

## 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 **hasel** – **unikalność**, powtarzalność
- Nie przepinaj **laptopa** pomiędzy sieciami **wifi** – kablowa RJ45

## 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.

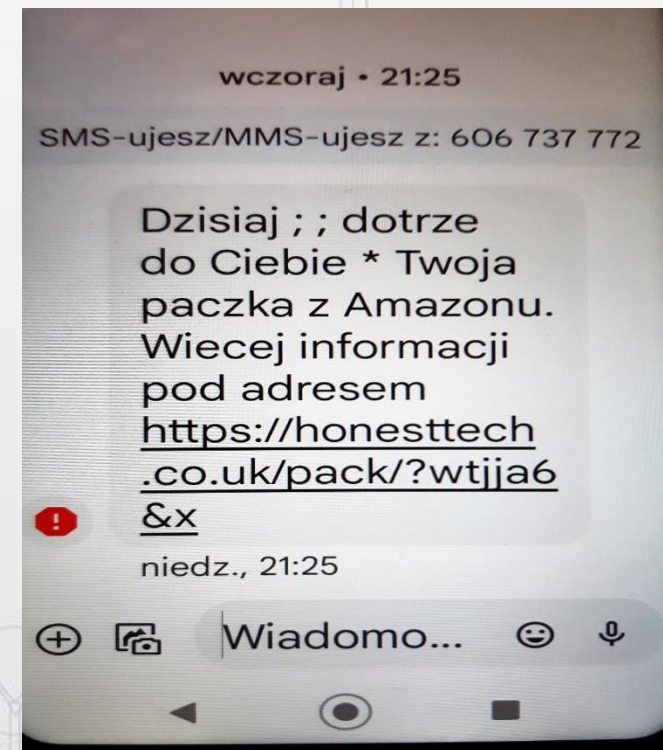
Zablokowanie takich maili jest praktycznie niemożliwe, dlatego najważniejsze jest informowanie i edukowanie pracowników o możliwych próbach wyłudzeń.

