

CYBER

B E Z P I E C Z N I

INSTRUKCJA

GRA STOLIKOWA



1-6



6+



20 min

TWÓRCY GRY:

Autor:

Karolina Kwiatkowska

Testy:

Piotr Krzystek

Ilustracje
i projekt graficzny:

Karolina Kwiatkowska

Skład instrukcji:
Bartosz Chomik

Specjalne podziękowania za konsultacje merytoryczne dla:

Przemysław Czajkowski właściciela firmy



SPIS TREŚCI

WPROWADZENIE	1
ELEMENTY GRY	2
ROLA BEGAMERA	3
PRZYGOTOWANIE ROZGRYWKI	3
CEL GRY	4
PRZEBIEG ROZGRYWKI	4
ZAKOŃCZENIE ROZGRYWKI	7
DODATKOWE TRYBY GRY	8
PYTANIA DO GRY	9
JAK SKŁADAĆ GRĘ	27



WPROWADZENIE

Internet to nieograniczone źródło wiedzy. W niewiarygodny sposób udoskonalił formy komunikowania się i pozyskiwania informacji. Jednak zawsze należy pamiętać o tym, że w rękach osób nieodpowiedzialnych i nieświadomych może okazać się bardzo niebezpiecznym narzędziem.

CYBERBEZPIECZEŃSTWO

Cyberbezpieczeństwo to przestrzeganie i stosowanie się do zasad dotyczących korzystania z Internetu. Bolesna prawda jest taka, że podczas gdy cieszymy się z nowoczesnych udogodnień, zapominamy o ich zabezpieczeniu przed nieautoryzowanym dostępem, niepowołanymi osobami, których zamiary nie są ani dobre, ani etyczne.

Aby skutecznie zadbać o bezpieczeństwo młodych internautów niezbędna jest wiedza na temat, w jaki sposób korzystają oni z sieci oraz jaka jest ich opinia i doświadczenia związane z zagrożeniami online.

JAK BYĆ BEZPIECZNYM W SIECI?

Nie podajemy nikomu swojego hasła oraz nie przechowujemy go w dostępnym miejscu - najlepszym rozwiązaniem jest jego zapamiętanie. Zmieniamy często hasło, na takie, które zawiera małe i duże litery, cyfry oraz znaki specjalne, starajmy się uczynić je silne. Warto korzystać z logowań i zabezpieczeń biometrycznych takich jak odcisk palca lub Face ID oraz zabezpieczeń wieloskładnikowych, np. dodatkowe logowanie z kodu sms. Pamiętajmy o zagrożeniach ze strony obcych użytkowników i o przestrzeganiu zasad tak, abyśmy sami nie stanowili zagrożenia. Instalujemy programy antywirusowe, nie odwiedzamy niezabezpieczonych stron www i nieznanych linków. Powinniśmy zgłosić wszelkie dotyczące nas lub niepokojące incydenty. Dlaczego bezpieczeństwo młodzieży w sieci jest takie ważne? Internet, w którym codziennie obserwujemy ludzką aktywność, ma swoje dobre i złe strony. Dlatego tak ważne jest, by z Internetu korzystać... MĄDRZE.

ELEMENTY GRY



PLANSZA DO GRY



INSTRUKCJA



KARTY Z PYTANIAMI



2 KOŚCI DO GRY



4 KOŚCI
Z PIKTOGRAMAMI



6 PIONKÓW



EKO SKRZYNKA LUB
TUBA NA GRĘ*

*wybrana
wersja gry

ROLA BEGAMERA

BEGAMER to bardzo odpowiedzialna rola. Najczęściej podejmuje się jej wychowawca grupy, najbardziej doświadczony lub najstarszy z uczestników. Jego zadaniem jest: czytać pytania, a potem weryfikować odpowiedzi. Przede wszystkim jednak dba o prawidłowy przebieg rozgrywki i dobrą atmosferę zabawy.

PRZYGOTOWANIE ROZGRYWKI

1. Na początku rozkładamy planszę (tak jak na rysunku poniżej).
2. Kładziemy **KARTY Z PYTANIAМИ** w wygodnym dla **BEGAMERA** miejscu.
3. Ustawiamy na "pajęczynie" kości z piktogramami.
4. Kości z oczkami stawiamy przy polu **START**.
5. Ustawiamy nasze pionki na polu **START** i możemy zaczynać.



CEL ROZGRYWKI

Dzięki tej grze dzieci i młodzież będą kształtować odpowiedzialną postawę korzystania z sieci, poszerzą wiedzę na temat zagrożeń i zasad przestrzegania bezpieczeństwa korzystając z Internetu.

Zadaniem graczy jest przejść przez tor gry, zaczynając na polu **START** i kończąc na polu **META**. Na torze gry spotkamy pola specjalne, które czasem pozwolą nam pójść naprzód, a czasem zmuszą do cofnięcia się lub pozostania na miejscu przez turę. Wiele z nich kryje w sobie pytanie, na które będziemy starać się odpowiedzieć.

Wygrywa gracz, który pierwszy przekroczy linię **METY**.

