# CYBER HIGIENA/CYBER HYGIENE

## ZASADY BEZPIECZNEGO KORZYSTANIA Z INTERNETU

**BRONIMY POLSKĄ CYBERPRZESTRZEŃ**

**#BEZPIECZEŃSTWO #TECHNOLOGIA #WIEDZA**

**https://ncbc.wp.mil.pl**

# CYBER HIGIENA/CYBER HYGIENE

ZASADY BEZPIECZNEGO KORZYSTANIA Z INTERNETU

## CYBERPRZESTRZEŃ

**to przestrzeń przetwarzania i wymiany informacji tworzona przez systemy teleinformatyczne, wraz z powiązaniami pomiędzy nimi oraz relacjami z użytkownikami.**

Na szczycie NATO w Warszawie w 2016 r. uznano ją za jedną z obecnie pięciu domen operacyjnych, równie ważną jak działania prowadzone na lądzie, w wodzie, powietrzu oraz przestrzeni kosmicznej. To jedyna przestrzeń stworzona całkowicie przez człowieka i jednocześnie – bez zachowania zasad bezpieczeństwa – mogąca zagrażać człowiekowi na globalną skalę.

### Pamiętaj: Internet rządzi się swoimi prawami.

- każda informacja wprowadzona do Internetu może pozostać w niej na zawsze – nawet, jeśli zostanie usunięta z urządzenia np. komputera czy telefonu komórkowego, za pomocą którego została do niej wprowadzona;
- można ją porównać do okna wystawowego: jeśli coś zostanie w nie wstawione, istnieje duże ryzyko, że również niepowołane osoby to zobaczą. Nie dawaj im do tego okazji;
- jest potężną bazą danych, która gromadzi wiele informacji o każdym z nas, a także naszych najbliższych. Chroń siebie i osoby, które są dla Ciebie ważne, uważaj na dane które wprowadzasz;
- współcześnie ludzie bardzo intensywnie korzystają z mediów społecznościowych i nie kryją się ze swoją tożsamością.

# #1 KTO I JAK WPROWADZA DANE DO INTERNETU

## Pamiętaj o tym!

**Człowiek jest najsilniejszym, a zarazem najsłabszym ogniwem w łańcuchu bezpieczeństwa, a poza nami - także nasza rodzina, znajomi, przełożeni, ale też nieznajomi robiąc zdjęcie, na którym zostaniemy uwidocznieni na bliższym czy dalszym planie.**
**Fakt, że my sami jesteśmy ostrożni, nie oznacza zatem, że jesteśmy całkowicie bezpieczni.**

**Mechanizm umieszczenia informacji w Internecie polega na wykorzystaniu urządzeń podpinanych do Internetu, a jest ich wiele:**

- urządzenia mobilne;
- urządzenia stacjonarne;
- karty płatnicze;
- Informatyczne Nośniki Danych (IND), np. USB (pendrive), płyty DVD, CD-ROM;
- Internet Rzeczy (IoT - Internet of Things).

**Nie bagatelizuj ich możliwości nawet wtedy, gdy fizycznie są małe.**

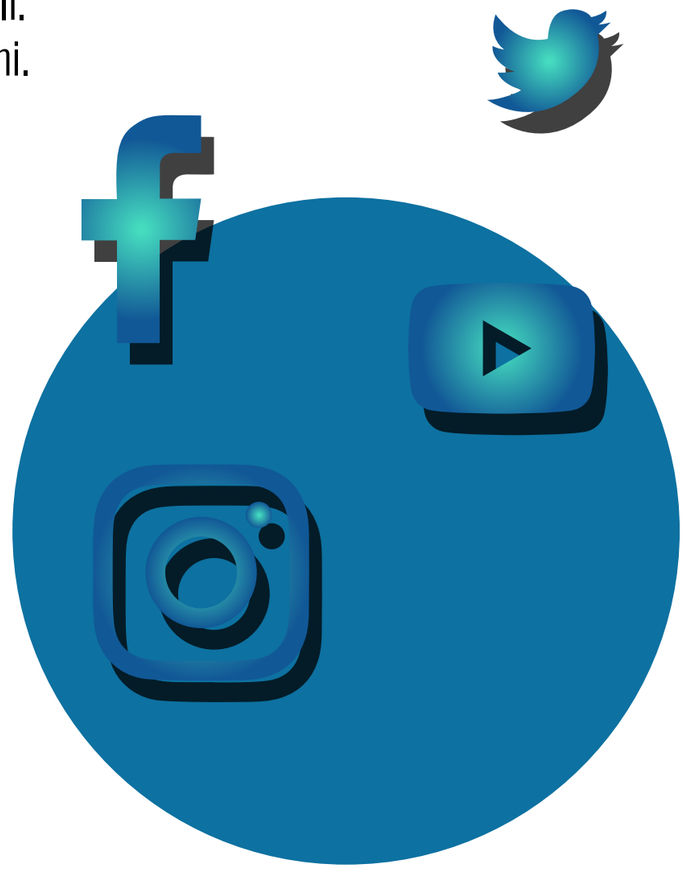
# CYBER HIGIENA/CYBER HYGIENE

ZASADY BEZPIECZNEGO KORZYSTANIA Z INTERNETU

## #2 KTO I JAK WPROWADZA DANE DO INTERNETU

**Największą skarbnicą wiedzy, w której można znaleźć informacje także na nasz temat, są media społecznościowe.**

Instalowanie różnego rodzaju aplikacji na urządzeniach mobilnych, bez zapoznania się z treścią regulaminu określającego na jakich zasadach można z tych aplikacji korzystać oraz czego ich twórcy chcą od nas w zamian, może doprowadzić do utraty danych zapisanych w pamięci tych urządzeń: zdjęć, plików, maili. Warto pamiętać, że nie wszystkie regulaminy zawierają pełne informacje o tym, co dzieje się z naszymi danymi. Pobierając aplikację, każdorazowo trzeba liczyć się z ryzykiem utraty danych.



## UWAGA!

W ekstremalnie niesprzyjających warunkach może to doprowadzić do kradzieży tożsamości!

