JUNIOR

PKO Bank Polski

JUNIOR BEZPIECZNY W SIECI

CYBERPORADNIK DLA DZIECI
I DOROSŁYCH

SPIS TREŚCI

WSTĘP

„Junior bezpieczny w sieci – cyberporadnik dla dzieci i dorosłych" to publikacja na temat świadomego korzystania z internetu i nowych technologii. Zawiera zbiór dobrych praktyk związanych z mądrym i bezpiecznym poruszaniem się w sieci, przydatnych zarówno dzieciom, jak i dorosłym posługującym się smartfonami, tabletami czy komputerami.

Nowoczesna forma przekazu, przyjazny język oraz kolorowe ilustracje sprawiają, że tematyka cyberbezpieczeństwa staje się łatwiejsza do przyswojenia. Liczne porady, przykłady zaczerpnięte z życia codziennego oraz quizy pomogą w utrwaleniu wiadomości.

Na podstawie doświadczeń bohaterów znanych z wcześniejszych publikacji – Kasi, Kuby oraz mamy i taty Pieniążków – przekonasz się, że:

- internet to ważna część naszej rzeczywistości. Za pomocą internetu wszyscy członkowie rodziny mogą wykonywać wiele ciekawych i pożytecznych działań,
- dbanie o bezpieczeństwo swoich danych osobowych, informacji o domu i rodzinie, a także oszczędności zgromadzonych na rachunkach bankowych może być łatwe, przyjemne, a przede wszystkim skuteczne,
- internet jest bardzo dynamicznym środowiskiem. Szybko się zmienia, dlatego regularnie trzeba aktualizować nie tylko oprogramowanie komputera, ale także swoją wiedzę w zakresie cyberbezpieczeństwa.

Życzymy miłej lektury oraz wielu pozytywnych doświadczeń zarówno w wirtualnym, jak i realnym świecie. ☺

CZY WIESZ, ŻE:

☺ – czyli **:** oraz **)** – symbol mający przypominać uśmiechniętą twarz był pierwszą powszechnie używaną emotikoną? Za jego twórcę uważa się amerykańskiego informatyka Scotta Fahlmana, który wykorzystał „buźkę" w wiadomości wysłanej w 1982 r.

WIRTUALNY ŚWIAT, REALNE WYZWANIA

Kasia i Kuba codziennie po kolacji mogą korzystać z komputera – każde z dzieci po pół godziny. Bardzo często towarzyszą im rodzice. Mama i tata chcieliby wiedzieć, jakie strony przeglądają ich dzieci.

Tego wieczoru pierwszeństwo przy komputerze ma Kasia. Dziewczynka nie chce, by dziś towarzyszył jej któryś z rodziców. Samodzielnie otwiera stronę, którą pokazała jej koleżanka.

– Trochę tekstów, regulamin, kilka okienek, w które chyba muszę kliknąć – wylicza Kasia.

Dziewczynka nie do końca rozumie pojawiające się treści. Nie wie, w jaki sposób zamknąć ekran. Nie wie również, czy słusznie zaznacza wszystkie pojawiające się „okienka" i wypełnia kolejne pola, wpisując np. imię, nazwisko, numer telefonu i adres e-mail. Po kilku minutach prosi o pomoc... mamę.

– Kasiu, przyjrzyj się tej stronie. Ona nie jest dostosowana do wyświetlania przez dzieci, ani nawet przez nastolatków. Aby móc w pełni z niej korzystać, trzeba mieć ukończone 18 lat. Trzeba też wyrazić zgody marketingowe – to znaczy pozwolić na to, aby właściciel strony zbierał, przechowywał i wykorzystywał podane przez ciebie dane w celu przesyłania reklam. Czy jesteś pewna, że to właśnie tę stronę poleciła ci koleżanka? – spytała mama.
– Tamta witryna wyglądała zupełnie inaczej... – odpowiedziała dziewczynka.
– To, co od razu powinno wzbudzić twoją czujność, to wygląd i treść tej witryny – tłumaczy cierpliwie mama. – Administratorzy stron dla dzieci nie mogą wymagać od nich podawania jakichkolwiek danych ani prezentować ofert zakupów. Jeśli chcesz, pomogę ci odnaleźć prawidłową stronę. Razem sprawdzimy, czy witryna, którą poleciła ci koleżanka, jest przeznaczona dla najmłodszych.
– Oczywiście, że chcę! – krzyknęła z radością Kasia. – Jednak widzę, że Kuba już czeka, aby skorzystać z komputera.
– Ja też chcę być bezpieczny w sieci. Chętnie się do was przyłączę – zaproponował chłopiec.
– Mamo, widzę, że jeszcze wiele możemy się od ciebie nauczyć – powiedziała Kasia.
– Ja od was również – odpowiedziała mama, uśmiechając się do dzieci.

Urządzenia elektroniczne i internet to istotna część naszego życia. Dzięki nim możemy kontaktować się z przyjaciółmi i rodziną, przesyłać dokumenty, zdjęcia, oglądać filmy, uczyć się np. języków obcych czy robić zakupy. Jeśli jednak coś wzbudzi Twój niepokój – powiedz o tym rodzicom lub nauczycielom.

PANCERNIK HATETEPES RADZI

- Chroń dane osobowe. Nie podawaj na portalach społecznościowych adresów e-mail, numerów telefonów ani danych kart płatniczych – swoich ani swoich bliskich. Złodzieje tożsamości chętnie przechwytują takie dane. Zakładają profile na portalach społecznościowych na nazwiska innych osób i w ich imieniu popełniają przestępstwa.

- W internecie zamieszczaj tylko takie treści, które nie zdradzają zbyt wielu informacji o Tobie, Twoim domu lub rodzinie. Potencjalny złodziej może zauważyć na zdjęciu wartościowe przedmioty i zaplanować włamanie. Może też wyczytać z opublikowanych przez Ciebie informacji, że przebywasz z dala od domu, np. na wakacjach.

- Zachowaj ostrożność przy korzystaniu z różnych ofert specjalnych, np. w zakresie programów, które trzeba ściągnąć na komputer, tablet lub telefon. Może to być zainfekowane oprogramowanie, które po instalacji wyrządzi wiele szkód. Jeśli masz wątpliwości, zapytaj rodziców lub nauczyciela.

- Korzystaj ze stron odpowiednich do Twojego wieku. Poproś rodziców lub nauczyciela o instalację na komputerze specjalnej przeglądarki – będzie ona filtrować strony internetowe, których zawartość jest odpowiednia do Twojego wieku.

CIEKAWOSTKA LOKATKI

Po czterech latach od wynalezienia internetu korzystało z niego już 50 milionów osób. Zdobycie takiej samej liczby użytkowników zajęło telefonowi 75 lat, radiu – 38 lat, telewizji – 13 lat, a grze Angry Birds – 35... dni. ☺

QUIZ

Zakładając profil na stronach internetowych, najlepiej:

1. Zawsze podawać fikcyjne, zmyślone dane.
2. Po zapoznaniu się z regulaminem podawać tylko niezbędne, prawdziwe dane.
3. Podać cały komplet danych osobowych – najlepiej opiekunów prawnych, osób pełnoletnich.

Poprawne odpowiedzi do quizu znajdziesz na końcu publikacji.
Data opracowania materiału: sierpień 2018.

KALAMBURY W PARACH

Zapisz na odrębnych kawałkach papieru poniższe przysłowia. Dobierz osobę do pary – kolegę, koleżankę, rodzeństwo. Waszym zadaniem będzie wylosowanie jednego hasła i wspólne pokazanie lub narysowanie go innym uczestnikom gry. Możecie naradzić się, w jaki sposób zaprezentujecie powiedzenie, a w przypadku improwizacji aktorskiej – kto odgrywa jaką rolę.
Po zaprezentowaniu hasła zastanówcie się, w jaki sposób sens zaprezentowanego powiedzenia można przełożyć na sytuacje związane z korzystaniem z komputera i internetu.

1. Co dwie głowy, to nie jedna
2. Czego Jaś się nie nauczy, tego Jan nie będzie umiał
3. Czuć się jak ryba w wodzie
4. Nie wszystko złoto, co się świeci
5. Ten się nie myli, kto nic nie robi
6. Wszystko dobre, co się dobrze kończy
7. Nie taki diabeł straszny, jak go malują
8. Każdy kij ma dwa końce
9. Kto pyta, nie błądzi
10. Apetyt rośnie w miarę jedzenia
11. Broda mędrcem nie czyni
12. Co nagle, to po diable

Bez względu na wiek rozwiąż wszystkie zadania. Wszystkie ćwiczenia utrwalają Twoją wiedzę, a jednocześnie przybliżają Cię do zdobycia Cybercertyfikatu. Znajdziesz go na końcu publikacji.

SEZAMIE, OTWÓRZ SIĘ!

Jest wieczór. Kuba sprawdza stan swoich oszczędności. W tym celu wchodzi na stronę serwisu internetowego Junior. Nagle obok jego biurka pojawia się Pancernik.

