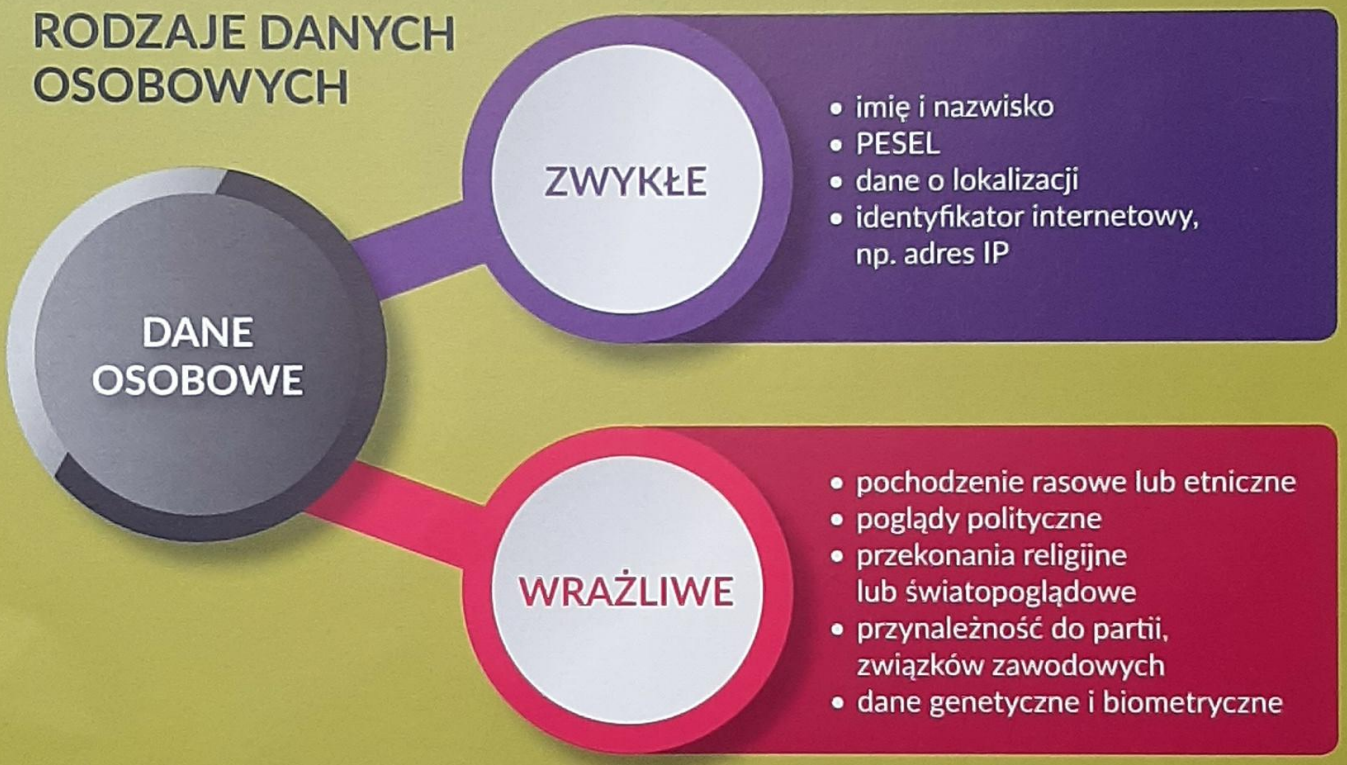
BEZPIECZNA PRACA Z KOMPUTEREM

- Ochrona danych osobowych, RODO
- BHP w pracowni komputerowej
- Złośliwe oprogramowanie
- Sposoby zabezpieczania kont

OCHRONA DANYCH OSOBOWYCH W SIECI

RODZAJE DANYCH OSOBOWYCH



PSEUDONIMIZACJA I ANONIMIZACJA

Marcin Nowak, urodzony 12 kwietnia 2004 w Warszawie, ukończył kurs na patent sternika motorowodnego

Pseudonimizacja to takie przetwarzanie danych osobowych, aby niemożliwe było zidentyfikowanie osoby na podstawie tych danych bez dodatkowego „klucza", który musi być przechowywany w innym miejscu. Jest to proces odwracalny.

MN, 2004, PSM

Anonimizacja to usunięcie wszystkich informacji umożliwiających w jakikolwiek sposób identyfikację osoby, której dane dotyczą. Jest to proces nieodwracalny.

