ODKRYWCY INTERNETU

GRA PLANSZOWA
O BEZPIECZEŃSTWIE W INTERNECIE

ZASADY GRY

oraz

BEZPIECZNIK

czyli

MINIPORADNIK INTERNAUTY

ODKRYWCY INTERNETU

SPIS TREŚCI

1. Wprowadzenie
2. Zawartość pudełka
3. Przygotowanie gry
4. Przebieg rundy
5. Koniec gry

1. WPROWADZENIE

Odkrywcy Internetu to edukacyjna gra planszowa dla dzieci i młodzieży, podczas której gracze dowiedzą się, jak bezpiecznie i świadomie korzystać z zasobów Internetu, respektując m.in. prawo autorskie czy ochronę wizerunku swojego i innych osób.

W grze uczestnicy będą zdobywać doświadczenie, zwiększając poziom różnego rodzaju umiejętności przydatnych online. Te umiejętności pozwolą im stawić czoło niebezpiecznym sytuacjom, a w razie potrzeby wykazać się zdobytą wiedzą. Przyda się ponadto łut szczęścia, który pomoże graczom uzyskać upragnione korzyści, a także dobra pamięć - w trakcie rozgrywki należy bowiem zapamiętywać wskazówki umieszczone na kartach. Jednym słowem: Trzeba być przygotowanym na wszystko - wtedy jest też spora szansa na zwycięstwo.

Zwycięzcą zostanie osoba, która zdobędzie najwięcej punktów!

2. ZAWARTOŚĆ PUDEŁKA

W pudełku z grą *Odkrywcy Internetu* znajdują się:

» plansza
» talia 60 kart internauty, 4 karty celu, 6 kart wydarzeń
» komplet 5 znaczników graczy w 4 kolorach
» kostka
» znacznik rundy i znacznik gracza rozpoczynającego
» instrukcja

znaczniki graczy

karty wydarzeń

znacznik rundy i znacznik gracza rozpoczynającego

plansza

karty celu

karty internauty

3. PRZYGOTOWANIE GRY

1. Rozłóżcie planszę na środku stołu tak, aby wszyscy gracze mieli do niej łatwy dostęp.
2. Wszystkie karty wydarzeń potasujcie i ułóżcie jako zakryty stos obok planszy.
3. Niech każdy z graczy weźmie komplet znaczników w wybranym przez siebie kolorze i ustawi je na planszy na startowych polach Toru Punktacji i Torów Umiejętności (oznaczonych cyfrą zero).
4. Talię kart internauty potasujcie i rozdajcie każdemu z graczy po dwie z nich. Resztę kart internauty odłóżcie obok planszy jako zakryty stos - będą potrzebne dopiero w dalszej części rozgrywki.
5. Znacznik rundy ustawcie na pierwszym polu Toru Rund, a znacznik gracza rozpoczynającego przekażcie osobie, którą wylosujeciecie lub wybierzecie. Osoba ta będzie graczem rozpoczynającym w pierwszej rundzie gry.

W wariancie rozszerzonym, który polecamy starszym lub bardziej doświadczonym graczom, należy rozdać każdemu po jednej karcie celu. Po zapoznaniu się z nią, gracz powinien trzymać tę kartę w tajemnicy i odkryć dopiero na końcu gry przy podliczaniu punktów. Na kartach tych zapisane są dwa warunki, które gracz musi spełnić, by otrzymać dodatkowe punkty.

4. PRZEBIEG RUNDY

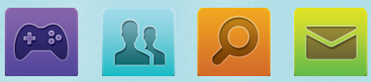
W każdej rundzie, najpierw gracz rozpoczynający, a potem pozostali - zawsze w kierunku zgodnym z ruchem wskazówek zegara, wybiera jedną z dwóch trzymanych w ręce kart i wykłada ją rewersem do góry przy krawędzi planszy przed sobą.

UWAGA!

Na każdej karcie *internauty znajdują się wskazówki przydatne później przy korzystaniu z Internetu. Warto je uważnie czytać i zapamiętywać treści zawarte na tych kartach, ponieważ w trakcie gry gracze będą musieli wykazać się ich znajomością.*

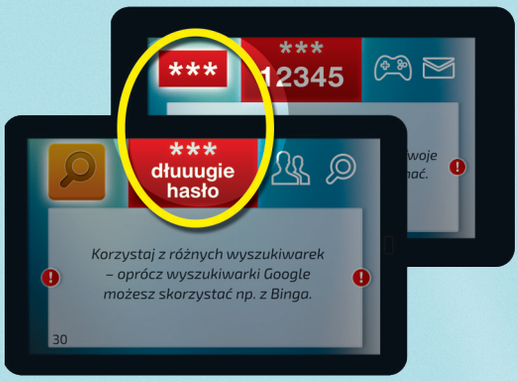
Zachowując tę samą kolejność, gracze wybierają jedną z wyłożonych przed chwilą kart lub kartę z wierzchu talii kart internauty. Wybierając kartę leżącą przy krawędzi planszy, gracz musi pamiętać, że nie może to być karta, którą sam wyłożył. Jeżeli w którymś momencie gry karty w talii kart internauty wyczerpią się, należy natychmiast przetasować stos kart odrzuconych i stworzyć z nich nową talię kart internauty.

Następnie gracze, według ustalonej wcześniej kolejności, wybierają i zagrywają jedną z kart, które trzymają w ręku.
Jeśli kolorowa ikona w lewym górnym rogu zagranej karty jest jedną z poniższych:



gracz sprawdza, czy po prawej stronie u góry drugiej karty znajduje się biały odpowiednik tej ikony. Jeśli tak - gracz zagrywa tę kartę i przesuwa swój znacznik o dwa pola na Torze Umiejętności oznaczonym wybraną ikoną. Jeśli natomiast na drugiej karcie brak jest odpowiedniej białej ikony, gracz również zagrywa kartę i porusza swój znacznik na tym torze o 1 pole.
Jeżeli podczas tego ruchu znacznik miałby przesunąć się na pole o wartości wyższej niż 9, zatrzymuje się on na polu o wartości 9.

Jeśli kolorowa ikona na zagranej karcie wygląda następująco:



gracz nie przesuwa znaczników na Torach Umiejętności, lecz tworzy swoje hasło. W tym celu odkłada obok siebie drugą z kart. Decydując się na taką akcję, gracz powinien zwrócić uwagę na ciąg znaków znajdujący się na czerwonym tle, na górze, pośrodku tej karty. Każda odkładana przez gracza karta powinna posiadać ciąg znaków z innej kategorii, np.: **!@#$%**, **12345**, **53zBr3**, **abcde**, **ABCDE**, **dłuuugie hasło**. Im więcej różnych kart gracz zdoła odłożyć w ciągu całej rozgrywki, tym więcej uzyska punktów za hasło na koniec gry.

Kiedy ostatni gracz wykona swój ruch, należy wszystkie zagrane w danej rundzie karty internauty (oprócz kart, które służą do tworzenia hasła) odłożyć na stos kart odrzuconych.

Następnie należy sprawdzić na Torze Rund, czy między polem oznaczającym aktualną rundę a polem kolejnej rundy nie zapisano informacji o dodatkowym wyzwaniu czekającym na graczy. Jeśli nie, gracz, który rozpoczynał zakończoną właśnie rundę przekazuje swój znacznik osobie siedzącej po jego lewej stronie oraz przesuwa znacznik na Torze Rund o jedno pole. Następnie ponownie rozdaje się po dwie karty z talii internauty i rozpoczyna nową rundę.

UWAGA!

Zauważ, że każda karta internauty ma na odwrocie umieszczone te same białe ikony oraz ciąg znaków hasła, co na awersie, aby ułatwić wybór przy dobieraniu karty.

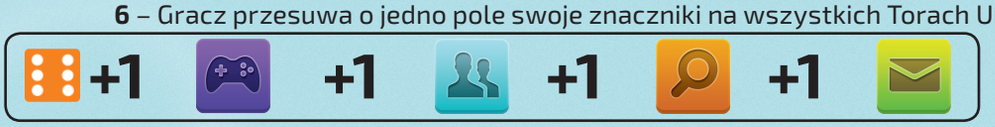
Jeżeli natomiast na Torze Rund, między polami minionej i kolejnej rundy, widnieje jakiś dodatkowy zapis, gracze - jeszcze przed rozpoczęciem nowej rundy - stawiają czoło odpowiedniemu, dodatkowemu wyzwaniu. Wyzwania rozgrywa się według następujących zasad:

A. **KOSTKA** – Każdy z graczy po kolei rzuca kostką i z żółtej karteczki, znajdującej się w lewym górnym rogu planszy, odczytuje, jaki bonus otrzymuje.