– Cześć, jestem Hatetepes i odpowiadam za twoje bezpieczeństwo w serwisie Junior – przedstawia się zwierzak. – Od kilku tygodni nie zmieniałeś hasła. Pomogę ci nadać nowe, trudne do odgadnięcia.
– Niesamowite! – chłopiec nie krył zaskoczenia. – Zjawiłeś się tutaj specjalnie dla mnie i w dodatku chcesz pomóc mi stworzyć nowe hasło? Zatem do dzieła, Pancerniku!
– Czy pamiętasz, kiedy urodził się twój tata?
– Urodziny mojego taty są... – mówił nieskładnie zaskoczony pytaniem chłopiec – ...10 lipca... 1975.
– Na podstawie tej frazy można utworzyć hasło „Umts10lip1975.". Można też utrudnić je przez dodanie innych znaków lub skrócenie roku do ostatniej cyfry, np. „Umts10/lip,5.". Co ty na to? Zapamiętasz takie hasło?
– No pewnie, że tak – powiedział zachwycony pomysłem Kuba. – Hatetepesie, dziękuję za pomoc.

Kuba zmienia dotychczasowe hasło na to, które podpowiedział mu Hatetepes. Wchodzi na stronę banku, a tam czeka na niego kolejna niespodzianka. Chłopiec widzi nadspodziewanie dużo pieniędzy. Przeciera oczy ze zdumienia. Patrzy raz jeszcze: środki na koncie nadal są. Ale gdzie podział się Pancernik?

– Czy wszystko w porządku? – pyta mama, wchodząc do pokoju chłopca. – Babcia prosiła, by powiedzieć, że przelała pieniądze na twój rachunek. To prezent z okazji zbliżających się imienin. Babcia wie, że zbierasz na zieloną szkołę.
– Mamo, a co z Pancernikiem? Stał tu przed chwilą.
– Kubusiu, chyba jesteś już zmęczony. Najwyższa pora położyć się do łóżka.

PANCERNIK HATETEPES RADZI

Trudne do złamania hasło m.in.:

- zawiera przynajmniej 8 znaków, małe i duże litery, cyfry i znaki specjalne (np. `!@#$%^&*()_+-={}[]:;',.<>),
- różni się od loginu,
- nie zawiera imion, nazwisk czy innych osobistych informacji (np. daty urodzenia),
- nie zawiera popularnych, łatwych do odgadnięcia ciągów znaków (np. 12345),

- nie składa się ze słów występujących w słownikach,
- jest unikatowe – nie jest przez nas używane w innych serwisach,
- jest regularnie zmieniane – najlepiej przynajmniej raz na 30 dni.

Imię Twojego zwierzątka, ulubiony owoc czy ciąg cyfr „12345" nie będą silnym hasłem, ponieważ zbyt łatwo można je odgadnąć lub złamać za pomocą zwykłych programów hakerskich.

Serwisy internetowe udostępnione dzieciom przez bank (np. sko.pkobp.pl, junior.pkobp.pl):

- są szyfrowane, co oznacza, że w adresie www najpierw znajduje się symbol kłódki, a następnie litery: https,
- wymagają logowania za pomocą loginu i hasła, a po zakończonej pracy – wylogowania się za pomocą kliknięcia w przycisk „wyloguj",
- powinny być przeglądane w domu, przy użyciu zabezpieczonej trudnym do złamania hasłem sieci oraz sprawdzonego, również zabezpieczonego hasłem komputera.

CIEKAWOSTKA LOKATKI

Dobrą praktyką wśród administratorów stron www jest szyfrowanie haseł użytkowników. W praktyce oznacza to, że osoby pracujące przy obsłudze strony zamiast haseł widzą np. *** (gwiazdki). Użytkownik – zapomniawszy hasła – samodzielnie odzyskuje dane do logowania lub ustala zupełnie nowe hasło.**

QUIZ

Przykładem silnego hasła jest:

1. Wyznanie miłosne, np. KochamAnie
2. Ciąg cyfr, np. 45678
3. Połączenie różnych znaków, np. 8ezPiEczNehA5l0!

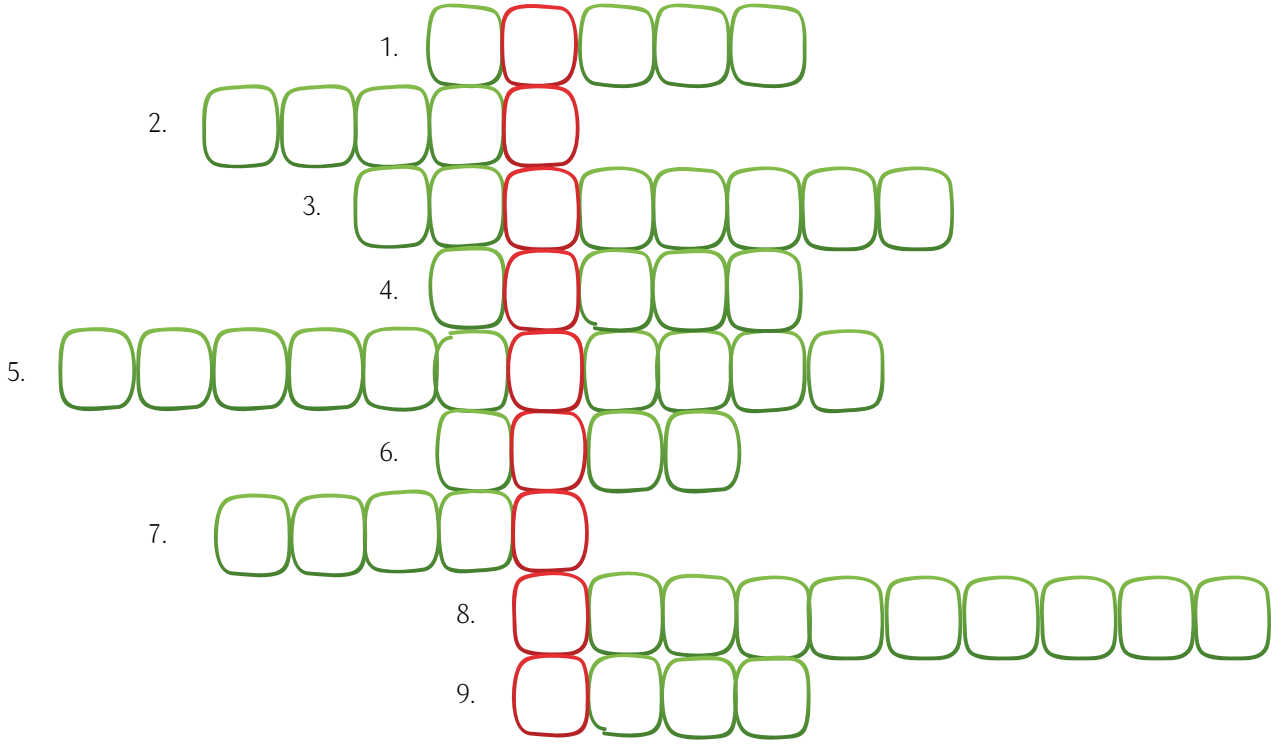
KRZYŻÓWKA

Rozwiąż krzyżówkę i sprawdź, jak nazywa się strażnik Twojego komputera.

1. Umożliwia zalogowanie się do serwisu. Nie powinno być zbyt łatwe do odgadnięcia. Warto je regularnie zmieniać.
2. Pełni funkcję identyfikatora w sieci.
3. Łączy ze sobą miliony komputerów. Dzięki niemu możemy szybko i skutecznie wyszukiwać oraz udostępniać informacje.
4. Aby hasło było silne, musi zawierać: małe i duże litery, znaki specjalne i....
5. Czynność, o której należy pamiętać, kończąc pracę przy komputerze.
6. Wyróżniony element tekstu na stronie internetowej, który umożliwia łatwe połączenia między kilkoma dokumentami. Jego inna nazwa to odsyłacz.

Poprawne odpowiedzi do quizu znajdziesz na końcu publikacji.
Data opracowania materiału: sierpień 2018.

7. Inaczej wirtualny, internetowy.
8. Inaczej osoba korzystająca z komputera lub internetu.
9. Zbiór połączonych ze sobą komputerów, które mogą komunikować się z pozostałymi urządzeniami. Może być np. lokalna.



Hasło: ..... – strażnik Twojego komputera

Poprawne odpowiedzi znajdziesz na końcu publikacji.
Bez względu na wiek rozwiąż wszystkie zadania. Wszystkie ćwiczenia utrwalają Twoją wiedzę, a jednocześnie przybliżają Cię do zdobycia Cybercertyfikatu. Znajdziesz go na końcu publikacji.

NIE WSZYSTKO ZŁOTO, CO SIĘ ŚWIECI

Kasia odkryła nową stronę z rywalizacją na... wiedzę! Zalogowała się do serwisu, wybrała poziom trudności oraz wylosowała pytania. Może też zakupić podpowiedzi i dzięki temu zwiększyć swoje szanse na wygraną.

– Hej, prześlę ci link, pod którym znajdziesz program zawierający komplet darmowych ściągawek – proponuje Kasi wirtualna koleżanka z czatu.

Aby otrzymać wskazówki, dziewczynka musi podać swój e-mail. Nie ma własnego, więc myśli o tym, by użyć adresu taty.