[redacted] urodzony 12 kwietnia 2004 w Warszawie, ukończył kurs na patent sternika motorowodnego

Dane osobowe to informacje, które pozwalają jednoznacznie zidentyfikować osobę. Wykorzystywanie (przetwarzanie) danych osobowych reguluje Rozporządzenie o Ochronie Danych Osobowych, powszechnie znane jako RODO, które obowiązuje w całej Unii Europejskiej od 25 maja 2018 r.

PAKIET PRAW KONSUMENTA

Wraz z wprowadzeniem RODO każdy użytkownik internetu otrzymał **prawa**, dzięki którym może zwiększyć ochronę swoich danych osobowych w sieci.

- prawo dostępu do informacji m.in. na temat rodzaju danych i celu ich przetwarzania
- prawo do poprawiania danych
- prawo do bycia zapomnianym, czyli do usunięcia danych z bazy
- prawo do ograniczenia przetwarzania danych
- prawo do przenoszenia danych

1. Ochrona systemu, danych i kont

- Zasady korzystania z pracowni komputerowej
- Dobre praktyki w zakresie ochrony oprogramowania
- Sposoby zabezpieczania kont

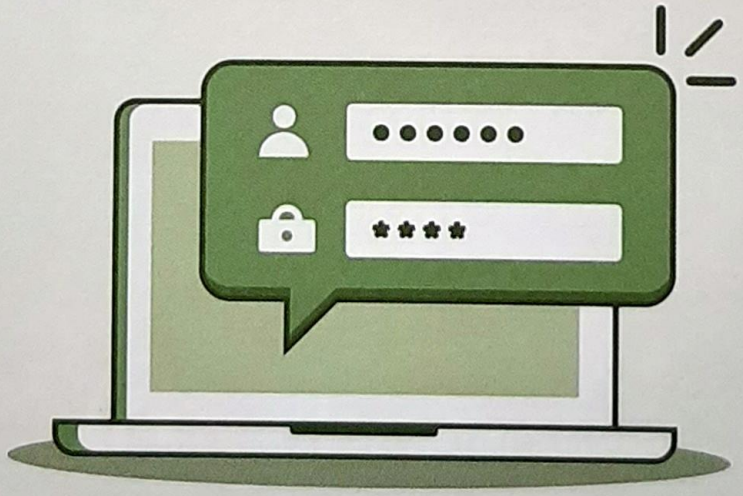
ZADANIE NA START

Jak szybko komputer złamie hasło?

Aby sprawdzić, ile maksymalnie prób potrzeba, aby złamać czterocyfrowy PIN do karty kredytowej, należy wyznaczyć liczbę wszystkich możliwych kodów w zależności od tego, czy w kodzie:

- cyfry mogą się powtarzać ($10 \cdot 10 \cdot 10 \cdot 10 = 10\,000$);
- cyfry mogą się powtarzać, ale nie czterokrotnie ($10 \cdot 10 \cdot 10 \cdot 10 - 10 = 9990$);
- cyfry nie mogą się powtarzać ($10 \cdot 9 \cdot 8 \cdot 7 = 5040$).

Oblicz, ile maksymalnie prób potrzeba, aby złamać czteroznakowy kod złożony z małych i wielkich liter alfabetu łacińskiego.



BEZPIECZNIE W PRACOWNI KOMPUTEROWEJ

W sali informatycznej obowiązuje regulamin uwzględniający specyfikę pracy z komputerem w szkole. Pamiętaj, że należy:

- korzystać z urządzeń zgodnie ze wskazówkami nauczyciela;
- informować nauczyciela o wszelkich usterkach zauważonych podczas pracy;
- logować się tylko na własne konto użytkownika;
- przechowywać dokumenty w miejscu wskazanym przez nauczyciela;
- dbać o porządek na stanowisku pracy.

OCHRONA SYSTEMU I DANYCH ZAPISANYCH NA KOMPUTERZE

Bezpieczeństwo komputerowe to niezwykle istotna sprawa. Komputer i dane na nim zgromadzone narażone są na działanie złośliwego oprogramowania (*malware*) oraz na innego rodzaju ataki cyberprzestępców.

ZAPAMIĘTAJ!

