(CYBER)SZKOLENIA

KRAJOWY SYSTEM CYBERBEZPIECZEŃSTWA

Podstawowe zasady cyberhigieny w pracy i w życiu prywatnym

Bezpieczne hasła, bezpieczne usługi cyfrowe

Ministerstwo Cyfryzacji

NASK

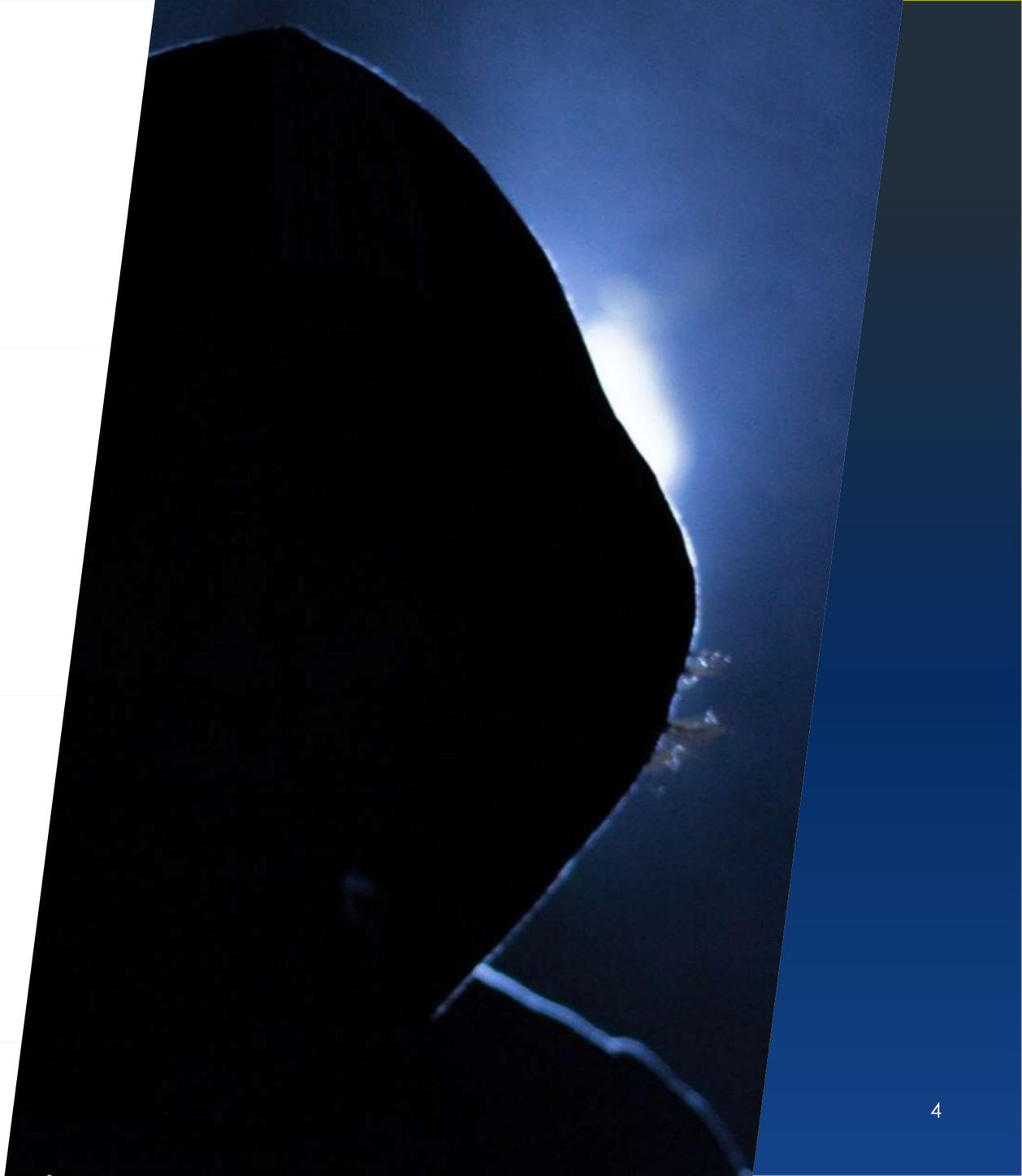
Hasła, uwierzytelnianie

- czyli brama do naszych usług cyfrowych

A w ogóle, to po co nam te hasła?

Po co nam hasła?

- chronią dostęp do danych
- chronią środki finansowe
- chronią naszą cyfrową tożsamość
- zasada ograniczonego zaufania w sieci!



Uwierzytelnianie, czyli potwierdzanie tożsamości za pomocą…

Czegoś, co znasz	Czegoś, co posiadasz	Czegoś, czym jesteś
**********	 	 
Np. hasło lub kod PIN	Np. token sprzętowy, telefon, karta Smart Card	Np. odcisk palca lub skan tęczówki oka

*__Uwierzytelnienie dwuskładnikowe__ (2FA) to weryfikacja __dwóch z trzech__ powyższych elementów przy logowaniu.

https://abgi-france.com/methodes-biometriques-d-identification-reconnaissance-faciale-et-digitale/
https://www.leukekinderactiviteiten.nl/activiteit/techniek/csi-vingerafdrukken/
https://www.yubico.com/blog/
https://pomoc.home.pl/wp-content/uploads/2020/10/1_T.png

Uwierzytelnianie a autoryzacja

Uwierzytelnianie

Weryfikacja tożsamości

Logowanie do konta

Autoryzacja

Uprawnienie dostępu do zasobu

Uprawnienie do wykonania operacji

Jak się łamie hasła (hashe haseł)?