– Hura! – cieszy się dziewczynka, co nie uchodzi uwadze reszty rodziny. – Dostanę podpowiedzi do gry i nie wydam przy tym ani złotówki! Szybko zaznaczę wszystkie odpowiedzi i sprawdzę swój wynik. Tato, chodź, zobacz, jak dobrze mi idzie.

– Kasiu, to może okazać się najdroższa gra w twoim życiu – tłumaczy tata. – Dane takie, jak imię, nazwisko, adres zamieszkania, a także adres e-mail, są bezcenne. Trzeba je chronić. Oprócz tego zwróć uwagę na link przesłany przez „koleżankę". Nie wiadomo, co kryje się pod tym ciągiem znaków.

Na szczęście tata zareagował w porę. Kasia nie podała „koleżance" adresu e-mail taty. Tym samym nie otrzymała od niej żadnej wiadomości i nie otworzyła linku z rzekomymi podpowiedziami do gry.


KAŻDEMU Z NAS ZDARZAJĄ SIĘ RÓŻNE POTENCJALNIE NIEBEZPIECZNE SYTUACJE. NA PRZYKŁAD PODCZAS PRZEGLĄDANIA STRON INTERNETOWYCH NAGLE WYSKAKUJE OKIENKO Z INFORMACJĄ „TWÓJ KOMPUTER ZOSTAŁ ZAINFEKOWANY", A POTEM REKLAMA PROGRAMU ANTYWIRUSOWEGO. PO KLIKNIĘCIU W REKLAMĘ NASTĘPUJE AUTOMATYCZNE ŚCIĄGNIĘCIE I INSTALACJA PROGRAMU.
WYDAJE SIĘ, ŻE PROGRAM DZIAŁA POPRAWNIE – CHRONI KOMPUTER PRZED ZŁOŚLIWYM OPROGRAMOWANIEM, A TAK NAPRAWDĘ MOŻE WYKRADAĆ Z NIEGO DOKUMENTY CZY FOTOGRAFIE I PRZESYŁAĆ JE CYBERPRZESTĘPCOM.
OSTATNIO PANI W SZKOLE OPOWIADAŁA NAM O ZASADZIE OGRANICZONEGO ZAUFANIA. MYŚLĘ, ŻE TRZEBA JĄ STOSOWAĆ NIE TYLKO JADĄC ROWEREM, ALE RÓWNIEŻ KORZYSTAJĄC Z INTERNETU.

PANCERNIK HATETEPES RADZI

Zachowaj czujność, gdy:

- ktoś stara się skłonić Cię do podjęcia szybkiej decyzji, bez jej przemyślenia (np. używając popularnych haseł: „kliknij teraz, a dodatkowo otrzymasz...”),
- ktoś prosi Cię o informacje, które powinien znać (np. podaje się za Twoją koleżankę ze szkoły, a pyta o Twoje imię i nazwisko),
- ktoś oferuje Ci coś cennego za darmo lub w bardzo okazyjnej cenie.

CIEKAWOSTKA LOKATKI

Dane osobowe to nie tylko imię, nazwisko czy adres. Są to wszelkie informacje pozwalające na ustalenie tożsamości konkretnej osoby, np. informacje odnoszące się do jej cech fizycznych, umysłowych, kulturowych lub społecznych. Takie informacje również należy chronić.

QUIZ

Aby ochronić się przed manipulacją ze strony cyberprzestępców, należy:

1. Nie włączać komputera.
2. Nie otwierać stron, na których nigdy wcześniej nie byliśmy.
3. Być ostrożnym i chronić swoje dane w internecie.

Poprawne odpowiedzi do quizu znajdziesz na końcu publikacji.
Data opracowania materiału: sierpień 2018.

REBUS

1.  ~~mak~~  ~~krze~~

2.  ~~zgb~~ + a   ~~s~~

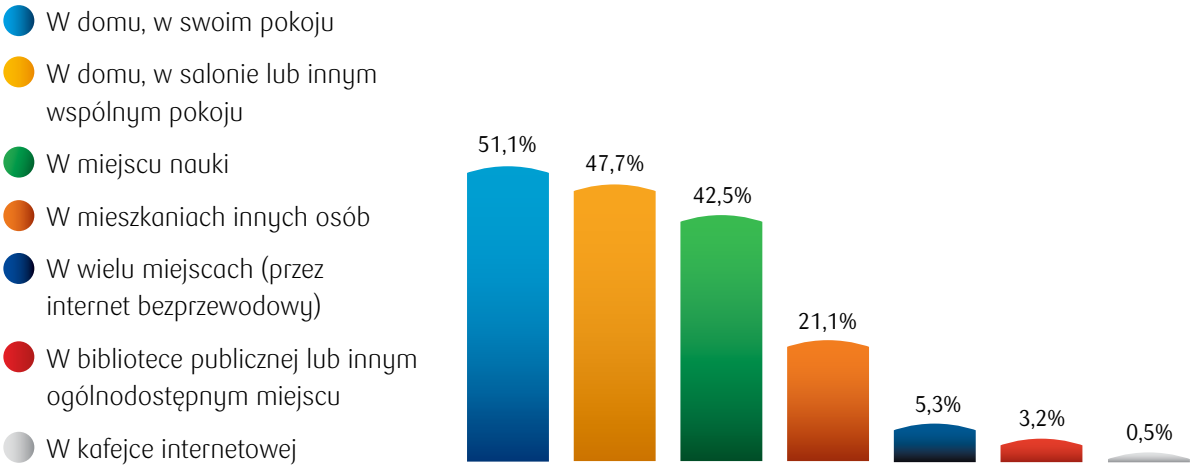
Zapraponuj swój rebus związany z tematyką cyberbezpieczeństwa.

Poprawne odpowiedzi znajdziesz na końcu publikacji.

Bez względu na wiek rozwiąż wszystkie zadania. Wszystkie ćwiczenia utrwalają Twoją wiedzę, a jednocześnie przybliżają Cię do zdobycia Cybercertyfikatu. Znajdziesz go na końcu publikacji.

ZADANIE

Kasia – jak większość dzieci w Polsce – korzysta z komputera, który stoi w jej pokoju. Kuba nie ma swojego komputera, więc używa tego samego sprzętu, co Kasia. Zapoznaj się z poniższym wykresem i odpowiedz na pytanie: gdzie polskie dzieci najczęściej korzystają z komputera?



1. W jakim miejscu Ty najczęściej korzystasz z komputera?
2. Kto ma dostęp do tego samego komputera, co Ty?
3. Czy w pobliżu są osoby dorosłe, które – w razie konieczności – możesz poprosić o pomoc?

Źródło: Główny Urząd Statystyczny, raport „Społeczeństwo informacyjne w Polsce. Wyniki badań statystycznych z lat 2012-2016", wykres „Gospodarstwa domowe, w których dzieci korzystały z internetu według miejsca korzystania", s. 155.

Bez względu na wiek rozwiąż wszystkie zadania. Wszystkie ćwiczenia utrwalają Twoją wiedzę, a jednocześnie przybliżają Cię do zdobycia Cybercertyfikatu. Znajdziesz go na końcu publikacji.

WIRUSY, ROBAKI I INNE ZWIERZAKI

Tata Kasi i Kuby chciałby poszerzyć swoją wiedzę na temat bezpieczeństwa w sieci. To zrozumiałe – ciężko nadążyć za wszystkimi zmianami. Na spotkaniu informacyjnym, organizowanym w szkole przez nauczyciela informatyki, tata dowiedział się, czym jest złośliwe oprogramowanie. Zrobił notatki, które teraz pokazuje rodzinie.

– Tato, jak ty ładnie piszesz – Kasia podziwia starannie wykonane notatki.
– Od zawsze notowałem ręcznie. Dzięki temu mam taki czytelny charakter pisma – wyjaśnił tata.
– Ćwiczenie czyni mistrza – dodała pani Pieniążek.
– Może przyczepimy tę kartkę do lodówki, by spoglądać na nią regularnie i utrwalać sobie wiedzę?

Członkowie rodziny chętnie przystali na propozycję mamy. Od tej pory ich lodówka stała się... bezcennym źródłem pięknie podanej wiedzy!

PANCERNIK HATETEPES RADZI

Aby ochronić się przed złośliwym oprogramowaniem, należy:

- regularnie instalować aktualizacje,
- zachowywać ostrożność przy pobieraniu aplikacji z internetu,
- nie klikać w komunikaty zachęcające do pobrania aplikacji mającej zapewnić ochronę komputera,
- używać regularnie aktualizowanego oprogramowania antywirusowego.

CIEKAWOSTKA LOKATKI

Jednym z najszybszych, a przez to najsłynniejszych wirusów komputerowych był wirus „I Love You". 4 maja 2000 r. – w ciągu jednego dnia – wirus ten rozprzestrzenił się na cały świat, zarażając 10 procent wszystkich komputerów podłączonych do internetu. Spowodował straty w wysokości aż 5,5 miliarda dolarów!

Data opracowania materiału: sierpień 2018.

Złośliwe oprogramowanie może dostać się do komputera przez:

pobieranie z internetu niepewnych, nieznanych nam aplikacji,

otwieranie specjalnie spreparowanych stron internetowych, przypominających np. prawdziwe strony bankowe,

klikanie na stronach internetowych w fałszywe komunikaty o błędach lub wyskakujące „okienka",

otwieranie załączników otrzymanych wraz z wiadomością e-mail od nieznanych nam nadawców.