1-4 – Gracz przesuwa o dwa pola swój znacznik na wylosowanym Torze Umiejętności według poniższego schematu:

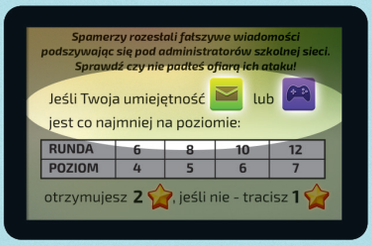
5 – Gracz może wyszukać sobie jedną kartę ze stosu kart odrzuconych i dołączyć ją do swojego hasła. Jeżeli w tym stosie gracz nie znajdzie żadnej przydatnej karty, może przeszukać zakryty stos kart internauty. W tym przypadku jednak, po wybraniu karty, stos ten należy od razu przetasować.

6 – Gracz przesuwa o jedno pole swoje znaczniki na wszystkich Torach Umiejętności.



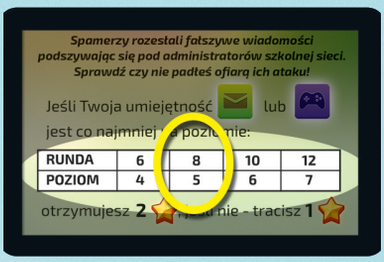
B. **QUIZ** – Gracz posiadający aktualnie znacznik gracza rozpoczynającego może - jako pierwszy - podać zapamiętaną przez siebie wskazówkę z dowolnej karty internauty. Jeśli to zrobi, otrzymuje 1 punkt, który natychmiast zaznacza sobie na Torze Punktacji. Następnie także kolejni gracze mogą przytoczyć zapamiętaną przez siebie wskazówkę z dowolnej karty internauty. Uwaga! Gracze otrzymują punkty tylko za wskazówki niewspomniane jeszcze ani w obecnej, ani żadnej wcześniejszej rundzie.

C. **TEST** – Aktualny gracz rozpoczynający odkrywa wierzchnią kartę z talii wydarzeń i czyta na głos jej tekst. Karta wydarzeń zawiera opis autentycznej sytuacji i powiązane z nią zadanie. Każdy gracz sprawdza, czy osiągnął wymagany dla danej rundy poziom którejś z wymienionych na karcie umiejętności.



Jeżeli w którejkolwiek z wymaganych umiejętności gracz osiągnął poziom wskazany w tabeli na karcie wydarzeń (lub poziom wyższy), otrzymuje 2 punkty. W innym wypadku gracz traci 1 punkt. Zyskane / utracone punkty gracze natychmiast zaznaczają na Torze Punktacji.

Przykład: *Na koniec ósmej rundy Jacek (kolor żółty), który jest graczem rozpoczynającym, odkrywa kartę z talii wydarzeń. Ponieważ poziom jego umiejętności E-MAIL wynosi 4 a GRY ONLINE 3, traci on jeden punkt. Natomiast poziom umiejętności E-MAIL Beaty (kolor czerwony) wynosi 0, ale GRY ONLINE ma na poziomie 7, więc spełniła warunek z karty i otrzymuje dwa punkty.*



> ***UWAGA!***
> Zwróćcie uwagę, że poziom umiejętności, jaki w danej rundzie powinniście osiągnąć, podany jest zawsze przy słowie TEST na Torze Rund.

Po rozpatrzeniu dodatkowego wyzwania, zgodnie ze wskazaniami Toru Rund (KOSTKA, QUIZ, TEST), rozpoczyna się kolejna runda gry. Gracz rozpoczynający poprzednią rundę przekazuje znacznik gracza rozpoczynającego osobie po swojej lewej stronie, a znacznik na Torze Rund przesuwa o jedno pole w prawo. Następnie nowy gracz rozpoczynający rozdaje każdemu z graczy po dwie karty internauty.

5. KONIEC GRY

Po dwunastej rundzie gra kończy się i gracze podliczają swoje punkty. Każdy z graczy - do punktów zdobytych już w trakcie rozgrywki - dodaje najpierw punkty za utworzone przez siebie hasło. Liczba otrzymanych punktów zależy od jakości hasła, czyli od liczby odłożonych kart z różnymi ciągami znaków (patrz tabela).

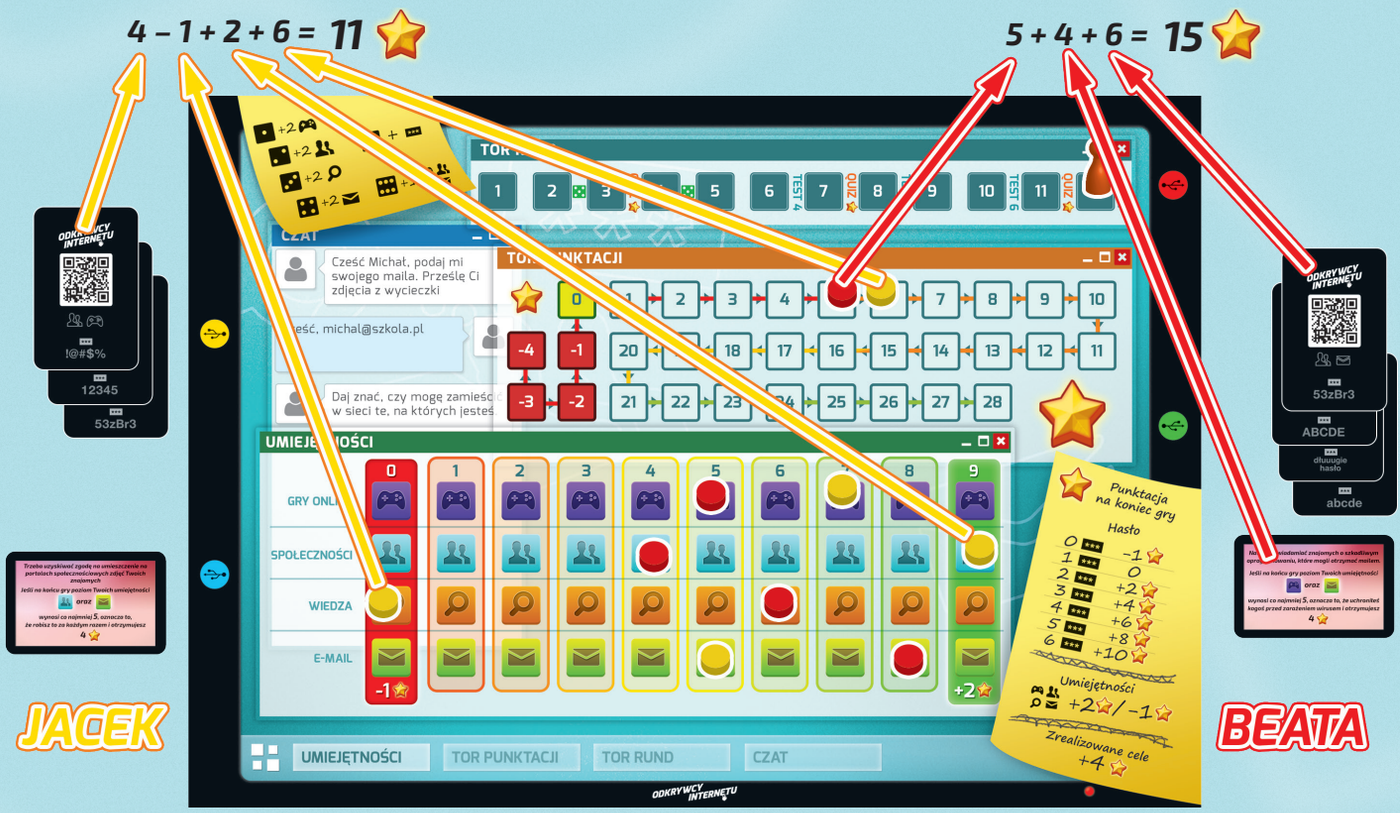
Liczba różnych odłożonych kart ***	Zdobyte punkty ★
0	–1
1	0
2	+2
3	+4
4	+6
5	+8
6	+10

Gdy gracz na którymś z Torów Umiejętności posiada znacznik na polu oznaczonym cyfrą 9, dodaje za każdy taki znacznik do swojej punktacji 2 punkty. Jeśli natomiast znacznik znajduje się na polu oznaczonym cyfrą 0, gracz odejmuje za każdy taki znacznik od swojej punktacji 1 punkt.

Jeżeli na początku gry uczestnicy otrzymali karty celów, należy je teraz odkryć. Wyszczególnione są na nich dwie umiejętności, na które gracze powinni zwrócić szczególną uwagę podczas gry. Zestawy tych umiejętności są inne dla każdego gracza. Aby otrzymać dodatkowe punkty, należy uzyskać na odpowiednich torach wskazany na karcie poziom.

Rozgrywkę wygrywa gracz z największą liczbą punktów. W przypadku remisu zwycięzcą zostaje gracz z najsilniejszym hasłem, czyli takim, w którym znajduje się najwięcej ciągów znaków różnego rodzaju.

Przykład punktacji na koniec rozgrywki między Jackiem i Beatą.