PRZEBIEG ROZGRYWKI

Grę rozpoczyna ten, kto ostatnio miał najdłuższą przerwę od Internetu. Zachęcamy w kolejnych rozgrywkach do wymyślenia nowego klucza wyboru. Kolejka idzie zgodnie z kierunkiem wskazówek zegara.

Gracz w swojej kolejce rzuca kością. Przesuwa się o tyle pól do przodu, ile widnieje na kostce. Gracz na swojej drodze może spotkać kilka rodzajów pól:



POLE POZYTYWNE – uczy bezpiecznych zachowań w sieci. Gdy gracz stanie na tym polu, jest nagradzany przejściem o jedno pole do przodu, ma to na celu utrwalenie prawidłowego postępowania.



POLE NEGATYWNE – zwraca uwagę na niebezpieczne zachowania w sieci. Gdy gracz stanie na tym polu, cofa się o jedno pole, bądź może wykupić się ćwiczeniami od **BEZPIECZNEGO**, np. przysiadami, podskokami.



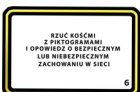
POLE Z PYTANIEM – gracz odpowiada na pytanie zadane przez **BEGANERA** z talii kart. Gdy odpowiedź będzie prawdziwa – gracz przechodzi pole do przodu. Gdy odpowiedź będzie błędna – **BEGANER** podaje poprawną odpowiedź i tłumaczy zagadnienie, a gracz cofa się o jedno pole. W niektórych pytaniach obie odpowiedzi są poprawne lub błędne.



ZADANIE OD BEGANERA – **BEGANER** wymyśla zadanie, które musi być związane z tematem gry, np. „Twoja młodsza siostra ustawiła hasło do swojego konta: ,1234’.

- Jak jej wytłumaczysz, dlaczego to zły pomysł? I jakie hasło byś jej zaproponował?”
- „Na komunikatorze dostajesz wiadomość od kogoś, kto twierdzi, że jest twoim nauczycielem i prosi o przestanie twojego numeru PESEL. Co robisz?”
- „Twoja koleżanka wrzuca na grupę zdjęcie kolegi, który robi dziwną minę. On nie wie, że zostało zrobione. Co jej powiesz?”

BEGANERA ogranicza tylko własna wyobraźnia. Gracz na tym polu nie porusza się ani w przód, ani w tył.



POLE Z ZADANIEM – gdy gracz stanie na tym polu, używa kości z piktogramami, które związane są z tematem bezpieczeństwa w sieci. Zadaniem gracza jest rzucić kostkami i opowiedzieć historię związaną z zachowaniem w sieci oraz ocenić jej bezpieczeństwo. Obrazki można interpretować na różne sposoby, ale ważne jest, aby miały związek z tematem gry.



PIKTOGRAFY NA KOSTKACH:

KOSTKA 1



- włączanie
- wyłączanie



- haker
- obcy



- kciuk do góry
- kciuk w dół



- linie papilarne
- dodatkowe zabezpieczenia
- logowanie biometryczne
- logowanie wieloskładnikowe



- strony internetowe
- wyszukiwanie informacji w sieci
- linki
- niechciane treści



- zdjęcie
- ikonka
- logo

KOSTKA 2



- folder
- dane
- dane osobowe
- informacje



- ustawienia
- aktualizacje



- karty płatnicze
- pieniądze
- płacenie, zakupy w Internecie
- dane na temat funduszy
- numery kart i kont
- kredyt



- ludzie
- użytkownicy Internetu
- komunikacja
- przepływ informacji między ludźmi



- własny wizerunek
- zdjęcie twarzy
- logowanie biometryczne, np. Face ID
- logowanie wieloskładnikowe



- program antywirusowy
- dobre i odpowiednie zabezpieczenia
- poprawne postępowanie w sieci

KOSTKA 3



- hasło
- logowanie
- zabezpieczenie



- wiadomość
- e-mail
- skrzynka e-mail
- przesyłanie informacji



- szukanie
- wyszukiwanie osób, informacji, danych itd.



- dobroć
- szacunek oraz pomaganie innym
- reagowanie na niebezpieczeństwo w sieci
- edukowanie o bezpieczeństwie w sieci



- otwarty dostęp do danych i sprzętu
- nieodpowiednie zabezpieczenia lub ich brak
- brak lub słabe zapory systemowe i wirusowe



- zabezpieczony dostęp do danych i sprzętu
- odpowiednie zapory systemowe i wirusowe

KOSTKA 4



- wirus
- robak



- wiadomość
- czat
- komunikator
- rozmowa
- kontakt z innymi osobami
- wymiana informacji



- login
- nick
- nazwa użytkownika



- wifi
- Internet
- sieć internetowa
- zasięg

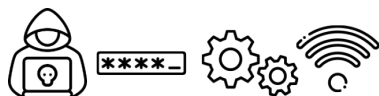


- lokalizacja
- adres
- numer i adres IP



- świat
- komunikacja
- różne lokalizacje

PRZYKŁADOWE ODPOWIEŚCI:



Ustawienie mocnego hasła w sieci, lepiej chroni Cię przed hakerami.



Płacąc na nieznanym stronie za zakupy i podając swój adres, dajesz oszustom otwarty dostęp do cyberkradzieży.



