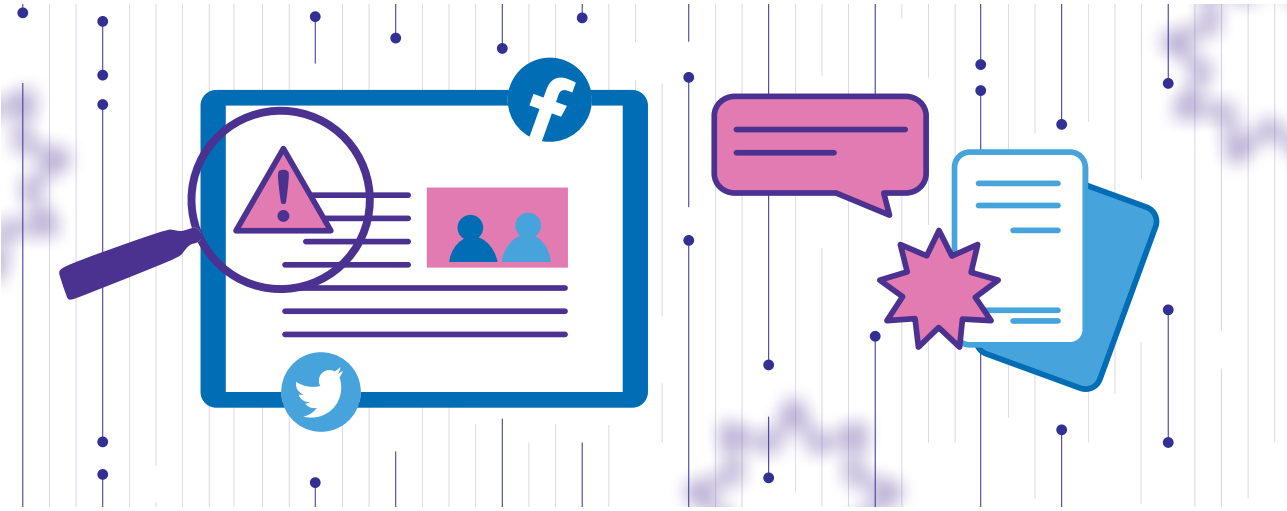
Obecnie większość przedsiębiorców wykorzystujących dropshipping określa swoją działalność jako pośrednictwo sprzedaży. Sprzedawcą towaru jest więc podmiot trzeci, niejednokrotnie mający siedzibę poza terenem Unii Europejskiej, z którym polski pośrednik prowadzący platformę nawiązał współpracę. Dzięki temu, część firm chce wyłączyć swoją odpowiedzialność np. za wady towaru, odsyłając klientów z reklamacją do producenta lub hurtownika.

Choć dropshipping upowszechnił się w Polsce niedawno, to już teraz jest realnym zagrożeniem dla konsumentów robiących zakupy w sieci. Dlatego chcąc uniknąć problemów, trzeba szczególnie zwracać uwagę na zapisy w regulaminach, ponieważ często atrakcyjne ceny, oznaczają niemniej atrakcyjne kłopoty. Kluczowe jest, abyśmy w regulaminie sprawdzili kto jest sprzedawcą. Jeśli polska firma określa się mianem pośrednika, to prawdopodobnie jest to dropshipper.

FAKE NEWS

W dobie powszechnego dostępu do Internetu, media społecznościowe stały się jednym z najważniejszych źródeł informacji dla milionów ludzi na całym świecie. Niestety, wraz z popularnością mediów społecznościowych, rośnie liczba fałszywych informacji i manipulacji, które przyczyniają się do rozpowszechniania dezinformacji, dezorientacji i podziałów w społeczeństwie. Zjawisko to znane jest jako fake news, czyli fałszywe informacje.

Fake news to nieprawdziwe, niezweryfikowane lub zmanipulowane informacje, które mają na celu wprowadzenie ludzi w błąd lub manipulowanie ich poglądami. Fałszywe informacje w sieci mogą dotyczyć różnych dziedzin, takich jak polityka, nauka, zdrowie, biznes czy rozrywka, a ich wpływ na społeczeństwo może być ogromny. Dlatego ważne jest, aby nauczyć się rozpoznawać fake news i unikać rozpowszechniania dezinformacji.



Jak rozpoznać fake newsów?

Rozpoznanie fake newsów może być trudne, ponieważ fałszywe informacje często wyglądają jak prawdziwe, a ich autorzy wykorzystują różne techniki manipulacyjne, aby przekonać ludzi do ich poparcia. Oto kilka wskazówek, które pomogą Ci w rozpoznawaniu fake news:

1. Sprawdź źródło informacji - przed podaniem informacji dalej, warto sprawdzić, czy źródło jest wiarygodne i autoryzowane. Pamiętaj, że wiele fałszywych informacji pochodzi z nieznanych lub nieautoryzowanych źródeł.