Najpopularniejsze typy złośliwego oprogramowania to:

Wirus – szkodliwy kod doklejający się głównie do plików, który potrafi samodzielnie przenosić się na inne pliki.

Robak – samodzielnie powielający się szkodliwy program, który nie potrzebuje nośnika w postaci żadnego pliku, tylko rozprzestrzenia się za pomocą sieci komputerowych.

Koń trojański (trojan) – program udający pożyteczną aplikację, który w niezauważalny dla użytkownika sposób wykonuje różne szkodliwe działania.

Spyware – program szpiegujący, który zbiera informacje o użytkowniku komputera i przesyła je za pomocą sieci komputerowych do cyberprzestępców.

Adware – oprogramowanie, które pobiera z internetu i odtwarza na ekranie dużo reklam, co może być uciążliwe i nieprzyjemne dla osób korzystających z komputera.

QUIZ

Aby ochronić Twój komputer przed złośliwym oprogramowaniem, powinieneś:

1. Codziennie czyścić obudowę komputera.
2. Zrezygnować z instalowania na komputerze jakichkolwiek gier.
3. Używać regularnie aktualizowanego oprogramowania antywirusowego.

LABIRYNT

Znajdź drogi, którymi Kuba dotrze do zasad chroniących jego komputer przed złośliwym oprogramowaniem.

Poprawne odpowiedzi do quizu znajdziesz na końcu publikacji.
Bez względu na wiek rozwiąż wszystkie zadania. Wszystkie ćwiczenia utrwalają Twoją wiedzę, a jednocześnie przybliżają Cię do zdobycia Cybercertyfikatu. Znajdziesz go na końcu publikacji.

NIE DAJ SIĘ ZŁOWIĆ W SIECI

Mama Kasi i Kuby postanowiła pójść w ślady taty. Jego notatki dotyczące złośliwego oprogramowania były naprawdę ciekawe! Wybrała się na szkolenie prowadzone wspólnie przez nauczycielkę ze szkoły dzieci oraz przedstawiciela banku, tajemniczo nazwane „phishing". Mama nie zrobiła jednak żadnych notatek.

– Nauczycielka obiecała przekazać uczestnikom prezentację ze spotkania w formie elektronicznej, drogą e-mail – oznajmiła mama. – Trzeba było otworzyć wiadomość, kliknąć w przesłany w niej link, wejść na specjalną stronę i wpisać odpowiednie dane, by móc pobrać plik z prezentacją. Dobrze, że w trakcie spotkania słuchacze zostali uprzedzeni, jak będzie wyglądało pobieranie materiałów – skomentowała mama. – Po dzisiejszym szkoleniu mam już ograniczone zaufanie do treści otrzymywanych pocztą elektroniczną.
– Racja. Cyberprzestępcy mogą robić strony wyglądające łudząco podobnie do tych, które znamy – odezwał się nagle Kuba.
– Skąd o tym wiesz? – zapytała brata Kasia.
– Powiedział mi Pancernik Hatetepes!

PANCERNIK HATETEPES RADZI

Aby ustrzec się phishingu, trzeba:

- unikać klikania w linki prowadzące do stron internetowych, które znajdują się w przesyłanych e-mailach – mogą to być łącza do fałszywych stron, które chcą wyłudzić nasze dane,
- aktualizować program do obsługi poczty elektronicznej oraz przeglądarkę internetową – ich najnowsze wersje są mniej podatne na ataki cyberprzestępców (nie zostały odkryte jeszcze ich słabe punkty, a błędy znane z poprzednich wersji zostały już naprawione).

JUNIOR
PKO Bank Polski

PHISHING

to metoda oszustwa. Polega na tym, że cyberprzestępcy rozsyłają za pomocą poczty elektronicznej wiadomości, które bardzo przypominają oficjalną korespondencję, np. banku, dostawcy poczty elektronicznej, portali aukcyjnych i innych znanych organizacji. W mailach oszuści internetowi umieszczają linki do specjalnie przygotowanych stron, które wyglądają jak prawdziwe strony instytucji lub firm.

JUNIOR
PKO Bank Polski

Co najczęściej znajduje się w wiadomości od cyberprzestępcy?

- link do fałszywej strony, która wygląda podobnie do prawdziwej strony znanej nam organizacji,
- prośba o zalogowanie się na nią,
- komunikat o konieczności ponownej aktywacji konta, które rzekomo przestało być aktywne.

Wpisując login i hasło (lub inne dane) na tak podrobionych stronach, użytkownik nieświadomie przekazuje je przestępcom.

CIEKAWOSTKA LOKATKI

Jednym z przykładów phishingu jest np. metoda „na przyjaciela". Cyberprzestępcy, po włamaniu się na konto pocztowe lub profil w mediach społecznościowych, przesyłają jego znajomym błagalny e-mail lub komunikat z prośbą o pomoc. Najczęściej taka prośba dotyczy jak najszybszego przekazania określonej sumy pieniędzy na podane konto bankowe, ponieważ przyjaciel znalazł się w kłopotach i bardzo potrzebuje tych środków. Oczywiście podane konto bankowe należy do cyberprzestępców i to oni zabiorą przekazaną kwotę.

W podobnych przypadkach najlepiej skontaktować się telefonicznie z przyjacielem i dowiedzieć się, czy rzeczywiście potrzebuje on pomocy. Jeśli nie – najlepiej, żeby porozmawiał ze swoimi rodzicami, którzy powinni zawiadomić policję o możliwości popełnienia przestępstwa.

QUIZ

Bank nigdy nie prosi klientów o:

1. Podawanie swoich danych osobowych drogą mailową.
2. Przeczytanie informacji o nowym rachunku.
3. Zabranie do domu ulotki.

Poprawne odpowiedzi do quizu znajdziesz na końcu publikacji.
Data opracowania materiału: sierpień 2018.

ZADANIE

Przeczytaj poniższą rymowankę. Następnie zaproponuj własne wierszyki związane z podanymi zagadnieniami.

Temat: wyszukiwarka internetowa
Rymowanka: Co, po co, komu i dlaczego?
Wyszukiwarka Ci podpowie – zapytaj, Kolego.

Temat: poczta internetowa (e-mail)

Rymowanka: .....
.....

Temat: link (adres strony, odnośnik, przekierowanie, hiperłącze)

Rymowanka: .....
.....

Temat: oprogramowanie antywirusowe („antywirus", zabezpieczenie komputera)

Rymowanka: .....
.....

Temat: ostrożność (rozwaga, mądre korzystanie z komputera i internetu)

Rymowanka: .....
.....

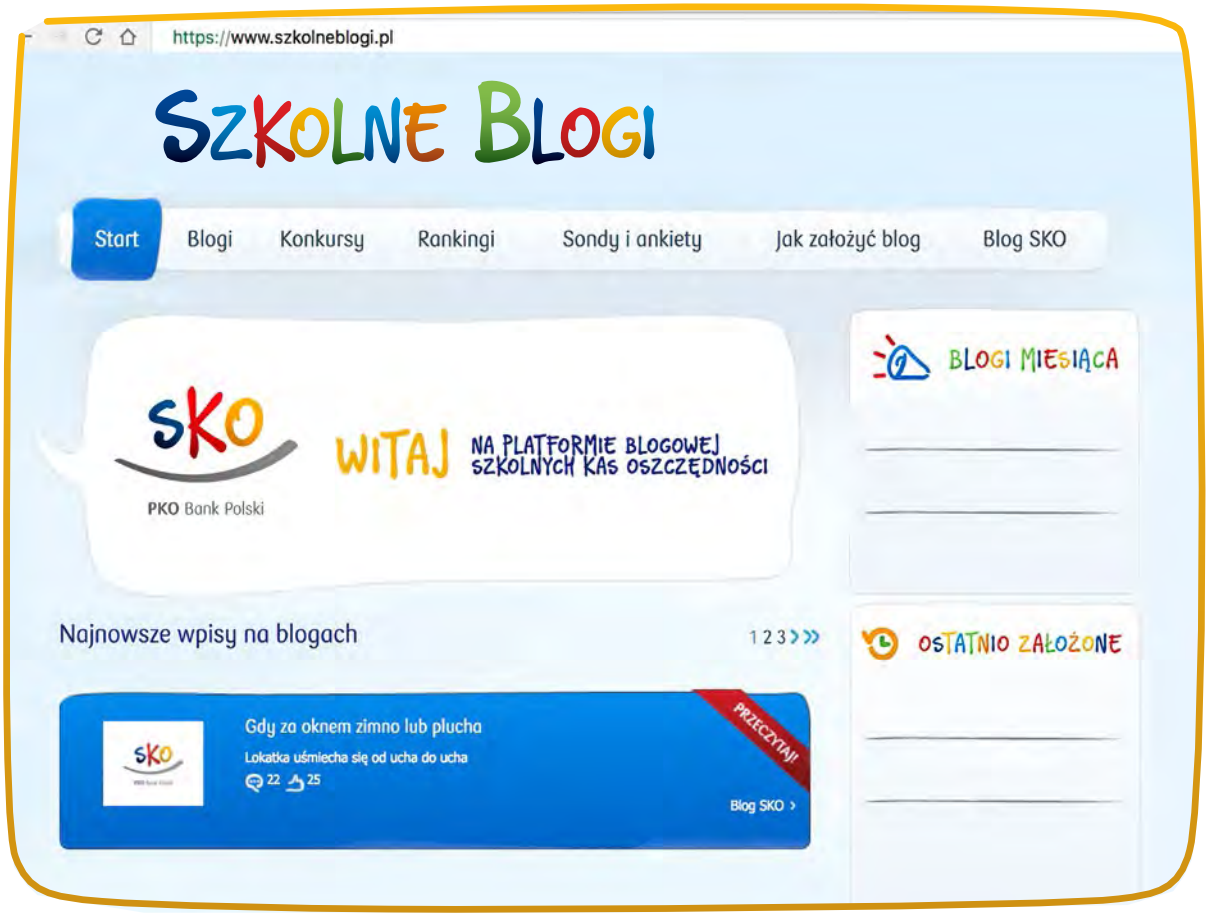
Twoja propozycja tematu związanego z cyberbezpieczeństwem:

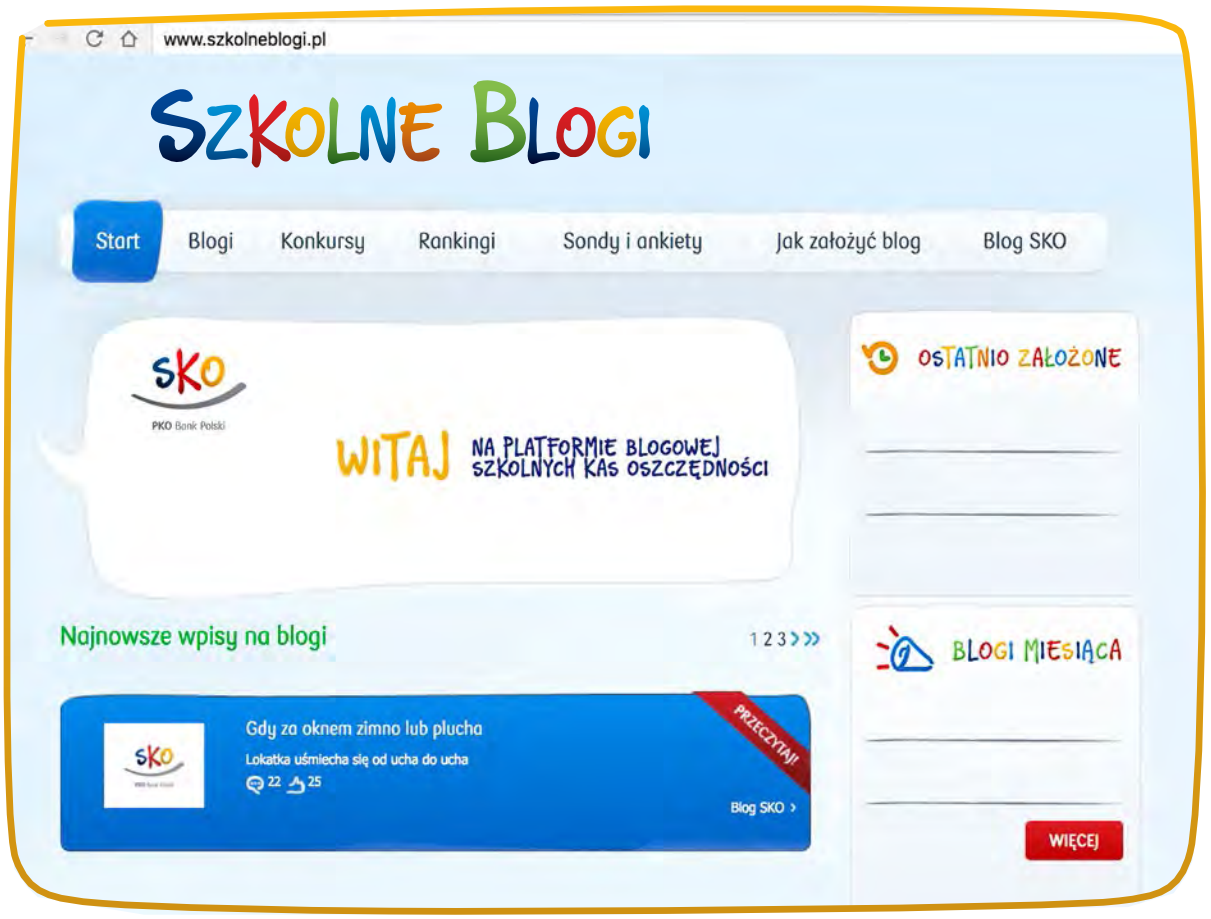
.....
Rymowanka: .....
.....

Bez względu na wiek rozwiąż wszystkie zadania. Wszystkie ćwiczenia utrwalają Twoją wiedzę, a jednocześnie przybliżają Cię do zdobycia Cybercertyfikatu. Znajdziesz go na końcu publikacji.

ZADANIE

Znajdź 6 różnic między poniższymi stronami www. Pierwsza z nich to strona Szkolnych Blogów – platformy udostępnionej przez Bank szkołom uczestniczącym w programie edukacyjnym Szkolnych Kas Oszczędności (SKO) PKO Banku Polskiego. Druga strona łudząco przypomina tę pierwszą, jednak różni się od niej kilkoma szczegółami.





Poprawne odpowiedzi znajdziesz na końcu publikacji. Bez względu na wiek rozwiąż wszystkie zadania. Wszystkie ćwiczenia utrwalają Twoją wiedzę, a jednocześnie przybliżają Cię do zdobycia Cybercertyfikatu. Znajdziesz go na końcu publikacji.

WSZYSTKO POD (CYBER)KONTROLĄ

Rodzice Kasi i Kuby niedawno widzieli się ze znajomymi, którzy opowiedzieli im o programie kontroli rodzicielskiej. Zainstalowali go na wszystkich sprzętach, za pośrednictwem których ich dzieci łączą się z internetem. Państwo Pieniążkowie postanowili pójść w ich ślady. Podczas kolacji opowiadają dzieciom o swoich planach.

– Tato, a czy będę mógł przeglądać serwis sportowy? – dopytuje Kuba.

– Kubusiu, w internecie jest wiele bezpiecznych i użytecznych stron, np. o charakterze informacyjnym, edukacyjnym czy rozrywkowym, których nie zamierzamy blokować. Wspólnie z mamą zastanowimy się jedynie nad tymi, które nie powinny być dostępne dla dzieci w waszym wieku – tłumaczy tata.

– Korzystanie z internetu możemy porównać do nauki jazdy na rowerze. Małe dzieci na początku uczą się jeździć na niewielkich, trzy- lub czterokołowych rowerach. Z wiekiem zdobywają nowe umiejętności i przesiadają się na rowery większe, dwukołowe. Zanim zaczną na nim samodzielnie jeździć, potrzebują pomocy rodziców. Z każdym kolejnym rokiem jeżdżą coraz sprawniej i zaczynają wybierać się na samodzielne wycieczki – mama próbuje wyjaśnić dzieciom, że pewne ograniczenia wynikają z troski o ich bezpieczeństwo oraz umiejętności.

– Ale przecież my już potrafimy samodzielnie jeździć na rowerze – mówi zaskoczony Kuba.

– Kubusiu, my o tym wszystkim dobrze wiemy. Dlatego pozwalamy wam bawić się bez naszej obecności, ale zawsze musicie nas pytać o to, czy możecie wyjść, oraz o której godzinie powinniście wrócić – tłumaczy tata. – Chcielibyśmy również wiedzieć więcej na temat tego, co robicie w internecie.

– W trosce o bezpieczeństwo rodzice zablokują nam dostęp do niektórych stron, np. tych dla dorosłych, za pomocą których moglibyśmy zostać oszukani bądź okradzeni, lub których treść jest nieodpowiednia dla dzieci. Przyda się nam taka pomoc – podsumowuje Kasia.

CZY WIESZ, ŻE:

Aplikacje służące do kontroli rodzicielskiej dają możliwość sprawdzania aktywności dzieci w sieci oraz blokowania dostępu do stron zawierających nieodpowiednie dla nich materiały. Rodzice mogą też ograniczać dzieciom korzystanie z wybranych aplikacji oraz ustawiać limity czasowe, w których dzieci mogą korzystać z komputera. To wszystko z myślą o ich bezpieczeństwie podczas korzystania z sieci.

PANCERNIK KATETEPES RADZI

- Można wykorzystać mechanizmy kontrolne wbudowane w system operacyjny lub samodzielnie zainstalować dodatkowe aplikacje – zarówno w przypadku komputera, jak i telefonu dziecka.
- Na początku warto przyjrzeć się raportom aktywności dziecka w trakcie używania przez niego komputera, które są udostępniane przez aplikacje do kontroli rodzicielskiej.
- Raporty aktywności udostępniają takie informacje, jak: odwiedzone strony internetowe (w tym: data ostatnich odwiedzin, liczba wizyt i czas spędzony na stronie), pobierane pliki, uruchamiane aplikacje, czas używania tych aplikacji.

