DIGITAL SECURITY
FOR SENIOR CITIZENS

2020-1-PL01-KA204-082121

Ramy kompetencji w zakresie bezpieczeństwa cyfrowego

Ten project został zrealizowany przy wsparciu finansowym Komisi Europejskiej. Niniejsza publikacja odzwierciedla jedynie stanowisko autora i Komisja Europejska nie ponosi odpowiedzialności za umieszczoną w niej zawartość merytoryczną.

Partnerzy

Cuiablue Ltd, UK

CWEP, Polska

FyG Consultores, Hiszpania

eSeniors, Francja

Innovation Hive, Grecja

Spis treści

Ramy

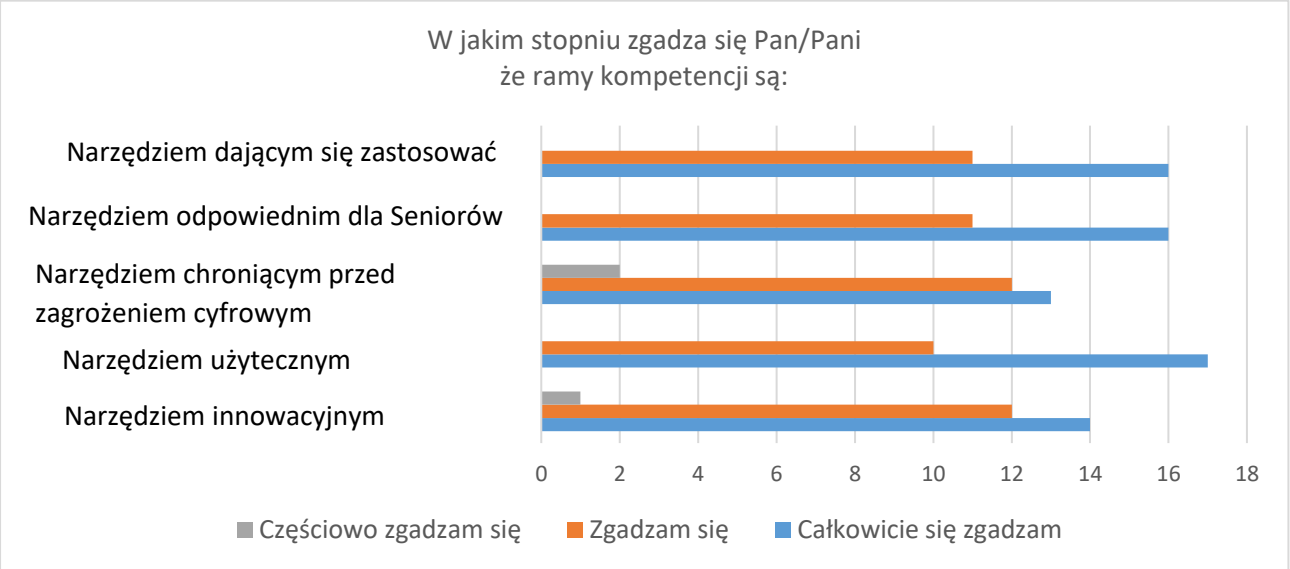
Niniejsze ramy zostały opracowane jako część pierwszego rezultatu w ramach projektu DiSC (Digital Security for Senior Citizens). W szerszym zakresie projektu DiSC, niniejszy materiał ma na celu wsparcie zespołu projektowego w budowaniu cyfrowych zdolności seniorów do rozpoznawania i proaktywnego reagowania na zagrożenia cyfrowe i oszustwa, a także stworzenie podstaw do wdrożenia i upowszechnienia ukierunkowanej polityki bezpieczeństwa cyfrowego na poziomie europejskim. Niniejsze ramy stanowią zaledwie jeden mały krok w kierunku osiągnięcia obu tych celów.

