beGame.pl

i-ht

CYBER
BEZPIECZNI

INSTRUKCJA

GRA STOLIKOWA

2-6

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:

Przemysława Czajkowskiego właściciela firmy

SPIS TREŚCI

WPROWADZENIE

Internet to nieograniczone źródło wiedzy. W niewiarygodny sposób udoskonalił formy komunikowania się i pozyskiwania informacji. Jednak zawsze należy pamiętać o tym, ze 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, ze podczas gdy cieszymy się z nowoczesnych udogodnień zapominamy o ich zabezpieczeniu przed nieautoryzowanym dostępem, niepowołanymi osobami, których zamiary mijają się z dobrem czy etyką...

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 udostępniamy nikomu swojego hasła oraz nie przechowujemy go w dostępnym miejscu – najlepiej, aby je zapamiętać. Ważne, aby często zmieniać hasto i aby było silne (zawierało małe, duże litery, cyfry oraz znaki specjalne). Warto korzystać z logowań i zabezpieczeń biometrycznych takich jak odcisk palca lub face id oraz zabezpieczeń wieloskładnikowych jak dodatkowe logowanie z kodu sms. Pamiętajmy o zagrożeniach ze strony innych, obcych użytkowników i o przestrzeganiu zasad tak, abyśmy sami nie stanowili zagrożenia. Instalujemy programy antywirusowe, nie odwiedzamy niezabezpieczonych stron www i obcych linków. Zgłaszajmy wszelkie nas dotyczące lub zaobserwowane incydenty. Dlaczego bezpieczeństwo młodzieży w sieci jest takie ważne? Internet, jak każda ludzka aktywność ma swoje dobre i złe strony. Skoro sieć działa na wszystkich polach ludzkiej aktywności, oznacza to, że funkcjonuje i na tych, z którymi na co dzień walczymy. Dlatego tak ważne jest, by z internetu korzystać... MĄDRZE.

ELEMENTY GRY

Plansza do gry

Instrukcja

144 karty z pytaniami*

2 klasyczne kości

4 kości z piktogramami

6 pionków

Eko skrzynka lub tuba na grę*

*wybrana wersja gry

ROLA BEGAMERA

BEGAMER to bardzo odpowiedzialna rola. Najczęściej rolę tę przejmuje wychowawca grupy lub najstarszy z uczestników. Jego zadaniem jest czytać pytania, sprawdzać odpowiedzi, przydzielać punkty. Przede wszystkim jednak dba on o prawidłowy przebieg rozgrywki i dobrą atmosferę zabawy.

PRZYGOTOWANIE ROZGRYWKI

1. Na początku rozkładamy plansze (tak jak na rysunku poniżej).
2. Kładziemy **KARTY Z PYTANIAMI** w wygodnym dla **BEGAMERA** miejscu.
3. Ustawiamy na “pajęczynie” kostki z piktogramami.
4. Kostki z oczkami stawiamy przy polu start.
5. Stawiamy nasze pionki na polu **START** i możemy zaczynać.

CEL ROZGRYWKI

Kształtowanie u dzieci i młodzieży odpowiedzialnej postawy korzystania z sieci, poszerzanie wiedzy na temat zagrożeń i przestrzegania bezpieczeństwa korzystając z Internetu.

Zadaniem graczy jest przejść przez tor gry, zaczynając na polu **START** i kończąc na polu **META**. Na torze tym spotkamy pola specjalne, które czasem pozwolą nam pójść naprzód, a czasem zmuszą do wycofania 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

Do rozpoczęcia gry potrzebne są minimum 2 osoby, kość z oczkami i 4 kości z piktogramami, karty z pytaniami.

Grę rozpoczyna ten kto ostatnio miał najdłuższą przerwę od Internetu. Ewentualnie pierwszego gracza można wyłonić w inny sposób, po prostu wybierzcie kogoś i już.

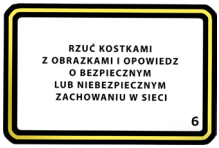
Gracz w swojej kolejce rzuca kością. Przesuwa się o tyle pól do przodu, ile widnieje na kostce. Gracz na swojej drodze może spotkać kilka rodzajów pól:

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 **beGamera**, np. przysiadami.

POLE Z PYTANIEM – gracz odpowiada na pytanie zadane przez **beGamera** z talii kart. Gdy odpowiedź będzie prawidłowa – gracz przechodzi pole do przodu. Gdy odpowiedz będzie błędna – **beGamer** podaje poprawną odpowiedź i tłumaczymy zagadnienie, a gracz cofa się o jedno pole.