**Dla przykładu - modna aplikacja FaceApp, która dzięki wsparciu sztucznej inteligencji pozwala na „postarzenie” wizerunku użytkownika w bardzo wiarygodny sposób, wymaga przesłania zdjęcia na serwery twórców mieszczące się w Petersburgu. Polityka prywatności aplikacji nie ukrywa, że twórcy mają dostęp do naszych zdjęć. Interpretacja zapisów zawartych w polityce może być wręcz dowolna, nie ma zatem kontroli, gdzie i do kogo trafią nasze zdjęcia.**
**Aplikacja zbiera też duży komplet danych: cookies, dane analityczne, logi, identyfikatory urządzenia oraz metadane zdjęć.**

# CYBER HIGIENA/CYBER HYGIENE

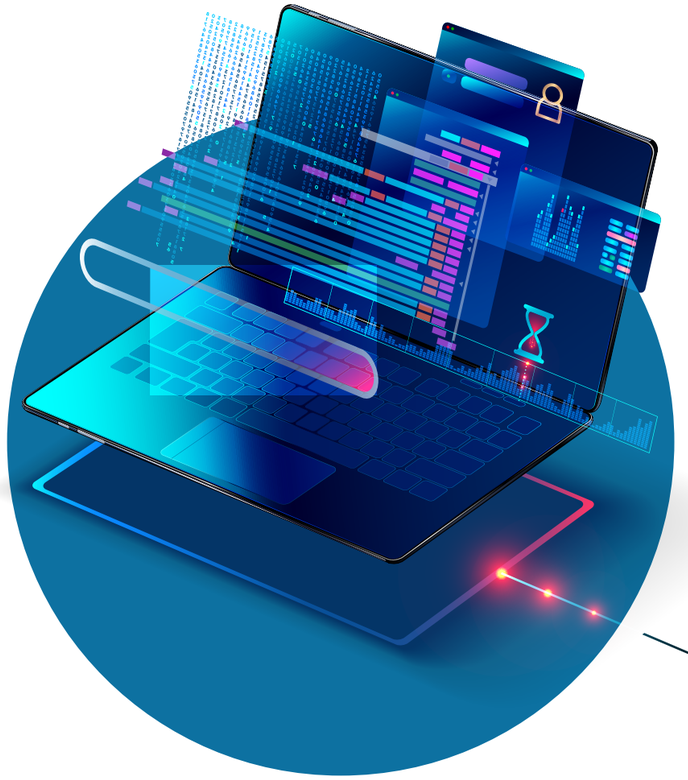
ZASADY BEZPIECZNEGO KORZYSTANIA Z INTERNETU

## #1 SOCJOTECHNIKA (INŻYNIERIA SPOŁECZNA): BYŁA, JEST I BĘDZIE .... SKUTECZNA!

**Uwaga!** Skuteczność takich metod jest bardzo duża. Wynosi nawet ponad 99%.

**SOCJOTECHNIKA** jest jedną z najbardziej efektywnych metod działania cyberprzestępców.
Polega na **WYWIERANIU OKREŚLONEGO WPŁYWU NA UŻYTKOWNIKÓW** w celu dotarcia do firmowych systemów, co jest o wiele łatwiejsze i często szybsze od hakowania technologii. Jest także zwykle dużo tańsze.
**Istotnym narzędziem** socjotechnicznym **jest zbieranie informacji.**
Czasami przestępcom wystarczy pobieżne wyszukanie informacji i wykorzystanie ogólnodostępnych narzędzi w celu wyśledzenia osoby, pod którą można się podszyć i osoby, z którą należy nawiązać kontakt, aby uzyskać dostęp do wszystkich pracowników firmy będących celem ataku.

**Inżynieria społeczna jest wyjątkowo skutecznym atakiem ukierunkowanym na pracowników firmy, którzy często z braku posiadania odpowiedniej wiedzy na temat cyberzagrożeń nie są dostatecznie wyczuleni na działanie przestępców.**
**Pracownicy firm szczególnie narażeni są na tzw. ataki ukierunkowane, zmierzające do zdobycia nieuprawnionego dostępu do informacji firmy cennych dla atakującego.**
**Przestępca odpowiednio manipuluje pracownikiem firmy, żeby zainstalować złośliwe oprogramowanie na dysku jego komputera, zainfekować sieć czy zdobyć login i hasło pozwalające na dostęp do zasobów firmy.**



# #2 SOCJOTECHNIKA (INŻYNIERIA SPOŁECZNA): BYŁA, JEST I BĘDZIE .... SKUTECZNA!

## Jak wygląda przykładowy atak?

**Pracownik otrzymuje wiadomość – np.  w mailu, podczas rozmowy telefonicznej, na stronie internetowej, za pośrednictwem aplikacji, SMSem lub inną drogą, skłaniającą do wykonania określonej czynności.**

**Najczęściej polega ona na zachęceniu do:**

- **kliknięcia w link przekierowujący do zainfekowanej strony internetowej (np. fałszywej strony logowania / oferującej ściągnięcie darmowej aplikacji na wybrany model smatfonu itp.);**
- **pobrania zainfekowanego pliku;**
- **przesłania określonych informacji pod wskazany adres e-mail, wypełnienia formularza z danymi osobowymi w celu wzięcia udziału np. w konkursie / otrzymania nagrody itp.**

# CYBER HIGIENA/CYBER HYGIENE

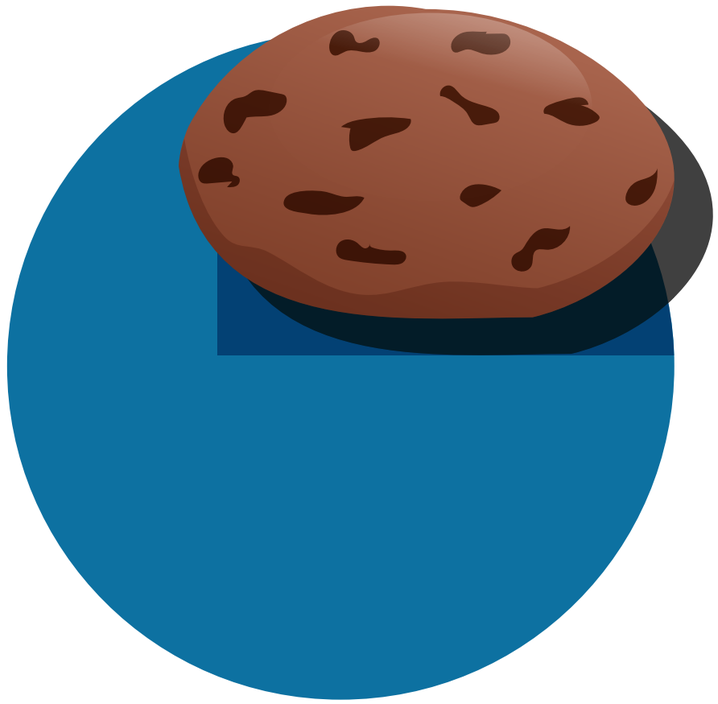
ZASADY BEZPIECZNEGO KORZYSTANIA Z INTERNETU

COOKIES

## Ostrzeżenie na stronie internetowej

**Ciasteczka, czyli cookies** i podobne technologie są wykorzystywane m.in. w celu efektywniejszego świadczenia usług, reklamy, opracowanie statystyk. Korzystanie z witryny zawierajacej ciasteczka bez zmiany ustawień Twojej przeglądarki oznacza, że będą one umieszczane w Twoim urządzeniu końcowym, czyli telefonie czy komputerze.