Metodologia

Konsorcjum omówiło i uzgodniło podejście metodologiczne do opracowania ram podczas spotkania inaugurującego projekt w grudniu 2020 roku. Po pierwsze, opracowano zestaw kwestionariuszy do spotkań konsultacyjnych z interesariuszami oraz szablon do analizy źródeł wtórnych, który został odpowiednio dostosowany i poprawiony, tak aby partnerzy mogli rozpocząć zbieranie informacji na temat aktualnego stanu wiedzy w zakresie bezpieczeństwa cyfrowego, porad, wytycznych i polityki na poziomie krajowym w każdym z reprezentowanych krajów. Podczas gdy konsorcjum prowadziło badania źródeł wtórnych, opracowano wstępny projekt ram. Po podsumowaniu i przeanalizowaniu wyników badań źródeł wtórnych oraz uwzględnieniu informacji zwrotnych otrzymanych podczas spotkań konsultacyjnych z zainteresowanymi stronami, opracowano drugą iterację ram, która została poddana komentarzom i uwagom konsorcjum. Po uwzględnieniu uwag i komentarzy, sfinalizowana wersja ram została przetłumaczona i przetestowana przez szersze grupy interesariuszy i użytkowników końcowych.

Konsultacje z zainteresowanymi stronami

W ramach podejścia projektu DiSC polegającego na współtworzeniu produktów projektu, poniżej znajduje się podsumowanie istotnych danych zebranych podczas pierwszych spotkań konsultacyjnych z interesariuszami na początku 2021 roku przez wszystkich partnerów projektu. Stwierdzenia odnoszące się do ram kompetencji są podsumowane poniżej, po czym interesariusze zostali poproszeni o skomentowanie swojej decyzji lub dodanie jakichkolwiek przemyśleń na temat ram.



Następnie poproszono interesariuszy o uzupełnienie odpowiedzi ilościowych poprzez udzielenie odpowiedzi na pytanie: "Czy masz jakieś uwagi lub zalecenia, które pomogłyby nam udoskonalić Ramy kompetencji w zakresie bezpieczeństwa cyfrowego? ". Interesariuszom udostępniono otwarte pole tekstowe, w którym mogli przedstawić swoje uwagi, przemyślenia lub ogólne wrażenia dotyczące koncepcji.

Konkretne zalecenia obejmowały zapewnienie odpowiedniego słownictwa zrozumiałego dla osób starszych oraz skupienie się na podstawowych, osiągalnych wymaganiach w celu zapewnienia dostępności i wykorzystania materiału. Kolejnym zaleceniem było zapewnienie użytkownikom środków i zasobów do rozwijania każdej z kompetencji, co potwierdza potrzebę rozwijania kolejnych rezultatów projektu (IO2 i IO3).

Najczęściej otrzymywaną rekomendacją było to, aby ramy uwzględniały najnowsze i szybko postępujące zmiany technologiczne oraz związane z nimi kwestie cyberbezpieczeństwa; dobrym przykładem są kryptowaluty i setki stale ewoluujących, kreatywnych podejść, które cyberprzestępcy stosują, aby próbować ukraść takie waluty. To właśnie w tym kontekście konsorcjum DiSC stoi przed największym wyzwaniem przy opracowywaniu ram: muszą one być wystarczająco wszechstronne, aby objąć szeroki zakres różnych wymaganych umiejętności i wiedzy, ale także wystarczająco elastyczne, aby dostosować się do przyszłych innowacji.

Badanie dokumentacji

Drugi etap podjęty przez konsorcjum skupił się na zebraniu istotnych informacji, porad, wskazówek i dokumentów polityki krajowej, które pomogłyby określić kontekst, w jakim ramy kompetencji w zakresie bezpieczeństwa cyfrowego funkcjonują zarówno na poziomie krajowym w każdym z krajów partnerskich, jak i na poziomie europejskim. W sumie konsorcjum przeanalizowało 10 istotnych dokumentów, po dwa dokumenty z Polski, Wielkiej Brytanii, Grecji, Francji i Hiszpanii; zostały one podsumowane poniżej. Wszystkie analizy dokumentów znajdują się w załączniku na końcu tego dokumentu.

Grecka krajowa strategia bezpieczeństwa cybernetycznego na lata 2020-2025: obejmuje krajowy plan na lata 2020-2025, w tym cele strategiczne, priorytety, środki polityczne i regulacyjne mające na celu zapewnienie wysokiego poziomu bezpieczeństwa komunikacji cyfrowej i systemów informacyjnych na poziomie krajowym. Kampania greckiego wydziału ds. cyberprzestępczości na temat mobilnego złośliwego oprogramowania przedstawia istotne informacje i pomysły dotyczące form zagrożeń cyfrowych oraz sposobów, w jakie hakerzy mogą naruszyć dane osobowe obywateli.

