CYBERSHIELD–
WZMOCNIENIE KOMPETENCJI POLICJI
W ZAKRESIE ZWALCZANIA
CYBERPRZESTĘPCZOŚCI

POLICJA
MAZOWSZE

CYBERSHIELD:

TWOJA TARCZA W SIECI

Praktyczny zbiór zasad bezpiecznego internetu, cyberhigieny i ochrony tożsamości.

„CyberShield – wzmocnienie kompetencji Policji w zakresie zwalczania cyberprzestępczości”. Projekt jest współfinansowany ze środków Unii Europejskiej z Programu Fundusz Bezpieczeństwa Wewnętrznego na lata 2021-2027.

Materiał opracowany zgodnie z wytycznymi Ustawy o Krajowym Systemie Cyberbezpieczeństwa oraz rekomendacjami NASK i CERT Polska.

Fundusze Europejskie na Migracje, Granice i Bezpieczeństwo
Rzeczpospolita Polska
Dofinansowane przez Unię Europejską

WSTĘP
I MAPA TREŚCI

Internet to przestrzeń nieograniczonych możliwości, ale i realnych zagrożeń. Projekt Cybershield powstał, aby dostarczyć konkretnych narzędzi i nawyków, które zmienią Twoje urządzenia w twierdzę.

Treść e-booka oparta jest na oficjalnych standardach bezpieczeństwa państwowego i międzynarodowego, przekładając skomplikowane przepisy na język praktycznych działań.

SPIS TREŚCI (PLAN TWOJEJ OCHRONY):

TWIERDZA HASŁO
– TWOJA PIERWSZA LINIA OBRONY

DŁUGOŚĆ ZAMIAST SKOMPLIKOWANIA:

Współczesne standardy (NIST) odchodzą od wymuszania znaków specjalnych na rzecz długości. Hasło składające się z 15-20 znaków tworzących łatwe do zapamiętania zdanie (np. MojaKawaPachnieO7Rano!) jest niemal niemożliwe do złamania metodą brute-force, a jednocześnie łatwiejsze do wpisania niż losowe X$z7!q.

ZASADA UNIKALNOŚCI:

Używanie tego samego hasła w wielu miejscach to „efekt domina”. Jeśli wycieknie Twoje hasło z mało bezpiecznego sklepu internetowego, hakerzy natychmiast sprawdzą je w bankach i na poczcie e-mail.

TWIERDZA HASŁO
– TWOJA PIERWSZA LINIA OBRONY

MENEDŻER HASEŁ JAKO STANDARD:

Pamięć ludzka jest zawodna. Używanie aplikacji - menedżerów pozwala na posiadanie setek unikalnych haseł, z których musisz pamiętać tylko jedno – główne.

KIEDY ZMIENIAĆ HASŁO?:

Zapomnij o zmienianiu haseł co 30 dni – to mit, który prowadzi do tworzenia słabych haseł. Zgodnie z zaleceniami NASK, hasło zmieniamy tylko w trzech przypadkach: gdy podejrzewasz wyciek danych, gdy serwis został zhakowany lub gdy przypadkiem podałeś hasło na podejrzanej stronie.

TWÓJ AUDYT HASEŁ
(Zrób to dzisiaj):

- [ ] Czy Twoje hasło do głównej poczty e-mail jest inne niż do pozostałych serwisów?
- [ ] Czy Twoje hasła mają co najmniej 12 znaków?
- [ ] Czy korzystasz z menedżera haseł zamiast zapisywania ich w przeglądarce?

TWIERDZA HASŁO
– TWOJA PIERWSZA LINIA OBRONY

CIEKAWOSTKA:

CZY WIESZ, ŻE...

Hakerzy korzystają z tzw. „tęczowych tablic” – gigantycznych baz danych zawierających miliardy już obliczonych skrótów popularnych haseł. Hasła takie jak „123456” czy „polska1” są łamane w ułamku sekundy, ponieważ znajdują się na samym początku każdej takiej listy.

ZŁOTA ZASADA:

Jeden uniwersalny klucz otwiera wszystkie drzwi – hakerowi też. Dbaj o unikalność: jedno konto, jeden unikalny klucz.

PODWÓJNY RYGIEL
– WERYFIKACJA DWUETAPOWA (MFA)

FUNDAMENT MFA (MULTI-FACTOR AUTHENTICATION):

To proces logowania wymagający dwóch z trzech składników: tego co wiesz (hasło), tego co masz (telefon, klucz USB) i tego kim jesteś (biometria – odcisk palca, skan twarzy).

DLACZEGO HASŁO TO ZA MAŁO?:

W dobie wycieków danych samo hasło to tylko połowa sukcesu. MFA sprawia, że nawet jeśli haker przejmie Twoje hasło, nie wejdzie na konto bez fizycznego dostępu do Twojego drugiego składnika.

METODY OD NAJSŁABSZEJ DO NAJMOCNIEJSZEJ:

- SMS (możliwy do przejęcia przez tzw. SIM-swap).
- Aplikacje autoryzujące – generują kody ważne tylko 30 sekund.
- Klucze sprzętowe U2F – fizyczne urządzenia, które całkowicie uodparniają na phishing.