ZADANIE OD BEGAMERA – **beGamer** wymyśla zadanie, które musi być związane z tematem gry, np. opowiedz jak zachowa sie w danej sytuacji, lub np. powiedz jak rozwiązałbyś dany problem. Dowolność wymyślenia zadania w temacie gry. Gracz przy tym polu nie porusza sie 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

PIKTOGRAMY NA KOSTKACH:

KOSTKA 1

- włączanie
- wyłączanie

- haker
- osoba

- kciuk do góry
- kciuk w dół

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

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

- zdjęcie

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. FaceID
- 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 dla innych
- pomoc
- reagowanie na niebezpieczeństwo w sieci
- edukowanie o bezpieczeństwie w sieci

- otwarty dostęp do danych i sprzętu
- nieodpowiednie zabezpieczenia lub ich brak
- słabe hasła, które łatwo złamać
- brak lub słabe zapory systemowe i wirusowe

- zabezpieczony dostęp do danych i sprzętu
- mocne i dobre zabezpieczenia
- odpowiednie zapory systemowe i wirusowe

KOSTKA 4

- wirus
- robak

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

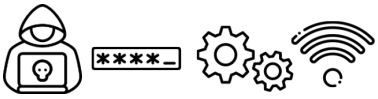
- login
- nick
- nazwa użytkownika

- wifi
- internet
- sieć internetowa
- zasięg

- lokalizacja
- adres
- numer i adres IP

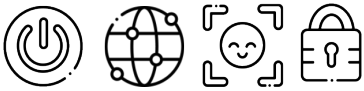
- świat
- komunikacja
- różne lokalizacje

Przykładowe opowieści:



Ustawienie mocnego hasła w sieci lepiej chroni Cię przed hakerami

Płacąc na nieznanych stronach za zakupy i podając swój adres dajesz oszustom otwarty dostęp do cyberkradzieży



Cały świat powinien włączać zabezpieczenia biometryczne – zamyka to dostęp i wykradanie 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 linie **mety**. Jest on zwycięzcą, zyskuje na 24h tytuł ,,CyberSzeryfa" i w związku z tym, przez dobę należy się tak właśnie do niego zwracać. **Gratulujemy!**

DODATKOWE TRYBY GRY

Wirusem staje sie 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 jedna kolejkę lub wykonuje zadanie od **BEGAMERA** (mogą być to ćwiczenia, np. przysiady).

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

BEGAMER wyznacza „hakera" lub on sam się zgłasza. Haker ma za zadanie pokazać realne i potencjalne zagrożenia czyhające na nas w sieci.

Gdy haker 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 jedna kolejkę, nie udało mu się zabezpieczyć przed hakerem.

Haker uczestniczy w grze tak samo jak reszta graczy – odpowiada na pytania, wykonuje zadania i 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, takich jak 10 przysiadów, pajacyków, skłonów lub inne wybrane aktywności.

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 telefony**
B) pewnie, nic w tym złego

2. Czy nadmierne korzystanie z Internetu ma jakieś konsekwencje?
A) nigdy, to czysta przyjemność
B) **oczywiście – stres, niewyspanie, problemy z koncentracją, pogorszone relacje z innymi**

3. Czy edukacja o bezpieczeństwie w Internecie jest potrzebna?
A) nie, po co?
B) **tak, to bardzo ważne**

4. Po co nam edukacja 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 policje nielegalne i szkodliwe treści, które napotkamy w Internecie?
A) nie, to nie moja sprawa
B) **tak, ktoś z tego powodu może cierpieć lub może to zagrażać innym użytkownikom Internetu**

7. Ktoś w Internecie zaczyna do Ciebie pisać, a Ty nie masz na to ochoty i robi się to problematyczne. Co robisz?
A) nie reaguję, kiedyś się znudzi
B) **blokuję tę osobę lub zgłaszam dorosłym**

8. Jakie negatywne strony ma Internet?
A) **np. uzależnienie, zagrożenia ze strony innych użytkowników**
B) nie ma żadnych

9. Jakie pozytywne strony ma Internet?
A) **dostęp do informacji, poznawanie świata, nauka**
B) **łatwe podtrzymanie kontaktu z innymi lub spędzanie wolnego czasu na rozrywce**

10. Czy Internet może spowodować uzależnienie?
A) **tak, musimy ograniczać korzystanie z Internetu oraz rozsądnie korzystać z możliwości, które nam daje**
B) nie, przecież to tylko super spędzanie czasu

11. Czy w Internecie możemy zderzyć się z przemocą?
A) **tak, nazywamy to cyberprzemocą**
B) nie, przecież w Internecie nikt mnie nie krzywdzi