We Francji dwa dokumenty, które poddano przeglądowi, to strona internetowa poświęcona nadzorowi nad bezpieczeństwem cybernetycznym, opublikowana w 2021 r. przez rząd francuski, oraz zwięzły dokument CNIL (Krajowej Komisji ds. Informatyki i Wolności) zatytułowany "10 wskazówek CNIL, jak zachować bezpieczeństwo w sieci". Oba dokumenty zostały opublikowane w celu zwiększenia świadomości i budowania zdolności do radzenia sobie z zagrożeniami cybernetycznymi wśród wszystkich obywateli. Oba dokumenty funkcjonują jako dwa różne projekty oraz przedstawiają różne poziomy informacji. Dzięki tym różnicom, oba dokumenty dobrze pasują do projektu DiSC pod względem sposobów, w jaki konsorcjum projektu DiSC będzie angażować i prezentować informacje użytkownikom końcowym.

W Polsce badania koncentrowały się na oficjalnym przewodniku dla obywateli w zakresie bezpieczeństwa cybernetycznego, opracowanym i opublikowanym przez polski rząd "Jak chronić się przed cyberatakami". Dokument ten stanowi punkt odniesienia, co można uznać za podstawową wiedzę na temat korzystania z Internetu, a w szczególności z mediów społecznościowych, i dlatego może być brany pod uwagę przy opracowywaniu ram oraz potencjalnie dostosowany i uwzględniony. Drugim dokumentem jest przewodnik opracowany w ramach innego projektu europejskiego. Dokument ten zawiera wskazówki dotyczące niezbędnej wiedzy i świadomości, którą wszyscy obywatele mogliby posiadać na poziomie podstawowym, a zatem można by je wziąć pod uwagę przy opracowywaniu ram oraz ewentualnie dostosować. Informacje zawarte w obu dokumentach zawierają istotne treści, które mają wartość w zastosowaniu projektu DiSC i są możliwe do zastosowania w wielu różnych kontekstach indywidualnych i rodzinnych.

Badania hiszpańskie doprowadziły partnerów do Narodowej Strategii Bezpieczeństwa Cybernetycznego na rok 2019 opublikowanej przez Krajową Radę Bezpieczeństwa Rządu Hiszpanii, która określa dyrektywy w ramach ogólnych kierunków działania w celu rozwiązania wyzwania, jakim jest dla kraju podatność na zagrożenia w cyberprzestrzeni. Drugą publikacją w ramach badania jest "Żyj bezpiecznie w Internecie: Nigdy nie jest za późno, aby korzystać z bezpieczniejszego Internetu", wydana przez Organización de Consumidores y Usuarios (OCU). Zawiera ona szereg praktycznych poradników dla różnych grup społecznych, w tym dzieci, rodziców, dorosłych i seniorów. Dla seniorów przewodnik oferuje zalecenia, dzięki którym mogą oni nauczyć się korzystać ze wszystkich zalet Internetu, bez względu na swój wiek.

Badanie w Wielkiej Brytanii skupiło się na stronie internetowej Krajowego Centrum Cyberbezpieczeństwa (National Advice and Guidance). Dostarczane informacje są osadzone w szerszym celu, jakim jest ochrona Wielkiej Brytanii, a zatem są skierowane do wszystkich obywateli, co znajduje odzwierciedlenie w treści. Drugim dokumentem jest Narodowa Strategia Bezpieczeństwa Cybernetycznego Rządu Wielkiej Brytanii na lata 2016-2021, która zapewnia kompleksowy przegląd strategicznych zagrożeń dla rządu, przedsiębiorstw i społeczeństwa, a zatem, chociaż jest istotna dla projektu DiSC, tylko w niewielkim stopniu obejmuje obszary, których dotyczy niniejszy projekt. Wyczerpująca lista rodzajów zagrożeń jest bardzo istotna dla projektu i jego całości.