2. Weryfikuj informacje - sprawdź, czy informacje, które otrzymałeś, zostały potwierdzone przez inne źródła. Jeśli nie możesz znaleźć potwierdzenia, to znaczy, że informacja może być nieprawdziwa.

3. Sprawdź datę - sprawdź, kiedy informacja została opublikowana. Często fake newsy wykorzystują stare, już dawno temu zdementowane informacje, aby wprowadzić ludzi w błąd.

4. Szukaj faktów - przed podjęciem decyzji, na podstawie informacji, jakie otrzymałeś, sprawdź, czy są one oparte na faktach. Fałszywe informacje często zawierają nieprawdziwe fakty lub statystyki, które mają na celu wprowadzenie ludzi w błąd.

Rozpowszechnianie fake news może przyczynić się do poważnych konsekwencji, takich jak dezinformacja, dezorientacja, podziały i konflikty w społeczeństwie. Dlatego ważne, aby informacje, które powielamy były przez nas weryfikowane.

KRADZIEŻ TOŻSAMOŚCI

Kradzież tożsamości to jedno z najpoważniejszych zagrożeń w dzisiejszych czasach. Osoba, która przejmuje naszą tożsamość może zrobić wiele niebezpiecznych rzeczy, w tym dokonywać zakupów, zaciągać pożyczki lub kredyty, a nawet popełniać przestępstwa w naszym imieniu. Dlatego tak ważne jest, aby wiedzieć, jak chronić swoją tożsamość w sieci.

Kradzież tożsamości może mieć różne formy. Najczęściej polega na pozyskaniu przez cyberprzestępcę informacji na temat naszej tożsamości, takich jak imię, nazwisko, data urodzenia, adres zamieszkania czy numer dowodu osobistego. Mogą to być informacje, które podaliśmy na stronach internetowych, w sieciach społecznościowych lub w wiadomościach e-mail. Kradzież tożsamości może mieć również formę podszywania się pod naszą osobę w sieci, np. poprzez założenie fałszywego profilu w mediach społecznościowych.

Aby uniknąć kradzieży tożsamości, warto przestrzegać kilku podstawowych zasad.

Po pierwsze, nie podawajmy w Internecie zbyt wielu informacji na temat swojej osoby. Szczególnie ostrożni powinniśmy być w przypadku informacji dotyczących naszych danych osobowych, takich jak numer dowodu osobistego czy numer konta bankowego. Warto również pamiętać, że wiele firm i instytucji nie wymaga podawania takich informacji drogą elektroniczną, dlatego zawsze warto upewnić się, czy rzeczywiście mamy do czynienia z oficjalnym przedstawicielem firmy czy instytucji.

Kolejnym ważnym krokiem, który warto podjąć, jest korzystanie z bezpiecznych haseł. Hasło powinno być trudne do odgadnięcia, składać się z różnych znaków, w tym dużych i małych liter, cyfr i znaków specjalnych. Powinniśmy również unikać korzystania z jednego hasła do wielu różnych kont w sieci.

Warto również zainstalować na swoim komputerze oraz smartfonie antywirusa i firewall. Dzięki temu będziemy mieli pewność, że nikt nieprzyjazny nie próbuje włamać się na nasze urządzenia, a nasze dane są bezpieczne.

W przypadku podejrzenia, że padliśmy ofiarą kradzieży tożsamości, powinniśmy jak najszybciej zgłosić to fakty organom ścigania oraz zmienić wszystkie hasła i loginy do naszych kont w sieci. Dobrym zwyczajem jest także sprawdzanie stanu swojego konta bankowego oraz historii transakcji, aby na czas wykryć niepokojące transakcje.

GDZIE SZUKAĆ POMOCY?

Instytucją, która oferuje pomoc w zakresie cyberbezpieczeństwa jest CERT Polska **https://cert.pl** Jest to zespół ekspertów, którzy zajmują się reagowaniem na niebezpieczne incydenty w sieci. CERT Polska oferuje m.in. poradnictwo w zakresie cyberbezpieczeństwa i przeprowadza szkolenia.

Kolejną instytucja jest policja, która zajmuje się sprawami dotyczącymi przestępstw w sieci, a Urząd Ochrony Danych Osobowych zajmuje się ochroną danych osobowych i informacji prywatnych w sieci. To kolejne instytucje, które zapewniają wsparcie osobom dotkniętym cyberzagrożeniami.

W przypadku podejrzenia incydentu cybernetycznego, warto skontaktować się z powyższymi instytucjami oraz szukać pomocy wśród specjalistów. Ważne jest, aby w przypadku zaistnienia incydentu, działać szybko i skutecznie, aby minimalizować skutki działań nieuczciwych osób.


LEXCULTURA