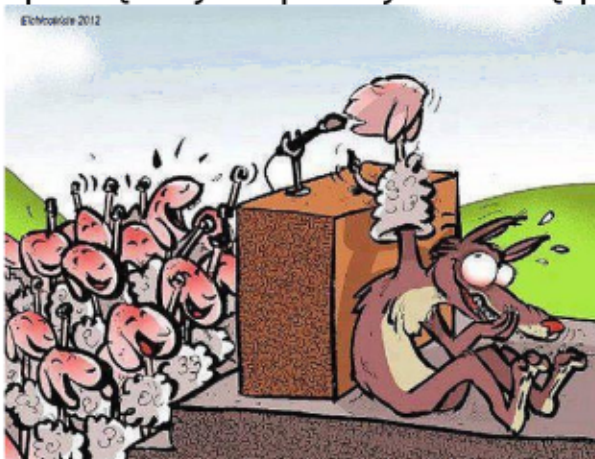


Szkolenie z bezpieczeństwa danych osobowych **2022**

Dane osobowe mogą wyciec na wiele sposobów:

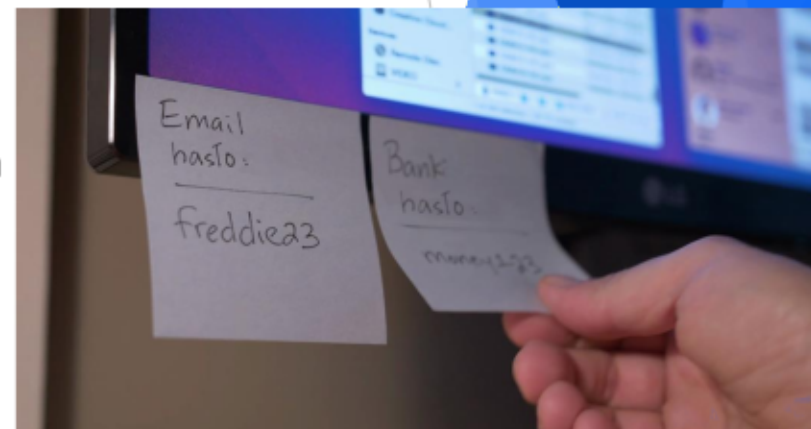
począwszy od podszywania się pod instytucje państwowe,