Cały świat powinien włączać zabezpieczenia biometryczne – zamyka to dostęp do wykradania danych.



Każdy może wyszukać Cię w sieci, to może być oszust. Gdy ktoś obcy do Ciebie napisze, nigdy nie wysyłaj mu swoich zdjęć.



Jeżeli zauważysz obraźliwe komentarze o innej osobie na portalu społecznościowym, wykaż się troską i zgłoś to dorosłym i policji lub administratorom strony.

ZAKOŃCZENIE ROZGRYWKI

Gra się kończy, jeżeli któryś z graczy przekroczył linię **NETY**. Jest on zwycięzcą, zyskuje na 24h tytuł „CyberSzeryfa” i w związku z tym, przez dobę należy się tak do niego zwracać.

GRATULUJEMY!

DODATKOWE TRYBY GRY



Wirusem staje się osoba, która miała najkrótszą przerwę od Internetu. Wirus ma za zadanie pokazać realne i potencjalne zagrożenie, czyhające na nas w sieci, które może zaatakować, w każdym momencie. Gdy wirus stanie na tym samym polu co gracz lub gdy gracz stanie na tym samym polu co wirus, wtedy gracz stoi jedną kolejkę lub wykonuje zadanie od **BEGANERA** (mogą być to ćwiczenia, np. przysiady, pompki, podskoki).

Wirus uczestniczy w grze tak samo jak reszta graczy – odpowiada na pytania, wykonuje zadania oraz reaguje na pola negatywne i pozytywne.



BEGANER wyznacza „hakera” lub on sam się zgłasza. Hacker ma za zadanie pokazać realne i potencjalne zagrożenia czyhające na nas w sieci.

Gdy hacker stanie na tym samym polu co gracz, wtedy gracz rzuca kostką z oczkami:

- **liczba parzysta** – gracz zabezpieczył się przed hakerem, nic się nie dzieje,
- **liczba nieparzysta** – gracz stoi jedną kolejkę, nie udało mu się zabezpieczyć przed hakerem.

Hacker uczestniczy w grze tak samo jak reszta graczy – odpowiada na pytania, wykonuje zadania oraz reaguje na pola negatywne i pozytywne.



Jeżeli czujecie niedosyt przygód, zagrajcie jeszcze raz.



Jeżeli chcecie przyspieszyć rozgrywkę, rzucajcie dwoma kostkami.



Na polach negatywnych gracz ma możliwość wyboru: zamiast cofać się lub tracić kolejkę, może wykonać jedno z ćwiczeń fizycznych np. 10 przysiadów, 10 podskoków na prawej nodze, 10 pajacyków itp.

PYTANIA DO GRY



PYTANIA ŁATWE

1. Czy podawanie numeru telefonu w Internecie to dobry pomysł?
A) nie, po tym łatwiej nas zlokalizować i narażamy się na niechciane wiadomości i rozmowy telefoniczne
B) pewnie, nic w tym złego
2. Czy nadmierne korzystanie z Internetu ma jakieś konsekwencje?
A) nie, przecież to czysta przyjemność
B) oczywiście – stres, niewyspanie, problemy z koncentracją, pogorszone relacje z innymi
3. Czy edukacja o bezpieczeństwie w Internecie jest potrzebna?
A) w dzisiejszym świecie nie ma takiej potrzeby
B) tak, to bardzo ważne
4. Dlaczego musimy się uczyć o bezpieczeństwie w sieci?
A) aby, wiedzieć jak chronić się i jak bezpiecznie korzystać z Internetu
B) aby znać realne zagrożenia i umieć reagować na łamanie prawa
5. Kto powinien edukować młodzież o bezpieczeństwie w sieci?
A) każdy, kto zdaje sobie sprawę z zagrożenia i umie przekazać nam informacje
B) rodzice i nauczyciele
6. Czy powinniśmy zgłaszać np. na policję nielegalne i szkodliwe treści, które napotkamy w Internecie?
A) nie, to nie moja sprawa
B) tak, gdyż mogą one zagrażać użytkownikom Internetu lub też, ktoś może przez takie treści cierpieć
7. Ktoś w Internecie zaczyna do Ciebie pisać, a Ty nie masz na to ochoty i czujesz się osaczony. Co robisz?
A) nie reaguję, przecież kiedyś się znudzi
B) blokuję tę osobę lub zgłaszam problem dorosłym



8. Jakie negatywne strony ma Internet?

A) np. uzależnienie, zagrożenia ze strony innych użytkowników

B) Internet nie ma negatywnych stron

9. Jakie pozytywne strony ma Internet?

A) dostęp do informacji, poznawanie świata, rozwój nauki

B) łatwe podtrzymanie kontaktu z dalszą rodziną, przyjaciółmi, znajomymi lub spędzanie wolnego czasu na rozrywce

10. Czy Internet może spowodować uzależnienie?

A) tak, musimy ograniczać korzystanie z Internetu oraz rozsądnie podchodzić do z możliwości, które nam daje

B) nie, przecież to tylko świetne spędzanie czasu

11. Czy w Internecie możemy spotkać się z przemocą?

A) tak, nazywamy to cyberprzemocą

B) nie, przecież w Internecie nikt mnie nie skrzywdzi

12. Co to jest cyberprzemoc?

A) to między innymi: wyśmiewanie, poniżanie i nękanie w formie memów, zdjęć, postów, komentarzy itd.