Podsumowując, analiza dokumentacji dostarczyła informacji na temat rozwoju ram poprzez przedstawienie kwestii związanych z bezpieczeństwem cybernetycznym, zagrożeń i terminologii stosowanej w każdym z kontekstów krajowych. Prezentacja i analiza różnych form przekazywania informacji stosowanych w odniesieniu do różnych grup docelowych miała również duży wpływ na kierunek rozwoju ram kompetencyjnych, ponieważ pewna terminologia i sposób przedstawiania informacji ma duże znaczenie dla osób starszych, co zostało potwierdzone w podobnych materiałach na poziomie krajowym. Wszystkie kraje partnerskie przekazują pewien rodzaj informacji dla seniorów w kontekście krajowym, albo w sposób szczególny, albo w ramach szerszej kampanii podnoszenia świadomości dla grup społecznych, a mimo to, po zakończeniu prac, ramy będą samodzielne pod względem zapewnienia zestawu odpowiednich kompetencji wymaganych do zwiększenia osobistych zdolności do łagodzenia skutków zagrożeń cybernetycznych.

Wprowadzenie do zasad ramowych

Ramy kompetencji są skuteczną metodą oceny, utrzymania i monitorowania wiedzy, umiejętności i atrybutów grup docelowych w zakresie świadomości, reaktywności i proaktywności w zakresie bezpieczeństwa cybernetycznego. Ramy DiSC zostały opracowane w oparciu o ramy kompetencji cyfrowychDigcomp, które nie obejmują bezpośrednio bezpieczeństwa przed agresywnymi atakami cybernetycznymi, spamem i sztuczkami oszustów wykorzystywanymi do kradzieży danych i informacji online.

W szerszym ujęciu, te kompetencje i umiejętności opierają się na punktach 4.1 i 4.2 ram DigComp 2.1:

4.1 Ochrona urządzeń - ochrona urządzeń i treści cyfrowych oraz rozumienie ryzyka i zagrożeń w środowisku cyfrowym. Znajomość środków bezpieczeństwa i ochrony oraz dbałość o niezawodność i prywatność.

4.2 Ochrona danych osobowych i prywatności - Ochrona danych osobowych i prywatności w środowiskach cyfrowych. Zrozumienie, jak używać i dzielić się informacjami umożliwiającymi identyfikację osoby, będąc w stanie chronić siebie i innych przed szkodami. Zrozumienie, że usługi cyfrowe wykorzystują "Politykę prywatności", aby poinformować, jak wykorzystywane są dane osobowe.

Konsorcjum projektu DiSC podzieliło punkt 4.1 ochrona urządzeń oraz 4.2 ochrona danych osobowych i prywatności na pięć podsekcji, które zostały wykorzystane do sklasyfikowania odpowiednich kompetencji w zakresie bezpieczeństwa cyfrowego:

1. Świadomość zagrożeń: świadomość różnych rodzajów zagrożeń dla bezpieczeństwa cyfrowego
2. Zrozumienie zagrożeń: wiedza na temat ryzyka związanego z zagrożeniami dla bezpieczeństwa cyfrowego
3. Planowanie: przygotowanie się
4. Wykrywanie zagrożeń: zastosowanie krytycznego i analitycznego myślenia do potencjalnych zagrożeń bezpieczeństwa cyfrowego
5. Przeciwdziałanie zagrożeniom: rozwiązywanie problemów w celu przeciwdziałania zagrożeniom i naruszeniom.

Ustanowienie ram kompetencji w zakresie bezpieczeństwa cyfrowego umożliwi zespołowi projektowemu DiSC zdefiniowanie wiedzy i umiejętności z zakresu bezpieczeństwa cybernetycznego wymaganych do radzenia sobie z potencjalnymi zagrożeniami, określenie konkretnych kompetencji w zakresie bezpieczeństwa cybernetycznego w formie zestawów tematów oraz wspieranie rozwoju i proponowanie konkretnych szkoleń osobistych i zawodowych oraz możliwości dla grup docelowych w oparciu o te ramy.

Docelowymi użytkownikami końcowymi ram kompetencji są seniorzy w wieku 55+. Oczekuje się, że ramy będą również istotne i interesujące dla nauczycieli ICT, trenerów, edukatorów i praktyków pracujących w dziedzinie budowania potencjału technologicznego seniorów.

Ramy kompetencji w zakresie bezpieczeństwa cyfrowego mają na celu zdefiniowanie umiejętności, wiedzy i postaw kluczowych kompetencji potrzebnych seniorom do skutecznego włączania protokołów bezpieczeństwa cyfrowego do ich lokalnych kontekstów,

a także zapewnienie unijnych ram odniesienia dla rozwoju i oceny kompetencji w zakresie bezpieczeństwa cyfrowego.