PODWÓJNY RYGIEL
– WERYFIKACJA DWUETAPOWA (MFA)

ZŁOTA ZASADA:

W sieci samo „puk, puk” nie wystarczy – prawdziwe bezpieczeństwo wymaga okazania dwóch różnych dowodów tożsamości.

CIEKAWOSTKA:

Badania firmy Microsoft wykazały, że włączenie weryfikacji dwuetapowej blokuje do **99,9%** ataków polegających na przejęciu konta. To obecnie najskuteczniejszy darmowy sposób na podniesienie swojego bezpieczeństwa.

CZY WIESZ, ŻE...

PODWÓJNY RYGIEL
– WERYFIKACJA DWUETAPOWA (MFA)

KODY ZAPASOWE:

Przy włączaniu MFA system wygeneruje kody jednorazowe. Wydrukuj je na kartce papieru i schowaj w bezpiecznym miejscu – to Twój "klucz zapasowy", gdybyś zgubił telefon.

PLAN WDROŻENIA
(Twoja checklista):

- [ ] Włącz MFA na głównej skrzynce e-mail (to serce Twojego cyfrowego życia).
- [ ] Aktywuj MFA w mediach społecznościowych (Facebook, Instagram, LinkedIn).
- [ ] Pobierz i zapisz kody odzyskiwania dostępu.

CYFROWA TOŻSAMOŚĆ
– ŚWIADOMA OBECNOŚĆ W SOCIAL MEDIA

ZARZĄDZANIE PRYWATNOŚCIĄ:

Domyślne i standardowe ustawienia mediów społecznościowych zazwyczaj faworyzują publiczność, nie prywatność. Każdy portal (np. FB, IG, LinkedIn) posiada sekcję „Prywatność”, gdzie należy ograniczyć widoczność postów tylko do „Znajomych”.

OVERSHARING
– PUŁAPKA NADMIARU

Publikowanie zdjęć biletów, kart pokładowych (z kodami kreskowymi!), nowych dokumentów czy kluczy do mieszkania to gotowy scenariusz kradzieży tożsamości. Twoje dane osobowe są zaszyfrowane w kodach QR i kreskowych na zdjęciach.

CIEKAWOSTKA:

Internet nie zapomina. Zjawisko „cyfrowego śladu” oznacza, że nawet usunięte zdjęcia mogą przetrwać na serwerach archiwizujących sieć lub w zrzutach ekranu innych osób. Twoja dzisiejsza aktywność buduje Twój wizerunek w oczach przyszłych pracodawców przez lata.

CZY WIESZ, ŻE...

CYFROWA TOŻSAMOŚĆ
– ŚWIADOMA OBECNOŚĆ W SOCIAL MEDIA

RYZYKO LOKALIZACJI:

Funkcja geotagowania zdjęć w czasie rzeczywistym informuje świat, gdzie dokładnie jesteś, a co ważniejsze – że nie ma Cię w domu. Publikuj zdjęcia z wakacji dopiero po powrocie.

KLONOWANIE PROFILI:

Przestępcy kopiują zdjęcia i listę znajomych, tworząc Twój „duplikat", by wyłudzać pieniądze od Twoich bliskich (metoda na BLIK-a). Ukrycie listy znajomych w ustawieniach niemal całkowicie eliminuje to ryzyko.

SZYBKI AUDYT TOŻSAMOŚCI:

- [ ] Czy Twoja lista znajomych jest widoczna dla wszystkich? (Zmień na "Tylko ja").
- [ ] Czy nieznajomi mogą zobaczyć Twój numer telefonu i e-mail w profilu?
- [ ] Czy na Twoich zdjęciach nie widać wrażliwych dokumentów w tle?

ZŁOTA ZASADA:

W internecie jesteś tym, co o sobie opowiesz – ale to, co przemilczysz, jest Twoim najbezpieczniejszym sekretem.