12. Co to jest cyberprzemoc?
A) **np. wyśmiewanie, poniżanie i nękanie w formie memów, zdjęć, postów, komentarzy itd.**
B) nie ma czegoś takiego

13. Czy cyberprzemoc jest karalnym przestępstwem?
A) **tak, oczywiście**
B) nie, bo nie da się złapać sprawcy

14. Jak udowodnić zachowanie cyberprzemocy?
A) nie da się
B) **np. zrobić zrzut ekranu, zachować sms, wiadomość**

15. Czy istnieje pojęcie takie, jak cyberkradzież?
A) **tak**
B) nie

16. Czy cyberkradzież to karalne przestępstwo?
A) **oczywiście, jak każda kradzież**
B) nie, w Internecie można wszystko

17. Czy kontrola rodzicielska jest ważna?
A) tak, rodzice i dorośli lepiej wiedzą co jest stosowne i bezpiecznie, a co nie
B) tak, rodzice wiedzą co 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
B) jeśli to zaufany kolega podaje 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) przygotowanie mielonki

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) 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 pobierać pieniądze z konta ich wiedzy i zgody**

27. Jak nazywają się osoby działające przestępczość w Internecie?
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 wyłudzać informacje**
B) mogą nas zaatakować

31. Jak, według netykiety (kultury i zasad zachowania), należy zachowywać się w sieci internetowej?
A) **w sieci nie należy nikogo obrażać**
B) gdy ktoś nas obraża w sieci, to i my go możemy obrażać

32. Otrzymałeś e-mail: „Wygrałeś komputer, otrzymasz go, gdy podasz hasło do swojego konta i zalogujesz się na stronę wysłaną 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 klasowego zdjęcia z wycieczki
B) **wysyłanie wulgarnych i obraźliwych wiadomości**

35. Kim jest hejter?
A) osoba wygłaszająca publicznie swoją opinię
B) **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 spowodować kradzież 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) ignorujemy je i nie zamykamy
B) **zamykamy jak najszybciej**

40. Co to jest Internet?
A) **sieć urządzeń mobilnych połączona 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 bezpiecznie podać swoje imię i nazwisko w Internecie?
A) pewnie, nie ma co ukrywać
B) **nie, to niebezpieczne**

43. Czy podawanie adresu zamieszkania w Internecie jest bezpieczne?
A) **nie, jest niebezpieczne**
B) pewnie, że jest

44. Jakich danych nie powinniśmy podawać nieznajomemu w Internecie?
A) **imienia i nazwiska**
B) adresu zamieszkania

45. Dlaczego nie podajemy osobistych informacji nieznajomym w Internecie?
A) **może to być oszust i wykorzystać te informacje**
B) żeby nie było mu smutno

46. Gdy coś złego spotka nas w Internecie czy powinniśmy to zgłosić?
A) po co? To tylko internet
B) **oczywiście, że tak (dorosłym)**

47. Komu zgłaszać problem z innym użytkownikiem Internetu?
A) nikomu, po co?
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, niby kim?

49. Dlaczego w sieci warto posługiwać się nickiem lub pseudonimem?
A) nie warto
B) **dzięki temu nie udostępniamy imienia i nazwiska potencjalnemu oszustowi, który może wykorzystać te dane**

50. Co zdrowiej robić?
A) **spędzać aktywnie czas na zewnątrz**
B) dzień i noc siedzieć przy komputerze

51. Czy wysyłanie zdjęć do nieznajomych jest bezpieczne?
A) tak, przecież 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) przecież to tylko żarty
B) **nie, to może kogoś bardzo urazić i mieć złe skutki oraz jest to przestępstwo**

53. Poznajesz super 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, to totalnie bez sensu i jest niebezpieczny**
B) oczywiście, że tak

56. Czy w Internecie zawsze znajdziemy prawdziwe newsy?
A) **nie, nie wszystko jest prawdą, to tak zwane FAKE NEWS**
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 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. Napotkałeś w Internecie wpisy obrażające Twojego kolegę. Co powinieneś zrobić?
A) przesłać 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 niełądnie się do Ciebie zwraca w Internecie?
A) odpowiedzieć mu w taki sam sposób
B) **zgłosić zdarzenie dorosłym lub do administratora strony**

64. Czy rozmawianie z nieznajomym w sieci jest bezpieczne?
A) **nie jest, nie wiemy kto to i czego od nas chce**
B) pewnie, a co mi zrobi przez Internet

