TARNÓW
Polski biegun ciepła

ŚWIADOMOŚĆ ZAGROŻEŃ CYWILIZACYJNYCH

- **BEZPIECZEŃSTWO**
- SAMOKONTROLA
- OSTROŻNOŚĆ

CUW UM Tarnowa, czerwiec 2022 r.

TARNÓW
Polski biegun ciepła

Czy jesteśmy przygotowani do dalszych zmian ?

CUW – rozwiązanie hybrydowe, przepis na Smart Samorząd”

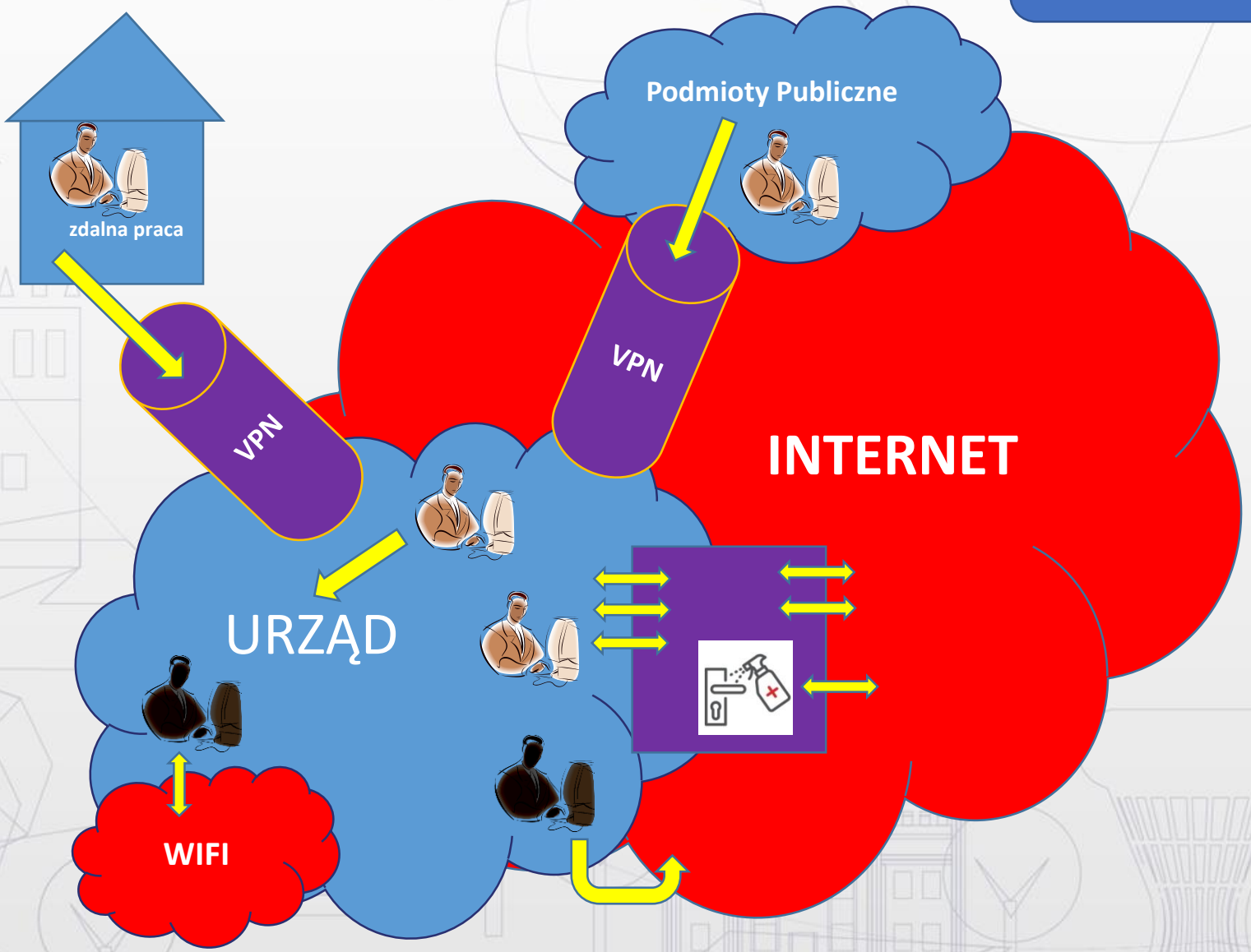
START

- **Infrastruktura**
- Zasoby ludzkie – specjaliści
- **Organizacja bezpieczeństwa**
- Budowanie kompetencji urzędników
- **Wdrożenie nowoczesnych rozwiązań systemowych**
- Zarządzanie, utrzymanie i rozwój systemów
- HelpDesk, szkolenia
- Propagowanie modelowych rozwiązań

META

TARNÓW
Polski biegun ciepła

BEZPIECZEŃSTWO – działania CUW



- Świadomość
- Odpowiedzialność
- Ostrożność
- Kopie danych
- Wsparcie
- Kontrola i audyty

Ransomware

ransom „okup” **software „oprogramowanie”**

szyfrowanie danych celem uzyskania okupu

JAK USTRZEC SIĘ PRZED RANSOMWARE ?

