Data: ..... **Nazwa:** .....

Połącz w pary

1. Tomek dostał zadanie domowe o Mikołaju Koperniku. Wszedł na stronę znanej encyklopedii dla dzieci, żeby znaleźć potrzebne informacje i zdjęcia

2. Basia dostała na komunikatorze wiadomość: „Prześlij tę wiadomość do 10 osób, a jutro spotka Cię szczęście. Jeśli tego nie zrobisz, będziesz mieć pecha!”.

3. Marek dużo rozmawiał na czacie w grze z graczem o pseudonimie „King_25”. Pewnego dnia „King_25” napisał: „Jesteś super. Może spotkamy się jutro po szkole w parku? Mam na imię Bartek i mam 11 lat”.

4. Kasia umówiła się z dziadkami, którzy mieszkają w innym mieście, na rozmowę wideo. Pokazała im swój nowy rysunek i opowiedziała, co dostała na urodziny.

5. Podczas grania w grę na ekranie pojawiło się okienko: „GRATULACJE! Wygrałeś 10 000 monet do gry! Aby je odebrać, podaj swój login i hasło na tej stronie”.

6. Karolina zobaczyła, że ktoś z jej równoległej klasy założył w mediach społecznościowych grupę, na której publikuje przerobione, ośmieszające zdjęcia innych uczniów, w tym jej koleżanki.

7. Paweł znalazł w internecie fajny quiz „Którą postacią z bajki jesteś?”. Żeby zobaczyć wynik, strona prosi go o podanie swojego adresu e-mail.

8. Ania i jej najlepszy przyjaciel z klasy, Piotrek, grają razem online w swoją ulubioną grę. Rozmawiają na czacie głosowym, używając swoich pseudonimów z gry.

1. Taka wiadomość to spam (niechciana wiadomość). Chociaż nie kradnie haseł, próbuje manipulować emocjami (strachem przed pechem) i zaśmieca internet. Co robić? Najlepiej skasować wiadomość i nie wysyłać jej dalej.

2. To jest cyberprzemoc – krzywdzenie innych za pomocą internetu. Jest to bardzo raniące i niedopuszczalne. Co robić? Nie dołączać do takiej grupy ani nie lajkować postów. Zrobić zrzut ekranu jako dowód i natychmiast pokazać to rodzicom, wychowawcy lub szkolnemu pedagogowi.

3. Nigdy nie wiemy, kim naprawdę jest osoba po drugiej stronie ekranu. Może to być dorosły, który udaje dziecko i ma złe zamiary. Co robić? Nigdy nie zgadzać się na spotkanie. Od razu powiedzieć o tej propozycji rodzicom. Pokaż im rozmowę i zablokuj tę osobę

4. Korzysta ze sprawdzonego, edukacyjnego źródła w celu nauki. Nie wchodzi na przypadkowe strony i realizuje konkretny, szkolny cel.

5. Dzieci grają ze sobą, znają się w świecie rzeczywistym i nie udostępniają prywatnych informacji publicznie. To bezpieczna forma wspólnej zabawy.

6. Rozmawia z osobami, które zna i którym ufa. Używa internetu do podtrzymywania więzi z rodziną, co jest wspaniałym zastosowaniem technologii.

7. Adres e-mail to prywatna informacja. Strona prawdopodobnie nie jest groźna, ale może zacząć wysyłać na ten adres dużo reklam. Co robić? Nie podawać swojego e-maila dla zabawy. Jeśli bardzo chcesz zobaczyć wynik, zapytaj rodzica, czy możecie użyć jego „zapasowego” adresu do takich celów.

8. To klasyczna próba oszustwa (phishing) w celu kradzieży konta. Prawdziwi twórcy gier nigdy nie proszą o hasło w ten sposób. Co robić? Natychmiast zamknąć okienko. Nigdy, pod żadnym pozorem, nie podawać nikomu swojego hasła.