65. Jak mogą działać wirusy?
A) **uszkadzać system, narazić nas na niebezpieczeństwo poprzez kradzież naszych danych**
B) zabezpieczyć 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 nieznajomy 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. Pobieranie z Internetu gier komputerowych, piosenek i filmów to?
A) **przestępstwo, gdyż rozpowszechnianie plików w sieci jest nielegalne**
B) nagroda za dobre zachowanie

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) **nękaniem**
B) rodzajem sportu

73. Co to jest siecioholizm?
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 wysyłać swoich zdjęć do nowo poznanej osoby w Internecie?
A) **nie wiemy, kto to i po co mu te 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 niestosownych i niebezpiecznych stron, które wzbudzają zagrożenie lub są niewłaściwe**

5. Jakie powinny być hasła?
A) **silne**
B) **poufne**

6. Czy ja mogę podpowiadać 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. Obraźliwe komentowanie treści zamieszczanych w Internecie to?
A) **hejtowanie**
B) spamowania

8. Jakie dane bezpiecznie jest podawać w Internecie?
A) imię, nazwisko, data 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 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**
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 upokorzenie 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 email itp. pamiętaj o:
A) usunięciu historii wyszukiwania
B) **wylogowaniu**

24. Jak powinniśmy zabezpieczyć swoje dane w Internecie?
A) nickiem
B) **2 etapowym 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) **aktualna dostępność w sieci**
B) aktualna niedostępność w sieci

27. Co to znaczy być offline?
A) **aktualna niedostępność w sieci**
B) aktualna dostępność 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, nie otwieranie 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 nr telefonu zaufania dla dzieci i młodzieży?
A) **116 111**
B) 222 011

39. Czym jest phishing?
A) **sposób wyłudzenia informacji**
B) podszywanie się pod kogoś

40. Zabezpieczenia biometryczne np. czytniki linii papilarnych. Co to jest?
A) dostęp po zweryfikowaniu oka
B) **dostęp 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) **zapora sieciowa, która blokuje niepowołany dostęp do komputera lub sieci komputerowych**

46. Który z programów zabezpiecza komputer przed internetowymi zagrożeniami?
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 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) Socket Secure Layer

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. Unieruchamia skanery antywirusowe, a nawet może je niszczyć:
A) wirus Makro
B) **wirus Retro**

66. Forma oszustwa polegająca na podszywaniu się pod osobę budzącą nasze zaufanie:
A) **phishing**
B) stalking

67. Adresy stron www, pozwalające bezpiecznie się logować i podawać hasła, rozpoczynają się od:
A) css://
B) **https://**

68. Wirusy przyczepiają się najczęściej do plików z rozszerzeniem:
A) **.exe i .com**
B) .pdf

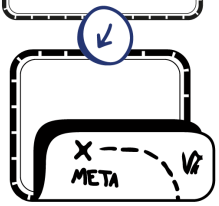
69. Czy Twoje relacje (np. instastory, snapy, itp.) znikają z Internetu?
A) znikają po 24 godzinach
B) **nie znikają nigdy**

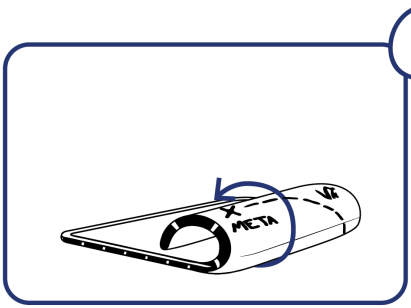
JAK SKŁADAĆ GRĘ

Planszę należy zwijać 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

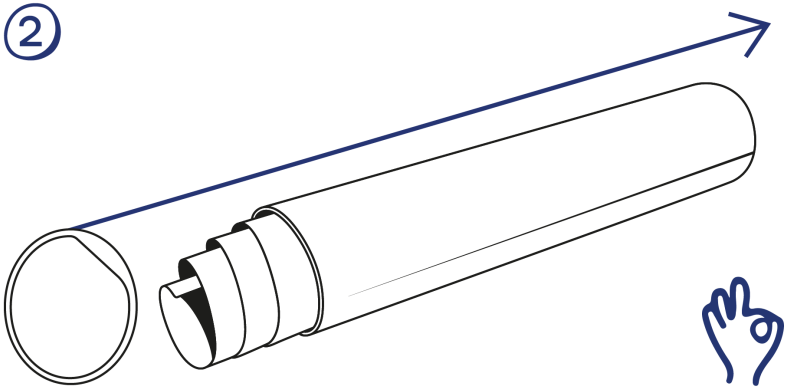
*Tył planszy





*Zwijać do pełnego złożenia

2



beGame.pl

Zobacz inne nasze gry z serii

beSafe

Bycie pionkiem
na naszych grach
to czysta przyjemność!