- **Stała edukacja** użytkowników. Nawet najlepsze techniczne zabezpieczenia nie pomogą, jeśli użytkownicy nie będą przestrzegać podstawowych zasad bezpieczeństwa.
- Wykonuj regularnie **kopię zapasową** istotnych danych. Zadbaj o to, by co najmniej jedna kopia zapasowa była przechowywana na odizolowanym systemie, niedostępnym z maszyn, których kopie przechowuje. **Dane z dysku lokalnego nie są kopiowane przez IT.**
- Zadbaj o odpowiednią architekturę sieci. Wyodrębnij odpowiednie segmenty, zwróć szczególną uwagę na to, jakie usługi dostępne są pomiędzy poszczególnymi maszynami oraz z internetu.
- Na bieżąco **aktualizuj system operacyjny** oraz oprogramowanie.
- **Używaj aktualnego oprogramowania antywirusowego** na serwerze poczty oraz stacjach roboczych.

W PRZYPADKU ATAKU RANSOMWARE

- **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** przez ransomware. Upewnij się, że wszystkie informacje są na zdjęciu czytelne. Przegraj plik z notatką okupu (ransom note) i przykładowe zaszyfrowane pliki na czysty przenośny nośnik danych (np. pendrive) – będą jeszcze potrzebne.
- W celu zminimalizowania strat (zaszyfrowania wszystkich plików) **wyłącz komputer.**
- **IT rozważy zgłoszenie incydentu do CERT Polska** – najlepiej zaraz po wykryciu zdarzenia. W tym celu skorzysta z https://incydent.cert.pl oraz podejmie działania zabezpieczające i ewentualna próbę odszyfrowania danych.
- **Jeśli dysponujesz kopią zapasową, przygotuj nowy komputer, sformatuj dysk, zainstaluj system od nowa i przywróć dane z backupu.**
- Po usunięciu skutków ataku **ustal, w jaki sposób do niego doszło** oraz podejmij działania zapobiegawcze, by uniemożliwić powtórzenie się sytuacji (edukacja użytkowników, zabezpieczenia fizyczne, aktualizacja oprogramowania).