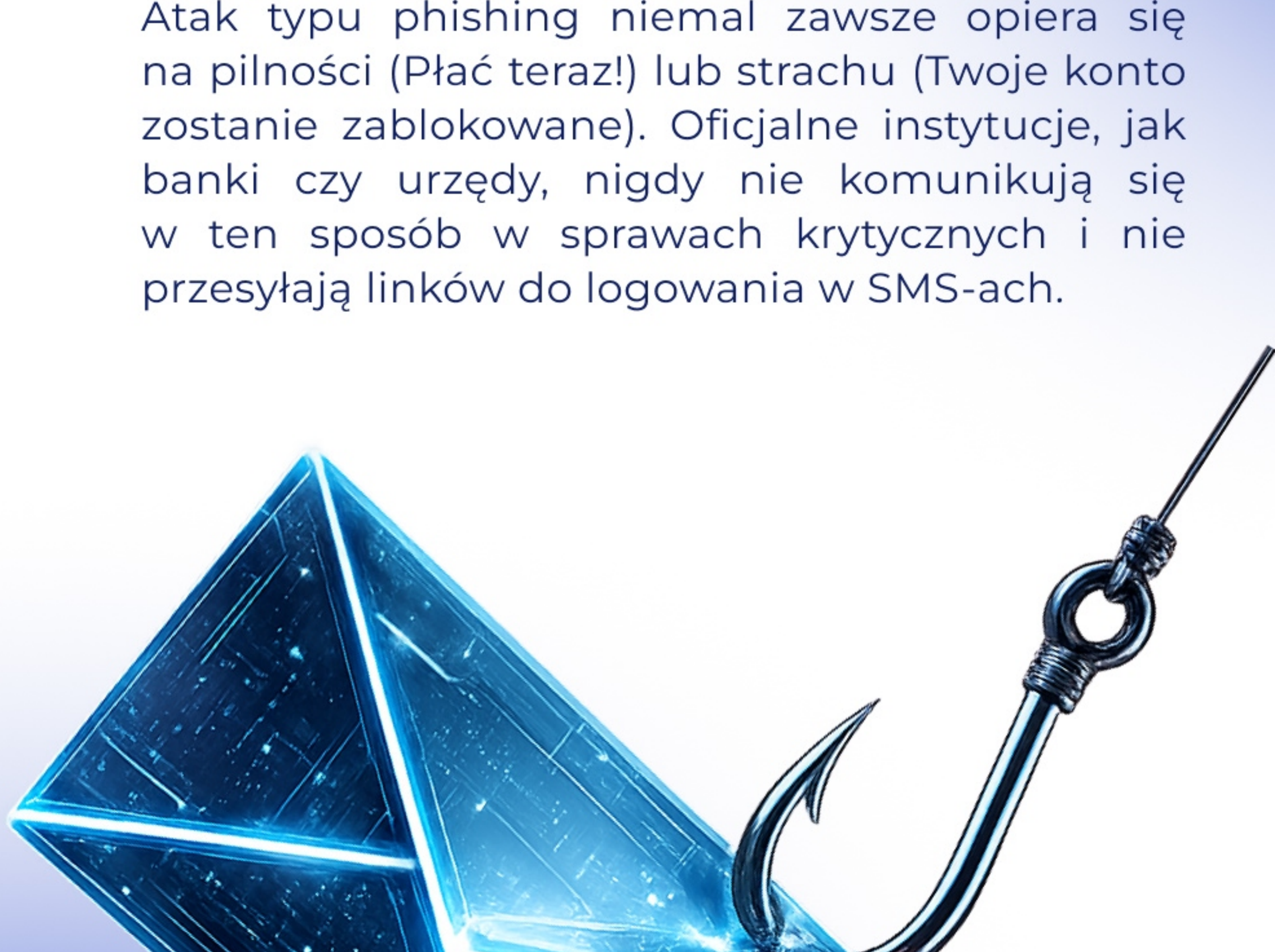
ANATOMIA PHISHINGU
– NIE DAJ SIĘ ZŁOWIĆ

ANALIZA DOMENY (URL):

To najsłabszy punkt oszusta. Zawsze sprawdzaj, czy Twój wpisywany adres to twojbank.pl, a nie twojbank.pl.security-check.com. Literówki w adresie typu peypa1.com zamiast paypal.com to standard. Pamiętaj: subdomeny mogą mylić, patrz zawsze na to, co jest tuż przed końcówką .pl czy .com.

MECHANIZM EMOCJONALNY:

Atak typu phishing niemal zawsze opiera się na pilności (Płać teraz!) lub strachu (Twoje konto zostanie zablokowane). Oficjalne instytucje, jak banki czy urzędy, nigdy nie komunikują się w ten sposób w sprawach krytycznych i nie przesyłają linków do logowania w SMS-ach.



ANATOMIA PHISHINGU
– NIE DAJ SIĘ ZŁOWIĆ

ZAŁĄCZNIKI-PUŁAPKI:

Faktury w formacie .zip, .exe lub dokumenty .docx z prośbą o „włączenie makr” to niemal pewna infekcja złośliwym oprogramowaniem. Nawet plik .pdf może być niebezpieczny, jeśli pochodzi z nieznanego źródła.

PROTOKÓŁ HTTPS TO NIE WSZYSTKO:

Zielona kłódka przy adresie oznacza tylko, że połączenie jest szyfrowane, a nie że strona jest bezpieczna. Oszuści masowo wykupują darmowe certyfikaty SSL, by uśpić Twoją czujność.

METODA 3 SEKUND (ZANIM KLIKNIESZ):

- Zatrzymaj się i weź głęboki oddech – pośpiech to Twój wróg.
- Najedź kursorem na link (bez klikania) i sprawdź adres docelowy w rogu ekranu.
- Zadaj sobie pytanie: „Czy spodziewałem się tej wiadomości w tym kanale komunikacji?”.

ANATOMIA PHISHINGU
– NIE DAJ SIĘ ZŁOWIĆ

ZŁOTA ZASADA:

**Ciekawość to „pierwszy stopień do piekła”,
ale w internecie to pierwszy stopień do utraty
Twoich oszczędności.**

CIEKAWOSTKA:

Pierwsze udokumentowane ataki phishingowe miały miejsce już w 1995 roku. Mimo upływu 30 lat, metoda pozostaje niemal niezmieniona, bo ewoluuje nie technologia, a sposób manipulacji ludzką psychiką. Dziś AI pomaga oszustom np. pisać maile bez błędów językowych, co utrudnia ich rozpoznanie.

CZY WIESZ, ŻE...