**Pamiętaj, że zawsze możesz zmienić te ustawienia. Szczegóły znajdziesz w Polityce Prywatności, która powinna być umieszczona na każdej stronie internetowej, z której korzystasz.**



## CO ROBIĄ COOKIES?

**Zwykłe ciasteczka** zwiększają komfort korzystania z sieci:

- używamy ich napełniając koszyk w e-sklepie,
- logując się na forum bez konieczności powtórnego wpisywania hasła.

Mogą służyć również do zbierania informacji o naszej wcześniejszej aktywności w sieci, a wtedy mamy do czynienia z czystą postacią spyware'u, czyli śledzenia.
W przeciwieństwie do innych szpiegów w naszym sprzęcie, cookies są nieszkodliwe, jeśli zbudowane są tylko z kilku linijek tekstu.

## Ciasteczka - ZOMBIE:

Evercookie – czyli „wieczne ciasteczka" to aplikacja oparta na Java Script, która tworzy odradzające sie ciasteczka:

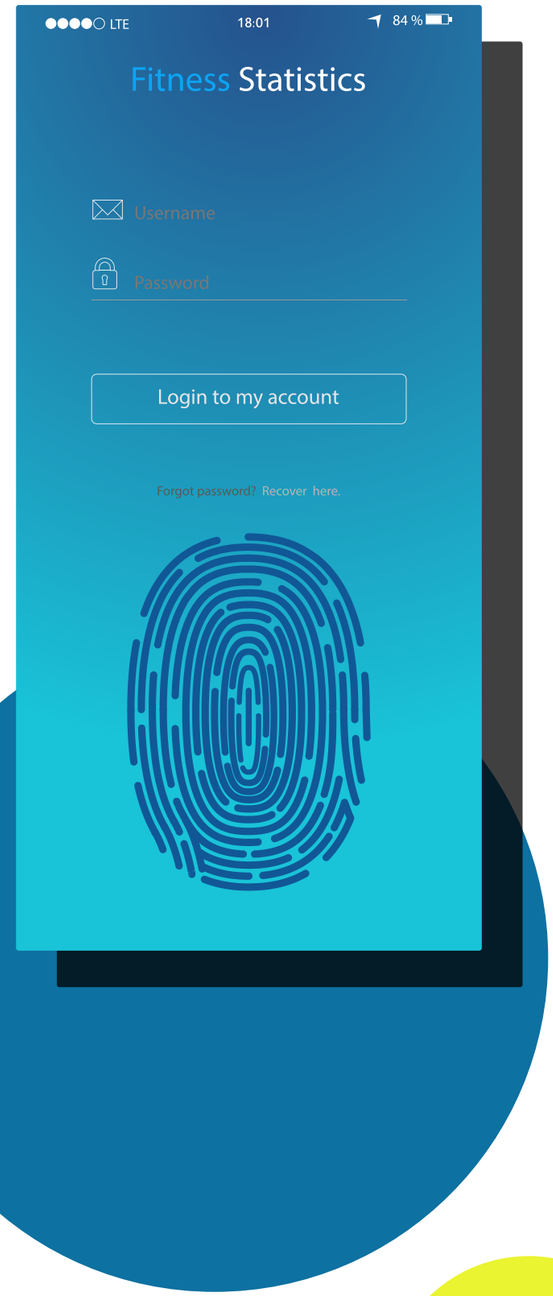
- pliki cookies zapisywane są przez serwer jednocześnie w kilku miejscach w systemie, a wtedy plik ma wiele możliwości nieuprawnionego dostępu do informacji;
- im więcej metod zagnieżdżenia zostanie zastosowanych, tym trudniej się ich pozbyć!

# CYBER HIGIENA/CYBER HYGIENE

ZASADY BEZPIECZNEGO KORZYSTANIA Z INTERNETU

## #1 CO ZDRADZA TWOJE URZĄDZENIE Z CHWILĄ PODŁĄCZENIA DO INTERNETU?

**Gdy odwiedzasz strony internetowe, moduły do śledzenia online i sama strona mogą Cię zidentyfikować - nawet jeśli zainstalowałeś oprogramowanie do ochrony.**




**Aplikacja PANOPTICLICK** to internetowe narzędzie zaprojektowane przez Electronic Frontier Foundation (EFF), które testuje „odcisk palca” Twojej przeglądarki, pokazuje informacje, które ona udostępnia, a dzięki którym Twoje urządzenie jest jednoznacznie identyfikowalne.

**Panopticlik działa z dowolną przeglądarką internetową na komputerze i urządzeniu mobilnym. Jednym słowem pozwala zrozumieć, w jaki sposób Twoje informacje są przesyłane do stron internetowych.**

**TA METODA CZYNI NIESKUTECZNYMI WSZELKIE SPOSOBY WALKI Z NIECHCIANYMI CIASTECZKAMI.**

# CYBER HIGIENA/CYBER HYGIENE

ZASADY BEZPIECZNEGO KORZYSTANIA Z INTERNETU

## #2 CO ZDRADZA TWOJE URZĄDZENIE Z CHWILĄ PODŁĄCZENIA DO INTERNETU?

**CANVAS FINGERPRINTING** to technika, która pozwala ustalić tożsamość konkretnej przeglądarki za pomocą jednego z elementów HTML5 o nazwie canvas. Służy on do dowolnego rysowania kształtów na ekranie monitora.

Witryny internetowe dysponujące tą technologią mogą w ten sposób pozyskać swoisty odcisk palca od przeglądarek internetowych.

Wszystkie te działania są niewidoczne dla nieświadomego użytkownika.