B) nie ma czegoś takiego

13. Czy cyberprzemoc jest przestępstwem karnym?

A) tak, oczywiście

B) nie, bo nie da się złapać sprawcy

14. Jak udowodnić zachowanie cyberprzemocy?

A) nie można tego zrobić

B) np. zrobić zrzut ekranu, zachować sms, lub wiadomości

15. Czy istnieje takie pojęcie, jak cyberkradzież?

A) tak

B) nie

16. Czy cyberkradzież to karalne przestępstwo?

A) oczywiście, jak każda kradzież

B) nie, w Internecie można robić wszystko



17. Czy kontrola rodzicielska jest ważna?

A) tak, rodzice i dorośli lepiej wiedzą, co jest stosowne i bezpiecznie, a co nie jest

B) tak, rodzice wiedzą, co jest dla nas dobre i chcą nas chronić

18. Dostajesz od obcej osoby wiadomość z nieznanym linkiem. Co robisz?

A) jestem ciekawy i otwieram link

B) ignoruję link, nie wiem, co to jest. Mogą być to wirusy, wiadomość od hakera bądź niestosowne treści

19. Kolega pyta Cię o hasło. Co robisz?

A) grzecznie odmawiam, hasło to bardzo prywatna rzecz, zabezpiecza moje dane i informacje o mnie

B) jeśli to zaufany kolega, nie widzę problemu, żeby podać mu hasło

20. Jakie są dodatkowe sposoby zabezpieczenia w Internecie?

A) dwuetapowe uwierzytelnienie

B) ubranie maseczki

21. Czy Internet pozwala nam rozwijać swoje hobby?

A) tak, przez dostęp do potrzebnych informacji i wiedzy

B) tak, możemy z innymi dzielić się naszymi zainteresowaniami oraz wymienić się doświadczeniami

22. Czy warto instalować programy antywirusowe na urządzeniach?

A) nie ma takiej potrzeby

B) oczywiście, warto się zabezpieczyć

23. Co to jest spam?

A) wysyłanie niechcianych wiadomości

B) przygotowana fabrycznie mielonka

24. O co zadbać, aby bezpiecznie dla zdrowia i wygodnie spędzać czas przed komputerem?

A) biurko dostosowane do wzrostu i krzesło z regulowaną wysokością oparcia, siedziska i podłokietników

B) można korzystać z laptopa, trzymając go na kolanach



25. Kiedy korzystasz ze zdjęć z Internetu w pracy domowej:

A) powinieneś podać źródło i ich autora

B) wystarczy, że je skopiujesz i podpiszesz swoim nazwiskiem

26. Czy podawanie numeru karty płatniczej rodziców w Internecie, to dobry pomysł?

A) tak, jeśli ktoś zapewnia mnie, że pracuje w banku

B) nie, ponieważ ktoś może pobrać pieniądze z konta bez ich wiedzy i zgody

27. Jak nazywają się osoby włamujące się do sieci i systemów komputerowych?

A) hakerzy

B) spamowicze

28. Co należy zrobić, jeśli zostaniesz ofiarą cyberprzestępczości?

A) zgłosić sprawę na policję

B) samemu rozprawić się z hakerami

29. Co to jest program antywirusowy?

A) program odzyskujący dane utracone w wyniku ataku na komputer

B) program blokujący i usuwający wirusy komputerowe

30. Dlaczego uważa się, że niektóre strony internetowe są niebezpieczne?

A) mogą zawierać wirusy, które przeniosą się na nasz komputer, lub będą służyć do wyłudzenia danych

B) mogą nas zaatakować

31. Jak, według netykiety (kultury i zasad zachowania w Internecie), należy zachowywać się w sieci internetowej?

A) w sieci nie należy nikogo obrażać

B) gdy ktoś nas obraża w sieci, to i my możemy go obrażać

32. Otrzymałeś e-mail: „Wygrałeś komputer, otrzymasz go, gdy podasz hasło do swojego konta i zalogujesz się na stronę wystaną w linku”. Co robisz?