Przykład: *Jacek podlicza swoje punkty na koniec gry. W trakcie rozgrywki zdobył ich 6 (5 za TEST i 1 za QUIZ), a dodatkowo za pomocą trzech kart stworzył hasło, które przyniosło mu 4 punkty. Jeden z jego znaczników znalazł się na polu 9 Toru Umiejętności WIEDZA i za to Jacek otrzymał 2 punkty, ale inny znacznik pozostał niestety na polu 0, co oznacza dla Jacka stratę jednego punktu. Okazało się też, że nie udało mu się spełnić warunku z Karty Celu, więc nie może dodać sobie 4 kolejnych punktów, które otrzymałby za jego realizację. Ostatecznie Jacek zdobywa 11 punktów.*

Beata natomiast w trakcie gry uzyskała 5 punktów (2 za TEST i 3 za QUIZ), a za 4 karty, które odłożyła dla stworzenia hasła, otrzymuje dodatkowo 6 punktów. Żaden z jej znaczników nie znalazł się na polu 9 w obszarze na Torach Umiejętności, ale żadnego znacznika nie pozostawiła tam na polu 0. Nie zyskuje więc i nie traci za nie żadnych punktów. Beata, w przeciwieństwie do Jacka ,zrealizowała swój cel, więc dodaje sobie 4 punkty. W sumie zdobywa 15 punktów i to ona właśnie zostaje zwycięzcą.

BEZPIECZNIK

czyli MINIPORADNIK INTERNAUTY

dr Augustyn Surdyk, dr Emanuel Kulczycki, Urszula Cimoch

Większość z nas nie wyobraża sobie życia bez Internetu. Jednak wciąż wśród użytkowników sieci ogromną rzeszę stanowią ci, którzy pamiętają czasy przed „erą Internetu". Mówi się, że pokolenie dorosłych, które wymyśliło Internet i jest jego pierwszym użytkownikiem, to cyfrowi imigranci. Natomiast pokolenie urodzone w latach 90–tych ubiegłego wieku miałoby być cyfrowymi tubylcami, czyli osobami, które wychowały się pośród globalnej sieci.

Powyższy podział, choć wygląda efektownie nie powinien być podstawą działań edukacyjnych. Okazuje się bowiem, że badania dotyczące cyfrowych tubylców nie potwierdzają czarno–białego podziału na „starych", którzy „nie czują" Internetu oraz „młodych", którzy „rodzą się" w świecie z Internetem , dorastają w nim i przez to „przesiąkają" siecią. Jak zwykle wszystko jest bardziej skomplikowane i okazuje się, że ci cyfrowi tubylcy, to raczej dzieci sieci, które trzeba nauczyć poruszania się w Internecie, wyszukiwania i krytycznej oceny informacji oraz korzystania z zasobów Internetu z poszanowaniem praw twórców.

Ma to oczywiście swoje dobre i złe strony: przede wszystkim ogromna odpowiedzialność spada na tych cyfrowych imigrantów, którzy muszą po prostu w procesie edukacji medialnej i informacyjnej nauczyć dzieci i młodzież korzystania z sieci oraz przebywania w Internecie (taki proces najczęściej jest prowadzony w szkołach i bibliotekach). Zatem edukację warto zacząć od uwrażliwienia na pewne zjawiska, objaśnienia tych obszarów, które najczęściej są przez dzieci pomijane.

Celem naszej gry jest zwrócenie uwagi na zasady i obyczaje panujące w sieci oraz przyjęcie metod postępowania wobec zagrożeń, z którymi można się spotkać. Są one w większości rozpoznane i nazwane (zob. opisy kart), można ich więc uniknąć.

Materiał ten nie jest systematyczną wykładnią „zasad użytkowania Internetu", lecz jest poradnikiem. Na konkretnych przykładach ma pokazać dzieciom i młodzieży, jakie mogą być konsekwencje niewłaściwych zachowań i co można zrobić, aby ich uniknąć.

Poniższy materiał przeznaczony jest przede wszystkim dla osób pracujących z dziećmi i młodzieżą. Ma na celu przekazanie wiedzy na temat świadomego korzystania z Internetu, wykorzystania jego możliwości i unikania zagrożeń. Tematyka i materiały do gry dotyczą więc bezpieczeństwa informacyjnego, prawa autorskiego i ochrony własnej prywatności w sieci.

Mimo, że tekst ma być wsparciem dla dorosłych, zwracamy się w nim bezpośrednio do naszych najważniejszych odbiorców, dzieci i młodzieży. Dlatego pewne rzeczy są uproszczone, a niektóre aspekty musieliśmy pominąć. Jednak celem naszej gry nie jest wpojenie pełnej wiedzy o kompetencjach medialnych, lecz sprawienie, iż nasi odbiorcy zauważą, że warto je rozwijać oraz że „świat Internetu" jest o wiele bardziej skomplikowany niż może się to wydawać na pierwszy rzut oka.

W dalszej części tekstu zamieszczamy opisy kart odpowiadające numerom kart internauty w grze planszowej „Odkrywcy Internetu". Oznacza to, że wiedzę z danej karty można poszerzyć zaglądając pod właściwy numer w zestawieniu.

I E-MAIL

1. *Nie wysyłaj wiadomości jednocześnie do wszystkich osób, które masz w książce adresowej.*

Kiedy chcesz wysłać e–mail jednocześnie do wielu osób, które się nie znają (np. Twoi znajomi, kuzyni, koledzy z klasy), pamiętaj o tym, aby odpowiednio zaadresować wiadomość. Najlepsze, co możesz zrobić, to ukryć odbiorców wiadomości (taka opcja nazywa się najczęściej „ukryty adresat", „ukryte do wiadomości", „UDW"). Możesz się zastanawiać, dlaczego jest to ważne? Przede wszystkim dlatego, że niektórzy odbiorcy Twoich wiadomości mogą sobie nie życzyć ujawniania ich adresu. Jeśli nie ukryjesz nieznających się adresatów, to nie złamiesz prawa. Natomiast sprawi to, że nie zastosujesz się do zasad dobrych obyczajów w komunikacji – a te są jednakowo ważne. Dowiedz się, jakie są inne zasady w komunikacji mailowej – przeczytaj opis karty **nr 8**.

2. *Kiedy przesyłasz znajomym zdjęcia wykonane przez innych, pisz kto jest ich autorem.*

Pamiętaj o tym, że przypisanie sobie autorstwa czyjegoś utworu jest plagiatem. Dlatego warto wiedzieć, kim jest twórca i czym jest plagiat. *Twórca* jest autorem utworów, czyli tego, co powstanie, gdy narysujesz obrazek czy napiszesz tekst piosenki. Kiedy jesteś twórcą, zawsze masz prawo podpisywać swoje dzieło i nikt nie może odebrać Ci autorstwa Twojego utworu. *Plagiat* to skopiowanie czyjegoś utworu lub jego części i przypisanie sobie autorstwa. Jeśli Twój kolega napisze wypracowanie, Ty je przepiszesz i powiesz, że sam je napisałeś, wówczas popełnisz plagiat.

3. *Nigdy nie podawaj przez telefon, w mailu lub SMS–ie żadnych danych osobowych (własnych lub znajomych), jeśli nie znasz osób, do których piszesz.*

Tak, jak nie otwierasz drzwi obcym, tak nie podawaj danych osobowych nieznajomym, którzy z Tobą korespondują. Tym nieznajomym może być ktoś, kto przedstawia się jako administrator poczty, znajomy z pracy Twoich rodziców, czy inna osoba próbująca zdobyć Twoje zaufanie, a której nie znasz osobiście. Nie podawaj żadnych informacji, o które prosi, aby nie wykorzystał ich przeciwko Tobie. To może być próba oszustwa – *scammingu* lub *phishingu*. Dowiedz się czym są wymienione zjawiska – zapoznaj się z opisem kart **nr 10 i 12**.

4. *Nigdy nie odwiedzaj linków przesyłanych w mailach od nieznajomych ani nie otwieraj od nich załączników – mogą zawierać złośliwe oprogramowanie i uszkodzić Twój komputer.*

Sam fakt, że ktoś nieznajomy do Ciebie pisze powinien wzbudzić Twoje podejrzenia. Nie tylko nie odpisuj na wiadomości od niego, lecz tym bardziej nie wchodź na strony, których linki Ci przesyła i na które zaprasza. Mogą zawierać złośliwe oprogramowanie.

Złośliwe oprogramowanie (ang. *malicious software*, w skrócie *malware*) to wszelkie aplikacje, skrypty i inne programy, które zostały stworzone dla szkodliwych, złośliwych lub przestępczych celów. Wyróżnia się wiele rodzajów złośliwego oprogramowania. Najpopularniejsze z nich to wirusy, robaki (ang. *worm*, *bug*), programy szpiegujące i trojany. Mogą zostać zakodowane niemal w każdym typie pliku wysłanym do Ciebie w załączniku wiadomości e–mail np. łańcuszka szczęścia (nawet wysłanego w pozornie szczytnym celu) – dlatego nigdy nie przesyłaj ich dalej, jakkolwiek by Cię do tego zachęcała lub próbowała zmusić ich treść. Złośliwe oprogramowanie może być też ukryte na stronach internetowych. Wejście na takie strony grozi ich automatycznym zainstalowaniem się na Twoim komputerze (patrz opis karty **nr 35** – *pharming*). Przez złośliwe oprogramowanie haker może przejąć kontrolę nad Twoim komputerem, wykraść lub usunąć dowolne pliki, poznać Twoje hasła lub wyrządzić inne szkody. Może również wysyłać bez Twojej wiedzy spam z Twojej skrzynki pocztowej do wszystkich znajomych i tym samym włączyć Twój komputer do sieci uśpionych komputerów będących pod kontrolą hakera (ang. *botnet*, *zombie network*).

