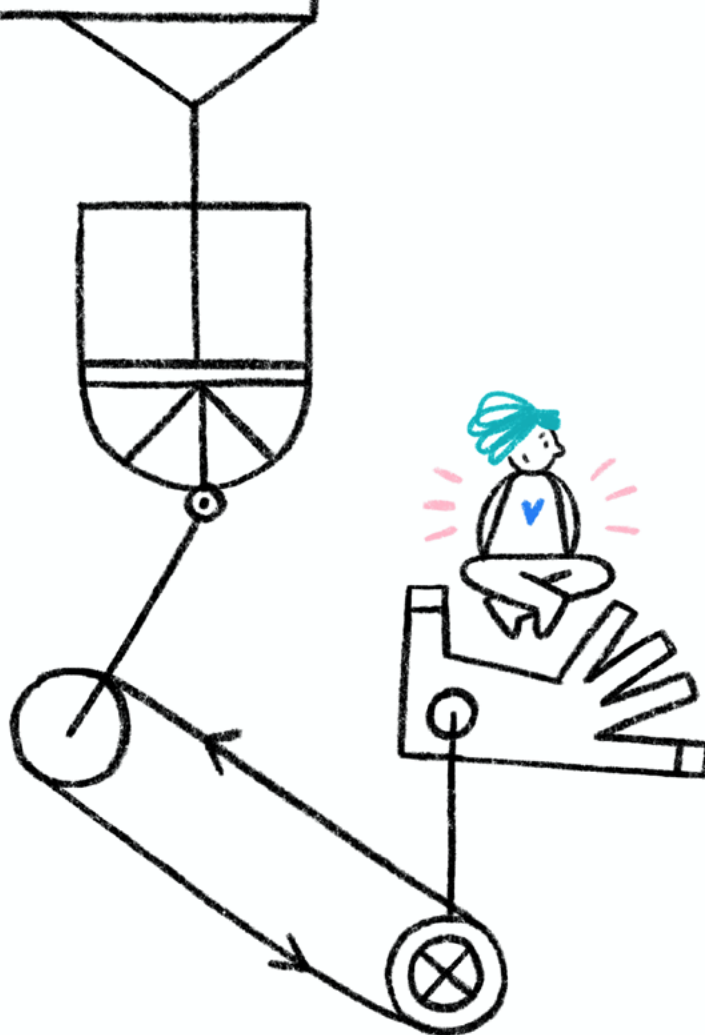


BEZPIECZEŃSTWO

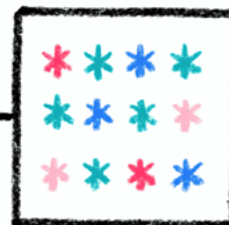
UŻYTKOWNIKŌW_UŻYTKOWNICZEK

W INTERNECIE



AUTOR:

Michał
Gapiński



SILNE HASŁA I MENEDŻERY HASEŁ

- > Używaj długich, unikalnych haseł dla każdej usługi. Najlepiej sprawdzają się hasła-frazy o długości 16 – 20 znaków. Ogólna zasada: im dłuższe, tym lepsze (nie bój się używać haseł nawet 32 znakowych).
- > Dobre hasło powinno zawierać między innymi znaki specjalne, np.: #, @, ! itd.
- > Twórz łatwe do zapamiętania frazy – składające się z minimum 3 słów (np. „ZielonyTraktorLata”)
- > Warto jednak dodatkowo zabezpieczyć te hasła dodając znaki specjalne zamiast liter np. dla frazy „ZielonyTraktorLata” można zrobić „Z!3l0nyTr@ktOrL@t@” – to dodatkowo wzmocni siłę hasła
- > Nie twórz tych samych haseł w wielu usługach – wyciek jednego serwisu naraża inne konta.
- > Korzystaj z menedżerów haseł: KeePassXC (<https://keepassxc.org>), Bitwarden (<https://bitwarden.com>).
- > Do tworzenia haseł możesz korzystać z menedżerów haseł lub osobnych generatorów haseł: <https://bitwarden.com/password-generator/>



2FA / MFA – DRUGA LINIA OBRONY

- > Włącz uwierzytelnianie wieloskładnikowe (2FA/MFA) wszędzie tam, gdzie jest to możliwe – coraz więcej portali społecznościowych i nie tylko wspiera tę funkcjonalność.
- > Najlepsze metody: aplikacje Microsoft Authenticator, Google Authenticator oraz/lub klucze sprzętowe (np. YubiKey).
- > Ochrona z wykorzystaniem SMSa jest lepszy niż brak ochrony, lecz jeśli masz wybór, to stosuj aplikację a jeszcze lepiej klucz sprzętowy – jest najbardziej odporny na ataki phishingowe.