firmy z nami współpracujące,

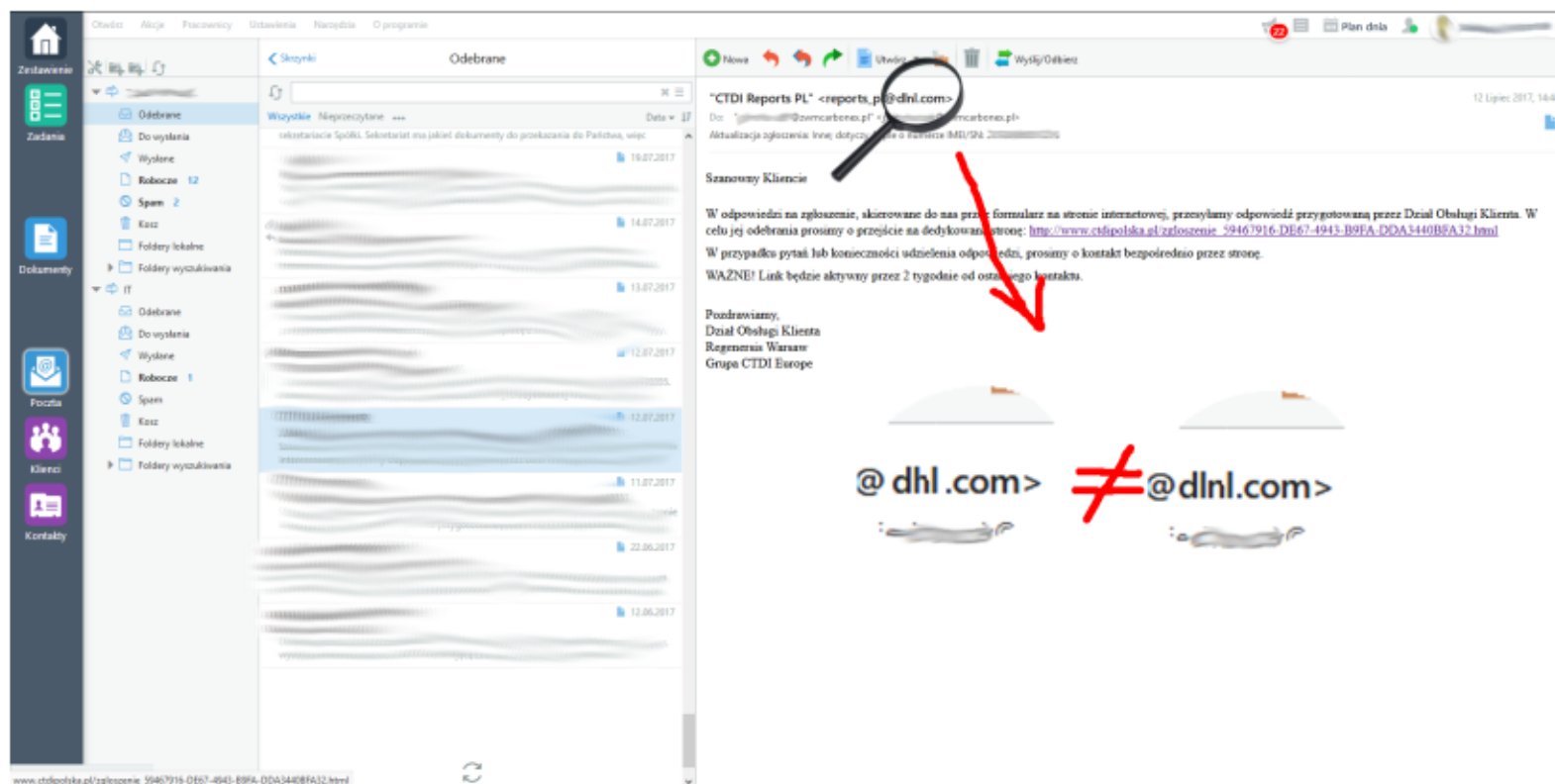
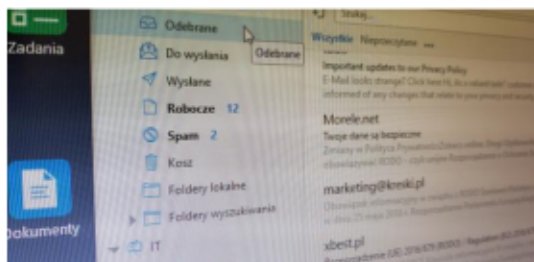
firmy świadczące nam usługi,

aż po włamania do systemów teleinformatycznych



i zwykłą nieostrożność pracowników...

Podszywanie się pod podmioty:



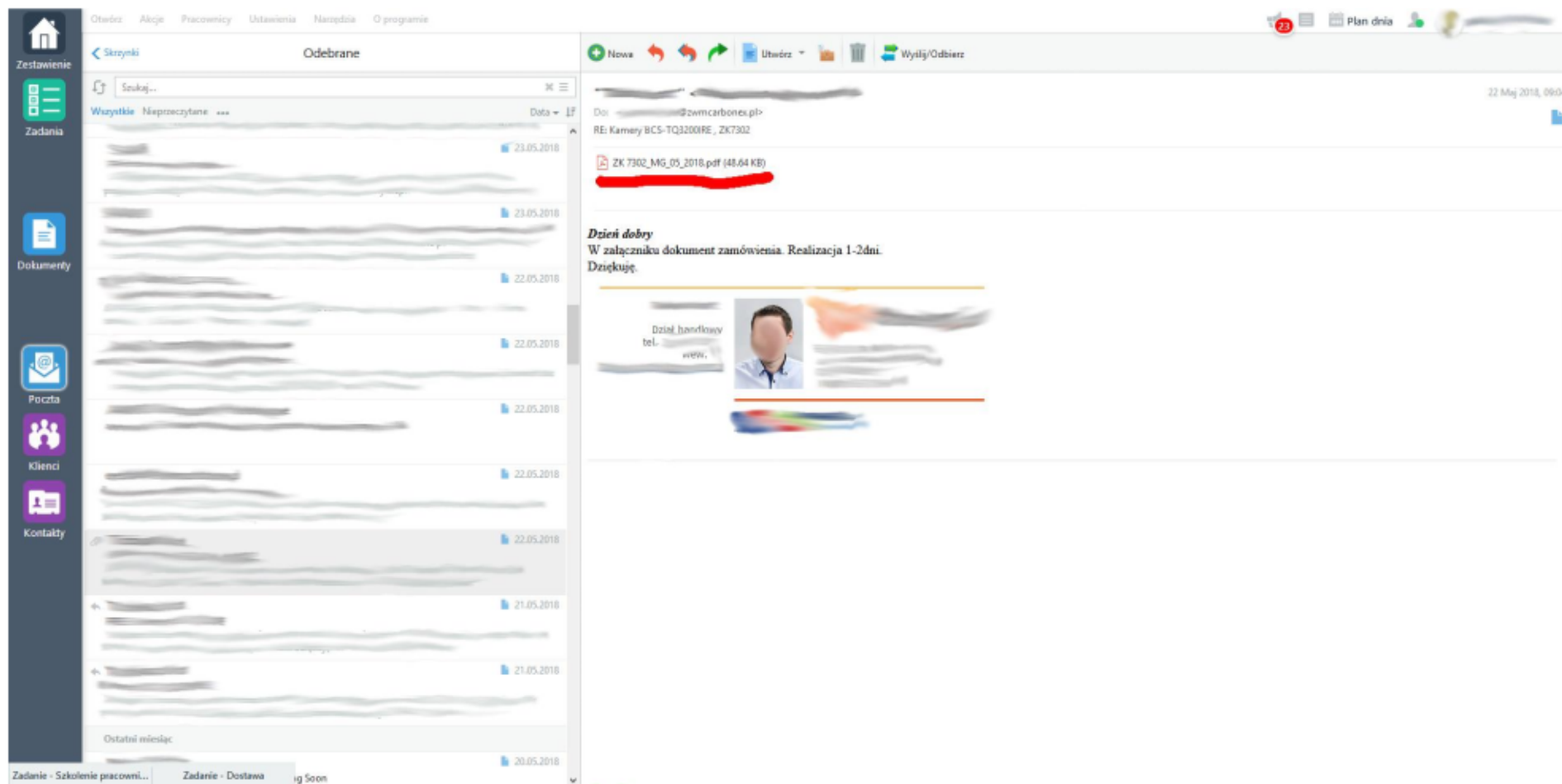
Uwaga!

Mimo poprawnego adresu e-mail nadal istnieje możliwość, że ktoś włamał się na konto pocztowe, bądź komputer nadawcy został zarażony złośliwym oprogramowaniem.

Jeżeli zauważysz coś dziwnego w treści wiadomości (łamana polszczyzna, brak polskich znaków, rażące błędy gramatyczne) lub otrzymasz np.: wiadomość o nadchodzącej przesyłce kurierskiej (której się nie spodziewasz), również zachowaj ostrożność. Najlepiej wszystkie takie sytuacje zgłaszaj natychmiast do działu IT.



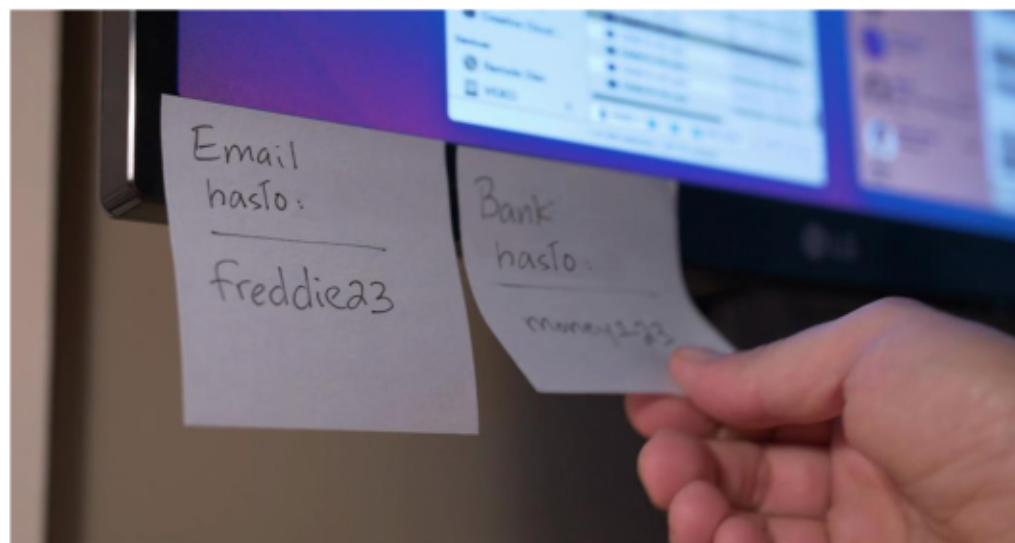
Należy uważać na załączniki przesyłane razem z wiadomością