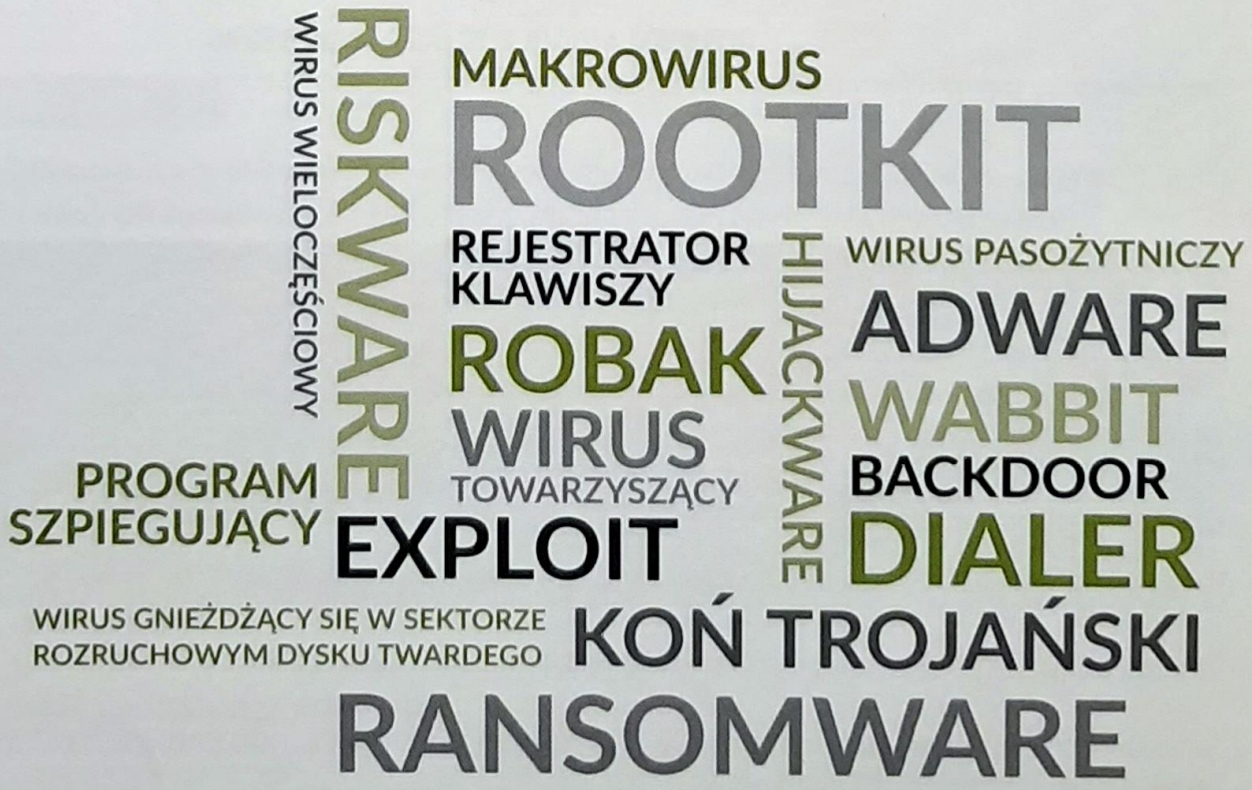
Złośliwe oprogramowanie obejmuje różne typy programów, których celem jest działanie na szkodę użytkowników, np. poprzez kradzież danych czy też przejęcie kontroli nad komputerem.

Do infekcji może dojść m.in. przez:

- użycie zainfekowanego nośnika;
- odwiedzenie witryny zawierającej kod, który z powodu błędu w zabezpieczeniach danej przeglądarki instaluje złośliwe oprogramowanie bez wiedzy użytkownika;
- pobranie zainfekowanego pliku, np. programu czy filmu;
- otworzenie e-maila z załącznikiem zawierającym złośliwy kod;
- kliknięcie zainfekowanego zdjęcia w portalu społecznościowym.

