

Wykaz aktów i źródeł: Trzy oszustwa, które trafiają do placówek

Każdy fakt, numer i procedura z lekcji ma odpowiednik w tym wykazie.

Cyfrowy żłobek, moduł 2, lekcja 2.2 · nagranie 11 minut · linki prowadzą do tekstów w źródłach urzędowych

Kurs: Cyfrowy żłobek, moduł 2 (Cyberhigiena kadry żłobka), lekcja 2.2.

Weryfikacja źródeł: 19.09.2026. Każdy fakt, numer i procedura w prezentacji i w transkrypcji

ma odpowiednik w tej tabeli. Liczby podajemy zawsze z datą i linkiem.

1. Zgłaszanie podejrzanых wiadomości do CERT Polska

Fakt użyty w lekcji	Źródło	Link	Data źródła
Podejrzany SMS przekazujemy na numer 8080 , numer działu od 22 listopada 2023	Portal gov.pl, Baza wiedzy, „Dostałeś niepokojący sms albo email? Zgłoś go do CERT Polska (CSIRT NASK)”	https://www.gov.pl/web/baza-wiedzy/dostales-niepokojacy-sms-albo-email-zglos-go-do-cert-polska-csirt-nask	publikacja 21.03.2023, aktualizowana
Przekazanie SMS na 8080 jest bezpłatne (poza granicami Polski koszt według taryfy operatora)	jak wyżej, cytata: „Przesłanie podejrzanego SMS-a na numer 8080 jest bezpłatne (poza granicami Polski koszt jest zgodny z taryfą operatora).”	jak wyżej	jak wyżej
SMS przekazujemy poleceniem „ Przekaż ” albo „Prześlij dalej”, a gdy telefon tego nie ma, kopiujemy treść i wysyłamy na 8080	jak wyżej, cytata: „Najlepiej posłużyć się poleceniem »Przekaż« (również w innych wariantach słownych, np. »Prześlij dalej«).”	jak wyżej	jak wyżej
Podejrzanе maile i strony zgłaszamy przez incydent.cert.pl albo na adres cert@cert.pl	jak wyżej	https://incydent.cert.pl	jak wyżej
Zgłoszenie trafia do analityków CERT Polska, którzy decydują o wpisaniu domeny na Listę Ostrzeżeń	CERT Polska, Lista Ostrzeżeń	https://cert.pl/lista-ostrzezen/	strona stała

2. Liczby z raportu CERT Polska za 2025 rok

Używane w prezentacji (slajd 2). Raport opublikowany 08.04.2026.

Liczba	Cytat / treść	Link
658 320 zgłoszeń przyjętych w 2025 roku	„Zespół CERT Polska otrzymał w 2025 roku 658 320 zgłoszeń”	https://www.nask.pl/aktualnosci/prawie-2-tys-zgloszen-kazdego-dnia-raport-cert-polska-za-2025-rok

Liczba	Cytat / treść	Link
260 783 unikalne incydenty bezpieczeństwa	„zarejestrowano 260 783 unikalnych incydentów bezpieczeństwa”	jak wyżej
97 procent incydentów to oszustwa komputerowe	„97 proc. incydentów stanowiły oszustwa komputerowe”	jak wyżej
Blisko 80 tysięcy przypadków phishingu, około 30 procent wszystkich incydentów	dane z raportu rocznego	jak wyżej
Blisko 250 tysięcy domen dopisanych do Listy Ostrzeżeń w 2025 roku	„blisko 250 tysięcy w 2025 roku”	jak wyżej
179 incydentów ransomware, wzrost o 21 procent rok do roku	„179 takich incydentów”	jak wyżej
Pełny raport (PDF)	Raport roczny z działalności CERT Polska w 2025 roku	https://cert.pl/posts/2026/04/raport-roczny-2025/ oraz https://cert.pl/uploads/docs/Raport_CP_2025.pdf

W lekcji podajemy tylko dwie z tych liczb (658 320 zgłoszeń i 97 procent), zawsze z nazwą źródła i rokiem, żeby nie robić ze slajdu tablicy statystycznej.