Pliki, na które należy zwracać szczególną uwagę:

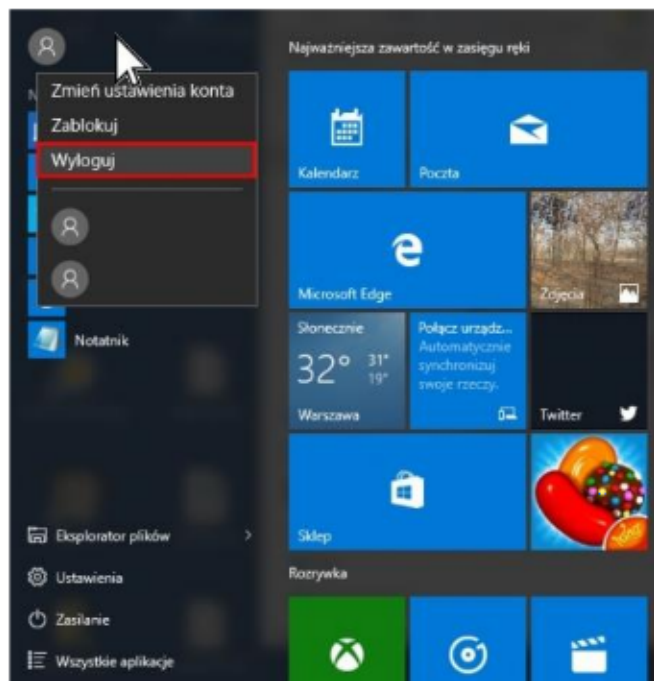
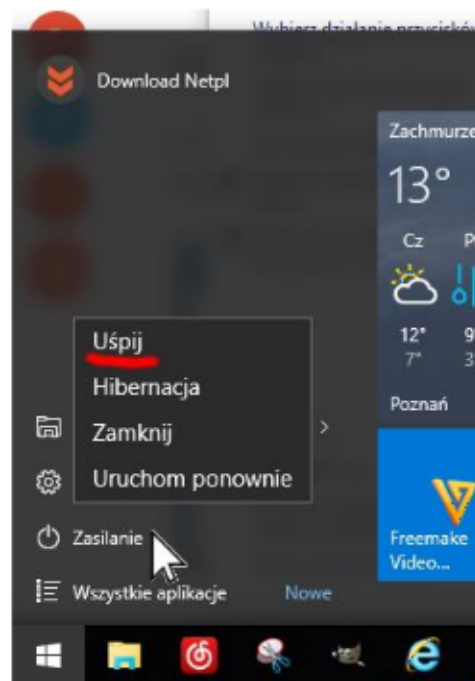
- .pdf
- .zip
- .rar
- .xls
- .xlsx
- .exe
- .bat
- .pif
- .js
- .doc
- .docx
- oraz takie, które przy otwieraniu proszą o uprawnienia administratora komputera, bądź uruchomienie makr tłumacząc to np.: błędnym wyświetlaniem dokumentu

Chronić hasła!



Nie podawaj ich nikomu, nie klej karteczek w okolicach swojego stanowiska pracy. Jeżeli potrzebujesz je gdzieś zapisać nie zostawiaj je na widoku osób postronnych.

Nie odchodź od komputera jeżeli masz
pozostawione otwarte ważne dokumenty,
jesteś zalogowany/a do systemu
zawierającego wrażliwe dane



Za każdym razem wyloguj się z portali i uśpij lub wyloguj się z systemu
Windows!