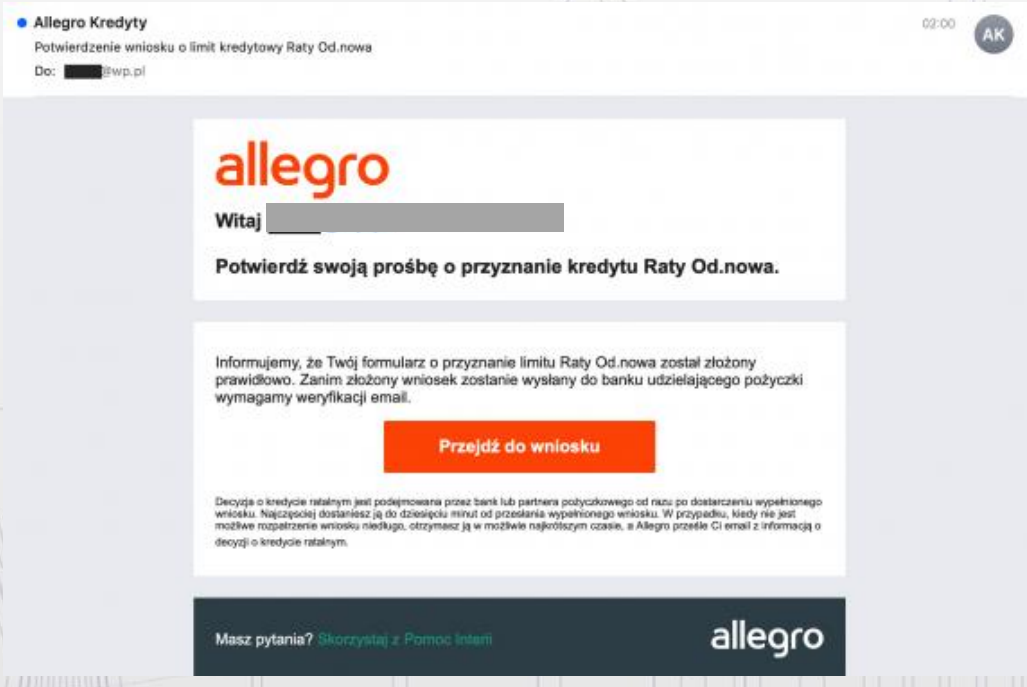
W PRZYPADKU ATAKU RANSOMWARE

Źródło	Przyczyny			
	bezpośrednia	pośrednia		
poprzez e-maila	niskie zabezpieczenia na serwerze	brak oprogramowania antywirusowego na komputerze	jeszcze nie wykrywalny wirus	ignorowanie ostrzeżeń systemowych przez użytkownika
poprzez FTP	środowisko niezbyt bezpieczne			
poprzez pendrive	pendrive używany w kilku komputerach min. (w zawirusowanym)			
poprzez podłączenie do WIFI	sieć niezabezpieczona, łączona jest z siecią wewnętrzną urzędu			

Skutki		Jak przeciwdziałać ?					
zaszyfrowanie danych na komputerze	zaszyfrowanie danych na kilku komputerach (w przypadku udostępnianych folderów)	Aktualizować oprogramowanie serwera, analizować zagrożenia (logi), kupować wsparcie na urządzenia i systemy bezpieczeństwa.	PILNOWA: aby oprogramowanie Windows (System) i NOD 32 ESET były aktualne	nie otwierać e-maili nieoczekiwanych - ostrożność co do linków i poleceń	podnoszenie świadomości, ostrzeżenia IOD	wykonywanie kopii okresowo na taśmach	deponowanie dodatkowych kopii danych na izolowanych serwerach danych

UWAŻAJ NA PHISHING

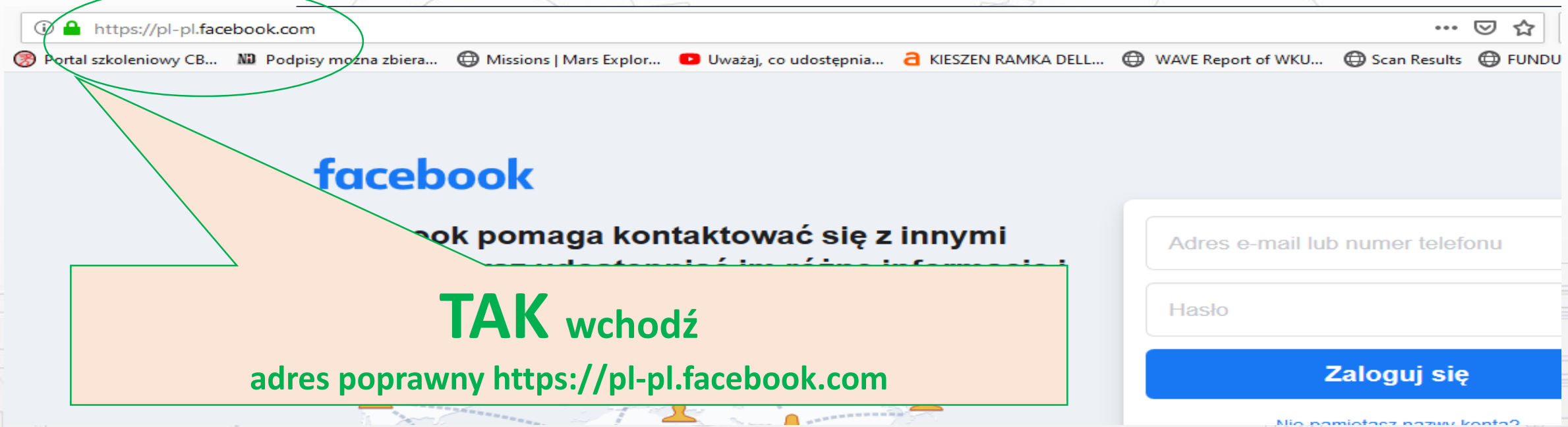
Metoda oszustwa, w której **przestępca podszywa się pod inną osobę lub instytucję, w celu wyłudzenia** określonych informacji (np. danych logowania, szczegółów karty kredytowej) lub nakłonienia ofiary do określonych działań.



Zagrożenia – fałszywy e-mail

Czy to jest bezpieczna strona internetowa ? https://pl-facebook.pl

Zagrożenia – fałszywy e-mail



TAK wchodź

adres poprawny https://pl-pl.facebook.com

NIE wchodź

Zagrożenia – fałszywy e-mail

Podszywanie się pod pracowników banku

Wiadomość dotycząca bezpieczeństwa. Twoje konto mBank zostało tymczasowo zablokowane. Odebrane ×

mBank przez s7.jupe.pl 14:15 (7 minut temu)

do mnie

Szanowny kliencie,

mBank

Twój dostęp do serwisu transakcyjnego mBank Online został tymczasowo zablokowany ze względów bezpieczeństwa.