A) natychmiast wysyłasz swoje hasło i logujesz się na stronie z linka

B) nikomu nie podajesz swojego hasła i nie logujesz się na obcych stronach



33. W sieci prowadzisz miłą rozmowę z chłopcem, który mówi Ci, że ma na imię Darek i ma 14 lat.

A) jest bardzo miły, nie może kłamać

B) **nie możesz mieć pewności, że jest tym, za kogo się podaje**

34. Cyberprzemocą jest:

A) zamieszczenie na blogu zdjęcia z wycieczki klasowej

B) **wysyłanie wulgarnych i obraźliwych wiadomości**

35. Kim jest hejter?

A) to osoba wygłaszająca publicznie swoją opinię

B) **to osoba obrażająca innych**

36. Osoba zajmująca się np. łamaniem zabezpieczeń komputerowych to:

A) dobry informatyk

B) **haker**

37. Klikanie w linki przysyłane smsem:

A) **może prowadzić do kradzieży danych**

B) jest karalne

38. Jaka grupa ludzi jest najbardziej narażona na niebezpieczeństwo w sieci?

A) dorośli

B) **małe dzieci i młodzież**

39. Pojawiło się nieoczekiwane „okienko wyskakujące” na stronie internetowej. Co robisz?

A) ignoruję je i nie zamykam okienka

B) **zamykam okienko jak najszybciej**

40. Co to jest Internet?

A) **sieć urządzeń mobilnych globalnie połączonych ze sobą**

B) dane przenoszone z pokolenia na pokolenie

41. O czym trzeba pamiętać, korzystając z otwartej sieci WIFI, np. w restauracji?

A) **żeby nie wpisywać żadnych haseł**

B) żeby otrzymać kupony



42. Czy podawanie swojego imienia i nazwiska w Internecie jest bezpieczne?

A) pewnie, nie powinno się go ukrywać

B) **nie, to niebezpieczne**

43. Czy podawanie swojego adresu zamieszkania w Internecie jest bezpieczne?

A) **nie jest bezpieczne**

B) pewnie, że jest bezpieczne

44. Jakich danych nie powinniśmy podawać nieznajomemu w Internecie?

A) **imienia i nazwiska**

B) **adresu zamieszkania**

45. Dlaczego nie podajemy osobistych informacji nieznajomemu w Internecie?

A) **może to być oszust i wykorzystać te informacje**

B) bo jak wpiszę swoje dane, komputer się zawiesi

46. Gdy coś złego spotka nas w Internecie, czy powinniśmy to zgłosić?

A) nie ma sensu, to tylko Internet

B) **oczywiście, że tak (powinniśmy porozmawiać z dorosłym)**

47. Komu zgłaszać problem z innym użytkownikiem Internetu?

A) nikomu

B) **rodzicom, policji, nauczycielom (dorosłym)**

48. Czy poznana w Internecie koleżanka może okazać się kimś innym?

A) **tak, w Internecie łatwo nas oszukać**

B) nie, przecież dziewczyna nie może mnie oszukać

49. Czy w sieci warto posługiwać się nickiem lub pseudonimem?

A) nie ma takiej potrzeby

B) **tak, dzięki temu nie udostępniamy imienia i nazwiska potencjalnemu oszustowi, który może wykorzystać te dane**

50. Co jest zdrowsze?

A) **spędzanie aktywnie czasu na zewnątrz**

B) siedzenie dzień i noc przy komputerze



51. Czy wysyłanie zdjęć do nieznajomych jest bezpieczne?

A) tak, przecież nieznajomy tylko się dowie, jak wyglądam

B) **nie, nie powinniśmy dzielić się naszym wizerunkiem z nieznajomymi**

52. Czy wyśmiewanie kolegów w Internecie jest fajne i zabawne?

A) tak, przecież to tylko żarty

B) **nie, to może ktoś bardzo urazić i skrzywdzić, co więcej jest to przestępstwo**

53. Poznajesz nową przyjaciółkę w Internecie. Ona chce się spotkać, co robisz?

A) super, od razu się zgadzam

B) **odmawiam i mówię o tym rodzicom, nie mam pewności czy to bezpieczne, może to być oszust**

54. Czy Internet posiada negatywne strony?

A) **tak, posiada wiele negatywnych stron**

B) nie posiada, Internet to najfajniejsza rzecz na świecie

55. Czy Internet posiada pozytywne strony?

A) nie posiada i jest bardzo niebezpieczny

B) **oczywiście, że tak**

56. Czy w Internecie zawsze znajdziemy prawdziwe newsy?

A) **nie, w Internecie często krążą FAKE NEWSy (fałszywe informacje)**

B) **pewnie, jeśli coś jest napisane w Internecie, to musi być prawdą**

57. Przed czym chronimy system korzystając z programów antywirusowych?

A) **wirusami**

B) **nieznanymi stronami**

58. Czy silne hasło w Internecie jest istotne?

A) **tak, musimy chronić swoje treści i dane**

B) **nie**

59. Gdzie najlepiej ukryć swoje hasło?

A) **pod klawiaturą**

B) **w głowie – zapamiętać**



60. Nie wszystkie informacje dostępne w Internecie są prawdziwe:

A) prawda

B) fałsz

61. Napotkales w Internecie wpisy obrażające Twojego kolegę. Co powinieneś zrobić?

A) przestać je dalej, niech inni się pośmieją

B) powiadomić zaufaną osobę dorosłą lub policję

62. Czy chcąc opublikować w Internecie zdjęcie z udziałem znajomej osoby, powinieneś zapytać ją o zgodę?

A) nie ma takiej potrzeby

B) tak, zawsze należy zapytać o pozwolenie

63. Co powinieneś zrobić, gdy ktoś nieodpowiednio się do Ciebie zwraca w Internecie?

A) odpowiedzieć mu w taki sam sposób

B) zgłosić zdarzenie dorosłym lub administratorowi strony

64. Czy rozmawianie z nieznanym w sieci jest bezpieczne?

A) nie jest, nie wiemy kto to i czego od nas chce

B) pewnie, przecież nie może nic mi zrobić przez Internet

65. Jak mogą działać wirusy?

A) uszkadzają system, narażają nas na niebezpieczeństwo poprzez kradzież naszych danych