BEZPIECZNE ZAKUPY
I FINANSE ONLINE

WERYFIKACJA E-SKLEPU:

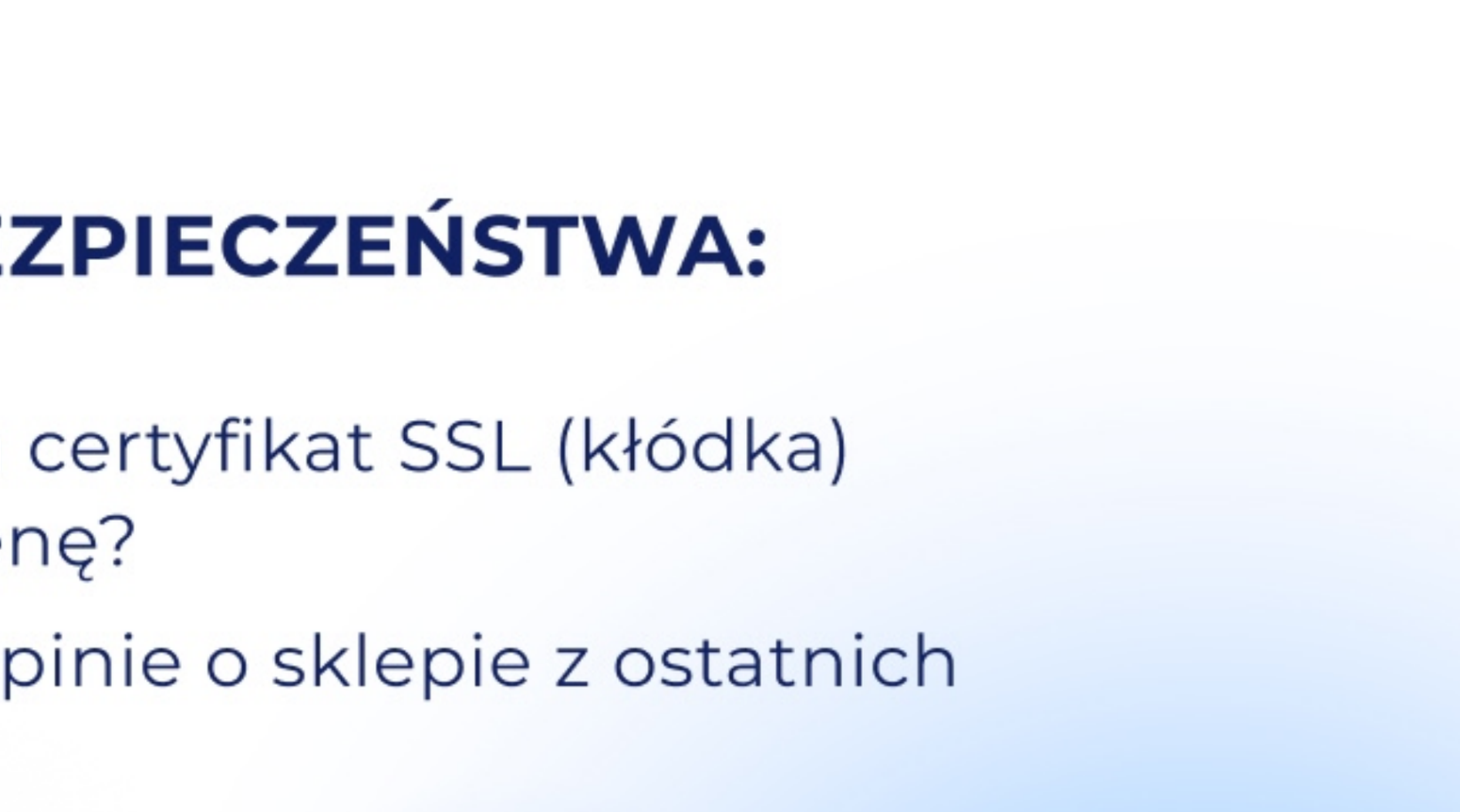
Zanim kupisz, sprawdź regulamin, NIP i dane adresowe firmy. Sklepy widmo często mają „super promocje” (-70% na wszystko), ale brak na nich fizycznego adresu siedziby lub możliwości kontaktu telefonicznego. Korzystaj z portali z opiniami, ale szukaj tych negatywnych – one są zwykle trudniejsze do sfałszowania.

BEZPIECZNE PŁATNOŚCI:

Unikaj przelewów tradycyjnych na prywatne numery kont. Korzystaj z bramki płatniczej, czasowych kodów jednorazowych (nigdy nie podawaj go przez telefon!) lub kart wirtualnych do transakcji jednorazowych, które po zakupie stają się bezużyteczne.

TWÓJ KOSZYK BEZPIECZEŃSTWA:

- Czy sklep posiada certyfikat SSL (kłódka) i poprawną domenę?
- Czy sprawdziłeś opinie o sklepie z ostatnich 30 dni?
- Czy korzystasz z unikalnego hasła do konta w sklepie?



BEZPIECZNE ZAKUPY
I FINANSE ONLINE

ZASADA CHARGEBACK:

Jeśli płacisz kartą płatniczą bezpośrednio, masz prawo do procedury chargeback. W przypadku oszustwa lub braku dostawy towaru, bank może pomóc Ci odzyskać środki od nieuczciwego sprzedawcy.