**Canvas Fingerprinting pozwala rozpoznać internautę lub jego komputer, śledzić ich działanie w Internecie i na tej podstawie określać ich zainteresowania.**

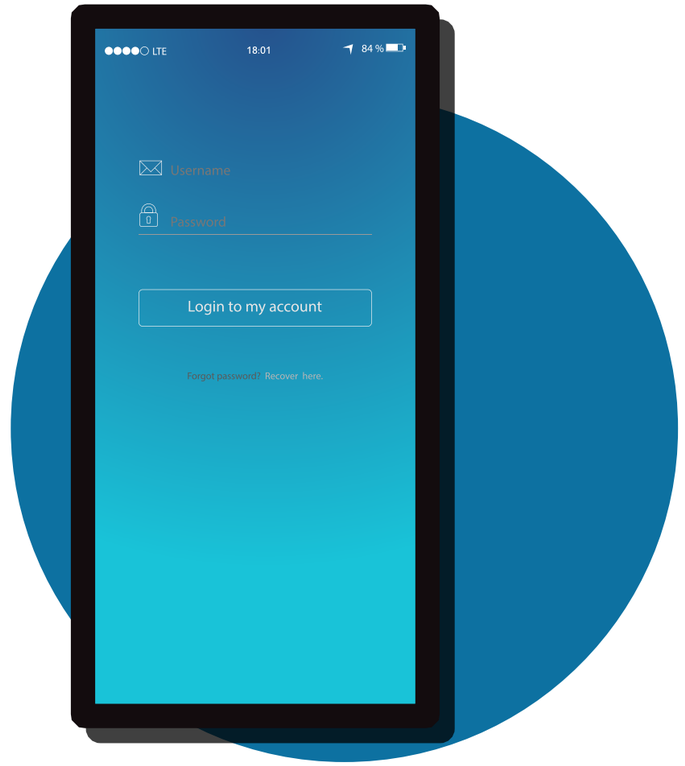
# CYBER HIGIENA/CYBER HYGIENE

ZASADY BEZPIECZNEGO KORZYSTANIA Z INTERNETU

## #1 URZĄDZENIA MOBILNE SMARTFONY, TABLETY, SMARTWATCH-E

### ŹLE ZABEZPIECZONE URZĄDZENIA MOBILNE TO ŁATWY CEL DLA CYBERPRZESTĘPCÓW

Rozmowy telefoniczne, to tylko jedna z wielu funkcji nowoczesnych smartfonów. Używane są one też do robienia e-zakupów, obsługiwania bankowości online, czy prowadzenia korespondencji elektronicznej. Dla przestępcy to dobry cel, gdyż w ich pamięci przechowujemy wiele cennych danych, a w kwestii zabezpieczeń najczęściej zdajemy się wyłącznie na systemowe mechanizmy, w których często istnieją luki. Dlatego smartfony są coraz częstszym celem ataku przestępców.




**Współczesne smarfony, tablety to potężne komputery w naszych kieszeniach. Ich moc przekracza te, które pozwoliły na pierwsze wylądowanie człowieka na Księżycu. Są włączone 24 godziny na dobę, zwykle bez żadnej ochrony, przechowują ogromne ilości danych dotyczących nas samych, naszych znajomych oraz naszej firmy. Telefon bliskich Ci osób będący w tej samej lokalizacji co Twój pozwala też na identyfikację także i Ciebie, czasu przebywania w tym samym miejscu, zwyczajów i trybu życia.**

#2 URZĄDZENIA MOBILNE SMARTFONY, TABLETY, SMARTWATCH-E

## JAK SPRAWDZIĆ CZY TYLKO JA MAM DOSTĘP DO DANYCH W MOIM SMARTFONIE Z SYSTEMEM ANDROID?

**Wystarczy skorzystać z kodów *#21#, *#62#, ##002#.**

W wyniku zainfekowania smartfonu, informacje na nim zgromadzone mogą być przekazywane bez wiedzy właściciela na urządzenia osób trzecich.

Aby upewnić się, że tak nie jest, wystarczy w przypadku systemu Android wprowadzić z klawiatury kod *#21# i nacisnąć słuchawkę. Na ekranie zostanie wyświetlona informacja, czy, a jeżeli tak, to dokąd przekazywane są informacje z urządzenia.
Następnie należy posłużyć się pozostałymi kodami w celu uściślenia informacji na ten temat. Jeżeli na wyświetlaczu uzyskamy informacje o braku przesyłania informacji, wtedy możemy spać względnie spokojnie :)

**Dobrze jest wiedzieć, że współczesne urządzenia mobilne podsłuchują swoich użytkowników, a zdobyte informacje są umieszczne na serwerach producenta w formie plików tekstowych, wystarczy użyć tylko np. frazy "ok, google" lub "ok, idź po to".**

# CYBER HIGIENA/CYBER HYGIENE

ZASADY BEZPIECZNEGO KORZYSTANIA Z INTERNETU

## URZĄDZENIA STACJONARNE

Należy pamiętać, że współczesne zasilacze do komputerów nie odłączają napięcia od stacji roboczej, dlatego potencjalny agresor jest w stanie uruchomić ją zdalnie wykorzystując kartę sieciową.
Może on wyłączyć diody sygnalizacyjne, spowolnić pracę wentylatorów i spokojnie przeszukać zawartość twardych dysków bez zwracania uwagi użytkownika na fakt, że stacja robocza pracuje, choć (teoretycznie) jest wyłączona.

**Dlatego chcąc faktycznie wyłączyć komputer należy kabel zasilający wypiąć z listwy zasilającej, gdyż odcięcie dopływu napięcia do niej spowoduje, że nasz komputer faktycznie zostanie wyłączony.**

Aby zabezpieczyć nasz komputer przed atakiem należy:

- usunąć oprogramowanie typu crapware czyli zainstalowane na dysku nowego komputera oprogramowanie o znikomej wartości, niepotrzebnie spowalniające sprzęt,
- zainstalować oprogramowanie antywirusowe,
- uruchomić ścianę ogniową (Firewall),
- zainstalować oprogramowanie anty-spaware, anty-trojan,
- pilnować stałej aktualizacji oprogramowania (zarówno systemowego jaki i użytkowego),
- nie pracować na koncie z uprawnieniami administratora,
- stosować silne hasła,
- szyfrować wszystkie informatyczne nośniki danych, a bezwzględnie typu pendrive.