CZY MOJE DANE WYCIĘŁY?

> Sprawdź adres e-mail w serwisie Have I Been Pwned:

<https://haveibeenpwned.com>

> Jeżeli konto pojawiło się w wycieku: zmień hasło, włącz MFA, sprawdź inne konta używające podobnego hasła i zmień je.



PHISHING - NAJCZĘSTSZE OSZUSTWO

> Phishing polega na podszywaniu się pod bank, firmę, kuriera, urząd lub znajomego wykorzystując przy tym jako formę komunikacji SMS, rozmowę głosową, mail czy różnego rodzaju komunikatory takie jak Messenger, WhatsApp, Telegram i wiele, wiele innych.

> Sygnały ostrzegawcze w komunikatach: presja czasu, groźby, duża nagroda, literówki lub niewłaściwy styl (zbyt idealny, oficjalny etc.) osoby, którą znasz, podejrzane linki, prośba o hasło lub kod do aplikacji uwierzytelniającej.

> Nie loguj się przez link z wiadomości – wpisz adres ręcznie w przeglądarce.

> Na tyle, na ile to możliwe zweryfikuj 'twarzą w twarz' lub inną metodą komunikacji (inną niż ta, która została użyta przez podejrzanego nadawcę) czy dana wiadomość pochodzi od określonej osoby (w przypadku osób Ci nieznanych, wyszukaj oficjalne telefony lub maile i skontaktuj się z daną organizacją)



KODY QR I SKRÓCONE LINKI

> Uważaj na nieznane kody QR, gdyż mogą prowadzić do fałszywych stron, np. w celu wyłudzenia Twoich danych logowania (quishing).

> Zanim zeskanujesz, przeanalizuj kod QR lub barcode:

<https://online-barcode-reader.inliteresearch.com/>

> Przed kliknięciem skróconego linku sprawdź jego przekierowanie w <https://urlscan.io/>





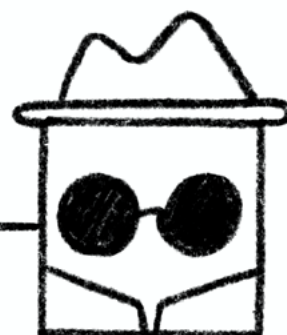
WERYFIKACJA LINKÓW, PLIKÓW, ADRESÓW IP I DOMEN

- > Zanim klikniesz link sprawdź go – skopiuj i wklej na stronie <https://urlscan.io>
- > Dokonaj analiza podejrzanych plików i adresów stron internetowych również i tutaj: <https://virustotal.com>
- > Sprawdź reputację domeny: <https://transparencyreport.google.com/safe-browsing/search> oraz <https://www.urlvoid.com>
- > Przydatne informacje o domenie np. jak długo istnieje i gdzie jest hostowana: <https://whois.domaintools.com> (zwróć uwagę czy nie istnieje np. tylko kilka dni lub nie jest hostowana w Chinach a podszywa się pod polską)
- > Reputacja i podgląd adresu IP danej domeny: <https://www.abuseipdb.com>



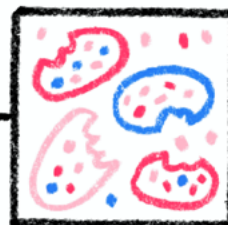
BEZPIECZEŃSTWO POCZTY E-MAIL

- > Zawsze sprawdzaj pełny adres nadawcy – nazwa wyświetlana może wprowadzać w błąd.
- > Kontroluj ustawienia skrzynki: przekierowania, automatyczne reguły, filtry.
- > Nagłówki wiadomości pomagają ustalić faktycznego nadawcę.
- > Sprawdzanie adresu e-mail: <https://emailable.com/email-verifier/>
- > Narzędzia do badania nagłówków wiadomości e-mail: <https://toolbox.googleapps.com/apps/messageheader/> oraz <https://mxtoolbox.com/EmailHeaders.aspx>



TRYB INCOGNITO – ZALETY I WADY

- > Jeśli chcesz ograniczyć jeszcze bardziej użycie plików cookies, używaj trybu incognito
- > Tryb incognito po zamknięciu okna usuwa lokalną historię oraz pliki cookies utworzone w czasie sesji incognito, co zwiększa Twoją prywatność w sieci.
- > Nie daje jednak anonimowości względem stron internetowych, sieci pracodawcy, ani dostawcy Internetu, z którego korzystasz.