NASK cyber profilaktyka NASK Ministerstwo Cyfryzacji PROJEKT FINANSOWANY ZE ŚRODKÓW MINISTERSTWA CYFRYZACJI

POPRAWNE ODPOWIEDZI

SYTUACJA	WYJAŚNIENE
Tomek dostał zadanie domowe o Mikołaju Koperniku. Wszedł na stronę znanej encyklopedii dla dzieci, żeby znaleźć potrzebne informacje i zdjęcia.	Korzysta ze sprawdzonego, edukacyjnego źródła w celu nauki. Nie wchodzi na przypadkowe strony i realizuje konkretny, szkolny cel.
Basia dostała na komunikatorze wiadomość: „Prześlij tę wiadomość do 10 osób, a jutro spotka Cię szczęście. Jeśli tego nie zrobisz, będziesz mieć pecha!”.	Taka wiadomość to spam (niechciana wiadomość). Chociaż nie kradnie haseł, próbuje manipulować emocjami (strachem przed pechem) i zaśmieca internet. **Co robić?** Najlepiej skasować wiadomość i nie wysyłać jej dalej.
Marek dużo rozmawiał na czacie w grze z graczem o pseudonimie „King_25”. Pewnego dnia „King_25” napisał: „Jesteś super. Może spotkamy się jutro po szkole w parku? Mam na imię Bartek i mam 11 lat”.	Nigdy nie wiemy, kim naprawdę jest osoba po drugiej stronie ekranu. Może to być dorosły, który udaje dziecko i ma złe zamiary. **Co robić?** Nigdy nie zgadzać się na spotkanie. Od razu powiedzieć o tej propozycji rodzicom. Pokaż im rozmowę i zablokuj tę osobę.
Kasia umówiła się z dziadkami, którzy mieszkają w innym mieście, na rozmowę wideo. Pokazała im swój nowy rysunek i opowiedziała, co dostała na urodziny.	Rozmawia z osobami, które zna i którym ufa. Używa internetu do podtrzymywania więzi z rodziną, co jest wspaniałym zastosowaniem technologii.
Podczas grania w grę na ekranie pojawiło się okienko: „GRATULACJE! Wygrałeś 10 000 monet do gry! Aby je odebrać, podaj swój login i hasło na tej stronie”.	To klasyczna próba oszustwa (phishing) w celu kradzieży konta. Prawdziwi twórcy gier nigdy nie proszą o hasło w ten sposób. **Co robić?** Natychmiast zamknąć okienko. Nigdy, pod żadnym pozorem, nie podawać nikomu swojego hasła.
Karolina zobaczyła, że ktoś z jej równoległej klasy założył w mediach społecznościowych grupę, na której publikuje przerobione, ośmieszające zdjęcia innych uczniów, w tym jej koleżanki.	To jest **cyberprzemoc** – krzywdzenie innych w internecie. Jest to bardzo raniące i niedopuszczalne. **Co robić?** Nie dołączać do takiej grupy ani nie lajkować postów. Zrobić zrzut ekranu jako dowód i natychmiast pokazać to rodzicom, wychowawcy lub szkolnemu pedagogowi.
Paweł znalazł w internecie fajny quiz „Którą postacią z bajki jesteś?”. Żeby zobaczyć wynik, strona prosi go o podanie swojego adresu e-mail.	Adres e-mail to prywatna informacja. Strona prawdopodobnie nie jest groźna, ale może zacząć wysyłać na ten adres dużo reklam. **Co robić?** Nie podawać swojego e-maila dla zabawy. Jeśli bardzo chcesz zobaczyć wynik, zapytaj rodzica, czy możecie użyć jego „zapasowego” adresu do takich celów.
Ania i jej najlepszy przyjaciel z klasy, Piotrek, grają razem online w swoją ulubioną grę. Rozmawiają na czacie głosowym, używając swoich pseudonimów z gry.	Dzieci grają ze sobą, znają się w świecie rzeczywistym i nie udostępniają prywatnych informacji publicznie. To bezpieczna forma wspólnej zabawy.

NASK cyber profilaktyka NASK Ministerstwo Cyfryzacji

PROJEKT FINANSOWANY ZE ŚRODKÓW MINISTERSTWA CYFRYZACJI