Zakres

W celu zdefiniowania zakresu ram partnerzy określili urządzenia, podejście i metody uwzględniane podczas stosowania ram kompetencji informatycznych. Pomoże to rozróżnić inne rodzaje działalności przestępczej, które nie są objęte kompetencjami zawartymi w ramach.

Urządzenia: urządzenie użyte do skontaktowania się z ofiarą oszustwa

- Telefony komórkowe i smartfony
- Komputery i Laptopy
- Tablety

Podejście: technika wykorzystana do oszukania ofiary

- Wyłudzanie informacji: oszukańcza próba uzyskania poufnych informacji lub danych, takich jak nazwy użytkowników, hasła i szczegóły kart kredytowych, poprzez podszywanie się pod godny zaufania podmiot w komunikacji elektronicznej.
- Wyłudzanie informacji: Phishing głosowy to forma przestępczego oszustwa telefonicznego, wykorzystująca inżynierię społeczną za pośrednictwem systemu telefonicznego w celu uzyskania dostępu do prywatnych informacji osobistych i finansowych dla uzyskania korzyści finansowych.
- Smishing (SMS Phishing): Działanie, które umożliwia przestępcom kradzież pieniędzy lub tożsamości ofiary, lub obu tych rzeczy, w wyniku odpowiedzi na wiadomość tekstową. Smishing wykorzystuje telefon komórkowy (smartfon lub tradycyjny telefon niepodłączony do Internetu) do manipulowania ludźmi w celu podjęcia różnych działań, które prowadzą do wyłudzenia pieniędzy.
- Oszustwo programowe: Działanie, w którym oszust wykorzystuje fałszywe lub skopiowane oprogramowanie, takie jak aplikacja lub program, w celu uzyskania dostępu do danych na urządzeniu cyfrowym, które następnie wykorzystuje do kradzieży pieniędzy lub tożsamości ofiary.
- Inżynieria społeczna: Termin używany dla szerokiego zakresu złośliwych działań realizowanych poprzez interakcje międzyludzkie. Wykorzystuje manipulację psychologiczną w celu nakłonienia użytkowników do popełnienia błędów bezpieczeństwa lub przekazania poufnych informacji.

Metoda: zamierzone oszustwo

- Phishing - oszustwo z wykorzystaniem poczty elektronicznej
- Oszustwo bogatego "księcia"
- Oszustwo związane z kartkami okolicznościowymi
- Oszustwo dotyczące kredytu bankowego lub karty kredytowej
- Oszustwo loteryjne

- Oszustwo wymuszenia
- Romans / oszustwo randkowe online
- Fałszywe oprogramowanie antywirusowe
- Oszustwo polegające na podszywaniu się pod Facebooka/porwanym profilu
- Oszustwa typu "Zarabiaj pieniądze szybko!"
- Oszustwa związane z podróżowaniem
- Oszustwa kryptowalutowe
    - Fałszywe giełdy Bitcoin
    - Systemy Ponzi
    - Codzienne próby wyłudzeń
    - Złośliwe oprogramowanie
- Oszustwo związane z fałszywymi wiadomościami
- Fałszywe strony internetowe z zakupami
- Oszustwa związane z ofertami pracy
- Wyłudzanie SMS-ów (Smishing)
- Oszustwo internetowe związane z nadpłatą
- Oszustwa online związane z pomocą techniczną

Uwaga: zagrożenia cyfrowe stale się zmieniają i ewoluują, a ze względu na ich charakter nie jest możliwe sporządzenie wyczerpującej listy. Aby być na bieżąco z zagrożeniami, DiSC zaleca subskrybowanie organizacji lub sieci zajmującej się bezpieczeństwem cybernetycznym, takiej jak na przykład HeimdalSecurity, która regularnie publikuje aktualizacje dotyczące kwestii, podejść i metod związanych z bezpieczeństwem cybernetycznym, lub strony Europolu poświęconej obszarom trendów przestępczości.