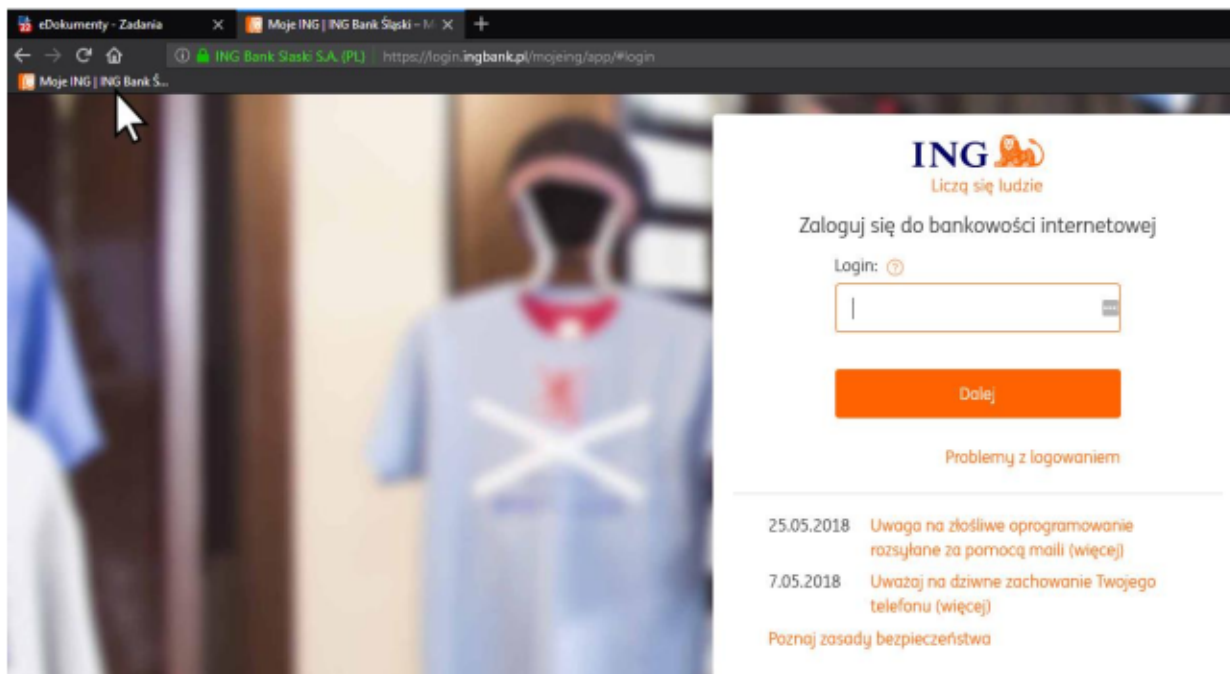
Nie ściągaaj ani nie instaluj samodzielnie żadnego oprogramowania



Poproś o to dział IT ☺



Do banku czy na inne portale zawierające wrażliwe dane, loguj się tylko z wcześniej utworzonych zakładek



Nigdy poprzez link wysłany w wiadomości e-mail!

Czytaj na bieżąco aktualizacje dotyczące bezpieczeństwa



The image shows a screenshot of the ING internet banking login interface. At the top is the ING logo with the tagline 'Liczą się ludzie'. Below it, the text 'Zaloguj się do bankowości internetowej' is displayed. The login section includes a 'Login:' label with an eye icon, a text input field, and an orange 'Dalej' button. A link for 'Problemy z logowaniem' is located below the button. At the bottom, there is a section for security updates with two entries: one dated 25.05.2018 about malicious email software and another dated 7.05.2018 about suspicious phone behavior. Both entries have red wavy lines underlining the titles. A link to 'Poznaj zasady bezpieczeństwa' is at the very bottom.

ING Liczą się ludzie

Zaloguj się do bankowości internetowej

Login: 

[Dalej](#)

[Problemy z logowaniem](#)

25.05.2018 Uwaga na złośliwe oprogramowanie rozsyłane za pomocą maili (więcej)

7.05.2018 Uważaj na dziwne zachowanie Twojego telefonu (więcej)

[Poznaj zasady bezpieczeństwa](#)

Nie ufaj nikomu!



Nawet jeżeli wiadomość e-mail zostanie wysłana od zaufanej osoby, przed odesłaniem poufnych informacji upewnij się np.: telefonicznie czy wiadomość jest autentyczna.

Pamiętaj! Dział IT nie rozsyła linków zachęcających do zmiany hasła!

Hasło
Zmień swoje hasło lub odzyskaj bieżące.

Obecne hasło

[Nie pamiętasz hasła?](#)

Nowe hasło

Potwierdź hasło

[Zapisz zmiany](#)

Jeżeli otrzymasz tego typu wiadomość, poinformuj o tym dział IT



Jeżeli mimo wszystko doszło do niebezpiecznej sytuacji...

...poinformuj o tym natychmiast dział IT!

