TARNÓW
Polski biegun ciepła

Jak się zabezpieczyć przed Cyberatakiem ?

- Nie klikaj w linki w treści emaila lub sms jeżeli nie posiadasz **100% pewności** o źródle informacji
- Uważaj na fałszywe emaile z załącznikami typu „faktura” szczególnie wymagające podania **hasła**.
- Wgrywaj **aktualizacje** systemu **Windows 10**
- Pilnuj **aktualności** programu antywirusowego
- **Aktualizuj przeglądarki**
- Ogranicz zapisywanie **haseł – unikalność,** powtarzalność
- Nie przepinaj **laptopa** pomiędzy sieciami **wifi** – kablowa RJ45

Tarnów, czerwiec 2022 r.

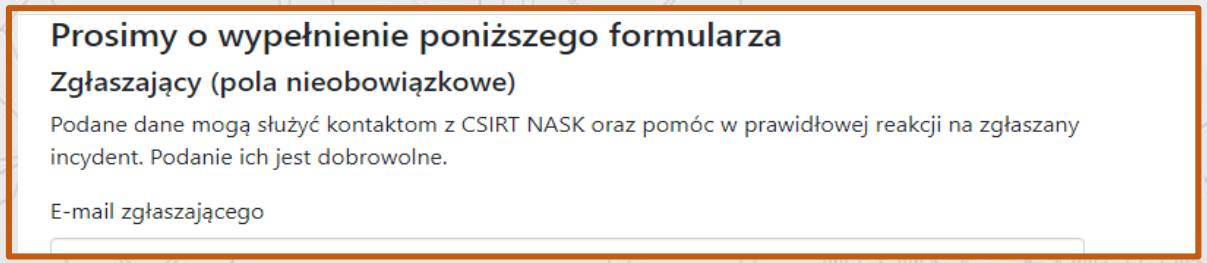
Fałszywy email


Subject: Pilne

Musimy wykonać przelew w wysokości 40 735,75 EUR. czy możemy to zrobić dzisiaj?

Pozdrowienia

Zgłaszanie incydentu: https://incydent.cert.pl


Prosimy o wypełnienie poniższego formularza

Zgłaszający (pola nieobowiązkowe)

Podane dane mogą służyć kontaktom z CSIRT NASK oraz pomóc w prawidłowej reakcji na zgłaszany incydent. Podanie ich jest dobrowolne.

E-mail zgłaszającego

Otrzymany przez Państwa **mail jest tak zwanym spear phishingiem, czyli próbą podszycia się pod konkretną osobę z wewnątrz organizacji** z prośbą o stan konta.
W dalszym etapie konwersacji dochodzi do próby wyłudzenia znacznej kwoty poprzez "pilny" przelew.
Niestety taki rodzaj ataku jest łatwy w przygotowaniu, ponieważ prawie wszystkie potrzebne dane (np. domena, sposób konstruowania adresu mailowego z nazwiska i imienia, dane pracowników wyższego szczebla) są ogólnodostępne. Często też pracownicy udostępniają informację o swoim stanowisku na mediach społecznościowych.

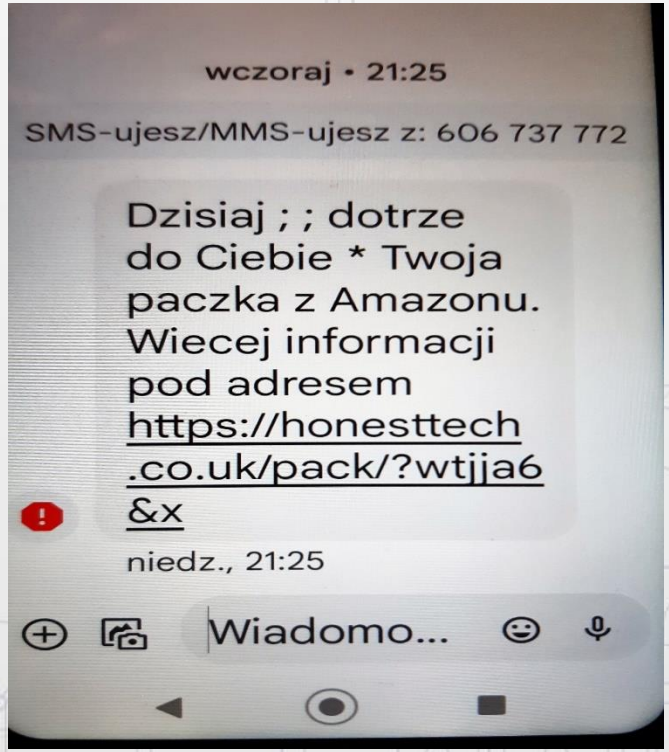
Zablokowanie takich maili jest praktycznie niemożliwe, dlatego najważniejsze jest informowanie i edukowanie pracowników o możliwych próbach wyłudzeń.