Ramy

Kompetencje podstawowe	Poziomy biegłości		
Deskryptory	Podstawowy Osoba rozumie podstawowe pojęcia, umiejętności i wymagania dotyczące wiedzy z zakresu bezpieczeństwa	Średniozaawansowany Osoba wykazuje krytyczne myślenie w odniesieniu do bezpieczeństwa cyfrowego, potrafi rozróżniać zagrożenia	Zaawansowane Osoba wykazuje się analitycznym myśleniem w zakresie bezpieczeństwa cyfrowego i potrafi reagować na

	cyfrowego i jest przygotowana do osiągnięcia najwyższego poziomu kompetencji, do którego jest zdolna.	cyfrowe na wszystkich urządzeniach oraz jest w stanie samodzielnie zaplanować i skutecznie przeprowadzić działania łagodzące w celu ochrony przed nimi.	zagrożenia w czasie rzeczywistym, oceniając i wybierając najskuteczniejszą reakcję w sytuacji wysokiego ciśnienia.

1. Świadomość zagrożeń

Świadomość zagrożeń	Podstawowy	Średniozaawansowany	Zaawansowane
Znajomość specyficznych zagrożeń, których celem są urządzenia cyfrowe.	Jestem świadomy typowych metod zagrożeń bezpieczeństwa cyfrowego.	Wiem o mniej popularnych metodach zagrożenia bezpieczeństwa cyfrowego.	Jestem na bieżąco z nowymi podejściami do bezpieczeństwa cyfrowego w miarę ich rozwoju.
	Znam typowe metody zagrożenia bezpieczeństwa cyfrowego.	Zdaję sobie sprawę z mniej popularnych metod zagrożenia bezpieczeństwa cyfrowego.	Jestem na bieżąco z nowymi metodami zabezpieczeń cyfrowych w miarę ich rozwoju.
	Jestem świadomy podstawowych działań socjotechnicznych w kontekście bezpieczeństwa cyfrowego.	Znam bardziej złożone techniki inżynierii społecznej.	Jestem świadomy różnych kombinacji technik, podejść i metod inżynierii społecznej.

2. Zrozumienie zagrożenia

Zrozumienie zagrożenia	Podstawowy	Średniozaawansowany	Zaawansowane
Znajomość cech i funkcji każdego z zagrożeń. Ocena zagrożeń cyfrowych i poziomu ryzyka z nimi związanego. Zrozumienie zmieniającego się charakteru zagrożeń cyfrowych. Świadomość znaczenia wiarygodnych, aktualnych i dokładnych źródeł informacji	Rozumiem kluczowe cechy i funkcje najbardziej powszechnych zagrożeń bezpieczeństwa cyfrowego.	Rozumiem kluczowe cechy i funkcje najrzadszych i najbardziej niezwykłych zagrożeń bezpieczeństwa cyfrowego.	Aktywnie odświeżam swoją wiedzę na temat zagrożeń cyfrowych poprzez wiarygodne, aktualne i dokładne źródła informacji na temat bezpieczeństwa.
	Rozumiem poziom ryzyka i potencjalne konsekwencje związane z prostymi zagrożeniami bezpieczeństwa cyfrowego.	Rozumiem poziom ryzyka i potencjalne konsekwencje związane z wieloaspektowymi zagrożeniami bezpieczeństwa cyfrowego.	Rozumiem poziom ryzyka i potencjalne konsekwencje związane ze złożonymi zagrożeniami bezpieczeństwa cyfrowego.

o bezpieczeństwie.			

3. Łagodzenie skutków

Łagodzenie skutków	Podstawowy	Średniozaawansowany	Zaawansowane
Umiejętności i doświadczenie umożliwiające podejmowanie świadomych decyzji w zakresie ochrony przed zagrożeniami cyfrowymi. Znajomość i zrozumienie różnych narzędzi i zasobów służących do ochrony przed zagrożeniami.	Potrafię zidentyfikować odpowiednie narzędzia ochrony cyfrowej w celu zmniejszenia zagrożeń dla bezpieczeństwa cyfrowego.	Potrafię wykorzystać moje wcześniejsze doświadczenia i umiejętności do podejmowania decyzji dotyczących ochrony przed zagrożeniami bezpieczeństwa cyfrowego.	Potrafię wykorzystać swoje doświadczenie i umiejętności do analizy potencjalnych skutków różnych zagrożeń i odpowiednio dobrać strategie ochrony.
	Potrafię stosować się do podstawowych instrukcji bezpieczeństwa cyfrowego w celu zmniejszenia zagrożeń bezpieczeństwa cyfrowego.	Potrafię zdecydować o wyborze najbardziej odpowiednich podstawowych narzędzi bezpieczeństwa cyfrowego w celu zmniejszenia zagrożeń bezpieczeństwa cyfrowego.	Potrafię analizować i oceniać zagrożenia dla bezpieczeństwa cyfrowego oraz dostosować strategię ochrony do tych zagrożeń.
	Wiem, jak skonfigurować urządzenie cyfrowe, aby zapewnić ochronę przed podstawowymi zagrożeniami bezpieczeństwa cyfrowego.	Wiem, jak sprawdzić i zaktualizować urządzenie cyfrowe, aby zapewnić odpowiednią ochronę przed najczęstszymi zagrożeniami bezpieczeństwa cyfrowego.	Wiem, jak zainstalować narzędzia i oprogramowanie ochronne na urządzeniach cyfrowych w celu ograniczenia zagrożeń cyfrowych.