5. *Nie przesyłaj dalej Twojej korespondencji ze znajomymi – mogą sobie tego nie życzyć*

Znajomy napisał do Ciebie e–mail i masz ochotę podzielić się jego treścią z innymi osobami z klasy. Nie zawsze możesz to zrobić. Prywatne listy oraz maile objęte są tajemnicą korespondencji, dlatego zanim przekierujesz czyjąś wiadomość, zastanów się czy na pewno jej autor chce, aby inni czytali Waszą rozmowę. Pamiętaj również, że cytując wypowiedź znajomego należałoby zapytać go o zgodę.

6. *Używaj dobrego programu antimalware (zwalczającego złośliwe oprogramowanie), dbaj o jego aktualizację i regularnie skanuj komputer.*

Używanie programu zwalczającego złośliwe oprogramowanie jest obecnie sprawą tak oczywistą, jak zabieranie parasola na spacer w deszczu. Kto ich nie używa sam prosi się o kłopoty. Bez parasola zmokniesz i nabawisz się kataru, bez programów ochronnych Twój komputer nabawi się wirusa lub robaka. Jak jeszcze możesz zadbać o swój komputer – przeczytaj opis karty **nr 7**.

7. *Używaj dobrego programu antywirusowego, dbaj o jego aktualizację i regularnie skanuj komputer.*

Posiadanie zainstalowanego na komputerze programu antywirusowego i zwalczającego złośliwe oprogramowanie jest pierwszym i najważniejszym warunkiem wejścia do Internetu. Bez tego surfowanie w sieci jest jak wsadzenie nogi w mrowisko. Programy systemowe (które zawierają fabrycznie systemy operacyjne) są zwykle niewystarczającą ochroną przed zagrożeniem wirusami i innymi atakami (np. złośliwego oprogramowania). Sam fakt posiadania programu antywirusowego nie wystarcza, by być bezpiecznym w sieci. Trzeba jeszcze zadbać o jego aktualizację – najlepiej uaktywnić opcję automatycznych aktualizacji zaraz po jego zainstalowaniu. Codziennie odkrywane są nowe, bardziej przebiegłe i szkodliwe wirusy a nieaktualizowany program nie potrafi ochronić przed nimi.

8. *Nie przesyłaj dalej „łańcuszków szczęścia", ponieważ zostaniesz spamerem.*

„Łańcuszki szczęścia" to wiaodomości e–mail, które niezależnie od ich treści kończą się prośbą o przesłanie ich dalej do jak największej liczby osób. Mogą do tego zachęcać różnego rodzaju korzyściami, popartymi wymyślonymi przykładami (np. „Janek wysłał tę wiadomość do 10 znajomych i po 2 dniach wygrał na loterii") lub mogą grozić tym, co złego może Cię spotkać, jeśli nie spełnisz tej prośby. Mogą również wyglądać na charytatywne akcje (np. zbieranie pieniędzy na leczenie chorego dziecka) lub przekazywać użyteczne informacje (np. jak postępować w przypadku zawału serca). Cokolwiek jednak by przekazywały zawsze chodzi o to samo – żeby je przesłać dalej do jak największej liczby odbiorców. Tym sposobem autor łańcuszka (haker) może gromadzić adresy pocztowe np. do przesyłania spamu. Łańcuszki mogą też przesyłać złośliwe oprogramowanie. Czym ono jest? Dowiedz się zaglądając do opisu karty **nr 4**.

9. *Nie odpowiadaj na żadne maile od nieznajomych.*

Z pewnością każdy byłby zdziwiony dostając e–mail od kogoś nieznajomego. Osoby dobrze wychowane zwykle przedstawiają się i piszą skąd Cię znają. Nawet jeśli podają takie informacje, a wiesz, że nie mogły Cię poznać we wspomnianych miejscach (w sieci lub w „realu"), to może być scam, więc powiedz o tym rodzicom. Dowiedz się, czym jest scam oraz jak działa. Zapoznaj się z opisem karty **nr 10**.

10. *Jeśli ktoś ofiaruje Ci w mailu wielkie pieniądze, to jest to scam – nie odpowiadaj na taką wiadomość.*

Scamming jest oparty na zdobyciu zaufania ofiary, a następnie wprowadzeniu w błąd poprzez informację, iż jest lub może być beneficjentem określonego dobra (najczęściej finansowego) np. wygranej na loterii, odziedziczenia spadku i nakłanianie do nieczystych transakcji. Jeśli ktoś ofiaruje Ci fortunę za nic, to zwykle jest to zbyt piękne, by było prawdziwe.

11. *Jeśli chcesz, żeby traktowano Cię poważnie pisz bez błędów ortograficznych i nie nadużywaj przycisku Caps Lock – inni mogą mieć wrażenie, że „krzyczysz".*

Pisząc e–mail stosuj zasady ortografii i interpunkcji (przecinki, kropki, pytajniki itp.) oraz używaj znaków diakrytycznych. Popełniając błędy w pisowni pokazujesz się z negatywnej strony i wpływa to na Twój wizerunek. Kiedy piszesz wielkimi literami, odczytujący Twoją wiadomość ma wrażenie, że „krzyczysz". Warto zwracać uwagę na wymienione zasady, aby Twój rozmówca dobrze Cię zrozumiał i czytanie Twojego tekstu nie było dla niego uciążliwe.

12. *Nie podawaj nikomu loginu i hasła do skrzynki pocztowej nawet, jeśli podaje się za administratora – to jest próba phishingu.*

Phishing (inna nazwa to *spoofing* – nabieranie) należy do najbardziej wyrafinowanych metod oszustw. Pochodzenie słowa *phishing* najczęściej rozszyfrowuje się jako ***p**assword **h**arvesting **fishing*** (łowienie haseł) Polega na podszywaniu się i odgrywaniu roli osoby lub instytucji godnej zaufania (np. informatyka, administratora sieci, banku itp.) i dokonania oszu-

stwa. Celem *phishingu* jest osiągnięcie korzyści finansowych poprzez wyłudzenie od ofiary danych, poświadczeń, haseł z zamiarem przejęcia konta poczty elektronicznej i dalszego rozsyłania z niego spamu lub/i wyłudzenie dostępu do konta bankowego, karty kredytowej itp. w celu kradzieży zasobów finansowych. Dlatego nie podawaj w treści wiadomości e–mailowej lub innych serwisach żadnych swoich haseł do konta.

II SPOŁECZNOŚCI

13. *Nie pisz postów na serwisach społecznościowych pod wpływem silnych emocji (np. gniewu, złości). Najpierw przemyśl, co chcesz napisać.*

Serwisy społecznościowe zachęcają nas do napisania, jak się czujemy, co dzisiaj robiliśmy, co oglądaliśmy. Za każdym razem, kiedy dodajesz takie wiadomości, pomyśl przez chwilę, czy na pewno chcesz, aby ktoś to jutro, za tydzień czy za rok mógł przeczytać. Często jesteśmy bardzo zdenerwowani i źli: na kolegę, na rodziców, na nauczyciela. Pod wpływem gniewu chcemy o tym napisać na naszym profilu. A co będzie, jeśli okaże się, że nasza złość i zdenerwowanie były nieuzasadnione? Dlatego pamiętaj, żeby swoje profile w serwisach społecznościowych traktować jako swoją wizytówkę. A taka wizytówka jest widoczna przez wiele lat.

Kiedy umieszczasz w Internecie komentarz na forum, piszesz post na Facebooku, czy zamieszczasz swoje zdjęcie na Instagramie, pamiętaj, że to pozostanie widoczne bardzo długo. Co ważniejsze, nie możesz całkowicie usunąć z sieci tego, co zostało tam przez Ciebie wprowadzone. Dlatego z Internetu, jak z każdego sposobu komunikacji, trzeba korzystać bardzo rozważnie.

14. *Kiedy zamieszczasz w serwisach społecznościowych zdjęcia swojego autorstwa, masz prawo je podpisać swoim imieniem i nazwiskiem lub pseudonimem.*

Zrobiłeś ciekawe zdjęcie na wycieczce? Sfotografowałeś swojego psa i chcesz pokazać zdjęcie znajomym przez portal społecznościowy? Pewnie! To bardzo dobry pomysł. Robiąc zdjęcie, stajesz się jego twórcą. A dzięki temu masz pełne prawo, aby mówić i pisać, że to Twoja praca. To sprawia, że jako twórca możesz je podpisywać swoim imieniem i nazwiskiem (lub pseudonimem). Dlatego też pamiętaj, aby nie podpisywać się w ten sposób pod zdjęciami, tekstami czy wypracowaniami, których nie jesteś autorem. Sprawdź, jak nazywa się podpisywanie pod nie swoimi utworami – przeczytaj opis karty **nr 2**.