Wykryliśmy podejrzane działania związane z Twoim kontem bankowym.

Aby uzyskać więcej informacji oraz odblokować dostęp online, należy przejść na stronę mBanku https://online.mbank.pl/pl/odblokuj i zweryfikować swoje dane.

Pozdrawiamy,
Zespół mBanku

Film źródło TouTube: https://www.youtube.com/watch?v=3C0piwRqt-o

Zagrożenia – fałszywy e-mail

Od: [redacted]
Do:
DW:
Temat: FW: ⊖ Potwierdź szczegóły dostępu aby uniknąć zawieszenia aktywności e-mail ⊖

From: Webmail Bezpieczeństwo <contact@notifysending.com>
Sent: Wednesday, December 4, 2019 8:47 AM
To: [redacted]rnow.pl
Subject: ⊖ Potwierdź szczegóły dostępu aby uniknąć zawieszenia aktywności e-mail ⊖

NIE POTWIERDZAJ !

roundcube
Polska Webmail Software

Drogi Klience umt.tarnow.pl,

Twój e-mail zostanie zawieszony z powodu kilku nieudanych prób logowania z urządzenia opisanego poniżej.

Potwierdź swoją tożsamość, naciskając przycisk poniżej. Następnie będziesz mógł wznowić swoją aktywność. Jeśli konto nie zostanie aktywowane w ciągu 48 godzin, nie będzie można się komunikować.

Powód:

Data: 2019-12-04

Powód: Logowanie nie powiodło się

Potwierdzać

SPAM – „ MIELONKA” - NIECHCIANA POCZTA jak się chronić ?

- Oprogramowanie antywirusowe
- Świadome otwieranie poczty
- Filtry antyspamowe (zarządza IT)
- Adres lub domena nadawcy znajduje się na jednej z aktualizowanych codziennie list adresów wysyłających SPAM - globalne RBL (Realtime blacklist)
- Klasyfikatory , analizatory treści (zabezpiecza IT) - treść wiadomości zawiera słowa sklasyfikowane jako SPAM lub ma mały współczynnik tekstu do grafiki - w tym przypadku wszystko zależy, jak potraktują nas filtry; wysłana przez nas wiadomość może trafić do SPAMu lub nie

paradoks administracji 700 zł (opłata za bezpieczeństwo)