B) zabezpieczają system

66. Które zdanie jest prawdą?

A) w Internecie nie każdy jest tym, za kogo się podaje

B) w Internecie nikt nie kłamie

67. W sieci ktoś nieznanym prosi Cię o przesłanie Twojego zdjęcia. Co robisz?

A) nie wysyłasz i mówisz o tym dorosłym

B) odpowiadasz, że możesz wysłać, ale tylko jedno



68. Czy mogę reagować, gdy jestem świadkiem przemocy w Internecie na innej osobie niż ja?

A) koniecznie należy poinformować osobę, że to przestępstwo, reagować i zgłosić odpowiednim organom

B) to nie moja sprawa

69. Co to jest weryfikacja dwuetapowa lub dwuskładnikowa?

A) test na inteligencję

B) metoda autoryzacji nie tylko hasłem, ale i specjalnym dodatkowym kodem

70. Czy udostępnianie obcym gier, książek, filmów, audiobooków jest legalne?

A) nie, to przestępstwo, gdyż udostępnianie treści objętych prawem autorskim nie jest legalne

B) jest legalne, kupiłem przecież plik i mogę z nim zrobić, co chcę

71. Co należy zrobić po włamaniu komputerowym?

A) powiadomić odpowiednie organy, rodzinę i znajomych

B) zwrócić się o pomoc do specjalisty

72. Błędy systemowe stwarzają możliwości ataków cybernetycznych

A) prawda

B) fałsz

72. Czym jest stalking?

A) nękanie

B) rodzajem sportu

73. Co to jest sieciorholizm?

A) uzależnienie od Internetu

B) rodzaj sieci internetowej





PYTANIA TRUDNIEJSZE

1. Ile trzeba mieć lat, aby móc założyć profil na Facebooku?

A) 13

B) 8

2. Dlaczego nie powinniśmy wysłać swoich zdjęć do nowo poznanej osoby w Internecie?

A) nie wiemy, kto to i do czego wykorzysta nasze zdjęcia

B) to może być oszust, który wykorzysta wiedzę o naszym wizerunku i naszych danych

3. Gdzie można zgłosić cyberprzemoc?

A) administratorowi strony

B) dorosłym, odpowiednim służbom i specjalistom

4. Co to jest kontrola rodzicielska w Internecie?

A) dostęp rodziców i dorosłych do sprzętu, kont internetowych i historii stron, które są odwiedzane

B) blokowanie niektórych nie stosownych i niebezpiecznych stron, które stanowią zagrożenie lub są niewłaściwe

5. Jakie powinny być hasła?

A) silne

B) poufne

6. Czy ja mogę przekazywać innym informacje z zakresu bezpieczeństwa w Internecie?

A) oczywiście, jeśli tylko mam odpowiednią wiedzę i informacje na ten temat

B) nie, bo nie mam na to dyplomu, certyfikatu, szkolenia

7. Obrażliwe komentowanie treści zamieszczanych w Internecie to?

A) hejtowanie

B) spamowanie



8. Jakie dane bezpiecznie jest podawać w Internecie?

A) imię, nazwisko, datę urodzenia

B) najlepiej żadne

9. Co to jest SPAM?

A) niechciane wiadomości

B) program do komunikacji

10. Co może zrobić wirus z naszym komputerem?

A) może uszkodzić system operacyjny

B) może wysyłać fałszywe wiadomości z naszego komputera

11. Co to jest malware?

A) złośliwe oprogramowanie

B) komunikator internetowy

12. W jaki sposób wirus komputerowy może dostać się do komputera?

A) poprzez pobranie programu z przypadkowej strony internetowej

B) poprzez pamięć USB lub inny dysk zewnętrzny, albo kliknięcie w załącznik w mailu

13. Co należy zrobić, gdy otrzymasz pocztę, która wygląda na SPAM?

A) usunąć bez otwierania

B) przeczytać, a następnie usunąć

14. W którym przypadku podawanie prawdziwych danych w Internecie jest bezpieczne?

A) włączając się w dyskusję na forum

B) podczas zakupów on-line na zaufanej stronie

15. Po czym poznasz, że ktoś włamał się na Twoje konto internetowe?

A) nie możesz się zalogować, pomimo wpisywania właściwych haseł

B) Twoi koledzy otrzymali od Ciebie e-maile, których Ty nie wysłałeś

16. Za jaką działalność administrator może usunąć konto użytkownika?

A) za łamanie regulaminu serwisu

B) za umieszczanie zbyt wielu postów



17. Informacje, które publikujesz w Internecie:

- ☒ **A) pozostają w nim na zawsze**
- ☐ **B) znikają na zawsze po ich usunięciu**

18. Programem antywirusowym powinniśmy zabezpieczać:

- ☒ **A) smartphone'a**
- ☐ **B) komputer**

19. Publiczne sieci wi-fi są bezpieczne

- ☐ **A) prawda**
- ☒ **B) fałsz**

20. Publiczne sieci wi-fi są niebezpieczne

- ☒ **A) prawda**
- ☐ **B) fałsz**

21. Jak nazywane jest upokarzanie i zastraszanie w Internecie?

- ☐ **A) stalking**
- ☒ **B) cyberprzemoc**

22. Kradzież tożsamości w Internecie to

- ☒ **A) np. przejęcie czyjegoś konta na portalu społecznościowym**
- ☐ **B) np. stworzenie fałszywego profilu innej osoby**