15. *Nie spędzaj zbyt wiele czasu w Internecie. Świat za oknem jest o wiele ciekawszy.*

Fajnie jest mieć znajomych w całej Polsce i nawet za granicą. Nie zapominaj jednak o Twoich

bliskich, których masz na wyciągnięcie ręki. Zamiast przesiadywać godzinami w Internecie spotkaj się z kolegami/koleżankami z klasy, wyjdź pobawić się na podwórko lub boisko, zaproś znajomych do domu, idź na urodziny kuzynki.

16. *Gdy zagrożone jest ludzkie zdrowie lub życie nie rób zdjęć, żeby umieścić je w sieci tylko dzwoń po pomoc.*

W sytuacji, w której zagrożone jest czyjeś zdrowie lub życie, nie skupiaj się na dokumentowaniu tych wydarzeń. Zamiast robić zdjęcie, które zamieścisz w sieci, pomóż innym dzwoniąc pod numer 112 po pogotowie lub straż pożarną.

17. *Jeśli ktoś nieznajomy prosi Cię w Internecie o Twoje zdjęcie lub film z Twoim udziałem lub chce się z Tobą spotkać „w realu", powiedz o tym rodzicom.*

Zachowaj ostrożność, jeśli nowopoznana osoba po wymianie kilku maili/postów na forum, lub nawet po kilku rozmowach na czacie prosi Cię o zdjęcie lub film z Twoim udziałem albo chce się z Tobą spotkać. Gdy to się wydarzy, powiedz o tym rodzicom.

18. *Nie zezwalaj znajomym na publikowanie w Internecie Twoich zdjęć lub filmów bez Twojej zgody.*

Nikt nie lubi, gdy ktoś pokazuje (tym bardziej udostępnia w Internecie) zdjęcia lub filmy, na których źle wyszedł lub nie chciałby, by były dostępne dla wszystkich z jakichkolwiek innych powodów. Dlatego poproś swoich znajomych, żeby za każdym razem, gdy chcą udostępnić w sieci zdjęcia lub filmy z Twoim udziałem, pytali Cię o zgodę i odwdzięcz się tym samym. Obiecaj, że też będziesz ich pytać o zgodę kiedy będziesz umieszczać zdjęcia z ich wizerunkiem. Czasem na zdjęciach lub filmach pokazujemy zbyt wiele, zachowujemy się zbyt swobodnie albo zrobiono nam zdjęcie w kłopotliwej sytuacji. Masz prawo do zachowania kontroli nad swoim wizerunkiem w sieci.

19. *Upewnij się, czy wydarzenie, które zakładasz na portalu społecznościowym (np. swoje urodziny) nie jest publiczne.*

Niedługo masz urodziny i chcesz zaprosić gości do swojego domu. Zakładasz wydarzenie na portalu społecznościowym i wysyłasz zaproszenia do znajomych. Pamiętaj, aby w ustawieniach oznaczyć spotkanie jako niepubliczne, ponieważ w sieci informacja o Twoich urodzinach może szybko się rozprzestrzenić i zamiast kameralnej imprezy zjawi się na niej 200 osób, których zupełnie nie znasz.

20. *Nie bądź „hejterem", nie umieszczaj na forach i portalach społecznościowych obraźliwych treści. Możesz za to ponieść konsekwencje.*

Nikt w sieci nie jest anonimowy nawet, jeśli posługuje się pseudonimem. Dlatego zachowuj się kulturalnie i nie obrażaj nikogo w Internecie. Każdy komputer pozostawia w sieci pliki cookies (tzw. ciasteczka), które są jak odciski palców i można wytropić jego użytkownika po indywidualnym i niepowtarzalnym numerze IP (ang. *Internet Protocole*), komputera. Sprawdź, w jakich innych sytuacjach warto o tym pamiętać – zapoznaj się z opisem karty **nr 13**.

21. Nie podawaj w Internecie więcej danych o sobie, niż to konieczne.

Pisząc w sieci swój adres domowy i chwaląc się na swoim profilu na portalu społecznościowym tym, w jakim domu mieszkasz, jego wyposażeniem, samochodem rodziców, tym, gdzie i kiedy wybierasz się z rodzicami na wakacje, możesz zaprosić do swego domu złodzieja. W pierwszej kolejności zabezpiecz profile na serwisach społecznościowych przed wizytami nieznajomych.

22. Jeśli musisz podać w Internecie swój e–mail, staraj się go zamaskować np. zamiast symbolu „@" użyj „[at]". Uchronisz się w ten sposób przed spamem.

Aby uchronić się przed spamem, należy unikać podawania własnego adresu poczty elektronicznej, zwłaszcza w miejscach ogólnodostępnych (jak strony i fora internetowe itp.). Jeśli musisz to zrobić, podaj go w zamaskowanej formie, na przykład poprzez zastąpienie znaku „@" innym symbolem lub ciągiem znaków („$", „#", „at" itp.): „adres[at]strona.pl", wstawienie w miejsce kropki wyrazu „kropka" (np. „adres@strona(kropka)pl"). Możesz też używać innych „wstawek antyspamowych" w postaci dodatkowego tekstu (np. „_wytnij_to_" lub „_NIE_SPAMEROM_"). Takie fałszowanie adresów utrudnia działanie automatycznych programów pozyskujących adresy mailowe (ang. harvester) przeszukującym sieć w poszukiwaniu „małpek". Jeśli wymagane jest podanie adresu poczty bez modyfikacji, warto przeznaczyć do tego celu osobne konto.

23. Ostrożnie wybieraj swoje zdjęcia, które chcesz zamieścić w Internecie. Możesz kiedyś żałować złego wyboru.

Zdarza Ci się zamieszczać na portalach społecznościowych zdjęcia z wycieczek lub spotkań ze znajomymi? Dobrze przemyśl, które z nich chcesz opublikować, ponieważ zostaną tam na bardzo długo. Planując swoją karierę w dorosłym życiu pamiętaj, że odkrycie kompromitującego zdjęcia może zaważyć na Twoim życiu zawodowym, np. gdy zostaniesz szanowanym prawnikiem, lekarzem, politykiem lub inną poważaną osobą lub po prostu będzie Ci wstyd. Co możesz zrobić, aby zadbać o swoją przyszłość – przeczytaj opisy kart **nr 13 i 18**.

24. Nie publikuj w Internecie zdjęć ani filmów, na których są Twoi znajomi, bez ich zgody.

Nikt nie lubi, gdy coś dzieje się bez jego wiedzy i pozwolenia. Zwłaszcza, gdy dotyczy to sfery prywatnej. Dlatego zapytaj znajomych czy zgodzą się, aby opublikować zdjęcia lub filmy, na których są widoczni. Każdy ma również prawo do ochrony swego wizerunku. Dowiedz się, co możesz zrobić, aby chronić swój wizerunek – przeczytaj opis karty **nr 18**.

III WIEDZA

25. *Kiedy pracujesz nad zadaniem domowym i wykorzystujesz zdjęcia znalezione w Internecie, podawaj informacje o autorze obrazka.*

W Internecie można znaleźć bardzo wiele przydatnych informacji. Znajdują się tam również zdjęcia, obrazki oraz filmy, które można wykorzystać do zilustrowania prac domowych. Pamiętaj jednak, aby za każdym razem, kiedy wykorzystasz czyjeś zdjęcie, napisać, kto jest jego twórcą, ponieważ autor ma do tego prawo. Kiedy wszyscy będą szanować prawa twórców, wówczas i Ty na tym skorzystasz, gdy udostępnisz swoje utwory. Dowiedz się dlaczego Ty również masz prawo do podpisywania zrobionych przez siebie zdjęć – zapoznaj się z opisem karty **nr 14**.

26. *Kiedy chcesz przywołać czyjąś wypowiedź, pamiętaj, aby zaznaczyć, że jest to cytat i podaj autora.*

W Internecie możesz przeczytać wiele ciekawych tekstów, obejrzeć mnóstwo interesujących wywiadów i filmów. Czasami ich fragmenty pasują wręcz idealnie do tego, aby je wykorzystać w pracy domowej czy wypracowaniu. Za każdym razem, kiedy przytaczasz dosłownie fragment jakiejś wypowiedzi, musisz zaznaczyć, że jest to cytat oraz musisz podać, kto jest autorem tych słów. Jak to zaznaczyć? Wystarczy użyć znaku cudzysłowu „ ". Dowiedz się, do czego jeszcze jest wykorzystywany ten znak – przejdź do opisu karty **nr 29**.