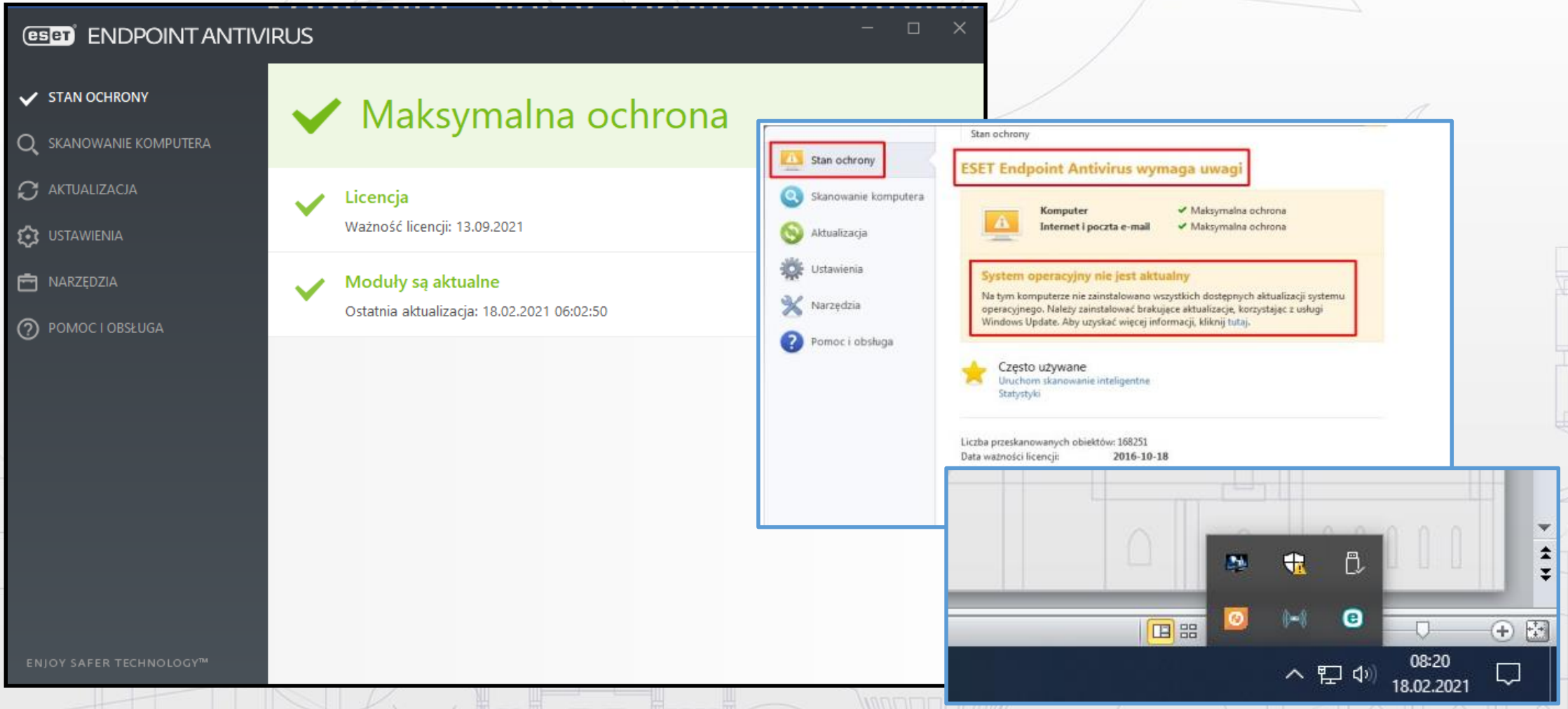
Kontroluj komputer - 10 przykazań

1. Będąc na stanowisku pracy nie używaj WIFI w laptopie podłączony do sieci internetowej.
2. Nie korzystaj na stanowisku z internetu smartfona.
3. Ogranicz korzystanie z Pendrive.
4. W sieci zawsze kieruj się zasadą ograniczonego zaufania i ćwicz swoją asertywność.
5. Czytaj regulaminy, komunikaty itp. – możesz tam znaleźć wiele ważnych informacji.
6. Unikaj usług ułatwiających Ci życie kosztem udostępniania Twoich danych,
7. Nie udostępniaj nikomu swoich haseł i zadbaj o ich siłę, unikalność i odpowiednie zabezpieczenie.

Kontroluj komputer - 13 przykazań

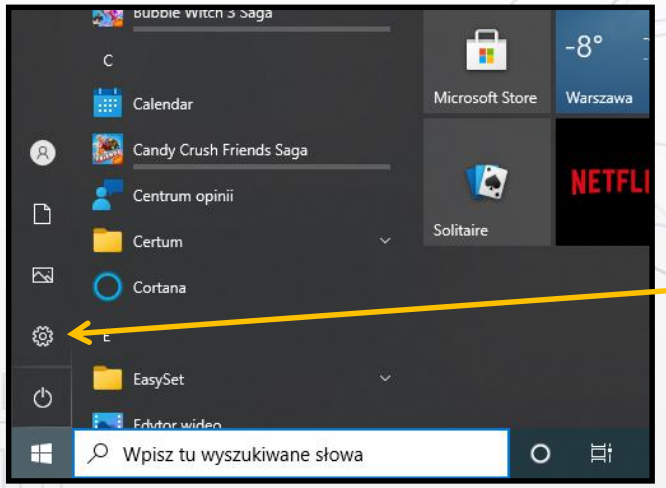
8. Nie udostępniaj nikomu swoich haseł i zadbaj o ich siłę, unikalność i odpowiednie zabezpieczenie.
9. Nie używaj w haśle swojego imienia i nazwiska ani związanych z Tobą informacji, np. daty urodzin, nr PESEL
10. Pamiętaj o zmianie hasła co pewien czas.
11. Nigdy nie używaj swojego imienia, identyfikatorów ani nicków jako hasła (nawet ze zmianą wielkości liter, pisane wspak). Nie używaj samych cyfr ani prostych pojedynczych słów.
12. Używaj wielkich liter, znaków specjalnych (.,*#@!^& etc.) i cyfr (najlepiej równocześnie).
13. Nie ignoruj informacji o wyciekach danych z serwisów, z których korzystasz. W razie wątpliwości zmień hasło.

Kontroluj „alerty” programu antywirusowego



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

Kontroluj aktualizacje Windows 10 (menu Start)