W razie dodatkowych pytań pozostajemy do dyspozycji.
Z poważaniem CERT Polska

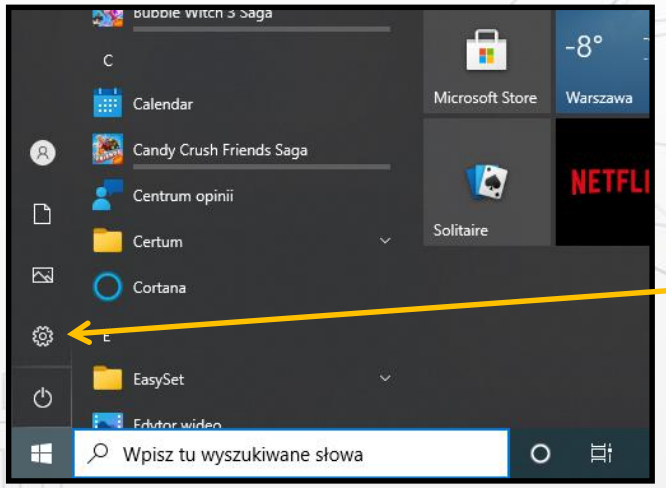
Przejmowanie hosta podczas zdalnej lekcji

Wyświetlany kontakt z książki telefonicznej

Fałszywa informacja o przesyłce



Kontroluj aktualizacje Windows 10 (menu Start)