27. *Pamiętaj, że nie wszystko, co możesz przeczytać w Internecie, jest zgodne z prawdą.*

Tak jak w telewizji możesz zobaczyć wiadomości z kraju i zagranicy, które przedstawiają fakty lub możesz obejrzeć film przygodowy, w którym oprócz ludzi występują orki, trolle i gobliny, tak również w Internecie znajdują się różne rodzaje materiałów. Nie wszystkie strony internetowe zawierają prawdziwe informacje. Musisz zatem nauczyć się odróżniać wiarygodne źródła informacji od tych niewiarygodnych. Jak to zrobić? Najprostszym sposobem jest porównanie informacji na kilku stronach i serwisach: jeśli w wielu miejscach (np. również na Wikipedii) potwierdzisz te wiadomości, to możesz uznać, że są one rzetelne.

Nie wszyscy użytkownicy Internetu piszą prawdę o sobie i innych. Niektórzy kłamią chcąc przedstawić kogoś w negatywnym świetle i sprawić, aby był źle oceniany. Może to wpłynąć negatywnie na wizerunek tej osoby i spowodować dalsze nieprzyjemne konsekwencje.

28. *Pamiętaj, że w wynikach wyszukiwania mogą pojawić się linki do nielegalnych filmów i gier.*

W wynikach wyszukiwania możesz znaleźć różne nieprawdziwe informacje czy zdjęcia, które zostały zmanipulowane. Mogą zostać wyświetlone linki do różnych nielegalnych materiałów. Musisz pamiętać, aby sprawdzić czy link lub informacja są wiarygodne (np. poprzez porównanie z innymi serwisami). Kiedy nie masz pewności, czy masz prawo pobrać grę lub film, najlepiej zapytaj rodziców, opiekunów, nauczycieli lub bibliotekarza. Dowiedz się, dlaczego nie wszystko co znajduje się w Internecie, znalazło się tam w sposób legalny – patrz opis karty **nr 44**.

29. *Wpisuj wyszukiwaną frazę w cudzysłowie, aby znaleźć najlepsze wyniki. Na przykład „prawo autorskie".*

Wyszukiwanie informacji w Internecie może wydawać się bardzo proste. I tak w rzeczywistości jest, jednak czasami uzyskujemy nadmiar wyników. To sprawia, że nie potrafimy odnaleźć tego najlepszego, którego naprawdę szukamy. Dlatego warto nauczyć się kilku trików, które sprawią, że nasze poszukiwania będą efektywniejsze. Jednym z najlepszych jest wpisywanie poszukiwanych fraz (czyli co najmniej dwóch wyrazów) pomiędzy znaki cudzysłowu. Jeśli szukasz frazy i wpiszesz: *prawo autorskie*, to uzyskasz wyniki, które zawierają słowo *prawo* oraz wyniki, które zawierają słowo *autorskie*. Ale Tobie przecież chodzi o wyniki, w których znajdziesz całą frazę, czyli *prawo autorskie*. Dlatego w wyszukiwarce wpisuj poszukiwane wyrazy w cudzysłów, czyli: „prawo autorskie". W ten sposób uzyskasz interesujący Cię efekt!

30. *Korzystaj z różnych wyszukiwarek – oprócz wyszukiwarki Google możesz używać innych.*

Tak jak jest wiele bibliotek, które mają różne księgozbiory i katalogi, tak też w Internecie znajdują się różne wyszukiwarki. Czasami jest tak, że w jednej wyszukiwarce nie możesz znaleźć żadnych interesujących Cię informacji. Wówczas warto skorzystać z innego narzędzia: chociaż najczęściej korzystasz z Google, spróbuj czasami użyć wyszukiwarki Bing (http://bing.com). Dowiedz się, jak mogą przydać się różne wyszukiwarki podczas porównywania źródeł informacji – zapoznaj się z opisem karty **nr 28**.

31. *Szukaj filmów, zdjęć i muzyki w legalnych serwisach – np. w Wikipedii.*

W Internecie znajduje się mnóstwo filmów, obrazków i muzyki. Wiele z tych utworów jest dostępnych w sposób legalny i bezpłatny. Dlatego warto korzystać z zasobów sieci. Ciekawe materiały znajdziesz w Wikipedii oraz na kanałach tematycznych na YouTube. Dowiedz się, dlaczego nie wszystko co znajduje się w Internecie, znalazło się tam w sposób legalny – przeczytaj opis karty **nr 44**.

32. *Nie wchodź na nieznane strony reklamowe w Internecie – mogą zawierać wirusy.*

W Internecie poza interesującymi nas informacjami możemy się też natknąć na różnego ro-

dzaju pułapki zastawione przez hakerów. Na stronach internetowych, na które Cię zapraszają, może znajdować się złośliwe oprogramowanie. Jak działa złośliwe oprogramowanie dowiesz się z opisu karty **nr 4**.

33. *Nie instaluj oprogramowania z nieznanych źródeł – może to być złośliwe oprogramowanie (ang. malware).*

Często w Internecie można znaleźć legalne i darmowe oprogramowanie. Jeśli jednak nie jest zamieszczone na wiarygodnej stronie, np. na stronie producenta lub w znanym serwisie z legalnym oprogramowaniem, może to być złośliwe oprogramowanie. Czym jest złośliwe oprogramowanie, dowiesz się z opisu karty **nr 4**.

34. *Nie reaguj na żadne informacje w sieci, w których jest wiadomość o Twojej wygranej, jeśli nie masz w zwyczaju brać udziału w konkursach.*

Czy można coś wygrać, nie biorąc udziału w żadnym konkursie? Oczywiście, że nie. Dlatego nie wierz w komunikaty „Jesteś milionowym gościem na tej stronie! Czeka na Ciebie nagroda!" Najczęściej to kłamstwo – pułapka zastawiona na Ciebie przez hakera. Jeśli podobna wiadomość pojawiła się na Twoim ekranie w postaci okienka, które uniemożliwia Ci opuszczenie strony dopóki nie klikniesz jednej z możliwych opcji np. TAK/NIE, CHCĘ NAGRODĘ/NIE CHCĘ NAGRODY nie wybieraj żadnej z tych opcji i nie klikaj niczego (nawet krzyżyka w prawym górnym rogu okienka, które zwykle je zamyka). W każdym z elementów takiego okienka (nawet w „krzyżyku") może być zakodowana pułapka w postaci linku do adresu, pod którym haker zamieścił złośliwe oprogramowanie (wirusa, trojana, robaka itp.). Kliknięcie oznacza zgodę na jego wtargnięcie do Twojego komputera. Użyj wtedy kombinacji klawiszowej Alt+Ctrl+Delete (w żargonie informatyków tzw. „trzech króli") i pozbądź się kłopotliwego okienka za pomocą menadżera zadań. Jak działa złośliwe oprogramowanie – dowiesz się z opisu karty **nr 4**.

35. *Sprawdzaj dokładnie adres strony internetowej, którą chcesz odwiedzić. Podobny może być próbą pharmingu.*

Pharming jest groźniejszą i trudniejszą do wykrycia formą phishingu (patrz opis karty **nr 12**). Jest to metoda ataku w ramach mechanizmu inżynierii społecznej polegająca na przekierowaniu nawet właściwie wpisanego przez użytkownika Internetu adresu na fałszywą stronę np. imitującą najczęściej oficjalną stronę banku, w celu przejęcia danych (haseł itp.) i docelowo – kradzieży środków z konta, karty kredytowej itp. Nazwa jest wynikiem połączenia wyrazów phishing i *farming* (rolnictwo).

36. *Używaj legalnego oprogramowania, aby tworzyć nowe teksty i grafiki.*

Do pisania tekstów i robienia rysunków na komputerze potrzebujemy odpowiednich programów. Na każdym komputerze znajdziesz podstawowe programy, które jednak mogą wydać Ci się niewystarczające do tego, co akurat chcesz zrobić. Pamiętaj o tym, że można używać tylko legalnego oprogramowania, pomimo tego, że w Internecie można znaleźć różne nielegalne (pirackie) wersje. Dowiedz się, dlaczego w Internecie znajdują się różne nielegalne programy – patrz opis karty **nr 44**.

I jeszcze jedna cenna rada: pamiętaj, że *legalne* nie znaczy *płatne*. Bardzo często można znaleźć programy, które są przez twórców udostępniane bezpłatnie – wystarczy tylko poszukać!

IV GRY ONLINE

37. *Pamiętaj, że świat gry to tylko fikcja i niewiele ma wspólnego z prawdziwym światem.*

To, co jest możliwe i dozwolone w grze, podobnie jak w filmie, rzadko kiedy jest możliwe w prawdziwym życiu. Za wiele rzeczy dozwolonych w grze (np. kradzież, bójki, używanie broni itp.) można iść do więzienia w prawdziwym świecie.

38. *Nie podawaj nikomu w grach online numerów kart kredytowych rodziców.*

Podczas gry w sieci ktoś może Cię prosić o podanie numeru karty kredytowej np. aby móc grać dalej. Wtedy powiedz o tym rodzicom i w żadnym wypadku nie podawaj numeru karty kredytowej bez ich pozwolenia. To może być próba oszustwa.