PRYWATNOŚĆ I ŚLEDZENIE

- > Wiele stron śledzi zachowanie użytkowników za pomocą tak zwanych trackerów i plików cookies.
- > Zaczynij korzystać z przeglądarek blokujących trackery i nadmiarowe pliki cookies: najlepiej Brave (<https://brave.com/download/>), jako zapasową możesz użyć DuckDuckGo <https://duckduckgo.com>
- > Wyszukiwarki nastawione na prywatność: <https://search.brave.com/> lub <https://duckduckgo.com/>.
- > Wyłączenie spersonalizowanych reklam w Google: <https://myadcenter.google.com/personalizationoff?sasb=true&ref=ad-settings>
- > Test prywatności przeglądarek (przetestuj na kilku przeglądarkach, aby przekonać się czy dana przeglądarka chroni Twoją prywatność w sieci): <https://coveryourtracks.eff.org/>



FAKE NEWS ORAZ DEEPPFAKE

- > Weryfikacja informacji: <https://demagog.org.pl> oraz <https://fakenews.pl>
- > Weryfikacja deepfake wideo lub obrazu: <https://scanner.deepware.ai>
- > Wyszukiwanie źródła obrazu: <https://tineye.com/>
- > Weryfikacja czy dane konto jest botem (jeśli nie widać konta, nie oznacza to, że nie jest botem): <https://botometer.osome.iu.edu>

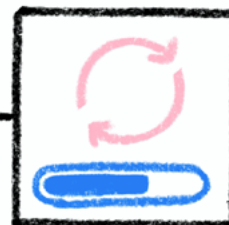


OSINT – CO WIDAĆ O MNIE W SIECI?

- > Sprawdź własny ślad cyfrowy i publiczne informacje.
- > Meta-narzędzia (tak zwane 'frameworki'): <https://osintframework.com>, <https://otwarteźrodla.pl/>,
- > Narzędzie do analizy nazwy użytkownika: <https://whatsmyname.app/>



AKTUALIZACJE I URZĄDZENIA



- > Regularnie aktualizuj system, przeglądarkę i aplikacje.
- > Sprawdzenie bezpieczeństwa przeglądarki: <https://checkcybersecurity.service.ncsc.gov.uk/browser-check>
- > Zabezpiecz telefon i komputer silnym hasłem a tam, gdzie to możliwe również biometrią i dodatkowym składnikiem uwierzytelnienia