CIEKAWOSTKA LOKATKI

Wiele dzieci lubi grać w gry komputerowe. Z myślą o ich bezpieczeństwie powstały tzw. PEGI (ang. Pan European Game Information, czyli Ogólnoeuropejski System Klasyfikacji Gier i Aplikacji). Utworzono je, aby pomóc nabywcom w podejmowaniu świadomych decyzji przy zakupie gier lub aplikacji komputerowych. Cyfra przy znaku PEGI to kategoria wiekowa – określa minimalny wiek gracza pozwalający mu na sprawne i bezpieczne przejście przez całą grę.

QUIZ

Kontrola rodzicielska ma na celu głównie:

1. Sprawdzanie, ile czasu dzieci spędzają codziennie w internecie.
2. Zabezpieczenie dzieci przed treściami i programami, które są dla nich nieodpowiednie.
3. Zakładanie profili dzieci na komputerach osób dorosłych.

Poprawne odpowiedzi do quizu znajdziesz na końcu publikacji.
Data opracowania materiału: sierpień 2018.

REBUS

1.  ~~st~~ + c

2.  ~~y~~  ~~ywo~~ + eńs  ~~arz~~ + o

Zaproponuj swój rebus związany z tematyką cyberbezpieczeństwa.

Poprawne odpowiedzi znajdziesz na końcu publikacji.
Bez względu na wiek rozwiąż wszystkie zadania. Wszystkie ćwiczenia utrwalają Twoją wiedzę, a jednocześnie przybliżają Cię do zdobycia Cybercertyfikatu. Znajdziesz go na końcu publikacji.

BĄDŹ SMART

Kasia zazwyczaj nie rozstaje się ze swoim smartfonem. Ma w nim ważne kontakty, zdjęcia, ulubioną muzykę. Teraz, gdy nie może go znaleźć, jest bardzo zdenerwowana, prosi Kubę o pomoc. Chłopiec pomoże, ale... chce za to 5 złotych.

– Zarobione w ten sposób pieniądze dołożę do środków przeznaczonych na zieloną szkołę – snuje plany Kuba.

Kasia jest zła na brata, ale godzi się na propozycję chłopca. Rozmowę rodzeństwa słyszy tata.

– Dzieci, rodzina powinna pomagać sobie bezinteresownie.

Okazuje się, że tata nie tylko słyszał całą rozmowę, ale również ma telefon Kasi. Znalazł go na kanapie. Pewnie wypadł dziewczynce z kieszeni spodni, choć rodzice często prosili, by nie nosiła go w tym miejscu. Tym razem telefon przez cały czas był w domu, jednak nie można zakładać, że dziewczynka zawsze będzie mieć takie szczęście.

– Poszukajcie proszę informacji na temat sposobów zabezpieczania telefonów. Później wspólnie sprawdzimy je na waszych urządzeniach i omówimy, w jaki sposób chronić zawarte na nich dane – powiedział tata.

– Czy to jest kara? – zapytała Kasia.

– Raczej nagroda – stwierdził Kuba.

– To będzie lekcja, która przyda się nam wszystkim nie tylko dziś, ale i w całym późniejszym życiu – zakończył dyskusję tata.


JA BĘDĘ NOTOWAŁ NAJWAŻNIEJSZE INFORMACJE.
KUBA, JA BĘDĘ SZUKAĆ PRZYDATNYCH INFORMACJI, A TY SPRAWDZAJ W TELEFONIE ICH ZASTOSOWANIE.

CZY WIESZ, ŻE:

Obecnie telefony komórkowe to w większości smartfony. To tak naprawdę małe komputery mieszczące się w kieszeni lub torebce. Posiadają system operacyjny, pamięć i można na nich – tak jak na komputerach – instalować aplikacje, w tym również te bankowe, oraz przechowywać różne dane, takie jak fotografie, filmy, dokumenty. Dane te powinny być – dla dobra ich właściciela – chronione przed kradzieżą.

Aby uchronić smartfon przed utratą danych, warto przestrzegać kilku zasad:

ucz się obsługi smartfona pod kontrolą i z pomocą osób dorosłych. Z nimi również dokonuj bardziej skomplikowanych działań związanych z Twoim telefonem,

regularnie wykonuj kopie ważnych danych znajdujących się w pamięci telefonu,

korzystaj z oprogramowania antywirusowego i aktualizuj je na bieżąco,

używaj aplikacji, które pochodzą z zaufanych sklepów internetowych,

zezwól na instalowanie aktualizacji. W starszych wersjach oprogramowania istnieją luki, które są znane cyberprzestępcom i mogą zostać przez nich wykorzystane,

jeśli musisz korzystać z otwartych sieci wi-fi, to nie realizuj przez nie transakcji bankowych, zakupów online, ani nie przesyłaj poufnych danych.

PANCERNIK HATETEPES RADZI

Na wypadek kradzieży lub zgubienia smartfona można:

- zaszyfrować telefon oraz kartę pamięci – współczesne smartfony posiadają możliwość łatwego, szybkiego szyfrowania,
- nadać hasło, kod dostępu czy odcisk lub charakterystyczny ruch palca,
- zainstalować aplikację antykradzieżową lub antyzagubieniową. Pozwoli ona na ustalenie miejsca, w którym znajduje się telefon, zablokowanie go, wyświetlenie komunikatu na ekranie czy też wykonanie zdjęcia z wbudowanego w telefon aparatu fotograficznego,
- umieścić na telefonie oznaczenia, których nie da się usunąć. Mogą to być np. inicjały właściciela, wydrapane lub wygrawerowane laserem na obudowie smartfona oraz w jego wnętrzu. Takie „oznaczenia" mogą zniechęcić potencjalnego złodzieja.

CIEKAWOSTKA LOKATKI

Każdy telefon komórkowy posiada swój niepowtarzalny numer nadawany przez jego producenta. Jest to tzw. numer IMEI (ang. International Mobile Equipment Identity). Warto znać IMEI swojego telefonu. Można znaleźć go na opakowaniu urządzenia. Za pomocą tego numeru można zlokalizować telefon, ponieważ jest on wykorzystywany przez nadajniki sieci komórkowej.

QUIZ

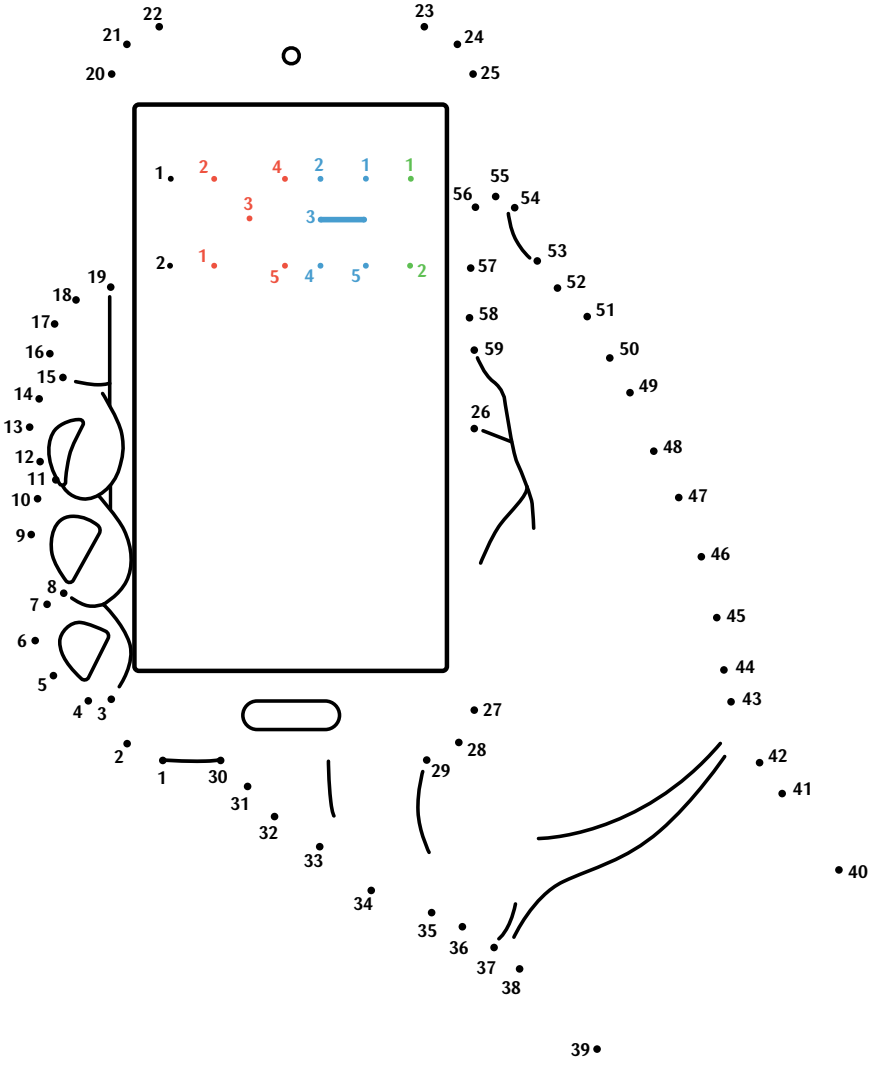
Aby zabezpieczyć dane lub zdjęcia zrobione telefonem, najlepiej:

1. Kasować je z urządzenia najszybciej, jak to możliwe.
2. Nie pokazywać osobom postronnym, że się je robiło.
3. Korzystać z oprogramowania antywirusowego na telefon.