Ćwiczenie 1. Rodzaje szkodliwego oprogramowania

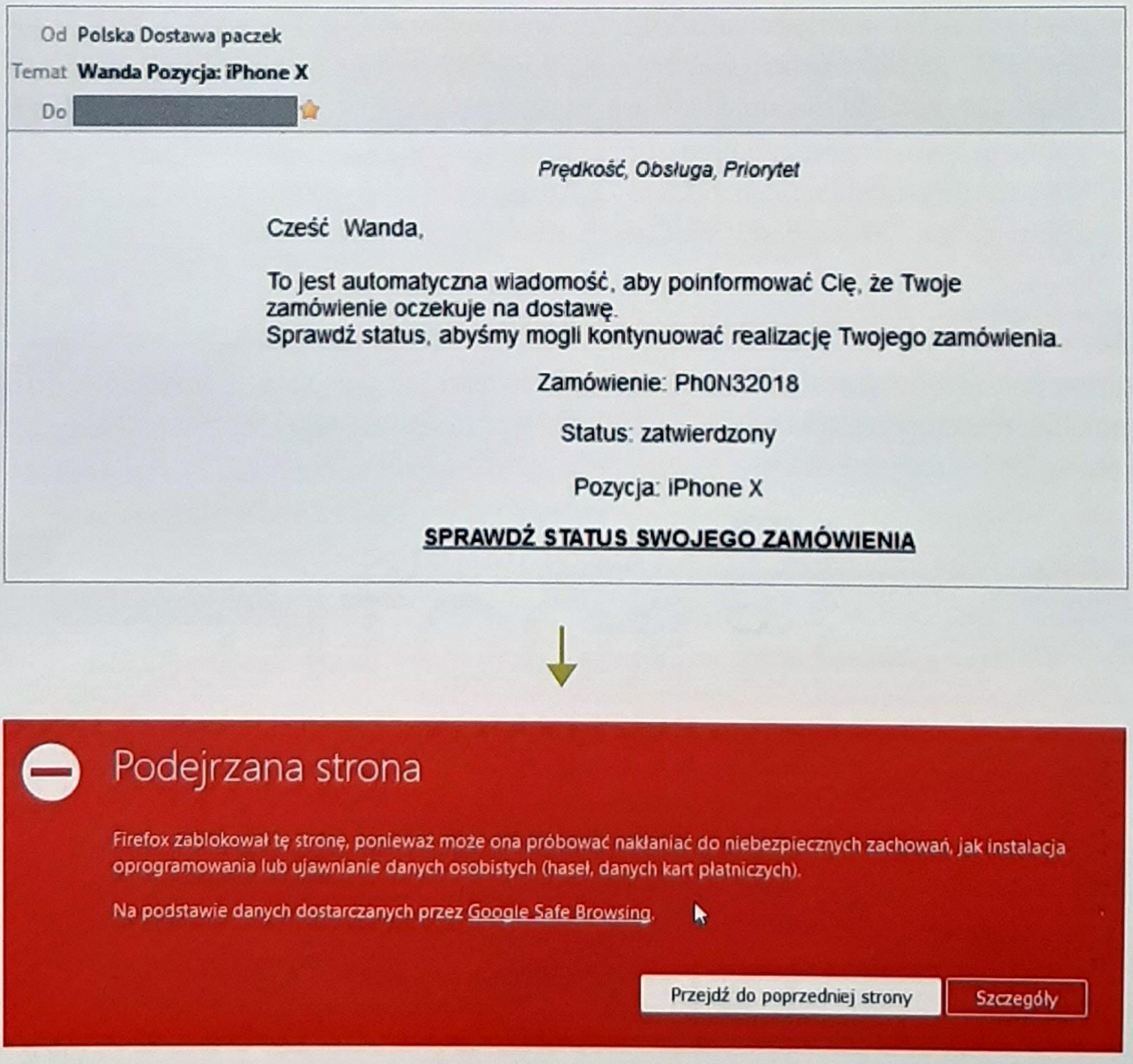
Zapoznaj się z poniższą grafiką, a następnie scharakteryzuj krótko wymienione grupy złośliwego oprogramowania. Potrzebne informacje wyszukaj w internecie.



POSZUKAJ W INTERNECIE

Zapoznaj się z dokumentem *Avoid and report Google scams*.

Cyberprzestępcy nie zawsze sięgają po specjalne programy. Niektórzy wykorzystują luki systemowe lub po prostu do skutku odgadują hasło dostępu (tzw. ataki *brute force*). Inni wyłudzają poufne dane przez zastosowanie **phishingu**. Ta metoda wykorzystuje socjotechnikę. Najczęstszą jej formą są e-maile udające wiadomości od danego nadawcy i kierujące na odpowiednio spreparowane strony internetowe, które mają nakłonić niedoświadczonego użytkownika do podania danych otwierających dostęp do konta bankowego, PayPala czy karty kredytowej. Wiele firm prowadzi specjalne strony z informacjami na temat oszustw, w ramach których wykorzystywane są ich nazwa i logo (np. Google).



Rys. 1. Przykład phishingu

Scharakteryzuj język listu i nadawcę. Co sprawia, że wiadomość nosi znamiona phishingu?

Aby zapewnić systemowi oraz danym właściwą ochronę, należy:

- systematycznie dokonywać aktualizacji – „łatać dziury" w zabezpieczeniach;
- aktywować systemową zaporę sieciową lub zainstalować preferowaną zaporę – zezwolić na monitorowanie pakietów danych przesyłanych między komputerem a siecią i blokowanie nieautoryzowanego dostępu do komputera;
- zainstalować oprogramowanie typu *internet security* – podstawową ochronę zapewnia skaner antywirusowy, który sprawdza zapisane na komputerze pliki i w razie potrzeby usuwa zagrożenie; takie oprogramowanie ma także często funkcje zaawansowane, dostępne w zależności od wybranego pakietu, np. moduł ochrony poczty elektronicznej, filtr antyspamowy, blokowanie niebezpiecznych stron, ochronę płatności dokonywanych online, skaner linków z portali społecznościowych, szyfrowanie danych, lokalizację skradzionego komputera;
- skanować programem antywirusowym nośniki zewnętrzne;
- nie odwiedzać witryn kwalifikowanych przez przeglądarkę jako niebezpieczne;
- nie pobierać plików z niesprawdzonych serwisów;
- nie otwierać wiadomości z nieznanych źródeł, o podejrzanie brzmiących tematach, z błędami ortograficznymi bądź językowymi;
- nie klikać linków w wiadomościach od nieznanych nadawców.

BEZPIECZNE HASŁO

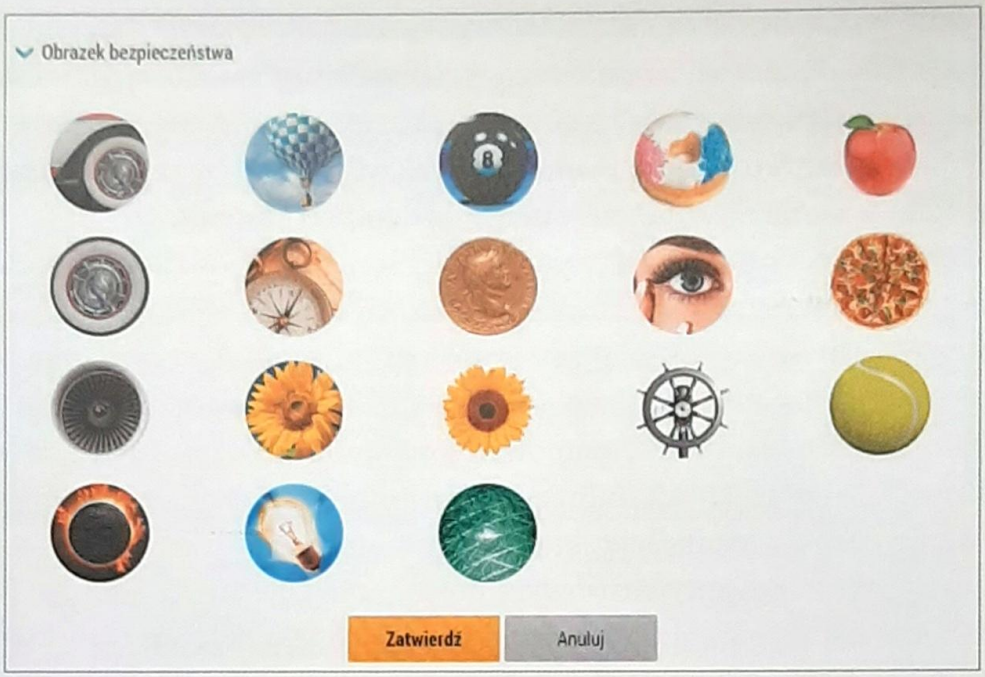
Hasła potrzebne są wszędzie – aby dostać się do poczty elektronicznej na serwerze, konta na portalu społecznościowym albo konta bankowego, aby sprawdzić historię zakupów w sklepie internetowym, zarezerwować z domu książkę w bibliotece czy pracować wspólnie z kolegami w chmurze.

WIEM WIĘCEJ

Niebawem, aby zalogować się do dowolnego serwisu, wystarczy odcisk palca, skan twarzy lub specjalny klucz USB. Nowy standard uwierzytelniania obsługują m.in. przeglądarki Mozilla Firefox, Google Chrome i Microsoft Edge.

Niektóre witryny wprowadzają dodatkowe zabezpieczenia przy logowaniu, np.:

- oferują maskowanie hasła, które polega na wprowadzaniu tylko wybranych elementów hasła (znaki wpisuje się tylko w jaśniejsze aktywne pola),
- wzmacniają hasło przez konieczność wpisania dodatkowo hasła z tokena,
- stosują drugie hasło wymagające podania wybranych losowo cyfr numeru PESEL,
- po wpisaniu loginu wyświetlają tzw. obrazek bezpieczeństwa wybrany w ustawieniach konta przez użytkownika – na znak, że jest to pożądana, bezpieczna strona, a nie podstawiona fałszywka.