**Do stacji nigdy nie należy podłączać urządzeń z niepewnego źródła!**

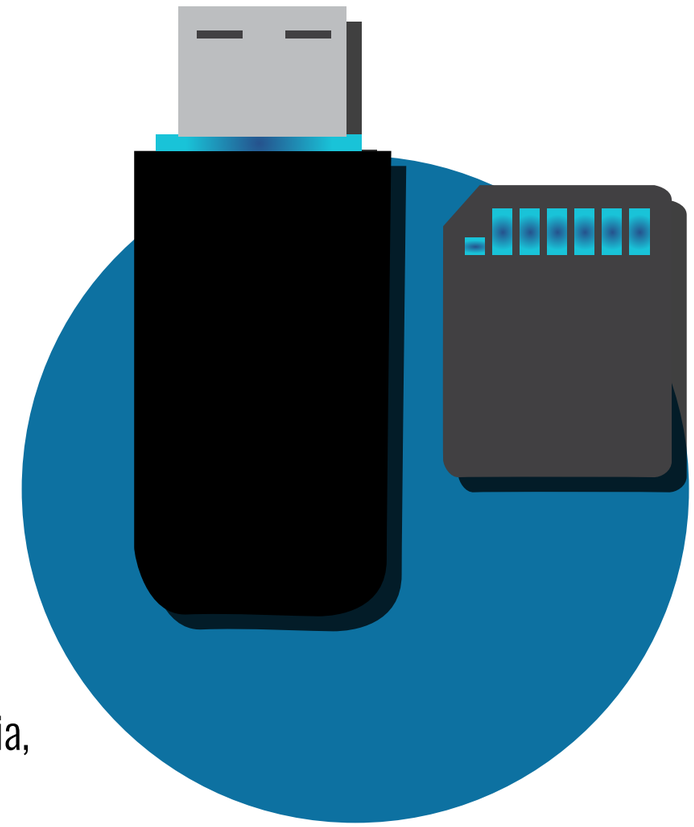
# CYBER HIGIENA/CYBER HYGIENE

ZASADY BEZPIECZNEGO KORZYSTANIA Z INTERNETU

## URZĄDZENIA PODŁĄCZANE PRZEZ USB I URZĄDZENIA INTELIGENTNE

**Pendrive** - odpowiednio zmodyfikowany przez agresora może pokazać się w systemie ofiary jako dowolne urządzenie peryferyjne np. klawiatura lub jako zewnętrzna karta sieciowa, zmienić ustawienia sieci i przekierować całą komunikację przez serwer agresora. Taki pendrive może również posłużyć do jednoczesnego pobrania przez użytkownika dodatkowych plików bez jego wiedzy. Ofiara ataku nie będzie świadoma, że nastąpiło pobranie i zapisanie danych, gdyż pliki te na pendrivie nie będą dla niej widoczne.

**Konstrukcja pendrive stosowanego do ATAKU ENERGETYCZNEGO polega na tym, że w jego wnętrzu zamiast kości pamięci znajduje się przetwornica oraz kondensatory. Pendrive ten zasilany jest ze złącza USB napięciem 5V, a następnie zwraca do stacji roboczej impuls 200-220V o natężeniu 1A, co powoduje zniszczenie urządzenia.**



**Z POWYŻSZEGO POWODU NIE NALEŻY KORZYSTAĆ Z NIEZNANYCH NOŚNIKÓW DANYCH I PODPINAĆ ICH DO SWOICH URZĄDZEŃ.**

Niewskazane jest też korzystanie z publicznych stacji ładowania smartfonów, tabletów lub innych urządzeń podpinanych przez port USB. Stacje te bowiem mogą być zainfekowane przez agresora oprogramowaniem złośliwym, które zainfekuje Twoje urządzenie, pozwalając np. na kradzież haseł oraz innych informacji.

Pod koniec 2012 r. Amerykańska Agencja Bezpieczeństwa Narodowego ostrzegła pracowników rządowych, aby używali wyłącznie swoich osobistych kabli do ładowania i nie korzystali z publicznych miejsc do ładowania, a także nie ładowali urządzeń przez komputery innych ludzi, szczególnie podczas podróży zagranicznych.