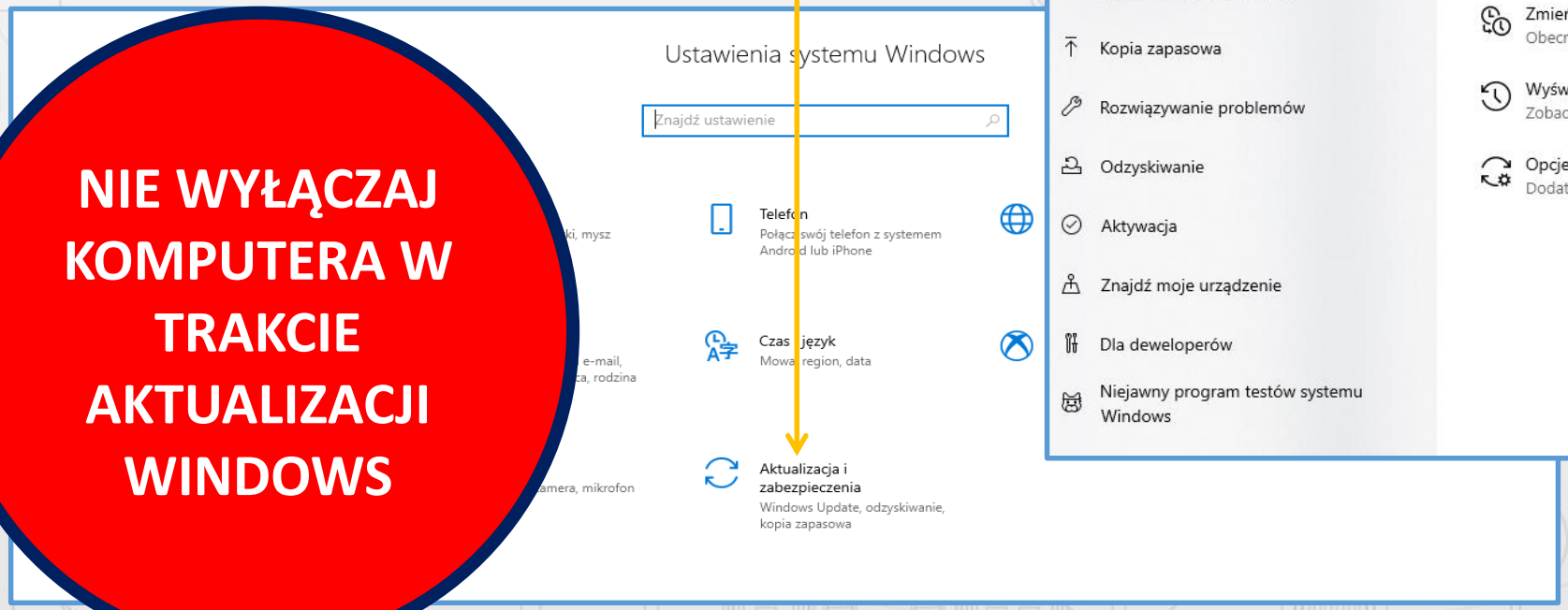


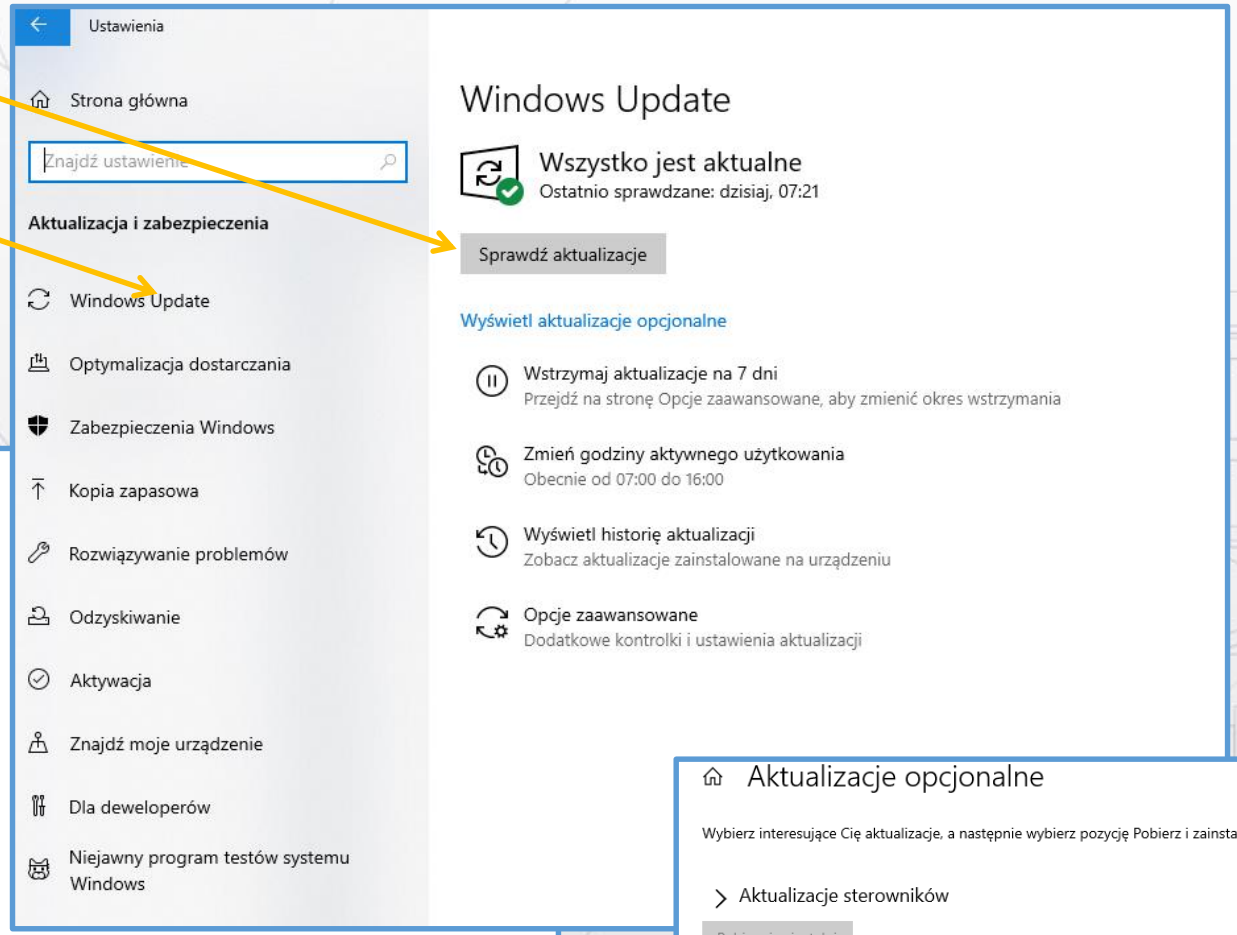
1

2

3