23. Gdy skończysz korzystać z portalu społecznościowego, poczty e-mail itp. pamiętaj o:

- ☐ **A) usunięciu historii wyszukiwania**
- ☒ **B) wylogowaniu**

24. Jak powinniśmy zabezpieczyć swoje dane w Internecie?

- ☐ **A) nickiem**
- ☒ **B) dwuetapowym uwierzytelnieniem oraz hasłem**

25. Korzystając z Internetu czym warto się posługiwać?

- ☐ **A) pełnym imieniem i nazwiskiem**
- ☒ **B) nickiem, pseudonimem, nazwą**



26. Co to znaczy być online?

A) to aktualna dostępność w sieci

B) to brak dostępności w sieci

27. Co to znaczy być offline?

A) to być niedostępnym w sieci

B) być dostępnym w sieci

28. Co pomaga w dobrej komunikacji w Internecie?

A) używanie słów: „proszę”, „dziękuję” i „przepraszam” tak, jak w codziennym życiu

B) używanie mnóstwa emotikon

29. Co to jest NICK?

A) nazwa komputera

B) wymyślone internetowe imię, ksywa bądź pseudonim, który nie zawiera naszego imienia, nazwiska i wieku w nazwie

30. Jakie informacje o sobie możesz bezpiecznie podać w sieci?

A) swoje zainteresowania

B) numer telefonu

31. Czy z całkowitą pewnością, możesz ustalić wiek osoby, z którą rozmawiasz w sieci?

A) tak, po informacji umieszczonej na jej profilu

B) nie mam takiej możliwości

32. Jakie konsekwencje niesie za sobą uzależnienie od Internetu?

A) brak odpoczynku, zaniedbanie nauki i obowiązków

B) napady złości, chwiejne nastroje, pogorszenie stosunków rodzinnych i towarzyskich

33. Co to jest cyberkradzież?

A) kradzież tożsamości, podszywanie się pod kogoś

B) kradzież pieniędzy, zaciąganie kredytu, zakupy w Internecie z obcego konta



34. Jaki jest najprostszy sposób chronienia systemu w Internecie?

- A) zdrowy rozsądek, usuwanie linków niewiadomego pochodzenia**
- B) program antywirusowy**

35. Silne hasło składa się z:

- A) liter i cyfr**
- B) dużych i małych liter, cyfr, znaków specjalnych i co najmniej 10 znaków**

36. Czy silne hasło jest wystarczające w Internecie?

- A) tak, nikt go nigdy nie zgadnie**
- B) nie, obecnie standardem jest stosowanie dwuetapowego uwierzytelnienia**

37. Co to jest NETYKIETA?

- A) portal społecznościowy**
- B) zbiór zasad zachowania obowiązujących w Internecie**

38. Jaki jest numer telefonu zaufania dla dzieci i młodzieży?

- A) 116 111**
- B) 222 011**

39. Co to jest phishing?

- A) To metoda oszustwa, w której ktoś próbuje wyłudzić od Ciebie dane, np. hasła lub numer konta**
- B) To zabawa w udawanie kogoś innego w Internecie dla żartu**

40. Czym są zabezpieczenia biometryczne np. czytniki linii papilarnych?

- A) to zabezpieczenia, które odblokowują się po zweryfikowaniu tęczyówki oka**
- B) to zabezpieczenia, które odblokowują się po zweryfikowaniu odcisku palca**

41. Złośliwy program, który nie potrzebuje nosiciela do rozprzestrzeniania się w sieci:

- A) koń trojański**
- B) robak**



42. Złośliwe oprogramowanie, podające się za oprogramowanie znane i potrzebne użytkownikowi:

A) koń trojański

B) rootkit

43. Oprogramowanie zbierające dane o użytkowniku oraz wykradające poufne dane:

A) spam

B) spyware

44. Oprogramowanie pozwalające przejąć komputer przez osoby trzecie:

A) rootkit

B) robak

45. Co to jest FIREWALL?

A) silne hasło zabezpieczające

B) zaporę sieciową, która blokuje niepowołany dostęp do komputera lub sieci komputerowych

46. Który z programów zabezpiecza komputer przed zagrożeniami płynącymi z Internetu?

A) program antyszpiegujący

B) firewall

47. Antywirus łącząc się za pomocą Internetu z bazą definicji najnowszych wirusów:

A) wykonuje aktualizację

B) wykonuje odnowienie

48. Aby dbać o swoje bezpieczeństwo w sieci należy:

A) zapewnić swoim profilom w sieci status prywatny

B) nie podawać swoich haseł

49. Jakim mianem określani są hakerzy działający legalnie lub tacy, którzy starają się nie wyrządzać szkód?

A) white hat

B) black hat



50. Jakim mianem określani są hakerzy działający nielegalnie i wyrządzający szkody?

- ☒ A) white hat
- ☒ B) black hat

51. Hakerzy używają zabawnych quizów na serwisach społecznościowych, aby uzyskać dostęp do Twoich informacji

- ☒ A) prawda
- ☒ B) fałsz

52. W którym roku odbył się pierwszy dzień Bezpiecznego Internetu?

- ☒ A) 2004
- ☒ B) 2017

53. Czym są ciasteczka?

- ☒ A) rodzajem reklam
- ☒ B) niewielkie informacje zbierane o nas w celach marketingu