Główne sposoby łamania haseł:

- ataki siłowe („bruteforce”)
- ataki słownikowe
- zgadywanie (hasła domyślne, listy najpopularniejszych haseł, hasła „testowe” – admin123 ...)

Skrypty automatyzujące pracę: wzory, maski i inne kombinacje

Skrypty tworzące słowniki na podstawie danych o użytkowniku

- Bazy login:hasło sprzedawane na czarnym rynku

1. 123456	18. 1qaz2wsx
2. qwerty	19. 1234567
3. 12345	20. qwerty123
4. 123456789	21. qwerty1
5. zaq12wsx	22. 123123
6. 1234	23. 0
7. 12345678	24. bartek
8. polska	25. damian
9. 111111	26. michal
10. misiek	27. qwe123
11. monika	28. polska1
12. 123	29. password
13. marcin	30. karolina
14. mateusz	31. kacper
15. agnieszka	32. maciek
16. 123qwe	33. samsung
17. 1234567890	34. qwertyuiop

Polityka haseł

- zasady utrudniające wykradanie i łamanie haseł
- przydatne dla administratorów systemów i zespołów bezpieczeństwa
- wskazówki dla użytkowników

Polityka haseł

Stare zasady:

- mała litera
- duża litera
- cyfra
- znak specjalny
- wyraz nie ze słownika (rzadko wymuszane)
- ...
- i zmieniaj co miesiąc

Matematycznie: ma sens

W praktyce: **wykształca złe nawyki i w efekcie zmniejsza bezpieczeństwo**

Polityka haseł

Stare zasady:

Założenia: **K;CLiR=)ZRDt**

Polityka haseł

Stare zasady:

Założenia: **K;CLiR=)ZRDt**

Rzeczywistość: **Misiaczek11!**

(oba spełniają warunki)

Polityka haseł

Stare zasady:

Założenia: **K;CLiR=)ZRDt**

Rzeczywistość: **Misiaczek11!**

(oba spełniają warunki)

Ludzie są fatalni w tworzeniu dobrych haseł

Trzeba im w tym pomóc

Polityka haseł – nowoczesne podejście

Sensowne rekomendacje:

(FBI, NIST 800-63-3, CERT Polska – zebranie i analiza dostępnych rekomendacji)

SP 800-63-3

Digital Identity Guidelines

Date Published: June 2017 (includes updates as of 03-02-2020)

Supersedes: SP 800-63-3 (12/01/2017)

Author(s)

Paul Grassi (NIST), Michael Garcia (NIST), James Fenton (Altmode Networks)

Abstract

These guidelines provide technical requirements for federal agencies implementing digital identity services and are not intended to constrain the development or use of standards outside of this purpose. The guidelines cover identity proofing and authentication of users (such as employees, contractors, or private individuals) interacting with government IT systems over open networks. They define technical requirements in each of the areas of identity proofing, registration, authenticators, management processes, authentication protocols, federation, and related assertions. This publication supersedes NIST Special Publication 800-63-2.

Keywords

authentication; ; authentication assurance; ; authenticator; ; assertions; ; credential service provider; ; digital authentication; ; digital credentials; ; identity proofing; ; federation; ; passwords; ; PKI

Control Families

None selected

Polityka haseł – nowoczesne podejście

- Nie wymuszamy okresowej zmiany haseł

- Zazwyczaj zmienia się pojedynczy znak z poprzedniego hasła
- Przewidywalne schematy
- Mało kto jest w stanie wymyślić i zapamiętać unikalne, silne hasło co miesiąc – pokusa zapisania hasła gdzieś albo ustawienia słabego
- Albo zapominamy – dostępność jest też elementem bezpieczeństwa, warto unikać blokowania pracowników bez powodu

Haslo!202306

Polityka haseł – nowoczesne podejście

- Nie wymuszamy okresowej zmiany haseł
- Sprawdzamy z listą najpopularniejszych haseł (niektóre strony i przeglądarki już oferują taką usługę)

Nie pozwalamy na użycie:

- listy słabych i często używanych haseł
- przewidywalne człony (nazwa firmy, usługi, imiona)

Polityka haseł – nowoczesne podejście

- Nie wymuszamy okresowej zmiany haseł
- Sprawdzamy z listą najpopularniejszych haseł (niektóre strony i przeglądarki już oferują taką usługę)
- Minimalna długość hasła – 12 znaków (i limit długości nie mniejszy niż 64 znaki)
- Rekomenduje się używanie dłuższych *niż* 12 znaków
- Krótkie hasła są łamane rutynowo, wystarczy komputer z dobrą kartą graficzną
- Przykład: wyciek z pewnego sklepu ok. 2 mln haseł; po miesiącu ok. 350 tys. złamanych i dostępnych w sieci; sporo z nich 9 znaków lub mniej