Poprawne odpowiedzi do quizu znajdziesz na końcu publikacji.
Data opracowania materiału: sierpień 2018.

ZADANIE

Połącz kropki i dowiedz się, jak nazywa się indywidualny numer każdego aparatu telefonicznego.
Warto go znać i na jego podstawie móc zidentyfikować telefon w przypadku zagubienia go lub kradzieży.



Bez względu na wiek rozwiąż wszystkie zadania. Wszystkie ćwiczenia utrwalają Twoją wiedzę,
a jednocześnie przybliżają Cię do zdobycia Cybercertyfikatu. Znajdziesz go na końcu publikacji.

KARTA WIELE WARTA

Kuba czyta książkę o dzieciach, które oszczędzały na wielką podróż do Afryki. Zainspirowany lekturą chciałby jak najlepiej przygotować się – również finansowo – do zielonej szkoły, na którą pojedzie pod koniec roku szkolnego. Nie będzie to wycieczka do Afryki, ale w okolice jednego z polskich parków narodowych.

– Ile tam będzie dzikich zwierząt! – cieszy się chłopiec.
– Może weźmiesz ze sobą kartę płatniczą mamy? – proponuje bratu Kasia. – Płacenie kartą jest wygodniejsze, szybsze i bezpieczniejsze od płacenia gotówką.
– Posługuję się kartą. Ta karta jest powiązana z moim kontem bankowym i służy do płacenia pieniędzmi, które znajdują się na moim rachunku. Jest na niej moje imię i nazwisko. Nie mogę pożyczać jej innym osobom. Nawet gdybym to zrobiła, to obsługa sklepu z pewnością zauważy niezgodność i nie pozwoli Kubie, by płacił moją kartą – wyjaśniła dzieciom mama. – A może chciałbyś mieć własną kartę? – zaproponowała pani Pieniążek. – Pani z banku mówiła mi, że dzieci mogą korzystać ze specjalnych, dedykowanych im kart. Niektóre dziecięce karty pozwalają na wypłaty z bankomatów, płacenie w sklepach stacjonarnych i robienie zakupów przez internet do kwoty, na jaką pozwolili im rodzice.

Chłopiec aż podskoczył z radości.
– Tak, chciałbym mieć własną kartę!
Wieczorem Kuba wyszukuje w internecie zasady bezpiecznego korzystania z kart.

CIEKAWOSTKA LOKATKI

Pierwsze karty płatnicze wcale nie zostały wymyślone przez banki. Ojczyzną kart płatniczych są Stany Zjednoczone, gdzie pod koniec XIX wieku zaczęto wydawać karty, przy użyciu których można było płacić za noclegi w hotelach. Kamieniem milowym w historii kart był rok 1914, kiedy jedna z firm finansowo-transportowych stworzyła dla swoich najwierniejszych klientów metalową kartę z wytłoczonymi danymi posiadacza. Dzięki niej można było płacić bezgotówkowo za usługi i produkty tej jednej firmy.

Data opracowania materiału: sierpień 2018.


W POLSCE JEST TYLE BANKOMATÓW I PUNKTÓW, W KTÓRYCH MOŻNA PŁACIĆ BEZGOTÓWKOWO, ŻE NAWET W PARKU PRZYDA MI SIĘ KARTA. ZAPŁACĘ NIĄ ZA PAMIĄTKI.

PANCERNIK KATETEPES RADZI

Jeśli zdarzy się, że w historii transakcji znajdziesz płatność, której nie wykonywałeś, lub jeśli otrzymasz SMS z informacją, że dokonałeś transakcji, choć za nic nie płaciłeś, to należy niezwłocznie poinformować o tym fakcie swoich rodziców. Powinni zastrzec kartę. Najszybciej zrobią to, dzwoniąc na infolinię i wybierając opcję zastrzegania karty.

PIN (z języka angielskiego Personal Identification Number) to osobisty numer identyfikacyjny, rodzaj hasła do karty. Składa się z czterech cyfr (od 0000 do 9999). Tego hasła nie można zapisywać na karcie, której używa się do płacenia lub wypłaty pieniędzy z bankomatu. Po prostu trzeba nauczyć się go na pamięć.

Data opracowania materiału: sierpień 2018.

PODSTAWOWE ZASADY, KTÓRE MOGĄ ZMNIEJSZYĆ RYZYKO OSZUSTWA LUB KRADZIEŻY PIENIĘDZY Z WYKORZYSTANIEM KARTY:

- po otrzymaniu karty podpisz ją i przechowuj w bezpiecznym miejscu,
- zapisz i schowaj wszelkie dane do kontaktu z bankiem oraz numer karty na wypadek jej kradzieży bądź zgubienia, możesz też wpisać numer infolinii banku do kontaktów w swoim telefonie,
- zapamiętaj numer PIN otrzymanej karty,
- możesz zmienić PIN na własną kombinację cyfr. Unikaj jednak prostych kombinacji, np. 0000, 1234 czy daty urodzenia,
- nie przechowuj zapisanego numeru PIN razem z kartą,
- nie podawaj PIN-u osobom postronnym, choć w przypadku dzieci dobrze jest, by znał go któryś z rodziców,
- regularnie sprawdzaj dokonane transakcje w historii rachunku – wszelkie niezgodności natychmiast należy zgłosić w banku,
- przy wprowadzaniu danych karty – w miarę możliwości należy unikać transakcji internetowych realizowanych przez nieszyfrowane połączenie (bez liter „https" lub symbolu „kłódki" przy adresie strony),
- ignoruj wiadomości e-mail z prośbami o zalogowanie się na wskazanych stronach internetowych i podanie tam danych karty, jak również telefony z prośbą o podanie danych karty. Jest to tak zwany „phishing", czyli próba wyłudzenia danych. Dotyczy to również sytuacji, gdy kontakt rzekomo pochodzi od instytucji zaufanej – np. banku. Pamiętaj, bank nigdy nie prosi mailowo ani telefonicznie o dane Twojej karty,
- do wykonywania transakcji internetowych kartą płatniczą wystarczy komputer z dostępem do internetu, wyposażony w standardową przeglądarkę internetową. Korzystaj z najnowszych wersji przeglądarek internetowych,
- dbaj o zabezpieczenie komputera, z którego wykonujesz operacje bankowości internetowej, w tym płatności kartą. Instaluj tylko legalne oprogramowanie oraz aktualizuj je zgodnie z zalecaniami jego producenta,
- używaj oprogramowania antywirusowego oraz korzystaj z oprogramowania lub urządzeń typu firewall (zapór sieciowych),
- jeśli do połączenia z internetem używasz domowego routera, koniecznie zabezpiecz dostęp do jego ustawień własnym, skomplikowanym hasłem.

QUIZ

Najlepszy PIN spośród poniższych to:

1. 1111 – ponieważ łatwo go zapamiętać.
2. 1407 – czyli urodziny posiadacza karty (14 lipca).
3. 1395 – niepowiązane ze sobą liczby, niezwiązane bezpośrednio z danymi posiadacza karty, nieułożone obok siebie (ani pod sobą) na klawiaturze bankomatu.