39. *Ten symbol zamieszczony na grze oznacza, że zawiera ona elementy przemocy.*

40. *Ten symbol zamieszczony na grze oznacza, że pojawiają się w niej używki.*

41. *Ten symbol zamieszczony na grze oznacza, że w grze pojawia się nagość.*

Wszystkie legalnie dostępne gry posiadają obrazkowe oznakowania PEGI (Pan European Game Information) wskazujące grupę wiekową graczy (patrz opis karty **nr 43**), do których gra jest skierowana i jakie nieodpowiednie treści zawiera.

Ten symbol oznacza, że gra zawiera elementy przemocy.

Ten symbol oznacza, że w grze występuje nawiązanie do używek (np. alkoholu, narkotyków, papierosów) lub pokazane jest ich zażywanie.

Ten symbol oznacza, że w grze pojawiają się nagość i/lub zachowania seksualne, bądź nawiązania do nich.

Inne popularne symbole z oznaczeń PEGI to: wulgarny język, dyskryminacja, strach (gra może przestraszyć młodsze dzieci), hazard, gra w Internecie z innymi ludźmi. Warto się z nimi zapoznać – znajdziesz je na stronie www.PEGI.info.

42. *Nie kopiuj kupionej przez siebie gry i nie udostępniaj jej wszystkim w Internecie, ponieważ łamiesz prawo i mogą Cię uznać za pirata.*

Kiedy kupujesz grę, możesz w nią grać sam, możesz grać z kolegami i koleżankami. Możesz również pożyczyć swój egzemplarz przyjaciołom, czyli osobom, które znasz i z którymi masz bliski kontakt. Jednak kupienie egzemplarza gry nie daje Tobie prawa do zrobienia kopii gry i rozpowszechniania jej w Internecie. Nie możesz zatem wrzucić jej w taki sposób np. na serwis *Chomikuj*, aby wszyscy mogli ją stamtąd pobrać. Ponieważ w ten sposób naruszasz interes twórców gry. Dowiedz się, kim jest twórca – przejdź do opisu karty **nr 2**.

43. *Ten symbol zamieszczony na grze oznacza, że jest ona przeznaczona dla graczy we wskazanym wieku.*

Gry dostępne w sprzedaży podlegają tzw. ratingowi (klasyfikacji wiekowej) i zawierają symbole informujące o minimalnym wieku graczy, dla których gra jest przeznaczona. W Europie powszechnie przyjętym systemem ratingowym jest PEGI (Pan European Game Information), wskazująca wiek graczy (3, 7, 12, 16, 18 lat). Uzupełnieniem oznaczeń wieku, jest informacja o treściach nieodpowiednich dla danego wieku. Poznaj przykładowe z nich w opisie kart **nr 39–41**. Wszystkie informacje dotyczące ratingu i systemu PEGI oraz jego oznaczeń można znaleźć na stronie www.PEGI.info).

44. *Pamiętaj, że nie wszystko, co możesz znaleźć w Internecie, znalazło się tam w sposób legalny, dlatego rozważnie korzystaj z tego, co znajdziesz w sieci.*

Internet jest tworzony przez ludzi, jedni działają zgodnie z prawem, inni natomiast nie zawsze się do niego stosują. Dlatego nie wszystko, co możesz wyszukać w Internecie, nawet przy użyciu powszechnie dostępnych narzędzi (np. wyszukiwarki Google) znalazło się tam zgodnie z prawem. Możesz zapytać, jak to możliwe? Nie zawsze użytkownicy robią to celowo. Czasami wystarczy, że internauta nie wiedział, że pewne czynności są niedozwolone. Chodzi tutaj np. o udostępnianie swojej gry wszystkim użytkownikom sieci. Dowiedz się, dlaczego nie można postępować w taki sposób – przeczytaj opis karty **nr 42**.

45. *To, czego Twój bohater może dokonać w grze najczęściej jest niemożliwe w prawdziwym świecie.*

W grze, jak w bajce, można fruwać, skakać z dużych wysokości, przeskakiwać nad przepaściami i pokonywać oddalone od siebie przeszkody. W prawdziwym życiu są one niewykonalne lub próba ich odtworzenia może skończyć się tragicznie. Tylko w grze Twój bohater ma kilka „żyć", a kiedy zginie wraca bez zadraśnięcia po ponownym uruchomieniu gry. Dlatego nie próbuj robić tego, co Twój bohater. W Twoim świecie masz tylko jedno życie i zdrowie, które warto szanować.

46. *Nawet darmowe gry w sieci mogą zawierać ukryte opłaty np. przez wysłanie SMS–a.*

Jeśli ktoś w grze prosi cię o wysłanie SMS–a aby uzyskać jakiś „bonus", ulepszyć lub odzyskać Twoją postać lub jej ekwipunek – pamiętaj, że nie musisz tego robić. Choć sama gra online może być dostępna bezpłatnie, zdarza się, że pewne specjalne opcje lub przywileje

są płatne. Dotyczy to różnych gier sieciowych, m.in. gier przeglądarkowych (tzw. browserowych), które nie wymagają instalowania gry na komputerze. Przed rozpoczęciem gry warto dokładnie przeczytać jej regulamin. Jeśli czegoś w nim nie rozumiesz, poproś rodziców o pomoc.

47. *Pamiętaj, że nigdy nie zapewnisz sobie anonimowości w grach online, nawet jeśli kryjesz się pod postacią swojego awatara.*

Kiedy rozmawiasz z innymi graczami na czacie aby zaplanować dalsze ruchy w grze, czasami możesz zapomnieć, że po drugiej stronie siedzi taka sama osoba, jak Ty. Często, gdy nie widzimy osoby, z którą rozmawiamy, wydaje nam się, że możemy sobie pozwolić na więcej. Tak jednak nie jest. Pamiętaj zatem, że na czacie obowiązują takie same zasady, jak w trakcie normalnej rozmowy.

48. *Pamiętaj, że kradzież postaci lub przedmiotu w grze online może być karana w prawdziwym świecie.*

Hakerzy lub po prostu nieuczciwi gracze mogą działać również w grach online. W grach sieciowych zwykle handel postaciami lub przedmiotami ich ekwipunku (ang. item) jest zabroniony i może być karany w prawdziwym świecie. Tym bardziej, jeśli ktoś włamie się na Twoje konto w grze i przejmie Twoją postać lub należące do niej przedmioty może za to zostać osądzony i ukarany w „realu". Policja lub administrator łatwo wytropią takiego złodzieja. W jaki sposób można łatwo wytropić złodzieja? Zajrzyj do opisu karty **nr 20**.

V GENERATOR HASŁA

49. *Tworząc swoje hasło używaj wielkich i małych liter, np. HaSłO.*

Istnieje wiele sposobów na zabezpieczenie Twojego hasła przed odgadnięciem lub złamaniem przez hakera. Jednym z nich jest używanie wielkich i małych liter w niekonwencjonalny sposób – np. naprzemiennie lub w nieregularny sposób. Jak inaczej zapisać hasło? Zapoznaj się z opisem karty **nr 56**.

50. *Tworząc swoje hasło wykorzystuj znaki specjalne (#, $, &, ! itp.) np. h@$Ło.*

Zabezpiecz hasło do konta przed włamaniem. Spróbuj wpleść w nie znaki specjalne zamiast poszczególnych liter (naprzemiennie lub w nieregularny sposób). Utrudni to hakerskim programom deszyfrującym złamanie Twojego hasła. Jak jeszcze możesz skomplikować hasło? Zajrzyj do opisu karty **nr 51**.

51. *Tworząc swoje hasło używaj naprzemiennie cyfr i liter np. h1A2s3L4o.*

Chcąc uchronić się przed hakerem, wpleć w swoje hasło cyfry zamiast liter lub oprócz nich

(naprzemiennie lub w mniej regularny sposób). Utrudni to hakerskim programom deszyfrującym złamanie Twojego hasła. Ciekawe rozwiązanie na utrudnienie odgadnięcia hasła znajdziesz w opisie karty **nr 52**.

52. *Tworząc swoje hasło, wykorzystuj wyrazy niesłownikowe np. zawierające błędy ortograficzne, literówki, neologizmy (wymyślone wyrazy) np. ChAsLoU.*

Jeśli chcesz utworzyć hasło, które będzie trudno złamać, możesz np. stosować wyrazy z błędami ortograficznymi lub wymyślone wyrazy (neologizmy), których nie można znaleźć w słowniku (np. „chasło" zamiast „hasło"). Jeśli dodasz do tego jeszcze inne sposoby szyfrowania Twojego hasła, będzie ono jeszcze trudniejsze do rozszyfrowania. Inny sposób poznaj w opisie karty **nr 49**.

53. *Im dłuższe jest Twoje hasło, tym jest bezpieczniejsze.*

Specjaliści od zabezpieczeń twierdzą, że bezpieczne hasło powinno liczyć przynajmniej osiem znaków. Ale na nic się zda wymyślanie skomplikowanego hasła, jeśli złodziej ma do niego łatwy dostęp – dowiedz się więcej z opisu karty **nr 54**.