WPA Benchmark

Hashmode: 2500 - WPA-EAPOL-PBKDF2 294.8

GPU	Hashes/s
RTX 3090	1065.9 k
RTX 2080 ti	744.9 k
RTX 2080	571.4 k
RTX 2060	370.7 k
GTX 1070 (L)	334.2 k
GTX 1660 SUPER	294.8 k
GTX 1060	223.2 k

Polityka haseł – nowoczesne podejście

- Nie wymuszamy okresowej zmiany haseł
- Sprawdzamy z listą najpopularniejszych haseł (niektóre strony i przeglądarki już oferują taką usługę)
- Minimalna długość hasła – 12 znaków (i limit długości nie mniejszy niż 64 znaki)
- Nie wymuszamy stosowania wzorów, złożoności itp. (ale pozwalamy na ich stosowanie – warto, żeby hasło je miało)

To samo co wcześniej:

- przewidywalne schematy

Misiaczek11!

Polityka haseł – nowoczesne podejście

- Nie wymuszamy okresowej zmiany haseł
- Sprawdzamy z listą najpopularniejszych haseł (niektóre strony i przeglądarki już oferują taką usługę)
- Minimalna długość hasła – 12 znaków (i limit długości nie mniejszy niż 64 znaki)
- Nie wymuszamy stosowania wzorów, złożoności itp. (ale pozwalamy na ich stosowanie – warto, żeby hasło je miało)
- Nie blokujemy funkcji wklejania hasła (menedżery haseł, kopiuj-wklej)

Blokada uniemożliwia korzystanie z narzędzi do bezpiecznego przechowywania haseł

Polityka haseł – nowoczesne podejście

Coraz rzadziej spotykane, ale:

- Nie stosujemy i nie korzystamy z podpowiedzi albo zamkniętych list pytań

(odpowiedzi bardzo łatwo można znaleźć, a użytkownicy są bardzo źli w tworzeniu dobrych pytań i podpowiedzi...)

No dobrze, a w praktyce?

Co to znaczy dobre hasło?

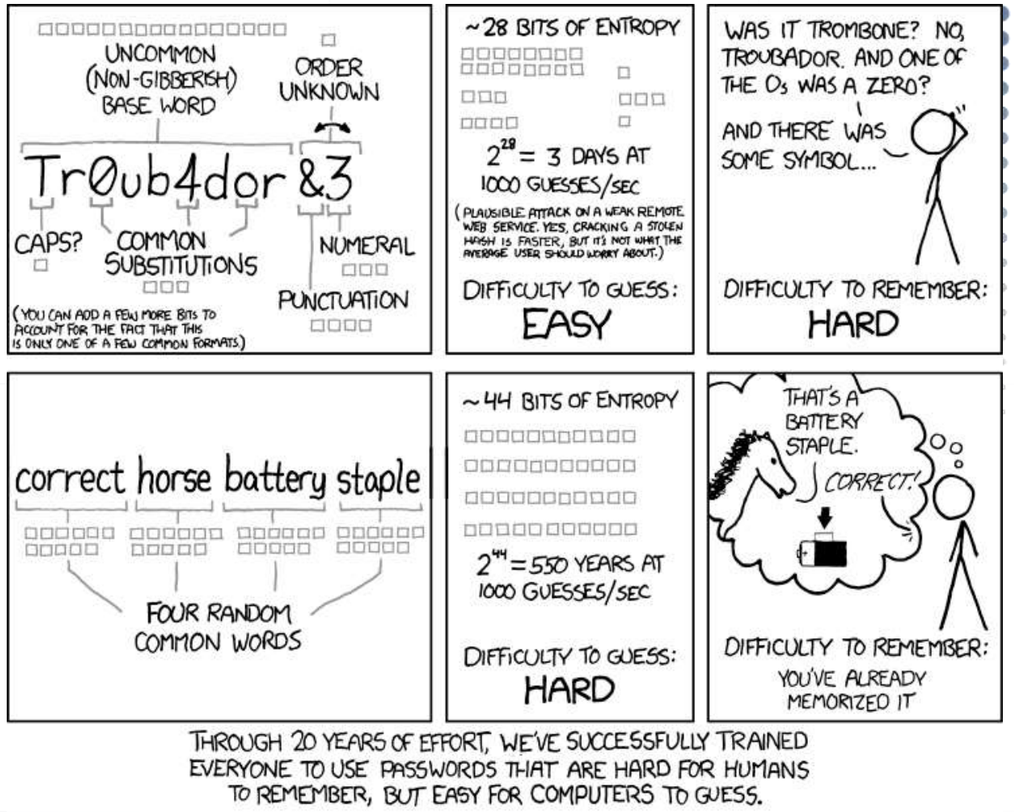
Stosuj długie hasła, co najmniej 14 znaków.

Dobrą metodą na długie hasło jest wymyślenie całej frazy, składającej się z kilku słów, np.

zyrafy-wchodza-do-szafy

2CzerwoneRoweryJedzaNalesniki

- minimum 4 losowe wyrazy
- obecnie rekomendowane jest co najmniej 5-6 wyrazów
- krytyczne dane i zasoby – 8 wyrazów



Co to znaczy dobre hasło?