3. Oszustwo pierwsze: podmiana numeru rachunku

Fakt użyty w lekcji	Źródło	Link
Mechanizm: przestępcy podszywają się pod kontrahenta i informują o zmianie numeru rachunku; pieniądze trafiają na konto oszusta	Policja, „Uwaga na oszustwo na podmiannę numeru rachunku bankowego”, 21.08.2019	https://www.policja.pl/pol/aktualnosci/177772,Uwaga-na-oszustwo-na-podmiane-numeru-rachunku-bankowego.html
Wiadomość może przyjść ze skrzynki byłego pracownika, z adresu różniącego się drobnym szczegółem albo jako dokument w identycznej szacie graficznej	jak wyżej	jak wyżej
Sprawdzenie samego adresu nadawcy nie wystarczy	cytat: „Sprawdzenie autentyczności adresu e-mailowego, z którego otrzymaliśmy wiadomość, nie wystarczy.”	jak wyżej
Zalecenie: skontaktować się z partnerem, przedstawić treść wiadomości i zweryfikować, czy jest prawdziwa	cytat: „należy skontaktować się z partnerem biznesowym, przedstawić mu treść wiadomości, którą otrzymaliśmy i zweryfikować, czy jest prawdziwa.”	jak wyżej

Fakt użyty w lekcji	Źródło	Link
Przestępcy przejmują firmową pocztę, czytają korespondencję i uderzają w momencie płatności	Policja mazowiecka, „Fałszywe faktury z podmienionym numerem konta! Firmy na celowniku cyberprzestępców”	https://mazowiecka.policja.gov.pl/ra/aktualnosci/aktualnosci/131942,Falszywe-faktury-z-podmienionym-numerem-konta-Firmy-na-celowniku-cyberprzestepco.html
Zalecenie: porównać numer z wcześniejszą fakturą i skontaktować się z wystawcą	Policja, KPP Łęczna, „Uważajmy na faktury z podmienionym numerem rachunku bankowego”	https://leczna.policja.gov.pl/le/informacje/aktualnosci/147980,Uwazajmy-na-faktury-z-podmienionym-numerem-rachunku-bankowego.html

4. Oszustwo drugie: SMS o dopłacie

Fakt użyty w lekcji	Źródło	Link
Fałszywy SMS o dopłacie do przesyłki to jeden z najczęstszych schematów; pretekst to niedopłata, nadwaga, dezynfekcja	CERT Polska, baza wiedzy, „Fałszywe SMSy”	https://cert.pl/baza-wiedzy/falszywe-smsy/
Strona oszustów wygląda prawie identycznie jak prawdziwa, różni się adresem domenowym	cytat: „Jedyna różnica, z pozoru błaha i trudno dostrzegalna to adres domenowy”	jak wyżej
Drobna kwota to tylko pretekst, celem są dane logowania i dane karty	cytat: „te kilka złotych to jedynie pretekst, by poznać dane”	jak wyżej
Sygnały phishingu: presja czasu, silna emocja, drobna kwota, nietypowy kanał, nieoczekiwany kontakt	CERT Polska, baza wiedzy, „Phishing: jak rozpoznać oszustwo i nie dać się nabrać”	https://wiedza.cert.pl/bezpieczenstwo-osobiste/rozpoznanie-phishingu/
Zasada: prośbę o pieniądze albo dane potwierdzamy innym kanałem, niezależnie od tego, kto ją rzekomo wysłał	jak wyżej	jak wyżej
Po szkodzie: kontakt z bankiem, zmiana hasła, zgłoszenie na Policję	jak wyżej	jak wyżej
Ostrzeżenie o SMS-ach o uzupełnieniu danych przesyłki	Policja mazowiecka, KPP w Grójcu	https://mazowiecka.policja.gov.pl/wgr/aktualnosci/89997,OTRZYMALES-SMS-Z-INFORMACJA-O-KONIECZNOSCI-UZUPELNIENIA-DANYCH-PRZESYLKI-UWAZAJ-.html