WYLOGUJ SIĘ:

Zawsze kończ sesję po zakończeniu zakupów lub korzystaniu z bankowości, zwłaszcza jeśli nie robisz tego na własnym, domowym komputerze.

ZŁOTA ZASADA:

Jeśli oferta w internecie wydaje się zbyt dobra, by była prawdziwa, to najprawdopodobniej nią nie jest.

BEZPIECZNE ZAKUPY
I FINANSE ONLINE

CIEKAWOSTKA:

Fałszywe sklepy internetowe często pojawiają się tuż przed Black Friday lub świętami. Potrafią zniknąć z sieci po zaledwie 48 godzinach od zebrania wpłat od nieświadomych klientów.

CZY WIESZ, ŻE...

HIGIENA SPRZĘTOWA
– NIE DAJ SIĘ ZŁOWIĆ

SIŁA AKTUALIZACJI:

System operacyjny i aplikacje to nie tylko nowe funkcje, ale przede wszystkim „łaty” bezpieczeństwa. Przestępcy wykorzystują luki w starym kodzie (tzw. exploity). Ustaw automatyczne aktualizacje wszędzie, gdzie to tylko jest możliwe – to Twoja najtańsza i najskuteczniejsza polisa ubezpieczeniowa.

OPROGRAMOWANIE ANTYWIRUSOWE:

To nie przeżytek. Nowoczesne systemy typu EDR/AV skanują pliki w czasie rzeczywistym i blokują podejrzane zachowania procesów, zanim te zdążą zaszyfrować Twoje dane.

ZASADA "CZYSTEGO BIURKA" W SYSTEMIE:

Usuwaj aplikacje, których nie używasz. Każdy zbędny program to potencjalna „furtka” dla intruza. Pobieraj oprogramowanie wyłącznie z oficjalnych źródeł i stron producentów.

HIGIENA SPRZĘTOWA
– NIE DAJ SIĘ ZŁOWIĆ

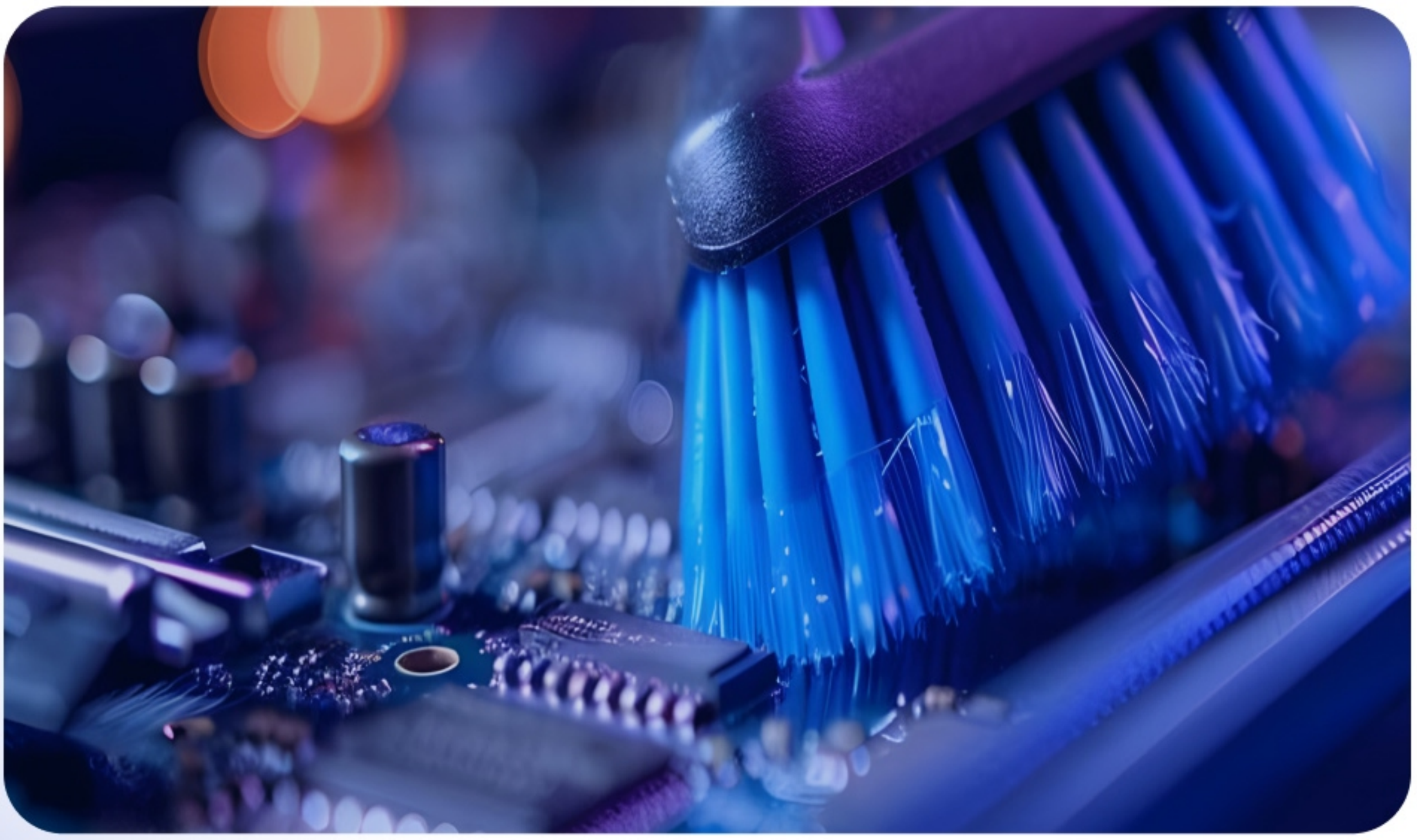
BLOKADA FIZYCZNA:

Cyberbezpieczeństwo zaczyna się od fizycznego dostępu. Zawsze blokuj swój ekran komendą (Win+L / Cmd+Ctrl+Q), gdy będziesz odchodzić od komputera, nawet w domu czy biurze.

ZASADY CYFROWEJ CZYSTOŚCI:

- Czy Twój system operacyjny jest aktualny?
- Czy masz aktywny program antywirusowy z aktualną bazą sygnatur?
- Czy odinstalowałeś zbędne wtyczki do przeglądarki (często to one szpiegują)?

HIGIENA SPRZĘTOWA
– NIE DAJ SIĘ ZŁOWIĆ



ZŁOTA ZASADA:

Aktualizacja systemu to nie uciążliwe powiadomienie, lecz wzmacnianie pancerza Twojej cyfrowej twierdzy.

CIEKAWOSTKA:

Wiele z największych ataków ransomware w historii (np. WannaCry) powiodło się tylko dlatego, że firmy i użytkownicy prywatni zwlekali z zainstalowaniem darmowej poprawki bezpieczeństwa, która była dostępna na miesiące przed atakiem.

CZY WIESZ, ŻE...

PUBLICZNE WI-FI I VPN
– BEZPIECZEŃSTWO W PODRÓŻY

ZAGROŻENIE „EVIL TWIN”:

Przestępcy tworzą fałszywe punkty dostępowe o nazwach identycznych jak kawiarniane czy lotniskowe (np. „Airport_Free_HighSpeed”). Gdy się z nimi łączysz, cały Twój ruch przechodzi przez komputer hakera.

ATAK MAN - IN - THE - MIDDLE (MITM):

W otwartych sieciach haker może przechwytywać dane przesyłane między Twoim urządzeniem a serwerem. Jeśli strona nie ma wymuszonego szyfrowania, haker widzi Twoje loginy i hasła w formie czystego tekstu.

ROLA VPN (VIRTUAL PRIVATE NETWORK):

To Twoja prywatna „tarcza” w publicznej sieci. VPN tworzy zaszyfrowany tunel – nawet jeśli haker przechwyci Twoje dane, zobaczy jedynie niezrozumiały ciąg znaków.

HIGIENA POŁĄCZEŃ:

Wyłącz funkcję „automatycznego łączenia z otwartymi sieciami Wi-Fi w telefonie i laptopie. Twoje urządzenie może nieświadomie połączyć się z siecią przygotowaną przez oszusta.

PUBLICZNE WI-FI I VPN
– BEZPIECZEŃSTWO W PODRÓŻY

TWÓJ PLAN DZIAŁANIA W PODRÓŻY:

- [ ] Czy masz zainstalowaną aplikację VPN od zaufanego dostawcy?
- [ ] Czy wyłączyłeś w telefonie automatyczne łączenie z publicznym Wi-Fi?
- [ ] Czy unikasz logowania się do banku lub poczty w otwartych sieciach bez aktywnego VPN?

ZŁOTA ZASADA:

Darmowe Wi-Fi jest jak rozmowa o Twoich finansach na środku pełnego rynku – każdy, kto przechodzi obok, może usłyszeć Twoje sekrety.

CIEKAWOSTKA:

Niektóre darmowe sieci Wi-Fi w regulaminie (którego nikt nie czyta) zawierają zapisy o zbieraniu i sprzedaży pełnej historii Twojego przeglądania firmom trzecim. "Darmowe" Wi-Fi często płacisz swoją prywatnością.

CZY WIESZ, ŻE...

PRYWATNOŚĆ I RODO
– TWOJE DANE TO NOWA WALUTA

ZARZĄDZANIE COOKIES:

Przycisk „Akceptuję wszystko” to zgoda na śledzenie Twojej aktywności przez setki firm reklamowych. Zawsze wybieraj „Ustawienia” i odrzucaj ciasteczka śledzące (marketingowe), zostawiając tylko niezbędne.

MINIMALIZM DANYCH:

Podawaj tylko te informacje, które są konieczne do realizacji usługi. Czy aplikacja z przepisami naprawdę potrzebuje Twojej daty urodzenia i dostępu do kontaktów?

AUDYT PRYWATNOŚCI:

- [ ] Czy przejrzałeś ustawienia cookies w swojej najczęściej używanej przeglądarce?
- [ ] Czy wiesz, jakie dane o Tobie zbiera Twój serwis społecznościowy? (Sprawdź panel "Twoje dane").
- [ ] Czy usuwasz nieaktywne konta w serwisach, z których przestałeś korzystać?

ZŁOTA ZASADA:

Jeśli nie płacisz za usługę pieniędzmi, to znaczy, że płacisz swoją prywatnością, a produktem są Twoje dane.