Unikaj haseł, **które łatwo powiązać z publicznymi informacjami na temat Twojej osoby**:

- imię, nazwisko, adres, data urodzenia
- imię kota albo dziecka też nie

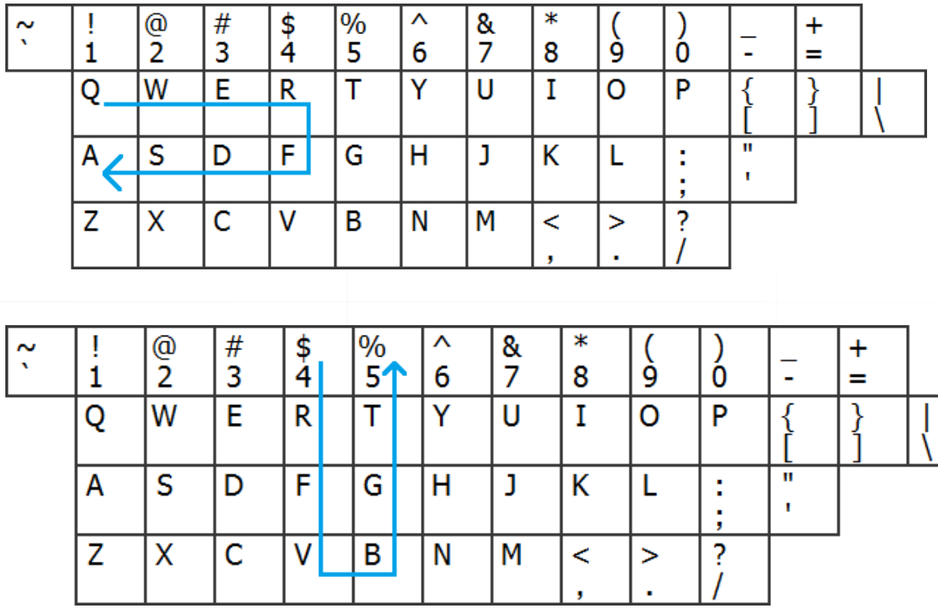
Nie używamy słów ze słownika (jedno lub dwa słowa):

- haslo
- mojehaslo

Nie tworzymy według schematów:

- hasloczerwiec2023
- haslo1!

Także: bez wzorów na klawiaturze!



Twórz unikalne hasła

E-mail

mojehaslo1

Facebook

mojehaslo1

- **Przepisykulinarne.pl**
  - mojehaslo1

Używaj niepowtarzalnego hasła do każdego konta/urządzenia.

- **W szczególności do e-maila, banku i innych wrażliwych kont.**

Jeżeli Twoje hasło zostanie złamane, przestępcy na pewno sprawdzą je na innych Twoich kontach i urządzeniach.

Aby ułatwić sobie „zapamiętanie" tych wielu haseł **korzystaj z menedżerów haseł**!

Menedżery haseł

Do dyspozycji jest wiele różnych rodzajów menedżerów, **wybór zależy od osobistych preferencji i wygody**. Można wybrać np. menedżer z plikiem z hasłami na urządzeniu, albo taki z hasłami „w chmurze".

Przy wyborze menedżera warto wziąć pod uwagę:

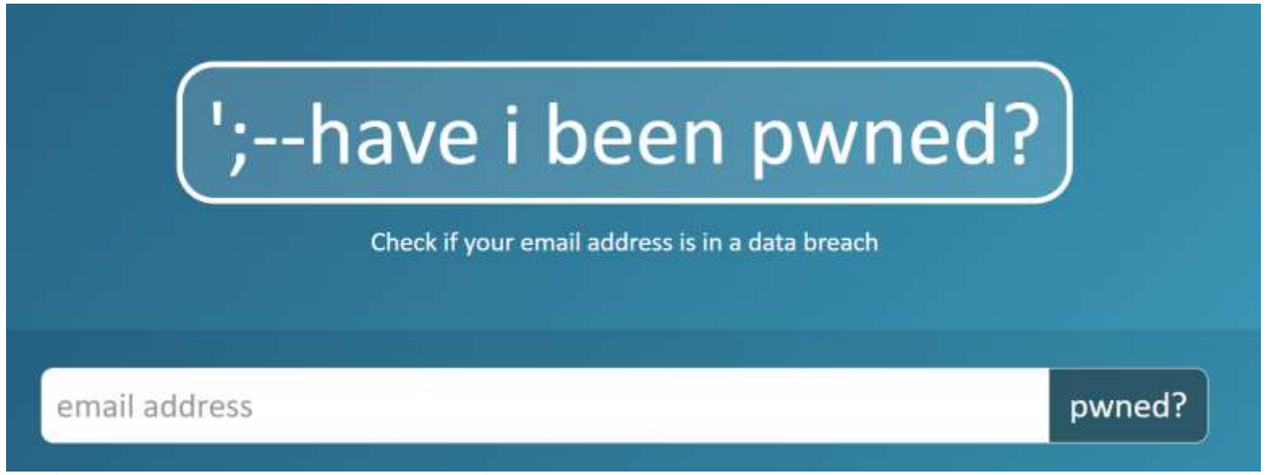
- czy korzystamy z kont na wielu urządzeniach;
- czy korzystamy z kont na wielu systemach;
- czy jesteśmy skłonni kopiować plik z hasłami ręcznie.