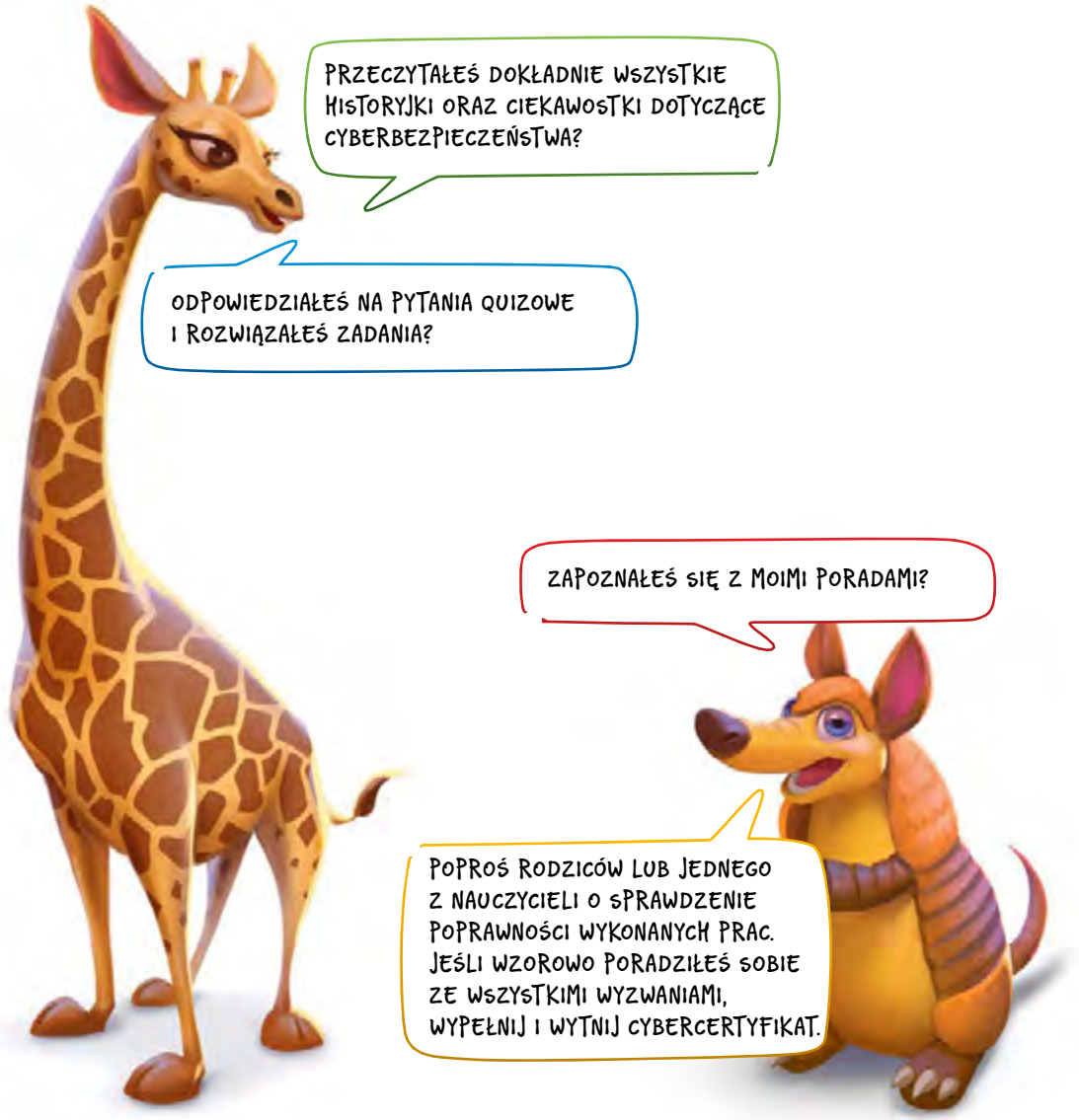
WYKREŚLANKA

W poniższej tabelce ukryte są słowa związane z bezpieczeństwem i bankowością. Jest ich 15. Szukaj ich zarówno w poziomie, jak i w pionie. Następnie wypisz pod tabelką znalezione słowa i zastanów się, co oznaczają. W przypadku trudności poproś o pomoc nauczyciela bądź rodziców.

B	A	H	A	G	K	O	N	T	O
A	N	T	Y	W	I	R	U	S	I
N	D	T	R	O	D	Z	I	C	N
K	A	P	I	N	K	W	A	P	F
I	N	S	Ł	C	H	A	S	Ł	O
R	E	B	L	O	K	A	D	A	L
A	P	L	I	K	A	C	J	A	I
M	K	O	M	P	U	T	E	R	N
E	M	A	I	L	I	C	Z	M	I
K	O	N	T	R	O	L	A	I	A

Poprawne odpowiedzi do quizu znajdziesz na końcu publikacji.
Bez względu na wiek rozwiąż wszystkie zadania. Wszystkie ćwiczenia utrwalają Twoją wiedzę, a jednocześnie przybliżają Cię do zdobycia Cybercertyfikatu. Znajdziesz go na końcu publikacji.

ZAMIAST ZAKOŃCZENIA

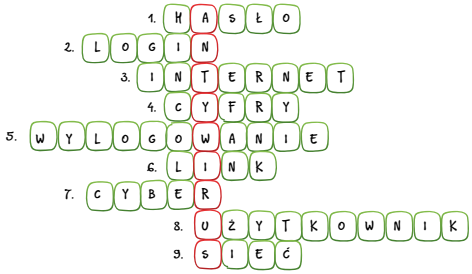


KLUCZ ODPOWIEDZI DO ZADAŃ

QUIZ ZE STR. 8:
Odp.: 2

QUIZ ZE STR. 12:
Odp.: 3

KRZYŻÓWKA ZE STR. 13



QUIZ ZE STR. 16:
Odp.: 3

REBUS ZE STR. 17:
hasło, gra komputerowa

QUIZ ZE STR. 21:
Odp.: 3

QUIZ ZE STR. 24:
Odp.: 1

RÓŻNICE MIĘDZY OBRAZKAMI ZE STR. 26–27:
Brak „https” w adresie strony, inny rozmiar i położenie logotypu „SKO” w polu „Witaj”, inne położenie boksu „Ostatnio założone”, inne położenie boksu „Blogi miesiąca”, przycisk „Więcej” na dole boksu „Blogi miesiąca”, napis „Najnowsze wpisy na blogach” innym kolorem i z błędem: „Najnowsze wpisy na blogi”

QUIZ ZE STR. 30:
Odp.: 2

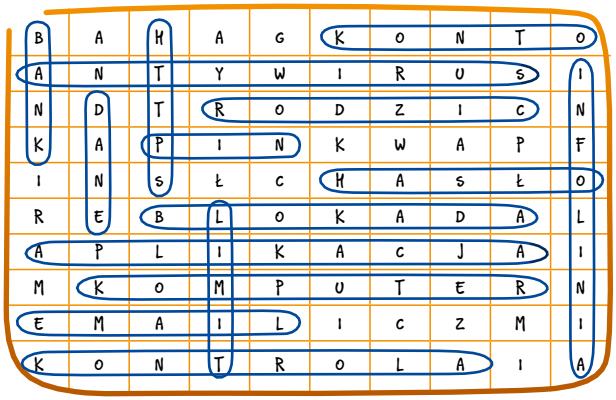
REBUS ZE STR. 31:
pomoc, bezpieczeństwo

QUIZ ZE STR. 36:
Odp.: 3

RYSUNEK ZE STR. 37:
IMEI

QUIZ ZE STR. 42:
Odp.: 3

WYKREŚLANKA – SŁOWA ZE STR. 42:
PIN, hasło, https, antywirus, bank, komputer, infolinia, aplikacja, limit, kontrola, blokada, email, dane, rodzic, konto



CYBERCERTYFIKAT

JUNIOR

PKO Bank Polski

dla

.....

.....

poświadczający wysoki poziom wiedzy na temat bezpieczeństwa w sieci oraz ponadprzeciętne zaangażowanie w zdobywanie umiejętności w zakresie bezpiecznego wykorzystywania nowych technologii.

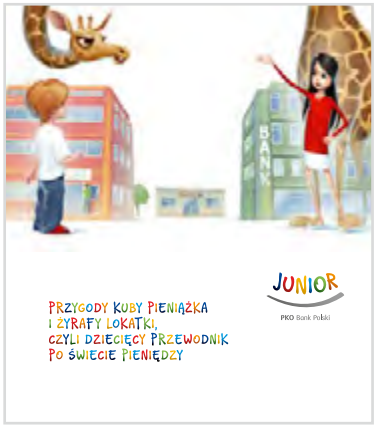
.....	.....
Miejscowość	Data
.....	.....
Podpis dziecka	Podpis rodzica lub nauczyciela

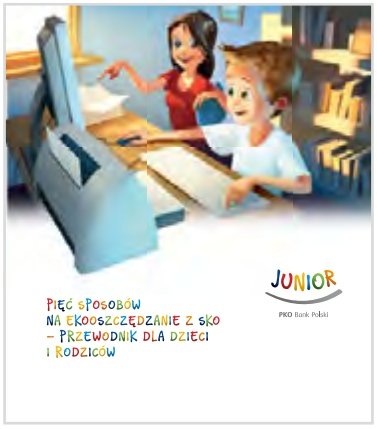
PAMIĘTAJ!

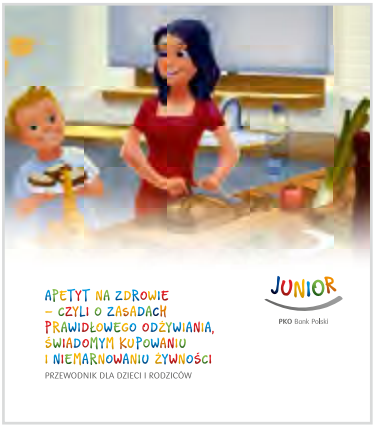
Nowe technologie rozwijają się bardzo dynamicznie. Regularnie aktualizuj swoją wiedzę i odświeżaj kompetencje w zakresie cyberbezpieczeństwa.

Certyfikat do pobrania (w wersji pdf) znajduje się na stronie www.pkobp.pl/sko oraz www.pkobp.pl/junior.

W TEJ SERII UKAZAŁY SIĘ M. IN.:







Wszystkie materiały dostępne są w wersji elektronicznej na stronie internetowej www.pkobp.pl/junior.

Wydawca: PKO Bank Polski
Ilustracje: Rafał Wojtunik

„Junior bezpieczny w sieci" to publikacja, która powstała w ramach Szkolnych Kas Oszczędności – największego i najbardziej nowoczesnego w Polsce programu edukacji finansowej prowadzonego od 1935 roku przez PKO Bank Polski.

Więcej informacji na temat edukacji finansowej w ramach Szkolnych Kas Oszczędności można znaleźć na www.pkobp.pl/junior.

SIERPIEŃ 2018