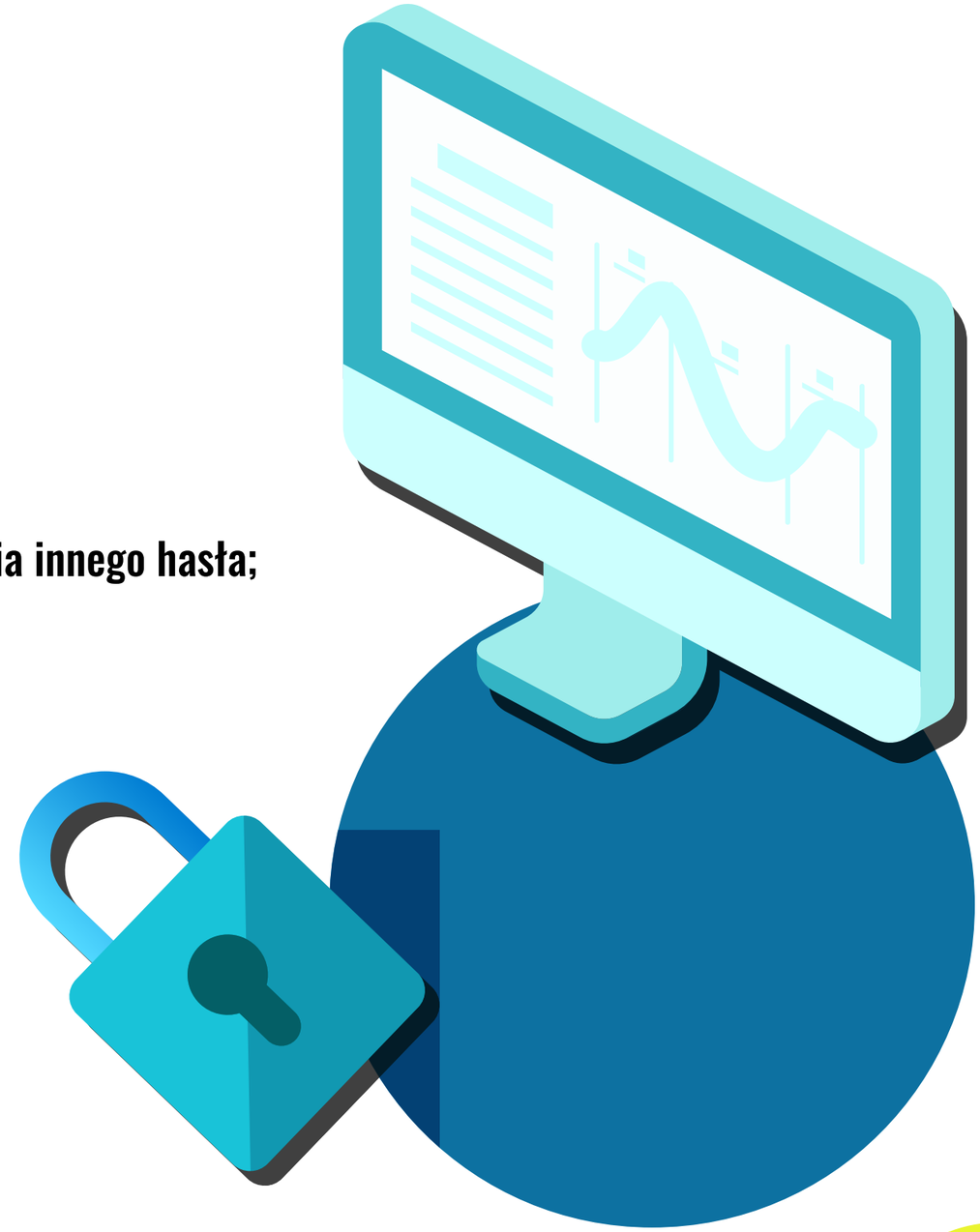
# CYBER HIGIENA/CYBER HYGIENE

ZASADY BEZPIECZNEGO KORZYSTANIA Z INTERNETU

#3 HASŁA

## JAK BEZPIECZNIE KORZYSTAĆ Z HASŁA?

- używaj długich i skomplikowanych haseł;
- nie używaj tego samego hasła w różnych serwisach;
- nie pozwalaj żadnym programom na zapamiętywanie hasła;
- ujawnienie jednego hasła nie powinno stanowić  wskazówki do ujawnienia innego hasła;
- zmieniaj co jakiś czas hasła;
- zawsze wyloguj się po zakończeniu pracy.



# CYBER HIGIENA/CYBER HYGIENE

ZASADY BEZPIECZNEGO KORZYSTANIA Z INTERNETU

## #1 OSZUSTWA W INTERNECIE

### CZYM JEST PHISHING?

Jest to **atak psychologiczny (socjotechniczny)** używany przez cyberprzestępców **w celu pozyskania poufnych informacji lub nakłonienia ofiary do wykonania określonych czynności.**

Oryginalnie pojęcie to oznaczało atak mailowy, dzięki któremu login i hasło ofiary mogły zostać skradzione. Jednak dziś phishing ewoluował i obecnie nazywa się tak prawie każdy atak oparty na wysyłaniu do ofiary wiadomości. Cyberprzestępca podszywa się wtedy pod kogoś znanego i zaufanego, jak przyjaciel, członek rodziny, bank czy dobrze znany sklep.

### CO TO JEST SPEAR PHISHING?

**Spear phishing jest atakiem ukierunkowanym na konkretne osoby lub organizacje. Jest poprzedzony niejednokrotnie pogłębionym wywiadem środowiskowym opartym na informacjach dostępnych w Internecie.**

**Cyberprzestępcy stosujący spear phishing nie wysyłają wiadomości do milionów przypadkowych użytkowników, ale starannie dobierają swoje ofiary. Wten sposób próbują uzyskać dostęp do konkretnych informacji (np. haseł dostępowych) lub tejemnic handlowych.**

# CYBER HIGIENA/CYBER HYGIENE

ZASADY BEZPIECZNEGO KORZYSTANIA Z INTERNETU

## #1 HASŁA

**Hasło to najprostsze, podstawowe zabezpieczenie.
Hasło nie powinno być zbyt krótkie i proste - co najmniej
osiem znaków - najlepiej, aby składało się z liter (dużych i małych),
liczb i znaków specjalnych (np. #%&@)**


**CECHY SILNEGO HASŁA:**

- jest dla Ciebie łatwe do zapamiętania, lecz trudne do odgadnięcia przez inne osoby,
- różni się znacznie od poprzednich haseł,
- nie zawiera powtórzeń znaków (np. 111111111), sekwencji (np. abcdefgh),
  ani ciągów znaków występujących obok siebie na klawiaturze (np. QWERTY).

**W hasłach nie wskazane jest używanie żadnych słów, które można znaleźć w dowolnym słowniku, w dowolnym języku.
Są one bowiem uwzględnione w słownikach używanych przez agresora, w słownikach służących do ataków typu
brute force uwzględniono również słowa z zamiennikami liter na znaki specjalne typu @, # itp.**

# CYBER HIGIENA/CYBER HYGIENE

ZASADY BEZPIECZNEGO KORZYSTANIA Z INTERNETU

#2 HASŁA

**Słabe hasło: agnieszka1975**
**Silne hasło: @Gnie$^ka!(75_*:+**

## Jak stworzyć silne hasło?

- wybierz zdanie, które łatwo zapamiętasz, np. „Bardzo lubię czerwone smażone pomidory”. Będzie to podstawa do zbudowania silnego hasła;
- utwórz nowe, pozbawione znaczenia słowo z dwóch pierwszych liter każdego wyrazu ze zdania powyżej: baluczsmpo;
- zwiększ siłę hasta dodając wielkie i małe litery oraz cyfry, np. BaLuczsmPO;
- zastąp część liter i cyfr znakami specjalnymi, np. B@l_ucz$mPO.

## Kategoryzacja siły haseł:

- PIN;
- symbol graficzny;
- skanowanie tęczówki;
- odcisk palca;
- zdjęcie twarzy.

# CYBER HIGIENA/CYBER HYGIENE

ZASADY BEZPIECZNEGO KORZYSTANIA Z INTERNETU

## #2 OSZUSTWA W INTERNECIE

### JAKIE SĄ OZNAKI PHISHINGU?

- **sprawdź e-mail adresata:** jeśli wiadomość wydaje się pochodzić z jakieś organizacji, a adres jest w dobrze znanej domenie oferującej darmowe konta, to prawdopodobnie jest to atak. **SPRAWDŹ POLA** wiadomości: **„DO”** oraz **„DW”**. Czy mail został wysyłany również do osób, których nie znasz lub z którymi nie pracujesz?;

- uważaj na maile zaadresowane jako „Dear Customer” lub podobnie. Jeśli zaufana organizacja chciałaby się z Tobą skontaktpowinna zwrócić się do Ciebie po imieniu. Zapytaj sam siebie, czy spodziewasz się maila od tej firmy?

- sprawdź również zastosowaną gramatykę i ortografię. Większość zaufanych organizacji nie popełnia błędów językowych, ortograficznych, stylistycznych i sprawdza swoje wiadomości dokładnie przed wysłaniem do klientów;

- uważaj na wszystkie maile, które nakłaniają Cię do podjęcia pilnego działania lub budują u Ciebie poczucie winy. To częsty zabieg psychologiczny wykorzystywany przez oszustów. **NIKT NIE POWINIEN PROSIĆ CIĘ O PODANIE DANYCH OSOBOWYCH!**

- uważaj z linkami i klikaj tylko na te, których się spodziewasz. Warto również ostrożnie najechać myszką na link i podejrzeć prawdziwy adres docelowy. Jeśli źródło jest inne niż pokazano w mailu, wskazuje to na atak hakerski;

- **UWAŻAJ NA ZAŁĄCZNIKI.** Otwieraj tylko te, których się spodziewasz;

- uważaj na wszystkie wiadomości, które brzmią zbyt dobrze, żeby były prawdziwe np. wygrana w konkursie, na loterii, przelew z banku na drugim końcu świata, czy zwrot podatku.