54. Czym jest tryb „incognito” w przeglądarce?

- ☒ A) tryb nie zapisujący „cookies” i historii przeglądania itp.
- ☒ B) tryb dający możliwość modyfikacji strony internetowej

55. Co to jest SSL?

- ☒ A) protokół, służący do szyfrowania transmisji danych
- ☒ B) serwer

56. Rozwiń skrót SSL:

- ☒ A) Secure Sockets Layer
- ☒ B) Super Safe Login

57. Czym jest Sniffing?

- ☒ A) podszywanie się pod legalną firmę
- ☒ B) podsłuch transmisji danych

58. Na czym polega cyberbullying?

- ☒ A) wykorzystywanie Internetu do aktów przemocy
- ☒ B) pomoc innym przez Internet



59. Adres IP może być:

- A)** stały
- B)** dynamiczny

60. Adres IP może być:

- A)** publiczny
- B)** prywatny

61. Co to jest adres IP?

- A)** numer identyfikacyjny nadawany komputerom lub innym urządzeniom łączącym się z siecią, który zapewnia im prawidłową komunikację
- B)** liczba odwiedzanych codziennie stron internetowych

62. WWW to skrót od:

- A)** Wielka Wyszukiwarka Wiadomości
- B)** World Wide Web

63. Za pomocą czego sprawdzimy, czy dane połączenie jest bezpieczne?

- A)** zielonego zaznaczenia lub kłódki koło paska adresu
- B)** komunikatu: „Niebezpieczeństwo”

64. Kiedy korzystasz z komputera dostępnego dla innych osób, co powinieneś zrobić?

- A)** zastosować tryb prywatny w przeglądarce
- B)** korzystać z najpopularniejszych witryn

65. Forma oszustwa polegająca na podszywaniu się pod osobę budzącą nasze zaufanie:

- A)** phishing
- B)** stalking

66. Adresy stron www pozwalające bezpiecznie się logować i podawać hasła, rozpoczynają się od:

- A)** css://
- B)** https://



67. Wirusy przyczepiają się najczęściej do plików z rozszerzeniem:

A) .exe i .com

B) .pdf

68. Czy Twoje relacje (np. instastory, snapy, itp.) znikają z Internetu?

A) znikają po 24 godzinach

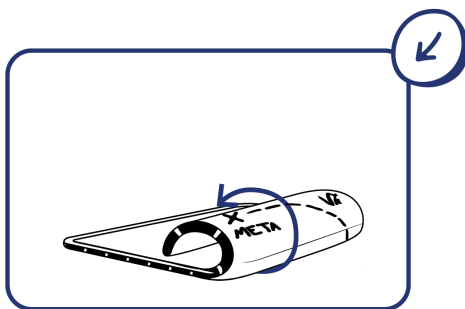
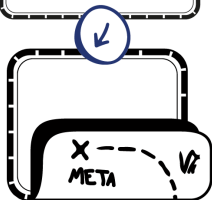
B) nigdy nie znikają

JAK SKŁADAĆ GRĘ

Planszę należy zwiąć grafiką na zewnątrz. Dzięki temu po wyjęciu z pudełka lub tuby plansza szybciej dopasuje się do stolika, co pozwoli na natychmiastowe rozpoczęcie gry bez konieczności prostowania jej rogów. To prosty sposób na utrzymanie planszy w idealnym stanie i wygodne jej użytkowanie podczas każdej rozgrywki.

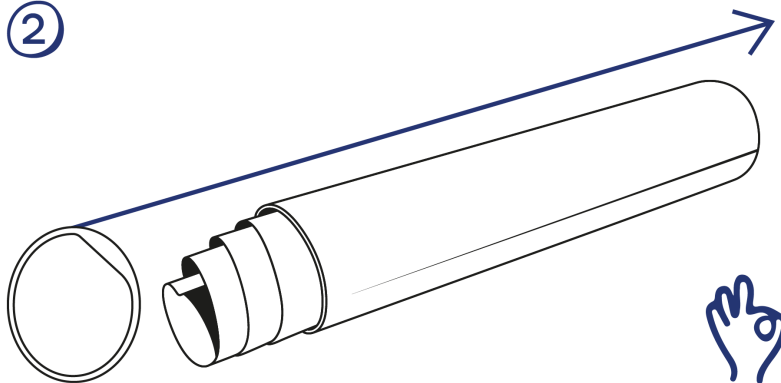
1

*Tył
planszy



*Zwijać do pełnego złożenia

2





CYBER

B E Z P I E C Z N I



beGame.pl

Zobacz nasze gry z serii



beEdu



beEko



beHist



beSafe



beKids



beMed

Bycie pionkiem
na naszych grach
to czysta przyjemność!