PRYWATNOŚĆ I RODO
– TWOJE DANE TO NOWA WALUTA

CIEKAWOSTKA:

Twoja lokalizacja, historia wyszukiwań i polubienia pozwalają algorytmom AI przewidzieć Twoje przyszłe decyzje zakupowe (a nawet stan zdrowia czy poglądy polityczne) trafniej niż zrobiłby to Twój najlepszy przyjaciel.

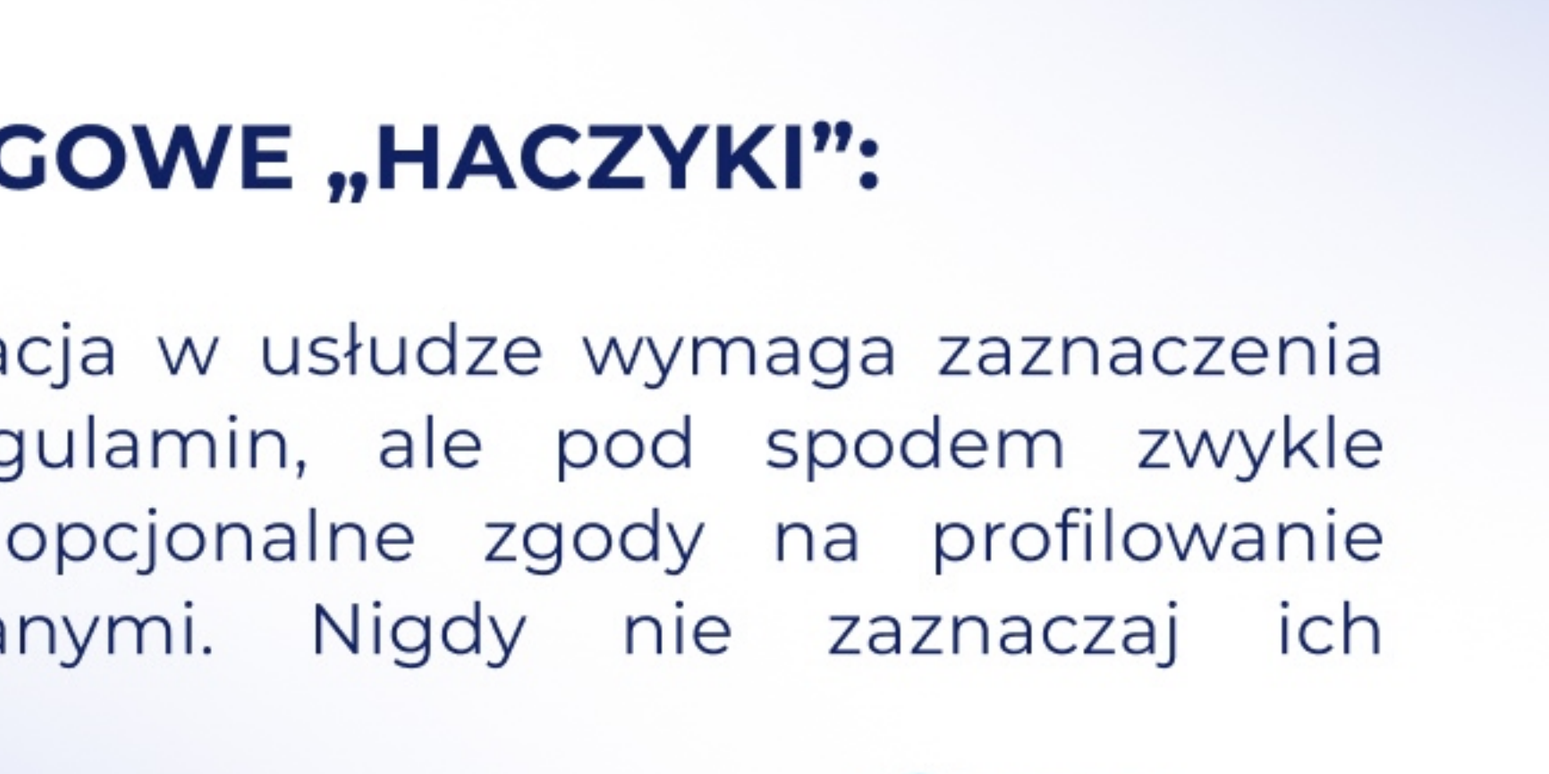
CZY WIESZ, ŻE...

PRAWO DO BYCIA ZAPOMNIANYM:

Zgodnie z RODO, masz prawo żądać usunięcia swoich danych z baz firm, z którymi nie masz już relacji. Korzystaj z tego, by ograniczyć swój ślad cyfrowy.

MARKETINGOWE „HACZYKI”:

Często rejestracja w usłudze wymaga zaznaczenia zgody na regulamin, ale pod spodem zwykle znajdują się opcjonalne zgody na profilowanie i handel danymi. Nigdy nie zaznaczaj ich „z automatu”.



FAKE NEWS I DEZINFORMACJA
– OCHRONA UMYSŁU

MECHANIZM EMOCJONALNY

Dezinformacja jest projektowana w taki sposób, by wywołać u Ciebie gniew, strach lub euforię. Jeśli nagłówek wywołuje u Ciebie silną reakcję – zatrzymaj się na chwilę. To prawdopodobnie manipulacja.