54. *Nie zapisuj nigdzie swoich haseł (ani na kartkach, ani w komputerze).*

Twoje hasło, nawet najbardziej skomplikowane i trudne do odgadnięcia, może zostać wykradzione przez hakera. Wystarczy, że włamie się do Twojego komputera i spisze je z pliku tekstowego, w którym je zapiszesz. Podobnie, jeśli odnotujesz je na kartce, która wpadnie w niepowołane ręce.

55. *Nie używaj tego samego hasła wszędzie, gdzie jest wymagane.*

Używanie tego samego hasła do logowania we wszystkich miejscach w Internecie jest wygodne, ale lekkomyślne. Narażasz się w ten sposób na niebezpieczeństwo. Jeśli w jednym z miejsc, w którym masz konto, ktoś je złamie, będzie mógł się włamać do wszystkich Twoich kont.

56. *Im bardziej zróżnicowane będzie Twoje hasło, tym trudniej będzie je złamać.*

Poza długością hasła (patrz opis karty **nr 53**) spróbuj zastosować różne rodzaje znaków (patrz opisy kart **nr 49–52**). Im więcej sposobów zabezpieczenia Twojego hasła używasz, tym trudniejsze będzie jego złamanie przez hakerskie programy deszyfrujące. Twórz hasła jako zlepek pierwszych liter wyrazów całych zdań lub fraz (np. MpwsB = Mój pies wabi się Burek), zastępuj litery cyframi, które je przypominają np. A=4, S=5, I=1, L=7 (przykładowo: 745 = LAS).

57. *Zmieniaj hasła jak najczęściej (minimum raz na pół roku) i nikomu ich nie zdradzaj.*

Specjaliści od zabezpieczeń radzą zmieniać hasła nawet co kilka tygodni. Rób to jak najczęściej. Swoje hasła możesz zdradzić jedynie osobom, których nie musisz się obawiać np. rodzicom.

58. *Twórz hasła trudne do odgadnięcia (nie używaj swojej daty urodzenia, imion).*

Osoby, które chcą złamać Twoje hasło i wiedzą coś o Tobie i Twoich bliskich (np. wyczytały te informacje na Twoim profilu w serwisie społecznościowym), mogą je odgadnąć, jeśli będzie zbyt proste np. będzie to Twoje imię, nazwisko. Do wymyślania haseł ludzie często używają prostych informacji o sobie lub rodzinie. Może to być np. pseudonim, imię któregoś ze znajomych (rodzeństwa, najlepszego przyjaciela), data urodzenia, imię zwierzęcia itp. lub kolejne litery/cyfry (ABC, 123), kolejne klawisze na klawiaturze (np. QWERTY). Nie używaj ich jako haseł – zbyt łatwo je odgadnąć. Stwórz bardziej skomplikowane hasło!

59. *Tworząc hasło, przeplataj ze sobą kilka wyrazów (zawierających wielkie i małe litery) oraz cyfry i znaki specjalne np. Ty; jA; 1,2; #,& utworzą: Tj1#yA2&.*

Żeby skomplikować swoje hasło i sprawić, że będzie trudniejsze do złamania przez deszyfrujące programy hakerskie, warto zastosować jak najwięcej sposobów kodowania oraz przeplatać je ze sobą.

60. *Wymyśl swój własny system tworzenia trudnych haseł.*

Łatwo jest się pogubić w wymyślaniu haseł. Stwórz własny system ich tworzenia. Najpierw ustal rodzaje znaków, z jakich będzie się składało (np. liczbę wyrazów, które zostaną pomieszane, małe i wielkie litery, cyfry, znaki specjalne itp.), a potem kolejność, w jakiej będziesz je przeplatać.

Wydawca:
Wojewódzka Biblioteka Publiczna i Centrum Animacji Kultury w Poznaniu
ul. B. Prusa 3
60–819 Poznań
tel. (61) 664 08 50

Koordynator projektu: ***Urszula Cimoch***

Autorzy: ***Jacek Szmania, Przemysław Wojtkowiak***

Grafika: ***Marek Rutkowski***

Partnerzy projektu: ***Gramajda***, ***Fundacja Ad Hoc***

Eksperci merytoryczni: ***dr Augustyn Surdyk***, ***dr Emanuel Kulczycki***

Wsparcie merytoryczne: ***Komisja ds. Edukacji Informacyjnej (SBP)***

Specjalne podziękowania:

Nadzieja Pawłowska, Hanna Gołębiowska, Matylda Michalska, Wiktoria Dudziak, Maciej Adamski, Daniel Banaszak, Grzegorz Bąkowski, Patryk Hemperek, Joanna Kalka, Honorata Janusz, Kuba Fabisiak, Zuzanna Rutkowska, Katarzyna Kornaś, Iga Kuczkowska, Ewa Rozkosz, Marta Kostecka, Matylda Filas, Agnieszka Świątecka, Jakub „KubaP" Polkowski, Krzysztof „Pirat Cristobal" Niziałek, Marcin Szrama, Kornelia Rutkowska, Justyna Daniel.

Dofinansowano ze środków Ministra Kultury i Dziedzictwa Narodowego.

Wojewódzka Biblioteka Publiczna i Centrum Animacji Kultury w Poznaniu to instytucja, która działa na rzecz upowszechniania wiedzy i kultury oraz zaspokajania potrzeb edukacyjnych i informacyjnych mieszkańców Wielkopolski. Poza rozwijaniem i wspomaganiem czytelnictwa prowadzi działalność bibliograficzną, edukacyjną i wydawniczą. Ważny segment działania biblioteki stanowi popularyzacja i dokumentacja problematyki regionalnej i krajoznawstwa z wykorzystaniem tradycyjnych i nowatorskich form pracy (questy, portal www.regionwielkopolska.pl). Jako placówka upowszechniania kultury WBPiCAK współpracuje z innymi instytucjami i stowarzyszeniami działającymi w tym obszarze, zwłaszcza w zakresie amatorskiego ruchu artystycznego.

www.wbp.poznan.pl

Fundacja Ad Hoc swoje cele realizuje przede wszystkim poprzez nieodpłatne świadczenie usług i doradztwa dla organizacji pozarządowych w kwestiach wykorzystania nowych technologii oraz działalności w internecie, a także realizację własnych projektów. Prowadzi też warsztaty dla młodzieży i dorosłych. Działalność Fundacji skupia się na wykorzystaniu nowych mediów i technologii w projektach społecznych, przede wszystkim na poziomie lokalnym. Priorytetem Fundacji są projekty innowacyjne, wykorzystujące najnowocześniejsze metody i technologie, lub poszukujące nowych zastosowań i kontekstów. Aktualne informacje o jej działaniach można znaleźć na stronie

www.adhoc.org.pl

GRAMAJDA to grupa planszówkowych zapaleńców, spotykających się kilka razy w miesiącu w różnych miejscach Poznania, najczęściej w pubie Alibi w centrum miasta. Powstała w 2006 roku, kiedy pierwsi pasjonaci nowoczesnych gier planszowych zaczęli się organizować, by wypróbowywać coraz to nowsze tytuły pojawiające się na polskim rynku gier. Dziś GRAMAJDA jest istotną częścią środowiska poznańskich graczy, a na jej spotkaniach pojawia się czasem nawet 70 osób! Grupa nie poprzestaje na rozgrywkach we własnym gronie, organizując takie akcje, jak Games Room podczas kolejnych edycji Festiwalu Fantastyki Pyrkon (od 2009 roku) oraz konwentu fantastyki Polcon (2011), a także szereg wydarzeń na uczelniach wyższych, w szkołach, bibliotekach i domach kultury. GRAMAJDA wciąż pozostaje forum aktywności dla wielu poznaniaków interesujących się grami, skupia bowiem zarówno zwykłych pasjonatów, jak i twórców, blogerów i recenzentów planszówek. GRAMAJDA zrzesza setki osób zarażonych planszówkowym hobby! Więcej informacji o GRAMAJDZIE i jej spotkaniach na stronie internetowej:

www.gramajda.pl.

Edukacja Informacyjna

Komisja ds. Edukacji Informacyjnej (KEI) działająca w Stowarzyszeniu Bibliotekarzy Polskich zachęca polskich bibliotekarzy do podejmowania różnych form edukacji informacyjnej. Organizuje nieodpłatne szkolenia, podczas których bibliotekarze poznają różne podejścia do uczenia się i uczenia innych efektywnego i refleksyjnego wykorzystania informacji. Rozwój edukacyjnej funkcji biblioteki jest więc podstawowym celem bibliotekarzy, bibliotekoznawców i informatologów wchodzących w skład Komisji. KEI podejmuje również współpracę z innymi organizacjami służącą rozpowszechnieniu w polskim społeczeństwie (wśród uczniów, studentów, nauczycieli, rodziców, użytkowników bibliotek, instytucji oraz innych organizacji) aktywnej postawy względem rozwijania kompetencji informacyjnych przez całe życie.

www.sbp.pl/kei