Menedżery wbudowane w przeglądarkę czy telefon są wygodne, bezpieczne i proste w użyciu.

Źródło: strony internetowe producentów

Bezpieczeństwo haseł

- Hasło należy zmienić wtedy, gdy **mamy podejrzenie, że mogła poznać je inna osoba, lub gdy wyciekło**.
- Nie ma potrzeby cyklicznej zmiany hasła.
- Na stronie haveibeenpwned.com można sprawdzić, czy nasz mail znalazł się w wycieku danych.
- **W takim przypadku należy zmienić wszystkie hasła powiązane z tym adresem mailowym.**



Bezpieczeństwo haseł – inne zasady

- **Nie zapisuj haseł na karteczkach** i nie przyklejaj na komputerze czy pod biurkiem ☺

- **Nie wpisuj danych logowania**, w tym haseł, **na niezaufanych stronach i urządzeniach!**

Bezpieczeństwo haseł – inne zasady

- **Nie zapisuj haseł na karteczkach** i nie przyklejaj na komputerze czy pod biurkiem ☺

- **Nie wpisuj danych logowania**, w tym haseł, **na niezaufanych stronach i urządzeniach!**

NIGDY

Uwierzytelnienie dwuskładnikowe (2FA)

Uwierzytelnianie dwuskładnikowe należy włączyć wszędzie tam, gdzie jest to możliwe.

W poczcie elektronicznej i w **mediach społecznościowych** 2FA jest konieczne!

Jeżeli obecny dostawca Twojej poczty nie udostępnia uwierzytelniania dwuskładnikowego, zmień go.

2FA **uniemożliwia atakującemu, który pozyskał nasz login i hasło, uwierzytelnienie się w usłudze** bez znajomości również drugiego składnika!

dlatego...

Twoje hasło nie ma żadnego znaczenia

– Microsoft

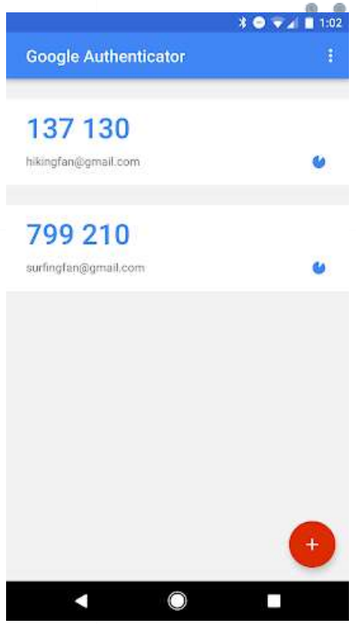
Uwierzytelnienie dwuskładnikowe

Biorąc pod uwagę wyniki badań i zapisy prób włamań na konta do usług Microsoft (Azure Active Directory, Active Directory, konta Microsoft online), **jeżeli użytkownik stosuje dwuskładnikowe uwierzytelnianie, prawdopodobieństwo przejęcia jego konta spada o 99,9%**

Używaj drugiego składnika gdzie się da!

https://techcommunity.microsoft.com/t5/microsoft-entra-azure-ad-blog/your-pa-word-doesn-t-matter/ba-p/731984

Twoje hasło nie ma żadnego znaczenia, ale uwierzytelnianie wieloskładnikowe ma!



Demo:
konto pocztowe ze znanymi danymi logowania

login: **szkolenie509@gmail.com**
hasło: **znanehaslo111**

Uwierzytelnienie dwuskładnikowe (2FA)

„Coś, co posiadasz”

Najlepszym drugim składnikiem uwierzytelniania i jedynym odpornym na ataki phishingowe **jest token sprzętowy U2F** (np. YubiKey).

https://www.yubico.com/blog/

Inne metody – biometria

„Coś, czym jesteś”

- W środowisku **nasyconym przez monitoring i wiele par oczu dużo bezpieczniejsza** niż hasło czy pin**.**
- Technologia ta jest dojrzała i bezpieczna na nowych urządzeniach.
- Nie wszędzie jest to dobre rozwiązanie (nie jest polecane do chronienia szczególnie istotnych informacji).

https://pixabay.com/pl/photos/bezpiecze%c5%84stwa-w-miejscu-pracy-kamery-2427499/

Inne metody – dostawcy tożsamości

- **Jedna usługa zarządzająca tożsamościami**, która udostępnia uwierzytelnianie użytkowników w innych usługach.
- Tylko **jedno hasło** do uzyskania dostępu **do wielu usług**.
- Odpowiednik w środowisku korporacyjnym – SSO (*single sign-on*), pojedyncze logowanie.
- Zmniejszona liczba logowań – **aplikacje „pamiętają” uwierzytelnienie**, więc konieczność powtórnego logowania może być ostrzeżeniem przed phishingiem.
- Problematyczna w przypadku zablokowania („zbanowania”) konta u dostawcy tożsamości.