4. Wykrywanie zagrożeń

Wykrywanie zagrożeń	Podstawowy	Średniozaawansowany	Zaawansowane
Umiejętność rozpoznawania zagrożeń cyfrowych i specyficznego	Potrafię rozpoznać i zidentyfikować najczęstsze zagrożenia bezpieczeństwa cyfrowego dla moich	Potrafię rozpoznać i zidentyfikować większość rzadkich i nietypowych zagrożeń bezpieczeństwa cyfrowego dla moich	Aktywnie utrzymuję świadomość zagrożeń bezpieczeństwa cyfrowego poprzez wiarygodne, aktualne

ryzyka z nimi związanego Wiedza umożliwiająca kategoryzację zagrożeń cyfrowych według poziomu ryzyka	danych osobowych i informacji.	danych osobowych i informacji.	i dokładne źródła informacji na temat bezpieczeństwa.
	Potrafię rozpoznawać jasne i oczywiste ryzyka i zagrożenia w środowiskach cyfrowych.	Potrafię rozpoznać niejasne zagrożenia bezpieczeństwa cyfrowego.	Potrafię rozpoznawać złożone ryzyka i zagrożenia w środowiskach cyfrowych.
	Potrafię wykorzystać swoją wiedzę do oceny potencjalnych zagrożeń bezpieczeństwa i zdecydować, czy są one podejrzane.	Potrafię wykorzystać moje analityczne podejście do bezpieczeństwa cyfrowego, aby wskazać cyfrowe zagrożenia.	Potrafię wykorzystać umiejętność krytycznego myślenia do analizowania, porównywania i oceniania zakresu zagrożenia cyfrowego i związanego z nim poziomu ryzyka.

5. Przeciwdziałanie zagrożeniom

Przeciwdziałanie zagrożeniom	Podstawowy	Średniozaawansowany	Zaawansowane
Podejmowanie pozytywnych, skutecznych decyzji przy jednoczesnym zachowaniu spokoju Siła psychiczna do radzenia sobie z niepewnością, stresem i trudnymi sytuacjami.	Jestem elastyczny i dobrze przygotowany na cyfrowe zagrożenia bezpieczeństwa.	Wykorzystuję zdolności adaptacyjne, aby przeciwdziałać cyfrowym zagrożeniom bezpieczeństwa.	Aktywnie przewiduję zagrożenia bezpieczeństwa cyfrowego i ryzyko z nimi związane oraz ćwiczę umiejętność dostosowania się do nich.
	Pozostaję pozytywnie nastawiony w obliczu zagrożeń lub naruszeń bezpieczeństwa cyfrowego.	Potrafię wykorzystać własne doświadczenia, aby z optymizmem i pewnością siebie podchodzić do potencjalnych zagrożeń i naruszeń.	Potrafię wyjaśnić, w jaki sposób pozytywna postawa, zachowania i działania wobec bezpieczeństwa cyfrowego przyczyniły się do mojego bezpieczeństwa cyfrowego.

	Mogę zastanowić się nad napotkanymi zagrożeniami i wyciągnąć z nich wnioski.	Mogę zastanowić się nad napotkanymi zagrożeniami i zmienić swoje zachowanie oraz postawę wobec zagrożeń cyfrowych, aby stać się bardziej odpornym na nie.	Mogę zastanowić się nad napotkanymi zagrożeniami i zmienić swoje zachowanie i postawę w życiu, aby stać się bardziej odporną osobą.