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

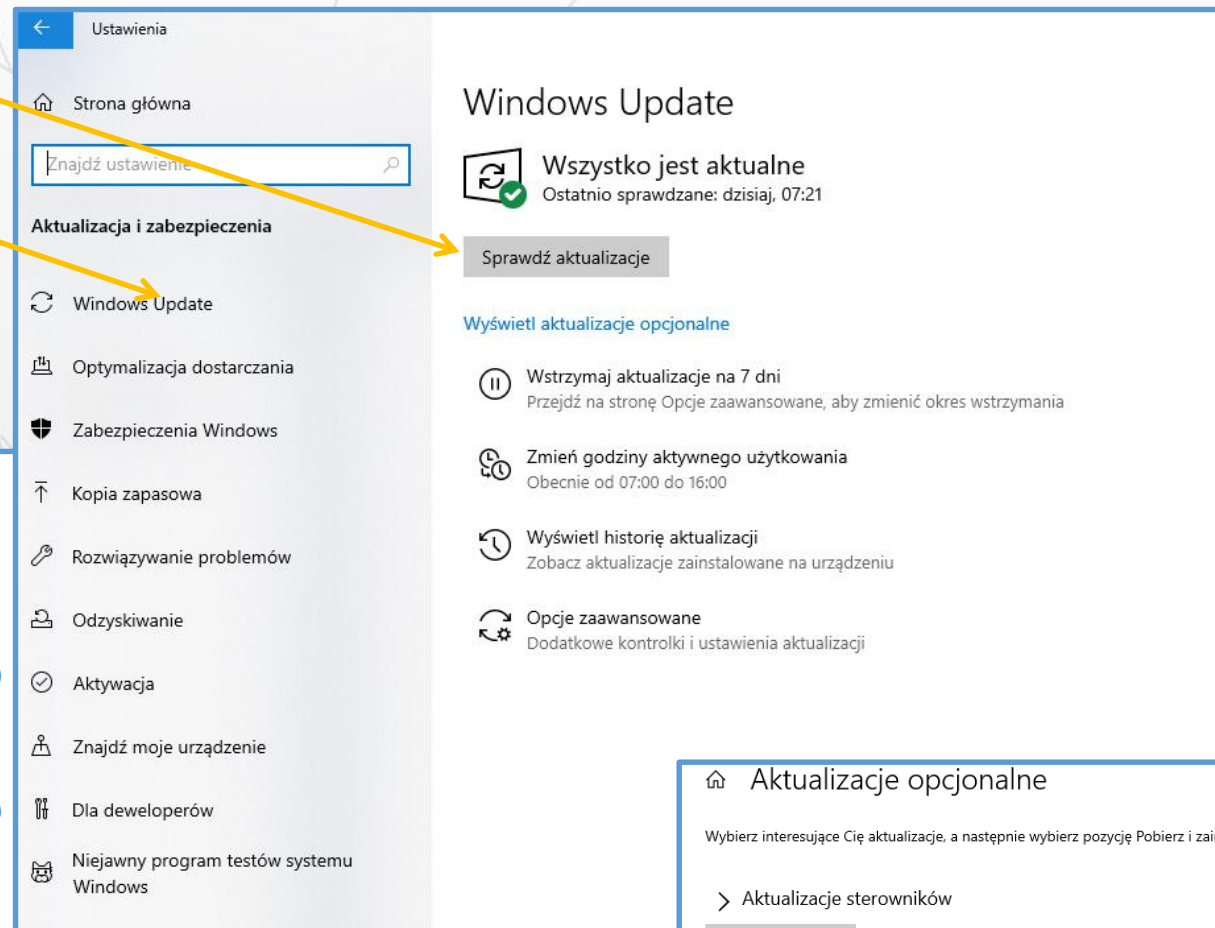
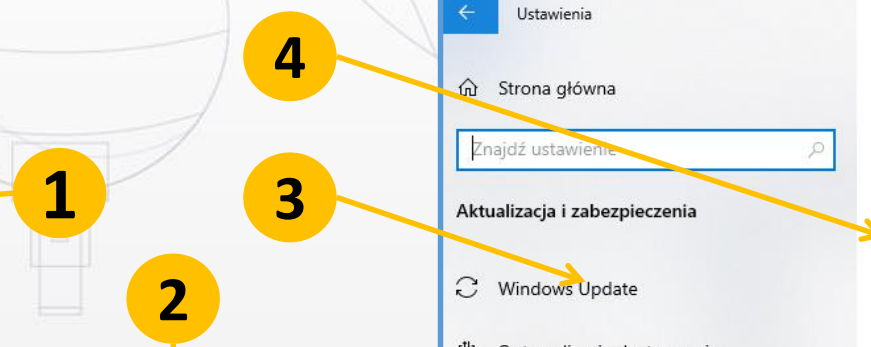
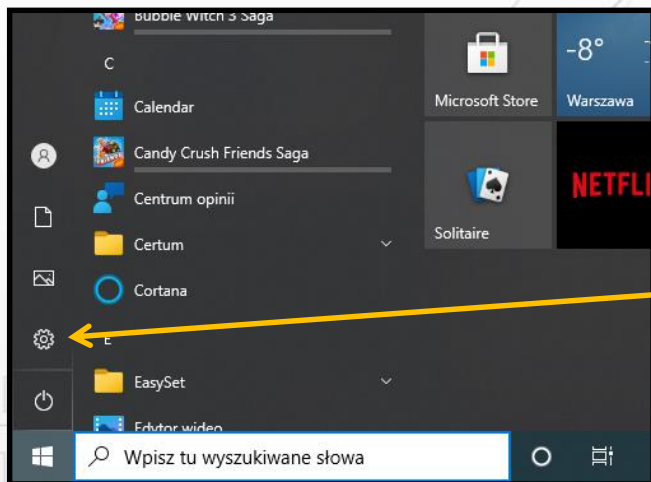
Przejmowanie hosta  
podczas zdalnej  
lekcji