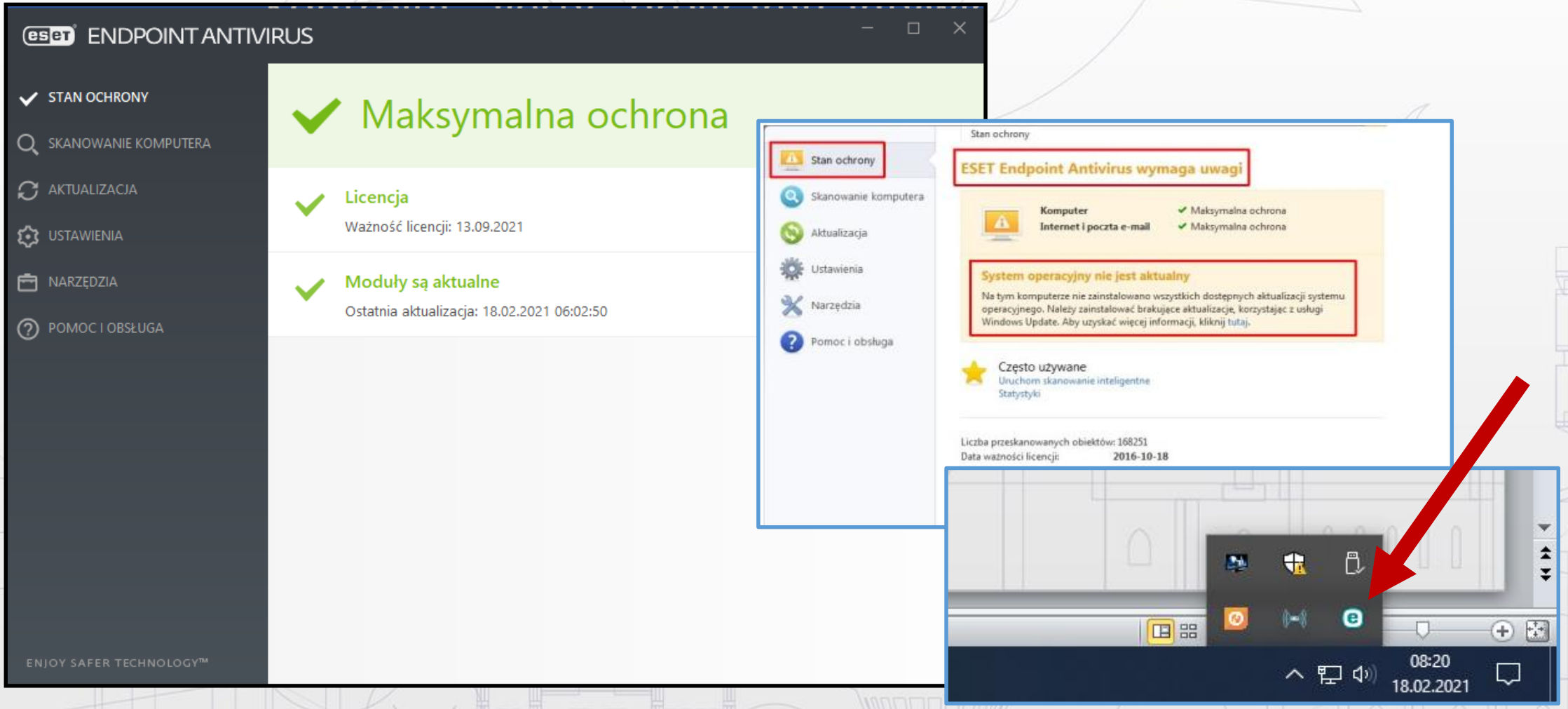
4





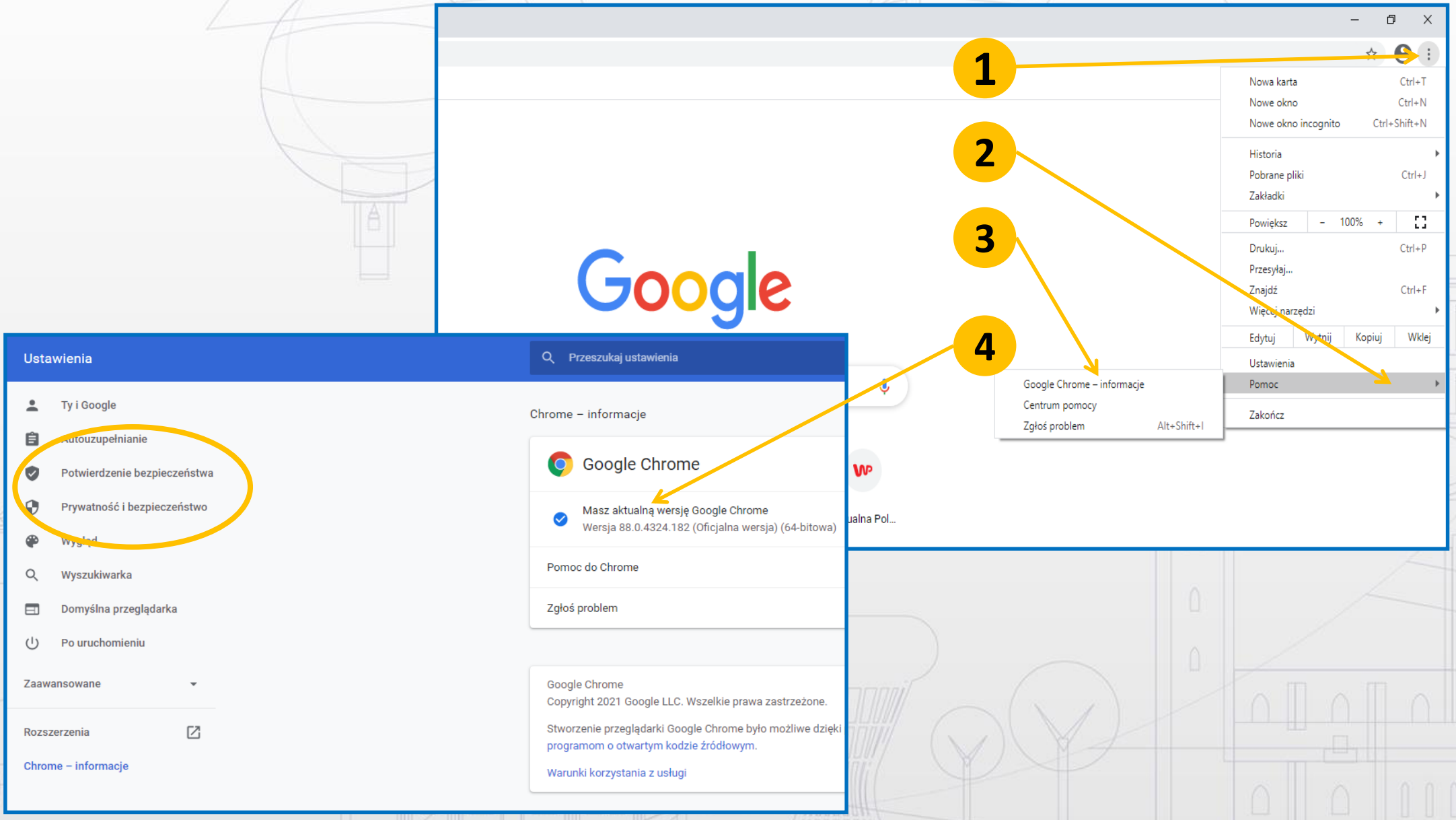
NIE WYŁĄCZAJ KOMPUTERA W TRAKCIE