5. Oszustwo trzecie: „to mój nowy numer” i podszywanie się pod rodzica albo dyrektora

Fakt użyty w lekcji	Źródło	Link
Mechanizm: wiadomość z nieznanego numeru, prośba o przeniesienie rozmowy na komunikator, potem prośba o pilny przelew	Policja, KMP w Wałbrzychu, „Mamo, zepsuł mi się telefon, to nowy numer, napisz do mnie. Uważaj, to oszustwo”, 16.05.2025	https://walbrzych.policja.gov.pl/dba/aktualnosci/bieza/145577,MAMO-ZEPSUL-MI-SIE-TELEFON-TO-NOWY-NUMER-NAPISZ-DO-MNIE-UWAZAJ-TO-OSZUSTWO.html
Zalecenie: zawsze zweryfikować, czy wiadomość pochodzi od znanej osoby, najlepiej krótkim telefonem	cytat: „Zawsze weryfikuj, czy wiadomość faktycznie pochodzi od bliskiej osoby, najlepiej wykonaj krótki telefon.”	jak wyżej
Zalecenie: nie przysyłać pieniędzy na prośbę z SMS albo komunikatora bez pewności, kto jest po drugiej stronie	cytat z tej samej publikacji	jak wyżej
Zalecenie: nigdy nie podawać kodów BLIK ani danych do przelewów osobom, których tożsamości nie potwierdzono	cytat z tej samej publikacji	jak wyżej
Kodem BLIK nie da się odebrać przelewu; prośba o kod BLIK oznacza próbę zapłaty albo wypłaty z konta	Policja, KPP w Cieszynie, „Oszustwo na Blika, co musisz wiedzieć”	https://cieszyn.policja.gov.pl/ka6/informacje/wiadomosci/428777,Oszustwo-quotna-Blikaquot-co-musisz-wiedziec.html
Spoofing, czyli podszywanie się pod cudzy numer telefonu, jest technicznie możliwe, więc sam wyświetlony numer nie jest dowodem tożsamości	Centralne Biuro Zwalczania Cyberprzestępczości, „Spoofing czyli podszywanie się pod inny numer telefonu”	https://cbzc.policja.gov.pl/bzc/aktualnosci/242,Spoofing-czyli-podszywanie-sie-pod-inny-numer-telefonu-Jak-sie-bronic.html

6. Po incydencie: kogo powiadomić

Fakt użyty w lekcji	Źródło	Link
Administrator zgłasza naruszenie ochrony danych Prezesowi UODO bez zbędnej zwłoki, w miarę możliwości nie później niż w terminie 72 godzin po stwierdzeniu naruszenia (art. 33 RODO)	UODO, „W jakim terminie należy zgłosić naruszenie Prezesowi UODO?”	https://uodo.gov.pl/pl/525/2584
Termin 72 godzin liczy się od stwierdzenia naruszenia przez administratora	jak wyżej	jak wyżej
Zgłoszenie nie jest wymagane, jeśli jest mało prawdopodobne, by naruszenie skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych	jak wyżej	jak wyżej
Gdy w 72 godzinach nie ma kompletu informacji, składa się zgłoszenie wstępne i uzupełnia je później	UODO, Zgłaszanie naruszeń	https://uodo.gov.pl/pl/492/2278

Fakt użyty w lekcji	Źródło	Link
Przy wysokim ryzyku administrator zawiadamia też osoby, których dane dotyczą (art. 34 RODO)	UODO, Zgłaszanie naruszeń	https://uodo.gov.pl/525
Zgłoszenie składa się elektronicznie przez e-usługę „Zgłoś naruszenie ochrony danych osobowych” na biznes.gov.pl , podpisane podpisem kwalifikowanym albo profilem zaufanym; usługa jest bezpłatna	biznes.gov.pl , opis usługi	https://www.biznes.gov.pl/pl/portal/ou889
Zgłoszenie robi administrator (placówka reprezentowana przez dyrektora), nie pojedyncza opiekunka	biznes.gov.pl , opis usługi: „administrator, przedsiębiorca lub jednostka publiczna przetwarzająca dane osobowe”	jak wyżej
Incydent zgłaszamy do CERT Polska przez incydent.cert.pl , podejrzany SMS na 8080	CERT Polska	https://incydent.cert.pl oraz https://cert.pl/
Oszustwo zgłaszamy na Policję	Policja, publikacje wymienione w sekcjach 3 do 5	https://www.policja.pl/

8. Czego świadomie nie używamy

- Nie podajemy liczb o skali oszustw w żłobkach i przedszkolach. Nie ma publicznej statystyki

branżowej, a szacunek bez źródła łamałby zasadę „żadnych liczb bez źródła”.

- Nie opisujemy prawdziwych placówek ani prawdziwych spraw. Wszystkie przykłady w prezentacji

są opisane jako typowe scenariusze, a dane w makietach są fikcyjne.

- W makietach nie pojawia się żadna prawdziwa marka: firma kurierska, bank, operator i dostawca

pożytków występują jako opisy, nie jako nazwy.

- Nie używamy sformułowania „największa konferencja”, „pierwsza platforma” i innych superlatywów

Materiał wyjaśnia przepisy i dobre praktyki. Nie jest poradą prawną i nie zastępuje inspektora ochrony danych ani prawnika placówki. Stan prawny na 20.09.2026. Quality Island Sp. z o.o., ul. Grzybowska 87, 00-844 Warszawa, KRS 0000972652, NIP 5273002880. Pełna lekcja i pozostałe materiały: <https://cyfrowyzlobek.pl/lekcje-otwarte>