# CYBER HIGIENA/CYBER HYGIENE

ZASADY BEZPIECZNEGO KORZYSTANIA Z INTERNETU

## #3 OSZUSTWA W INTERNECIE

**Miej czujne oko. Warto zwrócić uwagę na wprowadzane adresy URL (zwłaszcza na występujące w nich literówki) i rozsądnie udostępniać swoje dane osobowe.**

**WIDZISZ RÓŻNICĘ?:**

*www.bankofamerica.com*
*www.bankofamerico.com*
*www.bonkofamerica.com*
*www.bankofarnerica.com*
*www.bankofamerica.oom*

| | | | |
|---|---|---|---|
| rn | jako | m | (małe litery R i N jako mała litera M) |
| cl | jako | d | (małe litery C i L jako mała litera D) |
| q | jako | g | (mała litera Q jako mała litera G) |
| cj | jako | g | (małe litery C i J jako mała litera G) |
| vv | jako | w | (podwójna litera V jako litera W) |
| ci | jako | a | (małe litery C oraz I jako mała litera A) |
| l | jako | I | (duża litera i jako mała litera L) |
| I | jako | l | (mała litera L jako duża litera i) |
| 1 | jako | l | (cyfra 1 jako mała litera L) |
| 1 | jako | I | (cyfra 1 jako duża litera i) |
| l | jako | 1 | (mała litera L jako cyfra 1) |
| I | jako | 1 | (duża litera i jako cyfra 1) |

# CYBER HIGIENA/CYBER HYGIENE

ZASADY BEZPIECZNEGO KORZYSTANIA Z INTERNETU

## #1 NIEUPRAWNIONY DOSTĘP DO TWOICH DANYCH

**NIEUMYŚLNY PRZECIEK INFORMACJI MOŻE NASTĄPIĆ W WYNIKU BŁĘDU UŻYTKOWNIKA, PRZEZ JEGO BRAK ŚWIADOMOŚCI, NIEUWAGĘ, NIEROZWAŻNE DZIAŁANIE, np.:**

- wysłanie na zewnątrz organizacji źle zaadresowanej korespondencji, dołączenie listy mailingowej firmy itp.;
- doprowadzenie do utraty (czasowej czy trwałej) kontroli nad urządzeniem (zgubienie, kradzież przez osoby trzecie itp.)

**Kradzież informacji od wewnątrz, czyli przez tzw. złośliwego pracownika:**
to zjawisko jest niebezpieczne, gdyż wewnętrznego „kreta” ciężko jest namierzyć, nie przełamuje on bowiem żadnych zabezpieczeń, zatem szansa popełnienia błędu jest znacznie mniejsza niż atak z zewnątrz z koniecznością przełamywania zabezpieczeń.
**Kradzież informacji z zewnątrz** to wyprowadzenie jej z firmy przez agresora atakującego spoza organizacji przy wsparciu oprogramowania złośliwego.

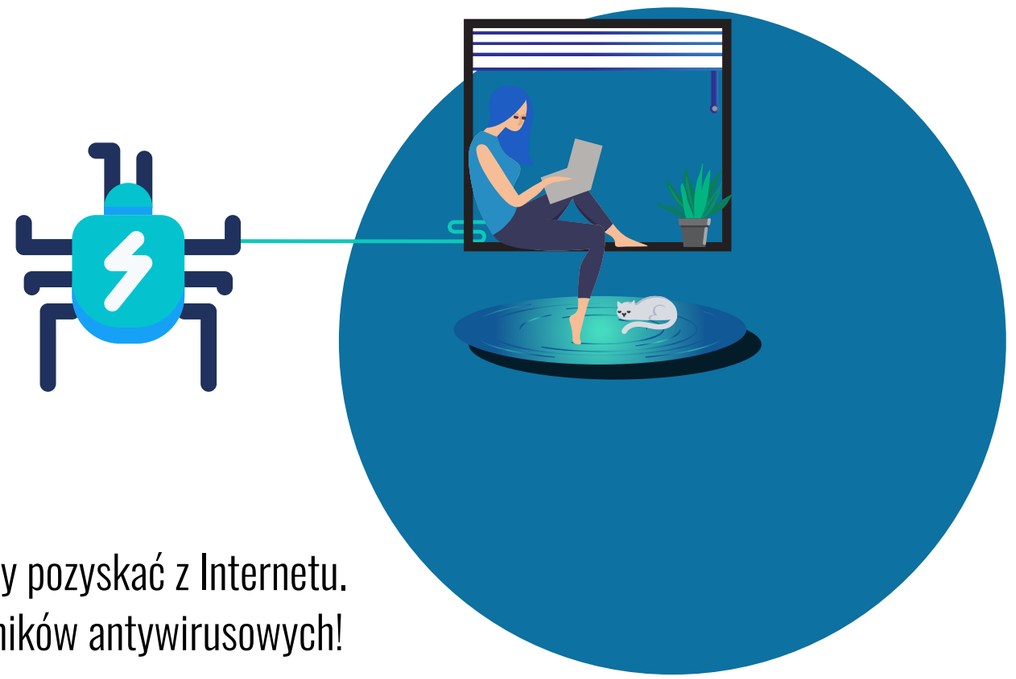
# CYBER HIGIENA/CYBER HYGIENE

ZASADY BEZPIECZNEGO KORZYSTANIA Z INTERNETU

## #2 NIEUPRAWNIONY DOSTĘP DO TWOICH DANYCH

**Oprogramowanie złośliwe:**

- Wirusy
- Robaki
- Konie trojańskie
- Bomby logiczne
- Keylogger'y
- Spyware



Oprogramowanie złośliwe jest proste do pozyskania. Można je napisać samemu czy pozyskać z Internetu. Już za 500 EUR można kupić oprogramowanie wyłączające 30 renomowanych silników antywirusowych!

Trojany z rodziny RAT są w stanie zrobić wiele:

- wyszukiwać dowolne dane na twardych dyskach, kopiować i kasować je, a nawet wgrywać nowe pliki;
- pobrać, zapisać i uruchomić keyloggery;
- włączyć mikrofon;
- włączyć kamerkę;
- dokonywać zrzuty ekranu, kręcić filmiki;
- podsłuchiwać telefonię internetową.