AKTUALIZACJI WINDOWS

Kontroluj „alerty” programu antywirusowego

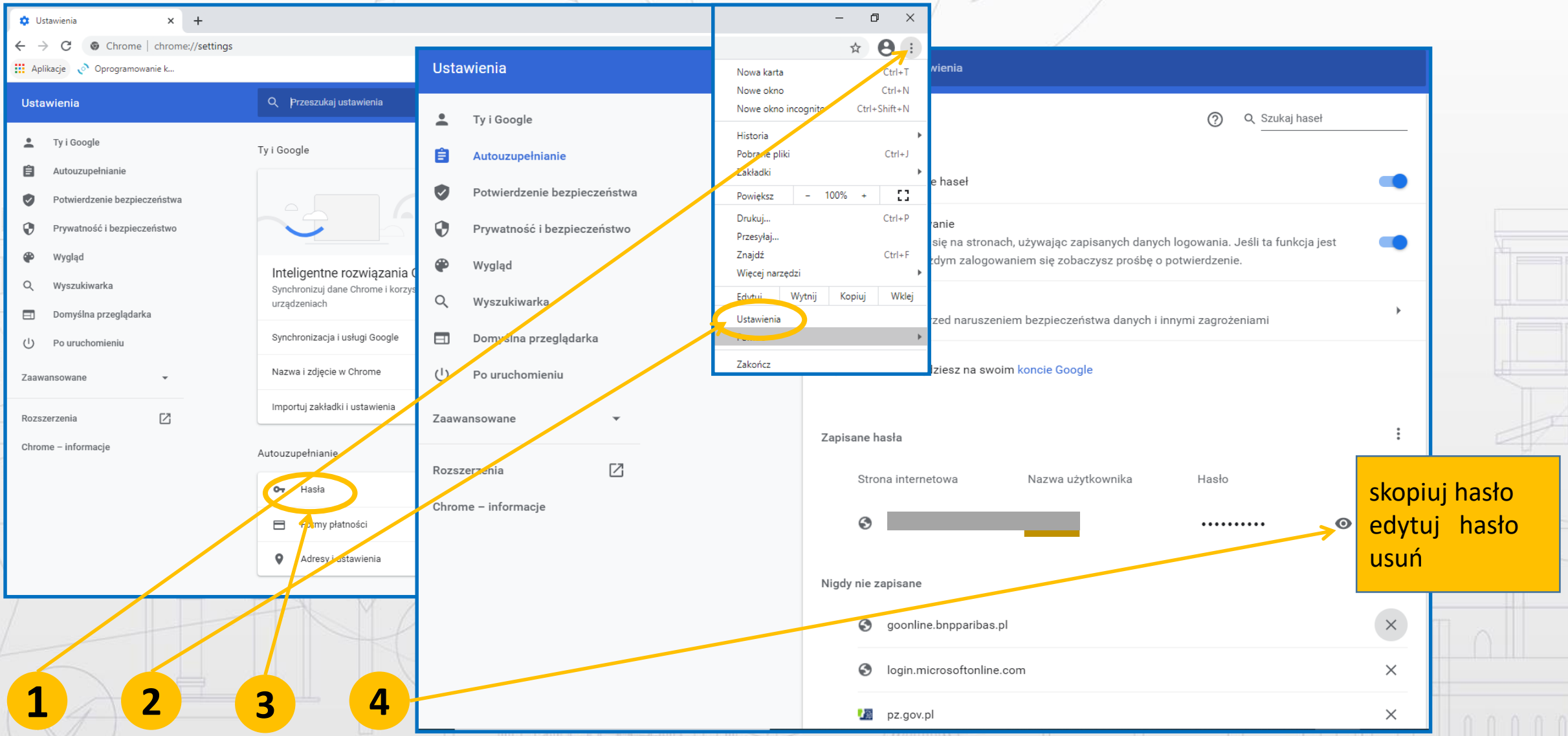


nie instaluj kilku programów antywirusowych, część stron/programów automatycznie proponuje instalację