Rys. 2. Zabezpieczenie procesu logowania za pomocą tzw. obrazka bezpieczeństwa

Jak pokazują badania, przeciętny użytkownik internetu korzysta z dwudziestu paru haseł do różnego rodzaju aktywności. Trudno je wszystkie zapamiętać, zwłaszcza te rzadko używane. Zapomniane hasło można zwykle zmienić na nowe za pomocą poczty e-mail, ale w ten sposób tworzy się tylko kolejne hasło do zapamiętania. Dobrym rozwiązaniem jest tzw. menedżer haseł, który generuje mocne hasła dla wszystkich kont oraz szyfruje przechowywane hasła. Użytkownik musi wówczas znać tylko jedno hasło – do menedżera haseł.

Bezpieczne hasło jest łatwe do zapamiętania dla użytkownika, lecz trudne do odgadnięcia przez inne osoby. Powinno się składać z minimum ośmiu znaków (długie hasło sprawia, że liczba możliwych kombinacji wzrasta i wydłuża czas potrzebny hakerowi na jego złamanie), zawierać małe i wielkie litery, cyfry oraz znaki specjalne. Jeśli korzystasz z serwisu bez podawania ważnych danych, możesz zastosować prostsze hasło.

Ćwiczenie 2. Samodzielne tworzenie silnego hasła

Utwórz silne hasło, którego podstawę będzie stanowić fraza łatwa do zapamiętania.

- Wybierz podstawę hasła, np. przysłowie: „Idzie luty, podkuj buty".
- Określ zasady tworzenia hasła, czyli sposób, który pozwoli ci je odtworzyć. Zasady mogą być np. takie:
  - pomiń wyrazy jednoliterowe;
  - z każdego wyrazu weź dwie pierwsze litery;
  - jeśli któraś z liter nie należy do alfabetu łacińskiego (np. ą, ó), zamień ją na odpowiadającą jej literę alfabetu łacińskiego;
  - każdą parę liter zapisz w formacie wielka-mała (np. Wi);

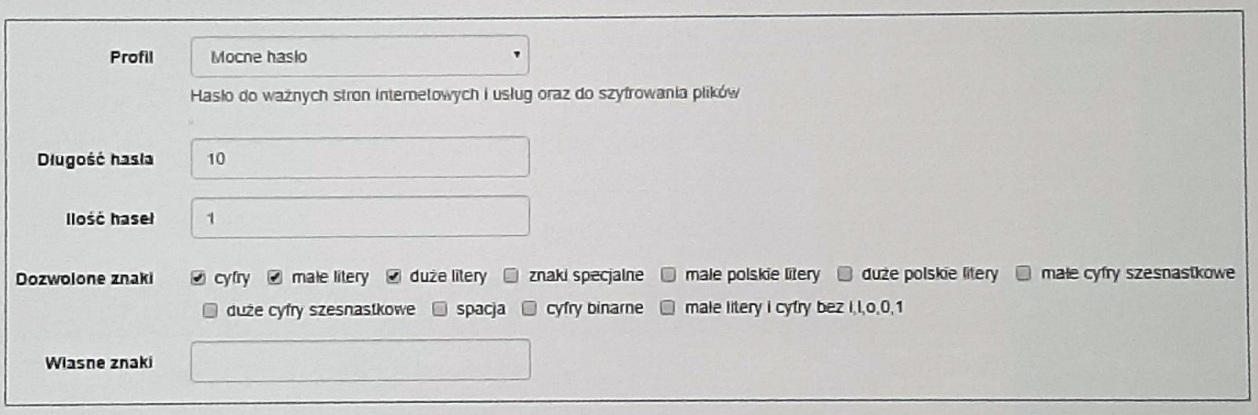
- po pierwszych dwóch literach i na końcu hasła wstaw znaki specjalne (np. #, *);
- dwie ostatnie litery poprzedź cyfrą.

- Zastosuj przyjęte zasady do wybranej podstawy hasła. Dla wskazanego wcześniej przysłowia hasło to np.: Id#LuPo7Bu*.