Cyberhigiena

– czyli bezpieczne usługi cyfrowe

(CYBER)SZKOLENIA
KRAJOWY SYSTEM CYBERBEZPIECZEŃSTWA

Ministerstwo Cyfryzacji

NASK

Cyberhigiena

- podstawowe zasady bezpieczeństwa
- zebranie i przypomnienie zasad

Oddzielaj sprawy służbowe od prywatnych

Pocztę, serwisy społecznościowe i inne.

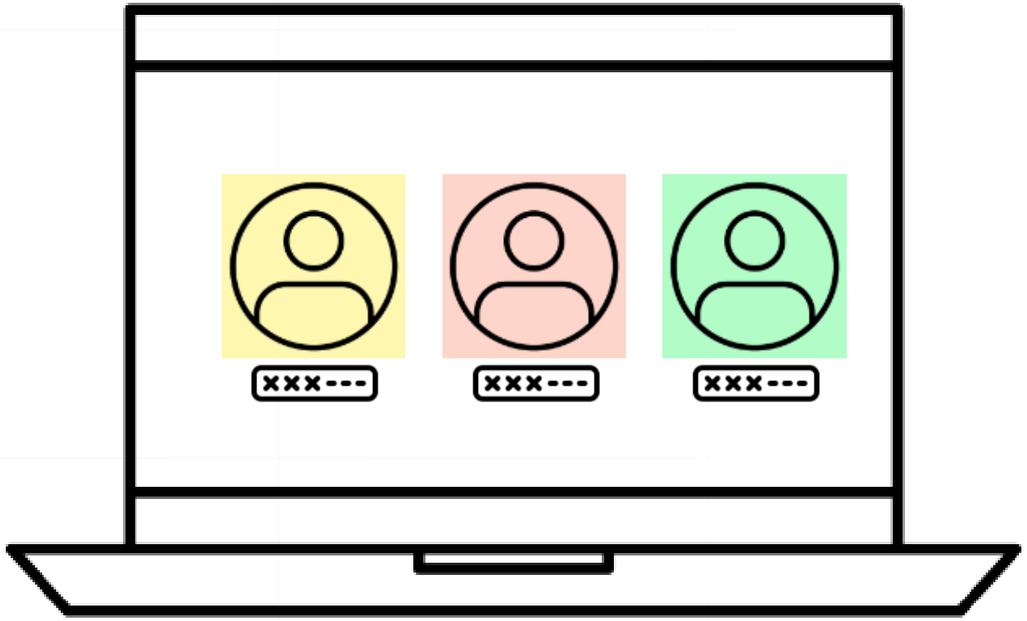
Dotyczy to również **wykorzystywanych urządzeń**, czyli:

- **Prywatne** konta poczty elektronicznej i komunikatory służą wyłącznie **do korespondencji prywatnej.**
- **Prywatne** komputery i telefony służą wyłącznie **do użytku prywatnego**
- **Służbowe** komputery i telefony, poczta i konta w portalach społecznościowych służą wyłącznie **do spraw służbowych,** nie udostępniaj ich członkom rodziny.

Konta użytkowników

Utwórz odrębne konta dla każdego z użytkowników komputera – w innym przypadku wiele pozostałych zasad bezpieczeństwa nie będzie miała zastosowania.

- Jeden użytkownik = **jedno konto na komputerze**
- **Jedno urządzenie mobilne** = jeden użytkownik
  (Na urządzeniach mobilnych stworzenie kont jest niedostępne lub utrudnione).



https://thenounproject.com/

Ochrona przez wirusami

Regularnie instaluj **aktualizacje systemu operacyjnego i programów** na używanym komputerze.

- Najlepiej włącz (albo pozostaw włączone) automatyczne aktualizacje.

Posiadaj **aktualny program antywirusowy**

- znany – w sieci dostępne są rankingi.

Instaluj **oprogramowanie tylko z zaufanych źródeł**, są to strony producenta lub dedykowane systemom oficjalne sklepy.

Bezpieczeństwo nośników pamięci

Korzystaj tylko z zaufanych nośników pamięci.

- Szczególnie USB – pendrive, dysk zewnętrzny.

Urządzenia USB przyczyną cyberataku na szpitale

27 czerwca, 2023

Jak doszło do infekcji?

Po powrocie z azjatyckiej konferencji jeden z pracowników szpitala użył pamięć USB na jednym ze służbowych komputerów, co doprowadziło do rozprzestrzenienia się infekcji na całą sieć szpitala.

Źródło: https://avlab.pl/urzadzenia-usb-przyczyna-cyberataku-na-szpitale/

Bezpieczeństwo nośników pamięci

Szyfruj urządzenia.

- Dyski zewnętrzne, pamięci USB,
- ale też dysk komputera i smartfon.

Fot. Ervins Strauhmanis

Logowanie, uwierzytelnianie i hasła

Logując się na konto wybranego serwisu zawsze sprawdź **czy domena danego portalu jest prawidłowa**.

Domena to nazwa zawierająca się między ***https://***, a pierwszym kolejnym znakiem **/**.

https://mojbamk.pl/

https://mojbank.pl.shady-hosting.online/

Bezpieczeństwo komunikacji i informacji

W korespondencji elektronicznej najbardziej należy uważać na:

zagrożenie złośliwym oprogramowaniem!

zagrożenie phishingiem!