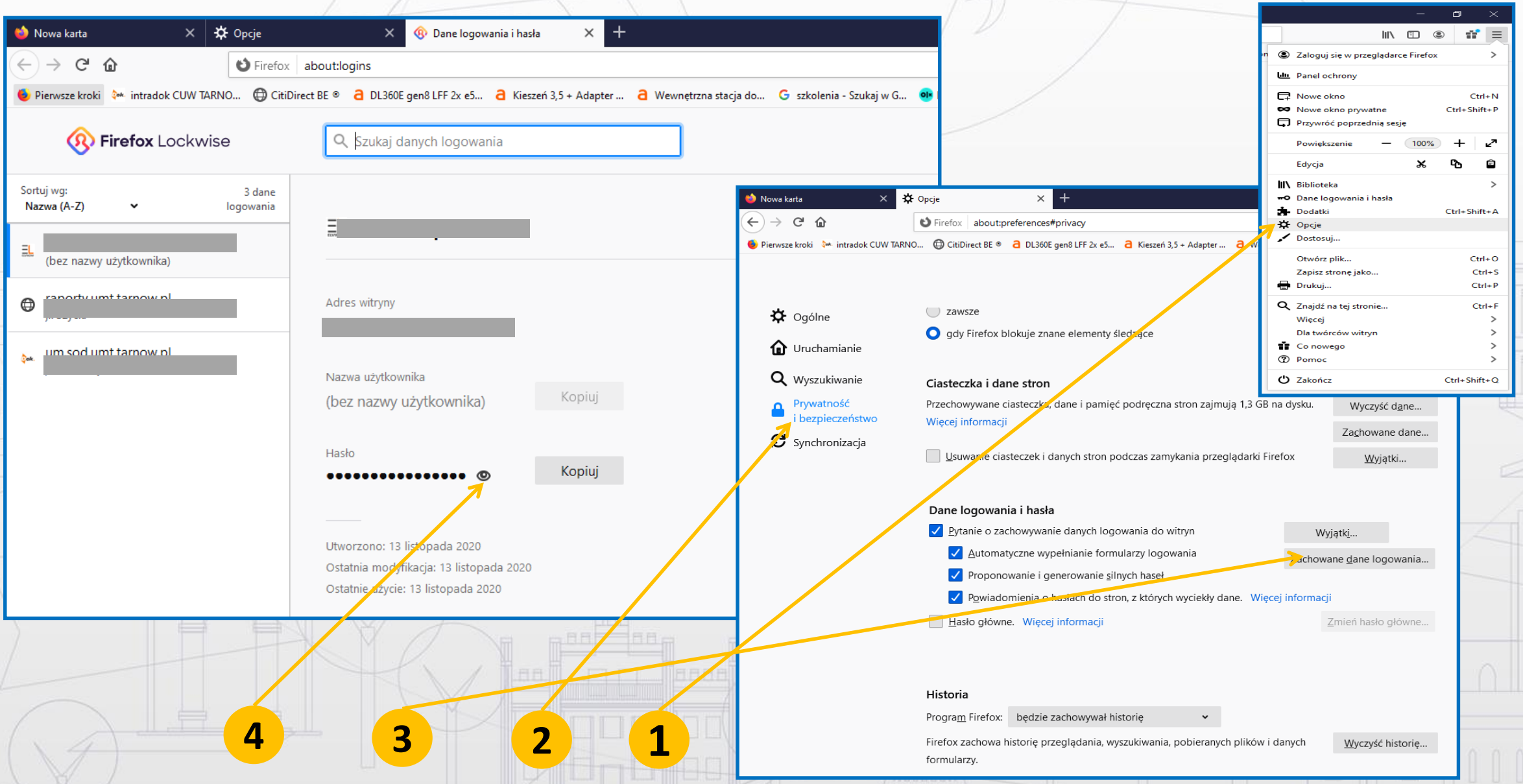
Aktualizuj przeglądarki internetowe (Google)



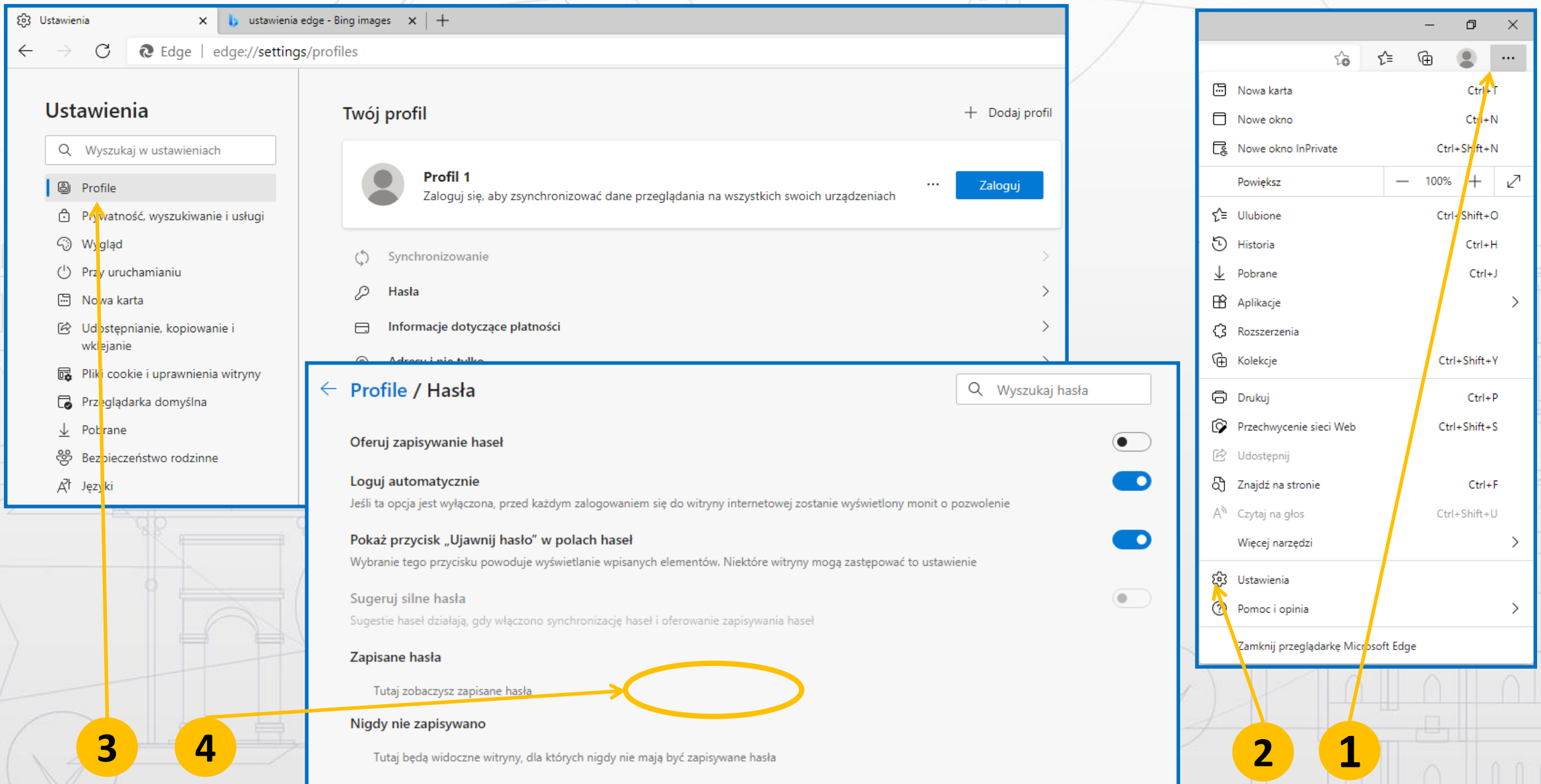
Miej świadomość- w zakładce „ustawienia” zapisane hasła (Google)