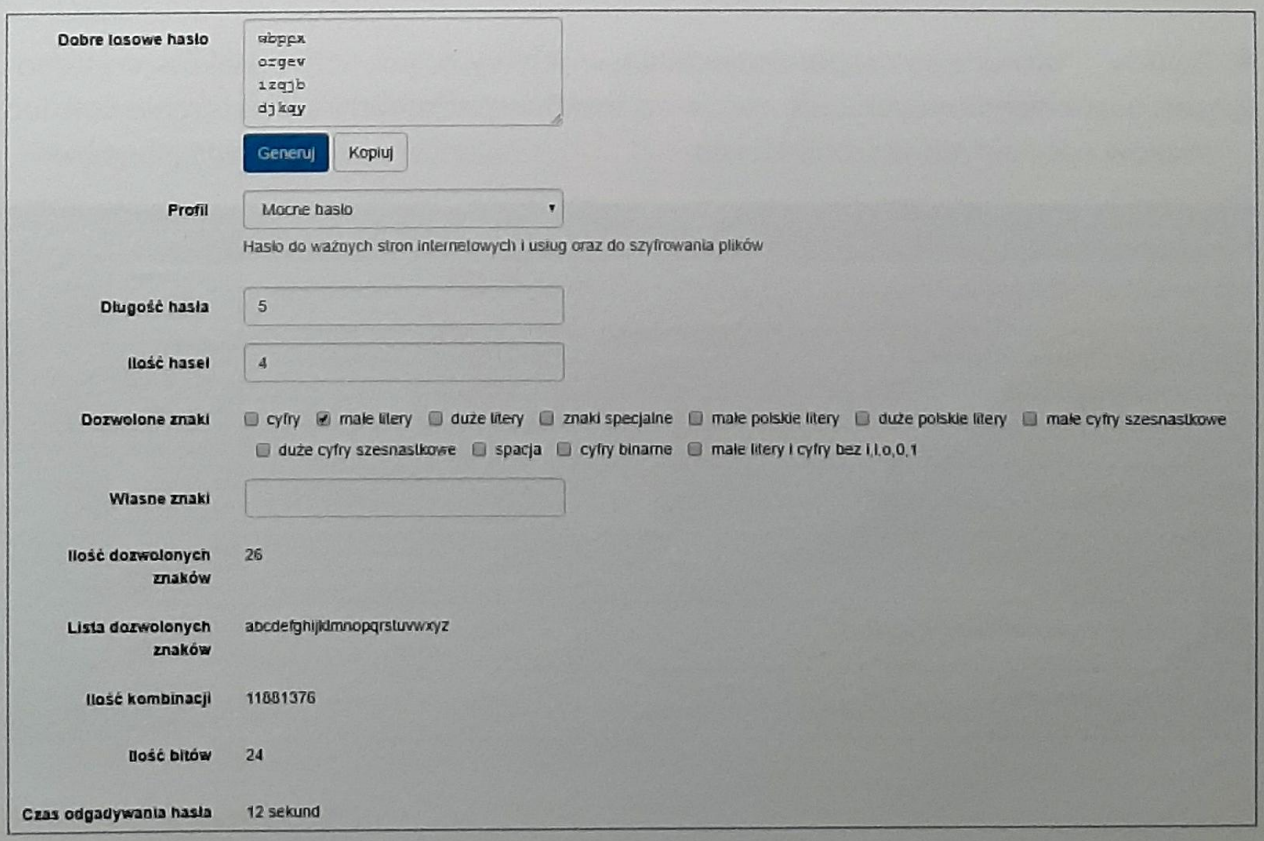
Ćwiczenie 3. Tworzenie hasła za pomocą generatora

Skorzystaj z generatora haseł na stronie **http://dobrehaslo.pl** i utwórz mocne hasło, z uwzględnieniem różnych parametrów, a następnie dokonaj analizy otrzymanych wyników.

- Wybierz profil hasła i określ parametry – długość hasła, znaki dozwolone, znaki własne.



- Dokonaj analizy otrzymanych wyników, np. takiej:
  - w przypadku hasła złożonego z pięciu małych liter komputer musi sprawdzić 11 881 376 kombinacji, co zajmie mu zaledwie 12 s;



- w przypadku zwiększenia liczby znaków hasła do siedmiu oraz liczby znaków do wyboru do 93 (cyfry, małe i duże litery, znaki specjalne) komputer musi sprawdzić już ponad 60 bilionów kombinacji, co może mu zająć dwa lata; gdyby zwiększyć liczbę znaków hasła do ośmiu, czas odgadywania hasła przekroczy czas życia człowieka.

POSZUKAJ W INTERNECIE

Sprawdź na stronie **http://www.bezpiecznypc.pl/czesto-zadawane-pytania.php**, na jakiej zasadzie działa zamieszczony w serwisie tester haseł.

Ćwiczenie 4. Testowanie haseł

Na podstawie wymagań opisanych na stronie **www.passwordmeter.com** dokonaj analizy podanych haseł: Br4aKtm@, kotek7, nap@rawa4, Duch09@21.

- Wpisz hasło w pole **Password** (koniecznie zaznacz opcję **Hide**, która maskuje tekst), aby program zaprezentował jego diagnozę w postaci punktacji procentowej (**Score**) oraz słownej (**Complexity**; hasło bardzo słabe – *very weak*, słabe – *weak*, dobre – *good*, silne – *strong*, bardzo silne – *very strong*).