Wiadomości zawierające załączniki, a zwłaszcza:

- archiwa i obrazy dysków (.zip, .rar, .iso, .img)
- pliki wykonywalne (.exe, .com, .js, .vbs)
- dokumenty Office z hasłem podanym w treści wiadomości (.xls, .xlsx, .xlsm, .doc, .docx, .one)

Wiadomości nakłaniające do natychmiastowej reakcji

Ignoruj wszystkie prośby o podanie swojego hasła, nawet jeżeli komunikat wygląda oficjalnie, wymaga natychmiastowej reakcji i grozi dezaktywacją konta.

Bezpieczeństwo komunikacji i informacji

Do wrażliwej prywatnej komunikacji używaj **komunikatorów szyfrowanych end-to-end**, np. Signala.

Rozważ włączenie opcji **automatycznego kasowania wiadomości** po upływie określonego czasu.

Usuwaj archiwalne wiadomości ze skrzynki odbiorczej oraz wysłanych.

Nie da się ukraść czegoś, czego już nie ma.

Komunikatory – co brać pod uwagę

poufność danych

szyfrowanie e2e

szyfrowanie serwer-użytkownik

Komunikatory – co brać pod uwagę

poufność danych

szyfrowanie e2e

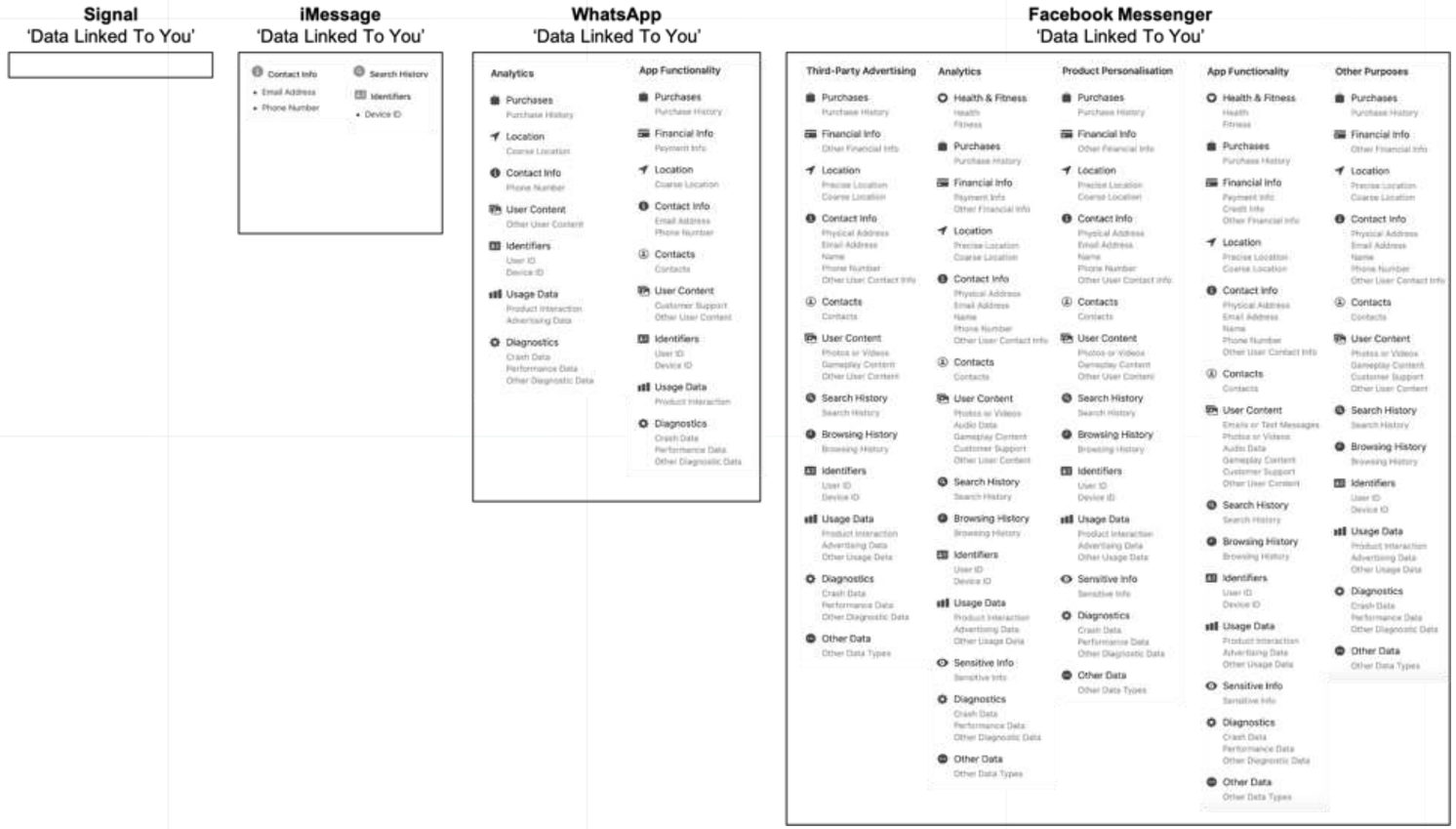
szyfrowanie serwer-użytkownik

dane osobowe i metadane

prywatność użytkowników

kto kontroluje serwer i może je zbierać

Komunikatory: poufność ≠ prywatność



https://www.forbes.com/sites/zakdoffman/2021/01/03/whatsapp-beaten-by-apples-new-imessage-update-for-iphone-users/