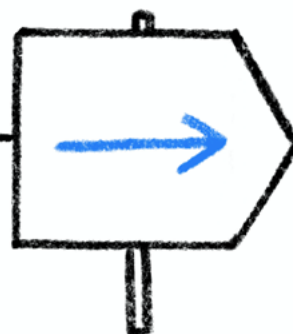
CO ZROBIĆ PO PRZEJĘCIU KONTA



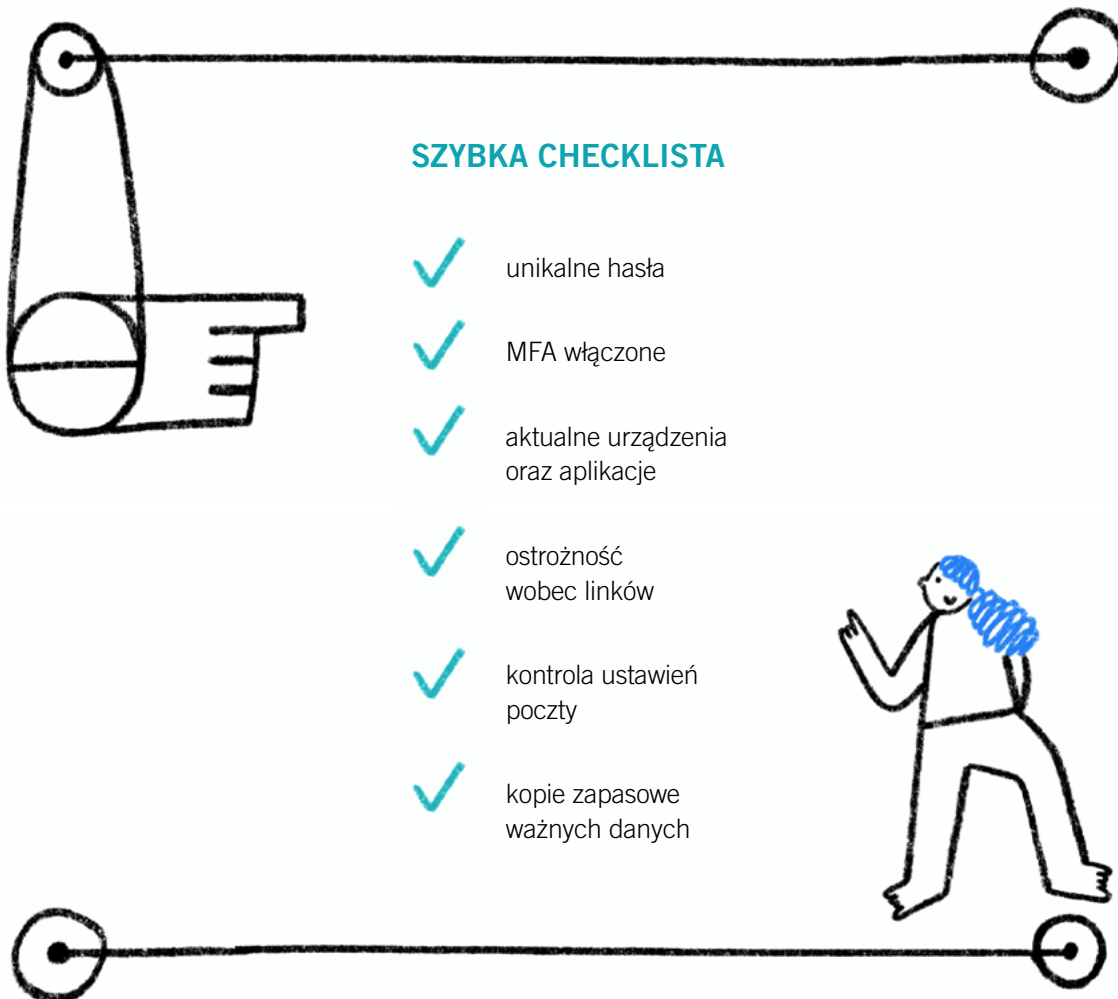
- > Zmień hasło.
- > Wyloguj wszystkie aktywne sesje.
- > Włącz MFA/2FA, jeśli nie masz włączonego
- > Jeśli to konto firmowe lub szkolne, poinformuj osoby zajmujące się ochroną danych osobowych
- > Sprawdź dane odzyskiwania konta – jeśli to możliwe, zwiększ ich wymagania
- > Ostrzeż osoby z otoczenia, aby wiedziały, że ktoś może próbować się podszyć pod Ciebie.



GDZIE SZUKAĆ POMOCY

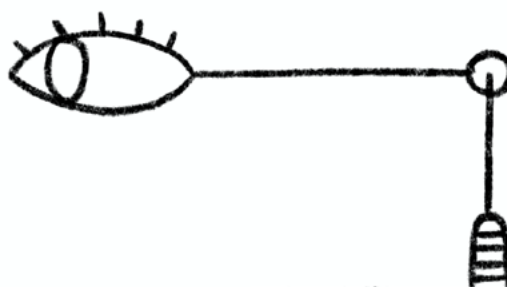


- > CERT Polska <https://www.cert.pl/> – zgłaszanie incydentów bezpieczeństwa.
- > Policja – groźby, stalking, oszustwa.
- > Operator usługi (np. Google, Meta, Microsoft) – odzyskiwanie konta.
- > Organizacje pomocowe wspierające osoby doświadczające przemocy online, np. <https://fdds.pl>, <https://dyzurnet.pl>, <https://cpk.org.pl>, <https://www.niebieskalinia.pl>, <https://116111.pl>, <https://www.rpo.gov.pl>



SZYBKA CHECKLISTA

- ✓ unikalne hasła
- ✓ MFA włączone
- ✓ aktualne urządzenia oraz aplikacje
- ✓ ostrożność wobec linków
- ✓ kontrola ustawień poczty
- ✓ kopie zapasowe ważnych danych



Sfinansowane ze środków UE. Wyrażone poglądy i opinie są jedynie opiniami autora lub autorów i niekoniecznie odzwierciedlają poglądy i opinie Unii Europejskiej lub Komisji Europejskiej. Unia Europejska ani organ przyznający nie ponoszą za nie odpowiedzialności.



**Finansowane przez
Unię Europejską**

Materiał powstał w projekcie *Algorytmy bez uprzedzeń – wzmacnianie praw mniejszości w sieci*.