Test Your Password		Minimum Requirements
Password:	Br4aKtm@	• Minimum 8 characters in length • Contains 3/4 of the following items: - Uppercase Letters - Lowercase Letters - Numbers - Symbols
Hide:	☐	
Score:	72%	
Complexity:	Strong	

- Punkty dodawane są za spełnienie minimalnych wymagań, liczbę znaków, występowanie wielkich i małych liter, cyfr oraz znaków specjalnych, umieszczenie cyfr lub znaków specjalnych w środku hasła.

Additions		Type	Rate	Count	Bonus
✓	Number of Characters	Flat	+(n*4)	8	+ 32
★	Uppercase Letters	Cond/Incr	+((len-n)*2)	2	+ 12
★	Lowercase Letters	Cond/Incr	+((len-n)*2)	4	+ 8
✓	Numbers	Cond	+(n*4)	1	+ 4
✓	Symbols	Flat	+(n*6)	1	+ 6
✓	Middle Numbers or Symbols	Flat	+(n*2)	1	+ 2
★	Requirements	Flat	+(n*2)	5	+ 10

- Punkty odejmowane są za użycie samych liter lub cyfr, powtarzające się litery, cyfry lub znaki specjalne (np. aRw4*a), albo następujące po sobie dowolne małe litery (jak na poniższym zrzucie), wielkie litery lub cyfry co najmniej trzy kolejne litery, cyfry lub znaki specjalne (np. abc, 345).

Deductions					
✓	Letters Only	Flat	-n	0	0
✓	Numbers Only	Flat	-n	0	0
✓	Repeat Characters (Case Insensitive)	Comp	-	0	0
✓	Consecutive Uppercase Letters	Flat	-(n*2)	0	0
!	Consecutive Lowercase Letters	Flat	-(n*2)	1	- 2
✓	Consecutive Numbers	Flat	-(n*2)	0	0
✓	Sequential Letters (3+)	Flat	-(n*3)	0	0
✓	Sequential Numbers (3+)	Flat	-(n*3)	0	0
✓	Sequential Symbols (3+)	Flat	-(n*3)	0	0

PODSUMOWANIE

- Dane osobowe, np. imię i nazwisko, PESEL, pozwalają jednoznacznie zidentyfikować określoną osobę. Serwisy WWW nie mogą gromadzić i udostępniać danych osobowych użytkowników bez ich wiedzy i zgody. Zgodę na przetwarzanie danych w każdej chwili można wycofać.
- Należy przestrzegać regulaminu szkolnej pracowni komputerowej.
- Komputer i dane narażone są na działanie złośliwego oprogramowania (m.in. wirusów, robaków, trojanów) oraz innego typu ataki hakerów (m.in. phishing). Aby zapewnić im należytą ochronę, należy zainstalować zaporę sieciową i oprogramowanie ochronne, w tym antywirusowe, oraz systematycznie aktualizować system operacyjny.
- Bezpieczeństwo w internecie może być zapewnione dzięki przestrzeganiu zasad dotyczących rozważnej komunikacji w sieci oraz stosowaniu odpowiednio skonstruowanych haseł do różnego rodzaju usług.
- Bezpieczne hasło jest łatwe do zapamiętania dla użytkownika, lecz trudne do odgadnięcia przez inne osoby. Powinno się składać z minimum ośmiu znaków, zawierać małe i wielkie litery, cyfry oraz znaki specjalne.

PYTANIA SPRAWDZAJĄCE

1. Czy PESEL należy do danych osobowych? Uzasadnij.
2. Jakie konsekwencje może mieć brak stosowania środków ochrony komputera oraz danych? Podaj cztery przykłady.
3. Jakie zasady trzeba uwzględnić przy ustalaniu hasła, aby było trudne do złamania?

ZADANIA DODATKOWE

Zadanie 1. Ergonomia pracy z komputerem stacjonarnym i laptopem

Zapoznaj się z serwisem Państwowej Inspekcji Pracy: **web.pip.gov.pl/ergonomia** i dokonaj oceny stanowiska komputerowego, na którym pracujesz w domu.

Zadanie 2. CERT

Sprawdź, czym jest CERT i jak działają CERT Polska oraz CERT Orange Polska. Zapoznaj się z aktualnymi ostrzeżeniami prezentowanymi w serwisach obu instytucji oraz danymi o zagrożeniach. Dowiedz się, w jaki sposób można zgłosić incydenty.

Zadanie 3. Przepis na zapamiętywanie haseł

Zapoznaj się z poradnikiem *Czy złamanie hasła jest trudne? Jak się zabezpieczyć?* przygotowanym przez CERT Orange Polska, a następnie wymyśl i opisz algorytm zapamiętywania hasła, który możesz polecić innym.