Wyświetlany  
kontakt z książki  
telefonicznej

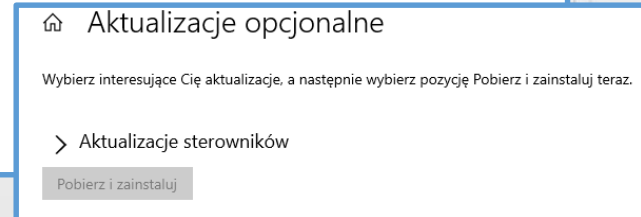
Fałszywa  
informacja o  
przesyłce



# Kontroluj aktualizacje Windows 10 (menu Start)



**NIE WYŁĄCZAJ  
KOMPUTERA W  
TRAKCIE  
AKTUALIZACJI  
WINDOWS**



# Kontroluj „alerty” programu antywirusowego

The image displays the ESET Endpoint Antivirus user interface. The main window shows a green status bar with the text "Maksymalna ochrona" (Maximum protection). Below this, two green checkmarks indicate that the license is valid (expiration date: 13.09.2021) and that all modules are up to date (last update: 18.02.2021 06:02:50). A sidebar on the left contains navigation options: STAN OCHRONY, SKANOWANIE KOMPUTERA, AKTUALIZACJA, USTAWIENIA, NARZEDZIA, and POMOC I OBSŁUGA. A smaller inset window titled "Stan ochrony" (Protection status) shows a warning icon and the text "ESET Endpoint Antivirus wymaga uwagi" (ESET Endpoint Antivirus requires attention). It lists protection status for "Komputer" and "Internet i poczta e-mail", both showing "Maksymalna ochrona". A red box highlights a warning: "System operacyjny nie jest aktualny" (Operating system is not up to date), with a message advising to install missing updates via Windows Update. A red arrow points from this warning to the system tray icon of the ESET antivirus program, which is also highlighted with a red box. The system tray shows the time as 08:20 on 18.02.2021.

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

# Aktualizuj przeglądarki internetowe (Google)

The image illustrates the process of updating Google Chrome. It features a main screenshot of the Chrome browser window with the Google logo on the page. A yellow circle with the number '1' points to the three-dot menu icon in the top right corner. A second yellow circle with the number '2' points to the 'Ustawienia' (Settings) option in the dropdown menu. A third yellow circle with the number '3' points to the 'Ustawienia' option in the Windows Settings application. A fourth yellow circle with the number '4' points to the 'Masz aktualną wersję Google Chrome' (You have the latest version of Google Chrome) notification in the 'Chrome - informacje' (Chrome - info) section of the Windows Settings app. The Windows Settings app is open to the 'Ustawienia' (Settings) page, with the 'Potwierdzenie bezpieczeństwa' (Security) option highlighted in a yellow circle. The 'Chrome - informacje' section shows the current version as 88.0.4324.182 (Official version) and indicates that the user has the latest version.

**1**

**2**

**3**

**4**

Ustawienia

Przeszukaj ustawienia

Ty i Google

Autouzupełnianie

Potwierdzenie bezpieczeństwa

Prywatność i bezpieczeństwo

Wyświetl

Wyszukiwarka

Domyślna przeglądarka

Po uruchomieniu

Zaawansowane

Rozszerzenia

Chrome - informacje

Chrome - informacje

Masz aktualną wersję Google Chrome

Wersja 88.0.4324.182 (Oficjalna wersja) (64-bitowa)

Pomoc do Chrome

Zgłoś problem

Google Chrome

Copyright 2021 Google LLC. Wszelkie prawa zastrzeżone.

Stworzenie przeglądarki Google Chrome było możliwe dzięki programom o otwartym kodzie źródłowym.

Warunki korzystania z usługi

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

The image shows a Chrome browser window with the settings page open. The settings are in Polish. The left sidebar shows the 'Ustawienia' (Settings) menu. The main content area shows the 'Autouzupełnianie' (Autofill) section, where the 'Hasła' (Passwords) option is highlighted. A yellow box with the number '1' points to this option. A yellow arrow points from the 'Hasła' option to the 'Ustawienia' (Settings) menu in the top right corner, which is also highlighted with a yellow box and the number '2'. A yellow arrow points from the 'Ustawienia' menu to the 'Zapisane hasła' (Saved passwords) section, which is highlighted with a yellow box and the number '3'. A yellow arrow points from the 'Zapisane hasła' section to a yellow box with the text 'skopiuj hasło edytuj hasło usuń' (copy password edit password delete), which is highlighted with a yellow box and the number '4'. The 'Zapisane hasła' section shows a table with columns for 'Strona internetowa' (Website), 'Nazwa użytkownika' (Username), and 'Hasło' (Password). The password column is currently masked with dots. Below the table, there is a section for 'Nigdy nie zapisane' (Never saved) with a list of websites: goonline.bnpparibas.pl, login.microsoftonline.com, and pz.gov.pl.

1

2

3

4

skopiuj hasło  
edytuj hasło  
usuń

# Kontroluj w zakładce „ustawienia” zapisane hasła (Mozilla)

The image illustrates the process of managing saved passwords in Mozilla Firefox. It consists of two overlapping browser windows and a menu.

**Top Window: Firefox Lockwise**  
URL: `about:logins`  
Search: `Szukaj danych logowania`  
Sortuj wg: `Nazwa (A-Z)` (3 dane logowania)  
List of logins:

- (bez nazwy użytkownika)
- `raport.umt.tarnow.pl`
- `um.sod.umt.tarnow.pl`

Fields for each login: Adres witryny, Nazwa użytkownika (bez nazwy użytkownika), Hasło (masked with dots and an eye icon). Buttons: `Kopiuj`. Metadata: `Utworzono: 13 listopada 2020`, `Ostatnia modyfikacja: 13 listopada 2020`, `Ostatnie użycie: 13 listopada 2020`.