Komunikatory – co brać pod uwagę

poufność danych

szyfrowanie e2e

szyfrowanie serwer-użytkownik

dane osobowe i metadane

kto jest właścicielem i kto kontroluje serwer

bezpieczeństwo prawne

twórca komunikatora

finansowanie

jurysdykcja

Komunikatory – co brać pod uwagę

poufność danych

szyfrowanie e2e

szyfrowanie serwer-użytkownik

dane osobowe i metadane

kto jest właścicielem i kto kontroluje serwer

bezpieczeństwo prawne

twórca komunikatora

finansowanie

jurysdykcja

audyt kodu

czy był przeprowadzany

kiedy był przeprowadzany

Komunikatory – co brać pod uwagę

poufność danych

szyfrowanie e2e

szyfrowanie serwer-użytkownik

dane osobowe i metadane

kto jest właścicielem i kto kontroluje serwer

bezpieczeństwo prawne

twórca komunikatora

finansowanie

jurysdykcja

audyt kodu

czy był przeprowadzany

kiedy był przeprowadzany

koszty

rozwiązania open source wcale nie muszą być najtańszymi

Bezpieczeństwo komunikacji i informacji

VPN nie chroni przed atakami phishingowymi i złośliwym oprogramowaniem!

brama VPN ≠ VPN komercyjny

(CYBER)SZKOLENIA
KRAJOWY SYSTEM CYBERBEZPIECZEŃSTWA

Ministerstwo Cyfryzacji

NASK

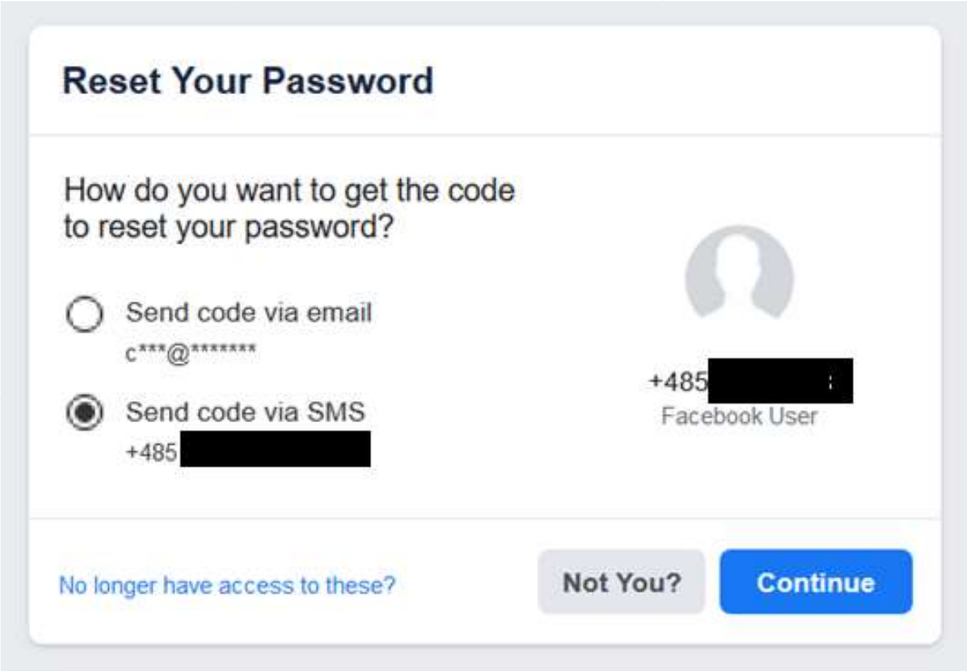
Bezpieczeństwo komunikacji i informacji

W miejscach publicznych **korzystaj z filtrów ekranowych.**

Nigdy **nie zostawiaj sprzętu niepilnowanego** w miejscu publicznym.

Jeśli przemieszczasz się z laptopem, wyłącz go lub „hibernuj”.

Konta pocztowe i społecznościowe



Przygotuj się na ewentualne włamanie.

- **Zweryfikuj swoje dane kontaktowe** podane w ustawieniach profilu poczty elektronicznej i mediów społecznościowych.

  Poprawna alternatywna metoda kontaktu ułatwi odzyskanie konta w przypadku jego utraty.

- Jeżeli podejrzewasz, że ktoś włamał się na twoje konto, **zmień hasło**, sprawdź dostępną w profilu **historię logowania i zakończ wszystkie aktywne sesje.**

(CYBER)SZKOLENIA
KRAJOWY SYSTEM CYBERBEZPIECZEŃSTWA

Podstawowe zasady cyberhigieny w pracy i w życiu prywatnym

Zespół Szkoleń i Ćwiczeń Cyberbezpieczeństwa

zbsc@nask.pl

Ministerstwo Cyfryzacji

NASK