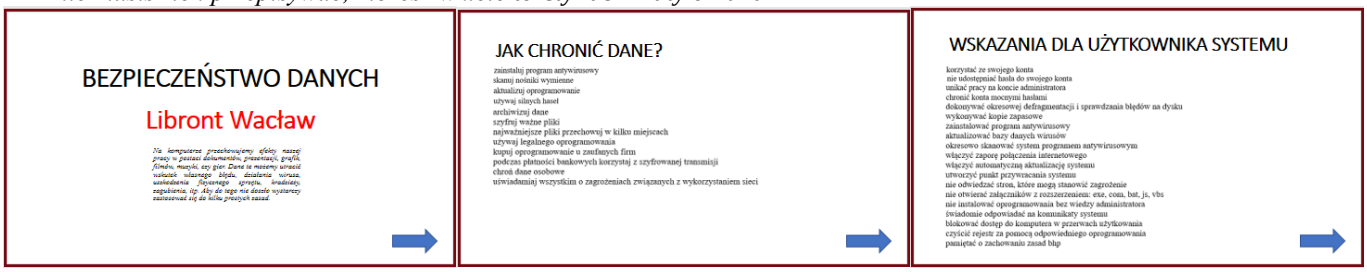
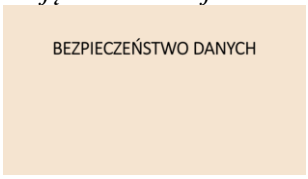
PSK - Zabezpieczanie systemu operacyjnego – Jak chronić dane?

- Przygotuj prezentację multimedialną (PowerPoint lub Impres)
- Prezentacja składa się z trzech slajdów
- Teksty (grafika) znajdują się poniżej
  nie musisz ich przepisywać, możesz wkleić teksty lub zrzuty ekranu



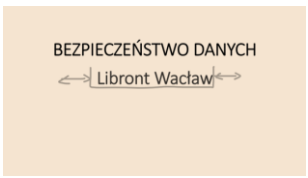
- Do animacji fragmentów tekstów wykorzystaj: **przylot, powiększanie i wylot**
- Animacje na slajdzie mają przebiegać automatycznie
- Kolejność animacji
  0 na ekranie znajduje się główny napis
  1 wolny **wlot od dołu** kolejnego fragmentu tekstu
  2 szybkie **wyróżnienie**, np. impuls, potrząsanie, powiększenie i zmniejszenie
  po wlocie i wyróżnieniu wszystkich fragmentów tekstów
  3 bardzo wolne (5 sekund) **powiększenie** głównego napisu
  4 wolny **wylot do góry** każdego fragmentu tekstu
  po wylocie wszystkich fragmentów tekstu
  5 **wlot z lewej** strzałki
  animację możesz obejrzeć tutaj: ***https://zsobobowa.eu/pliki/testy/psk22.gif***

0



1

2



1

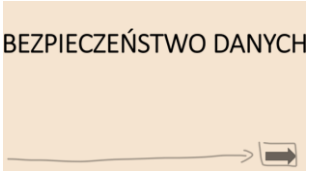
2

3

4

4

5



BEZPIECZEŃSTWO DANYCH

Na komputerze przechowujemy efekty naszej pracy w postaci dokumentów, prezentacji, grafik, filmów, muzyki, czy gier. Dane te możemy utracić wskutek własnego błędu, działania wirusa, uszkodzenia fizycznego sprzętu, kradzieży, zagubienia, itp. Aby do tego nie doszło wystarczy zastosować się do kilku prostych zasad.

JAK CHRONIĆ DANE?

zainstaluj program antywirusowy
skanuj nośniki wymienne
aktualizuj oprogramowanie
używaj silnych haseł
archiwizuj dane
szyfruj ważne pliki
najważniejsze pliki przechowuj w kilku miejscach
używaj legalnego oprogramowania
kupuj oprogramowanie u zaufanych firm
podczas płatności bankowych korzystaj z szyfrowanej transmisji
chroń dane osobowe
uświadamiaj wszystkim o zagrożeniach związanych z wykorzystaniem sieci

WSKAZANIA DLA UŻYTKOWNIKA SYSTEMU

korzystać ze swojego konta
nie udostępniać hasła do swojego konta
unikać pracy na koncie administratora
chronić konta mocnymi hasłami
dokonywać okresowej defragmentacji i sprawdzania błędów na dysku
wykonywać kopie zapasowe
zainstalować program antywirusowy
aktualizować bazy danych wirusów
okresowo skanować system programem antywirusowym
włączyć zaporę połączenia internetowego
włączyć automatyczną aktualizację systemu
utworzyć punkt przywracania systemu
nie odwiedzać stron, które mogą stanowić zagrożenie
nie otwierać załączników z rozszerzeniem: exe, com, bat, js, vbs
nie instalować oprogramowania bez wiedzy administratora
świadomie odpowiadać na komunikaty systemu
blokować dostęp do komputera w przerwach użytkowania
czyścić rejestr za pomocą odpowiedniego oprogramowania
pamiętać o zachowaniu zasad bhp