**Uwaga!**

**Od 2016 roku oprogramowanie typu ransomware jest w stanie szyfrować dyski autonomicznych stacji roboczych i sieci wydzielonych!**

# CYBER HIGIENA/CYBER HYGIENE

ZASADY BEZPIECZNEGO KORZYSTANIA Z INTERNETU

## #1 IoT – INTERNET RZECZY

**Liczba podłączonych urządzeń do Internetu cały czas rośnie:
tworzą one obszar zwany Internetem Rzeczy, w skrócie IoT (ang. Internet of Things).
Są to urządzenia elektroniczne typu „smart”, czyli inteligentne telewizory, lodówki, pralki, odkurzacze, tostery, żarówki czy też zamki w drzwiach lub kamery monitorujące nasze mieszkanie.**

Łączność z Internetem to obecnie standard w nowych telewizorach i innych urządzeniach systemów domowej rozrywki. Urządzenia korzystające z funkcji rozpoznawania poleceń głosowych mogą przekazywać firmom trzecim wszystkie odgłosy zarejestrowane w pomieszczeniu.
Ponadto należy mieć świadomość, że każdy telewizor typu smart posiada jednoznaczny identyfikator pozwalający zdalnie rejestrować aktywność użytkownika w niezanonimizowanej formie.
Pozwala to przesłać na serwery producenta informacje o czasie włączenia urządzenia, uruchamianiu aplikacji, odtwarzaniu lokalnym plików, czy też korzystaniu z usług dodatkowych HbbTV.

**HbbTV (ang. Hybrid Broadcast-Broadband Television) to tzw. standard “hybrydowy”**
umożliwiający odbieranie sygnału TV razem z interaktywnymi danymi z Internetu.
Dzięki temu standardowi możliwe jest przeprowadzenie ataku na nasze telewizory,
gdyż w trakcie oglądania kanałów HbbTV w tle pobierane są interaktywne treści z Internetu.

# CYBER HIGIENA/CYBER HYGIENE

ZASADY BEZPIECZNEGO KORZYSTANIA Z INTERNETU

## #2 IoT – INTERNET RZECZY

**Urządzenia typu smart bardzo często zawierają szereg słabych punktów stanowiących idealny punkt dostępowy do naszych systemów dla potencjalnego agresora.**

Należy zaliczyć do tego:

- dostęp bez uwierzytelnienia;
- słabość uwierzytelniania;
- ustawienia domyślne;
- słabość kodów bezpieczeństwa;
- przestarzałe metody szyfrowania;
- ukrycie przez programistów tzw. backdoor'ów, czyli luk w zabezpieczeniach systemu utworzonych w celu późniejszego wykorzystania.

Przykładami takiego działania mogą być: włamanie do systemu przez lodówkę w Wielkiej Brytanii, termometr w kasynie, inteligentną deskę sedesową w Japonii, czy też włamania do kamerek podłączonych do Internetu na całym świecie.

# CYBER HIGIENA/CYBER HYGIENE

ZASADY BEZPIECZNEGO KORZYSTANIA Z INTERNETU

## FAŁSZYWE NEWSY, NAGRANIA, FILMY...

**Technologia DEEPFAKE powstała w laboratorium Samsunga w Rosji. Pozwala ona w czasie rzeczywistym podłożyć głos dowolnej osoby pod wypowiedź np. innej osoby, wygenerować film na podstawie jednego zdjęcia, wykonać kompromitujące nagranie. Jest też zdolna do wytworzenia realistycznych scen z osobą fikcyjną.**

**W Chinach niektórzy prezenterzy występujący w programach telewizyjnych to awatary, a odbiorcy przed TV widzą ludzi z krwi i kości. W Internecie można znaleźć nagranie prezydenta Richarda Nixona wygłaszającego orędzie o tym, że wyprawa na Księżyc skończyła się porażką czyli nagranie, które nigdy nie zostało zrealizowane.**

Szczególnie groźne może być wykorzystywanie bazujących na sztucznej inteligencji (AI) metod **CYBERMANIPULACJI.**
Systemy AI są już na tyle zaawansowane, że można dzięki nim tworzyć bardzo realistyczne nagrania audio i wideo, w których wykorzystywany jest cudzy wizerunek i głos.
Algorytmy potrafią udawać głos danej osoby, czy też generować sfałszowane filmy. To potężne narzędzia, które mogą służyć m.in. do wpływania na opinię publiczną za pomocą tzw. **FAKE NEWSÓW**.
Odróżnienie ich od prawdziwych informacji będzie coraz trudniejsze, a być może nawet niemożliwe - również ze względu na prawdopodobne rozwijanie technik zapobiegających szybkiemu wykrywaniu fałszywych treści.

**JEDYNĄ OBRONĄ JEST OGRANICZONE ZAUFANIE DO WSZYSTKIEGO, CO WIDZIMY CZY SŁYSZYMY.**

# CYBER HIGIENA/CYBER HYGIENE

ZASADY BEZPIECZNEGO KORZYSTANIA Z INTERNETU

## JAK SIĘ CHRONIĆ - PODSUMOWANIE:

- zainstaluj antywirusa oraz firewall;
- szyfruj wszelkie nośniki danych (dyski, IND);
- instaluj programy tylko z tzw. sprawdzonego źródła: wyłącznie z oficjalnych repozytoriów Apple'a, Google'a i Microsoftu;
- przed otwarciem kodu QR przeskanuj go programem antywirusowym, również wtedy, kiedy korzystasz z systemu iOS;
- regularnie aktualizuj oprogramowanie;
- stosuj unikatowe hasła (różne dla każdego konta);
- korzystaj z VPN;
- ładuj akumulatory urządzeń tylko z zaufanego źródła (własny zasilacz, power bank min. 10 000 mAh, a jeśli chcesz skorzystać z portu USB stosuj blokery USB);
- nigdy nie korzystaj z publicznej stacji ładowania ani obcego notebooka lub innego komputera do ładowania swoich urządzeń elektronicznych takich jak smartfon, tablet czy notebook;
- nie korzystaj z przygodnych kabli;
- jeśli często podróżujesz, pomyśl o zakupie SyncStop: to małe urządzenie uniemożliwia przesyłanie danych kablem USB przez blokowanie pinów danych;
- nie pracuj na koncie z uprawnieniami administratora, jeśli nim nie jesteś;
- każdorazowo zastanów się nad tym, co umieszczasz w sieci i kieruj się zasadą: **Im mniej, tym lepiej!**