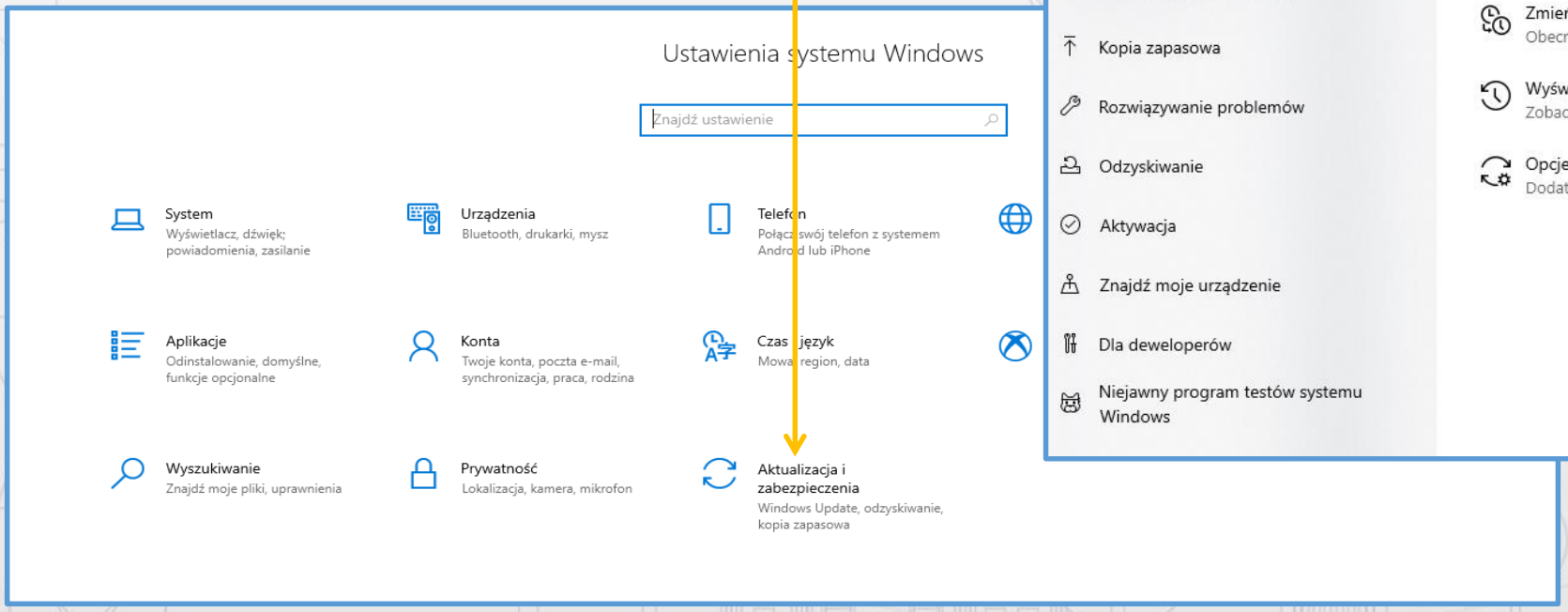


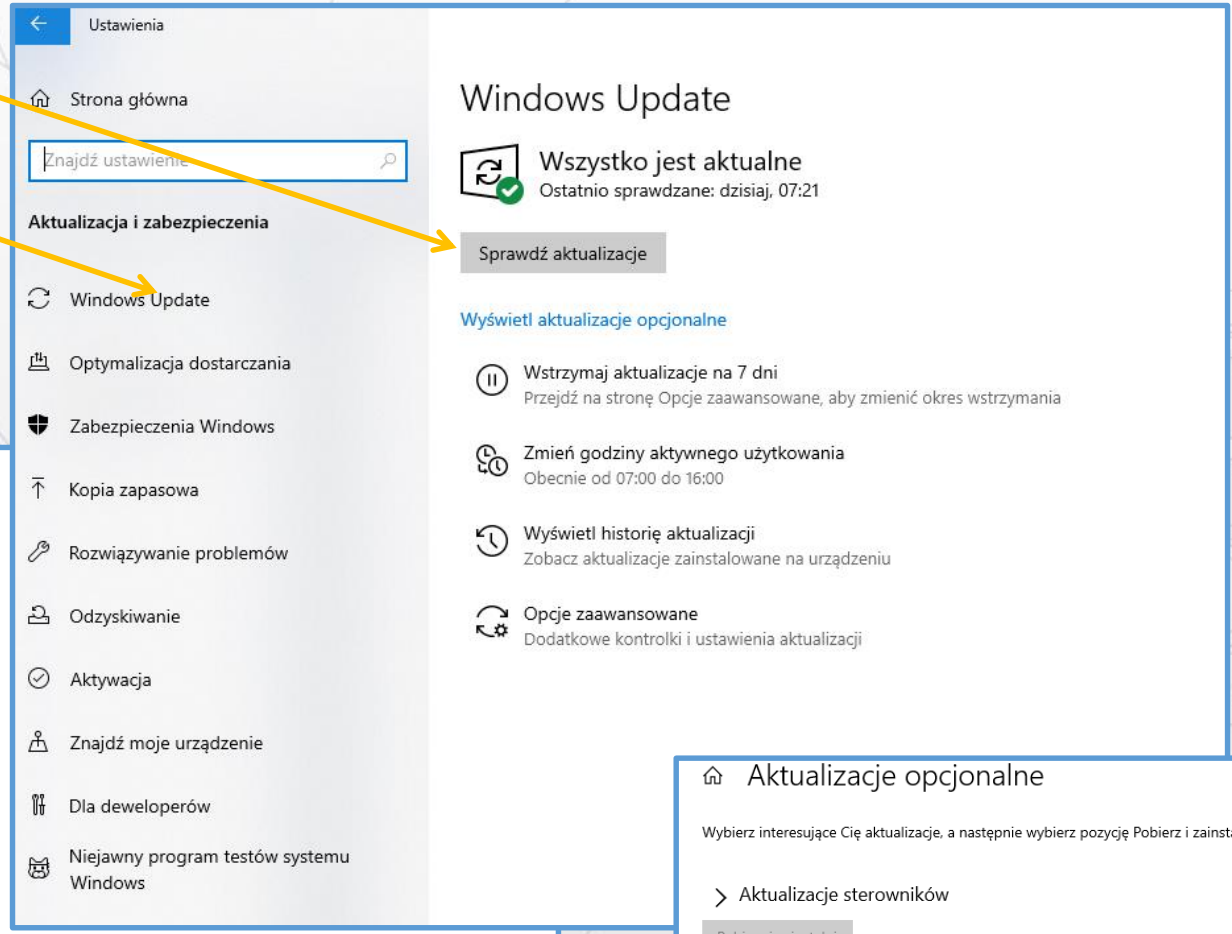
1

2

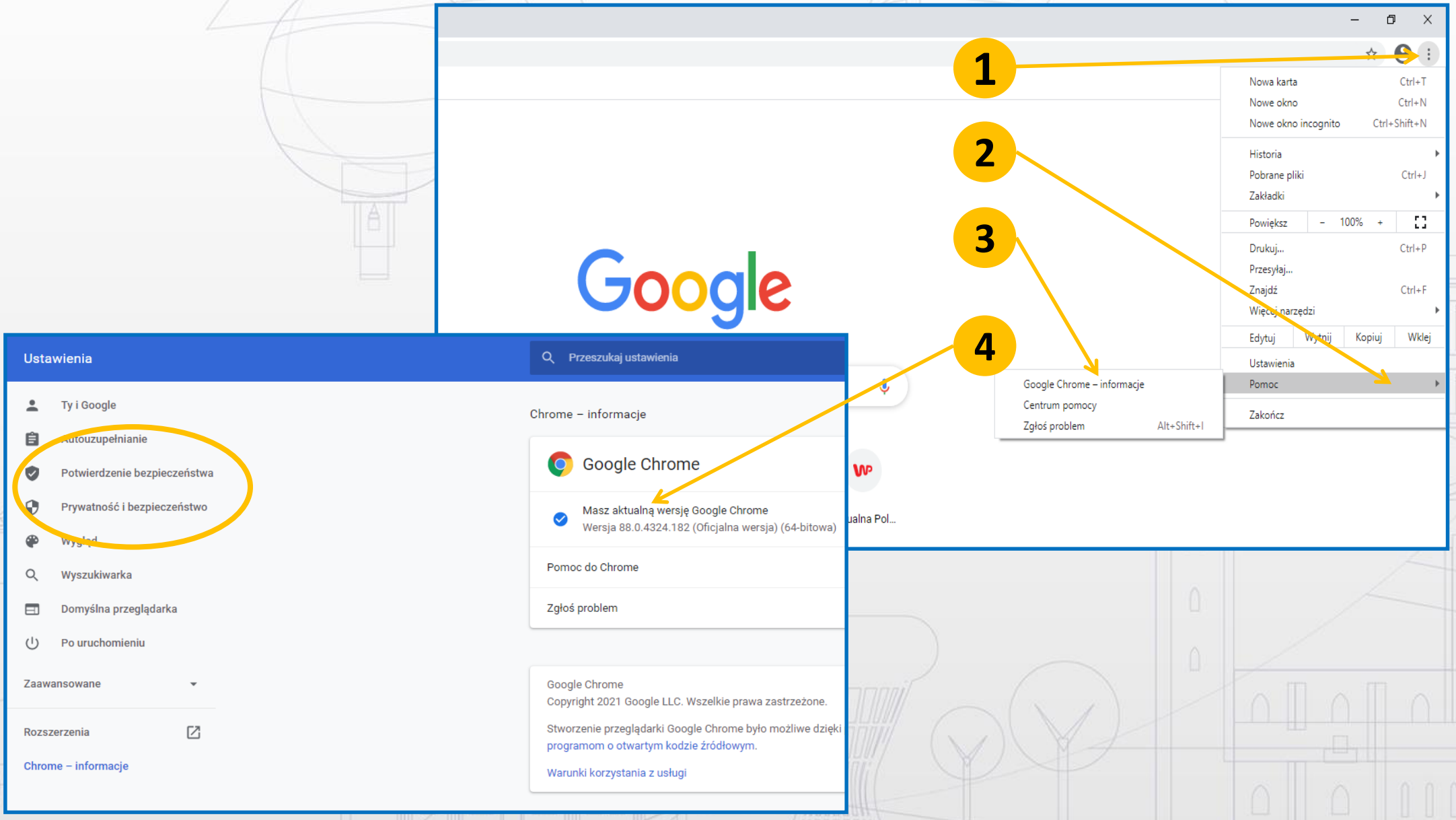