**Bottom Window: Firefox Options**  
URL: `about:preferences#privacy`  
Section: **Prywatność i bezpieczeństwo**  
Sub-section: **Dane logowania i hasła**

- Pytanie o zachowywanie danych logowania do witryn
- Automatyczne wypełnianie formularzy logowania
- Proponowanie i generowanie gięlnych haseł
- Powiadomienia o hasłach do stron, z których wyciekły dane. [Więcej informacji](#)
- Hasło główne. [Więcej informacji](#)

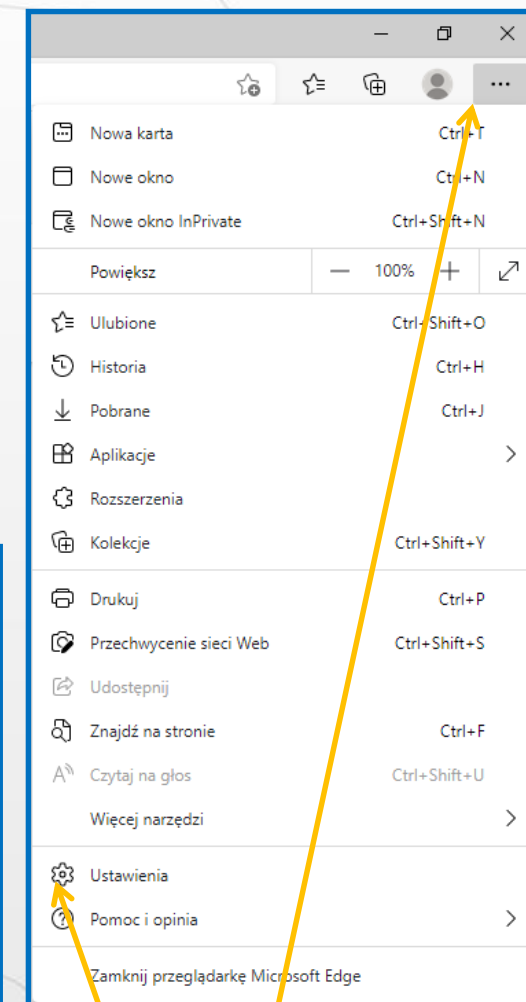
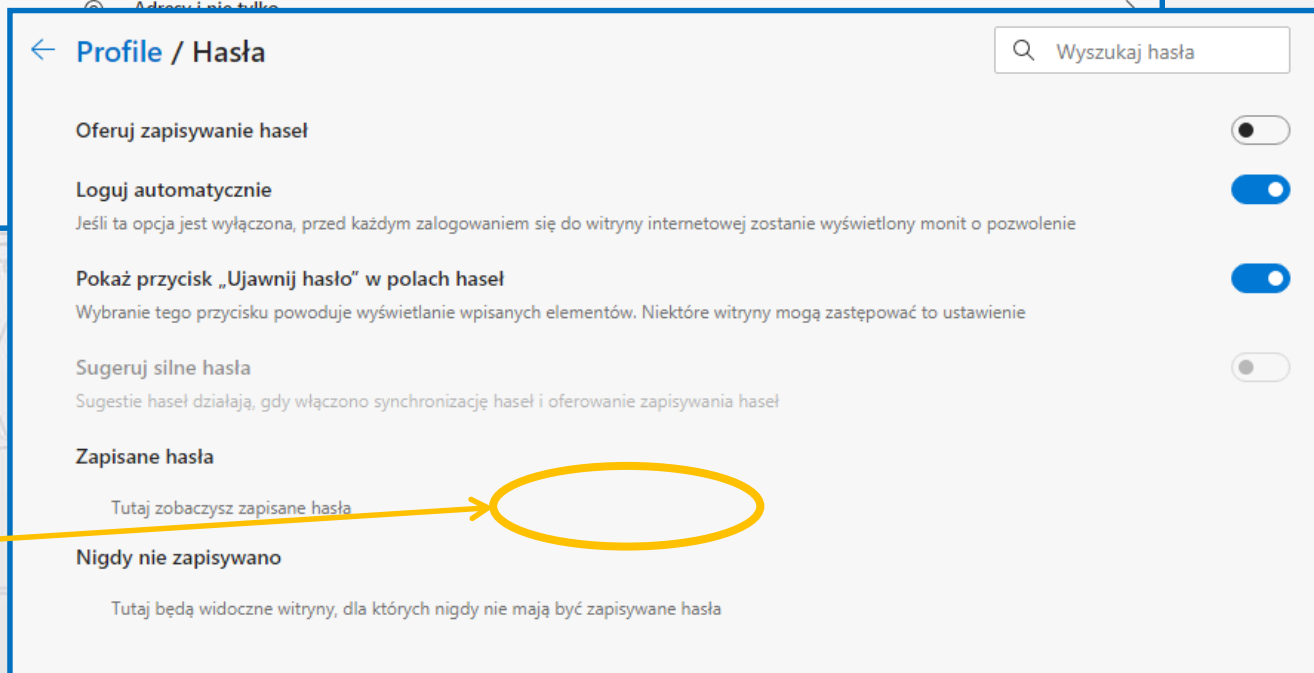
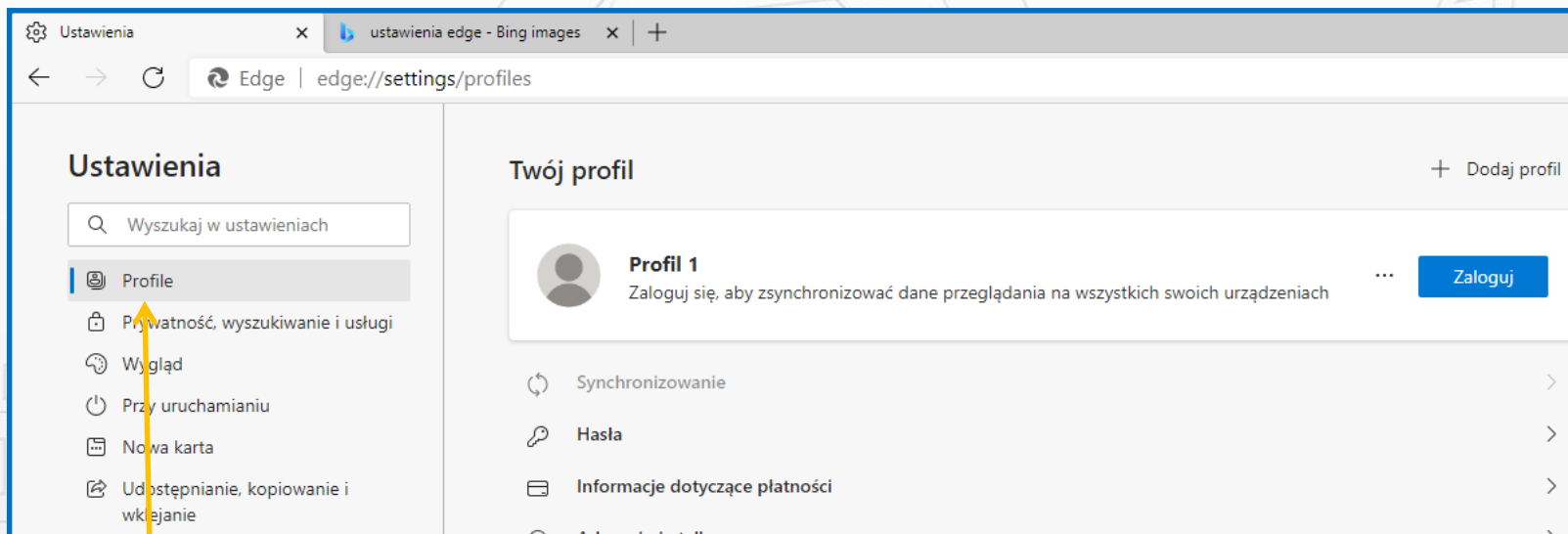
Buttons: `Wyjątki...`, `Zachowane dane logowania...`, `Zmień hasło główne...`

**Right Window: Firefox Menu**  
Item: `Dane logowania i hasła` (Ctrl+Shift+A)

**Numbered Circles and Arrows:**  
1: Points to the 'Dane logowania i hasła' section in the bottom window.  
2: Points to the 'Automatyczne wypełnianie formularzy logowania' checkbox.  
3: Points to the 'Zachowane dane logowania...' button.  
4: Points to the eye icon in the password field of the top window.



# Kontroluj w zakładce „ustawienia” zapisane hasła (Edge)



3

4

2

1

## 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 **hasel** – **unikalność**, powtarzalność
- Nie przepinaj **laptopa** pomiędzy sieciami **wifi** – kablowa RJ45

**TERAZ JUŻ WIEM**