Kontroluj w zakładce „ustawienia” zapisane hasła (Mozilla)



Kontroluj w zakładce „ustawienia” zapisane hasła (Edge)



JAK USTRZEC SIĘ PRZED RANSOMWARE ?

- **Pamiętaj,** że na komputerze mogą być zapisywane hasła;
- Wykonuj regularnie **kopię zapasową** istotnych danych. Zastanów się czy podczas komputera stracisz istotne informacje. **Dane lokalnego nie są kopiowane;**

Poprawa bezpieczeństwa danych lokalnych i pracy grupowej „Cyfrowa Gmina”

- Miej świadomość, że korzystając **z laptopa przyłączasz się do różnych (w tym niezabezpieczonych) sieci WIFI**. Wtórne wpięcie zainfekowanego laptopa do sieci UM Tarnowa (skrętką) może powodować zagrożenie dla całego urzędu;
- Na bieżąco **aktualizuj** system operacyjny **Windows ;**
- **Aktualizuj** używane **przeglądarki;**
- **Używaj aktualnego oprogramowania antywirusowego** na serwerze poczty oraz stacjach roboczych.

Co jeżeli komputer wykazuje oznaki cyberataku ?

- **Jak najszybciej odizoluj zarażone maszyny od reszty sieci** – odłącz je od wszelkich połączeń sieciowych (**przewodowych i bezprzewodowych**) oraz urządzeń do przechowywania plików (**dyski przenośne i podobne**).
- **Zrób zdjęcie ekranu z wyświetlanym komunikatem** lub „dziwnym” wyglądem ekranu. Upewnij się, że wszystkie informacje są na zdjęciu czytelne.
- **Skontaktuj się z jednostką wspierającą** i działaj wg wskazówek.
- W celu zminimalizowania strat (np. zaszyfrowania wszystkich plików) **wyłącz komputer.**
- Poinformuj przełożonego i IOD.
- Po usunięciu skutków ataku **ustal, w jaki sposób do niego doszło** oraz podejmij działania zapobiegawcze, by uniemożliwić powtórzenie się sytuacji.

Jak się zabezpieczyć przed Cyberatakiem ?

- Nie klikaj w linki w treści emaila lub sms jeżeli nie posiadasz **100% pewności** o źródle informacji
- Uważaj na fałszywe emaile z załącznikami typu „faktura” szczególnie wymagające podania **hasła**.
- Wgrywaj **aktualizacje** systemu **Windows 10**
- Pilnuj **aktualności** programu antywirusowego
- **Aktualizuj przeglądarki**
- Ogranicz zapisywanie **haseł – unikalność,** powtarzalność
- Nie przepinaj **laptopa** pomiędzy sieciami **wifi** – kablowa RJ45

TERAZ JUŻ WIEM