3

4

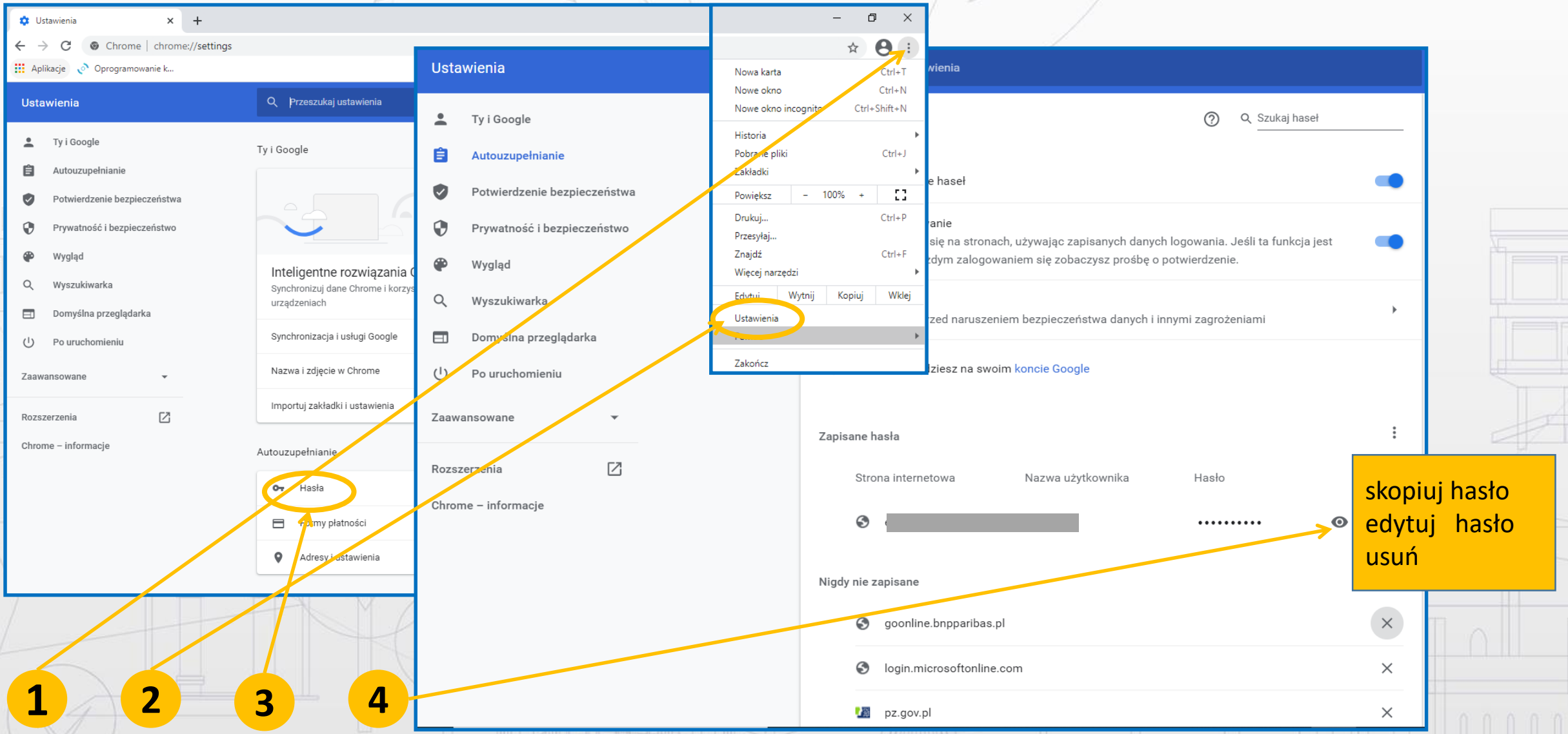




Aktualizuj przeglądarki internetowe (Google)



Kontroluj w zakładce „ustawienia” zapisane hasła (Google)



Dziękuję za uwagę

Janusz Różycki - Inspektor Ochrony Danych Urzędu Miasta Tarnowa, iod@umt.tarnow.pl