WERYFIKACJA ŹRÓDŁA:

Sprawdź sekcję „O nas” na portalu. Czy redakcja istnieje? Czy autorzy są prawdziwymi osobami? Fałszywe strony często podszywają się pod znane portale informacyjne, zmieniając jedną literę w nazwie.

TWÓJ FILTR PRAWDY (ZANIM PODASZ DALEJ):

- Czy informacja jest potwierdzona przez co najmniej dwa niezależne, wiarygodne źródła?
- Czy sprawdziłeś datę publikacji? (Często stare newsy są podawane jako nowe).
- Czy nagłówek pokrywa się z treścią artykułu, czy jest tylko „clickbaitem”?

FAKE NEWS I DEZINFORMACJA
– OCHRONA UMYSŁU

WSTECZNE WYSZUKIWANIE OBRAZEM:

Oszuści często używają starych zdjęć z wojen lub katastrof, przypisując im nowy kontekst. Użyj ogólnodostępnych wyszukiwarek grafiki lub narzędzi do identyfikacji obrazów, by sprawdzić, skąd naprawdę pochodzi zdjęcie.

BAŃKI INFORMACYJNE:

Algorytmy pokazują Ci to, co chcesz widzieć. Szukaj opinii z różnych stron spektrum, by nie stać się ofiarą jednostronnej narracji.

FAKE NEWS I DEZINFORMACJA
– OCHRONA UMYSŁU

ZŁOTA ZASADA:

W cyfrowej wojnie informacyjnej Twoja pauza przed kliknięciem „Udostępnij” jest najpotężniejszą bronią.

CIEKAWOSTKA:

Badania MIT wykazały, że fake newsy rozprzestrzeniają się w mediach społecznościowych 6 razy szybciej niż prawda. Dzieje się tak, ponieważ kłamstwo jest zazwyczaj bardziej sensacyjne i "atrakcyjne" dla odbiorcy niż nudne fakty.

CZY WIESZ, ŻE...

SMARTFON
– TWOJE NAJBARDZIEJ OSOBISTE URZĄDZENIE

ZARZĄDZANIE UPRAWNIENIAMI:

Aplikacje mobilne często proszą o dostęp do kontaktów, mikrofonu czy galerii, mimo że nie jest im to potrzebne. Regularnie sprawdzaj w ustawieniach, co wiedzą o Tobie Twoje gry i narzędzia.

OFICJALNE ŹRÓDŁA:

Nigdy nie instaluj aplikacji z plików pobranych bezpośrednio z internetu. Oficjalne sklepy z aplikacjami systemowymi automatycznie skanują oprogramowanie pod kątem złośliwego kodu – zewnętrzne serwisy i strony internetowe tego nie robią.

BIOMETRIA I KOD:

Używaj biometrii (odcisk palca, skan twarzy), ale zawsze miej silny, co najmniej 6-cyfrowy kod PIN. Unikaj prostych wzorów graficznych („zetek” czy „kwadratów”), które łatwo podejrzeć na ekranie.

ZDALNE CZYSZCZENIE:

Skonfiguruj usługę „Znajdź moje urządzenie” (Android) lub „Find My iPhone”. W przypadku kradzieży możesz zdalnie wymazać wszystkie dane, by nie wpadły w ręce złodzieja.

SMARTFON
– TWOJE NAJBARDZIEJ OSOBISTE URZĄDZENIE

CHECKLISTA MOBILNA:

- [ ] Czy regularnie weryfikujesz uprawnienia aplikacji do pracy w tle?
- [ ] Czy włączyłeś automatyczną hibernację nieużywanych aplikacji?
- [ ] Czy kontrolujesz dostęp urządzeń w tle (Bluetooth/UWB)?

ZŁOTA ZASADA:

Twój telefon wie o Tobie więcej niż Ty sam – upewnij się, że nie opowiada o Twoim życiu każdemu, kto o to zapyta.

CIEKAWOSTKA:

CZY WIESZ, ŻE...

Biometria w smartfonie (odcisk palca lub skan twarzy) nie przesyła Twojego wizerunku do sieci. Dane te są zamieniane na unikalny kod matematyczny i szyfrowane w odizolowanym, fizycznym procesorze telefonu, do którego nie ma dostępu ani system operacyjny, ani żadna zainstalowana aplikacja.

PROCEDURA RATUNKOWA
– CO ZROBIĆ PO CYBERATAKU?

CYFROWA KWARANTANNA:

Jeśli zorientujesz się, że na Twoim komputerze lub telefonie dzieje się coś podejrzanego natychmiast odłącz urządzenie od internetu. Wyłączenie Wi-Fi lub wyciągnięcie kabla sieciowego przerywa połączenie hakera z Twoim sprzętem i zatrzymuje ewentualny wyciek danych w tle.

ZGŁASZANIE INCYDENTÓW JAKO STANDARD:

Cyberatak to nie wstyd, to przestępstwo. Oficjalnym, krajowym punktem kontaktowym jest CERT Polska. Zgłoszenia można dokonać szybko i anonimowo za pomocą prostego formularza internetowego.

TWOJA CHECKLISTA RATUNKOWA:

- [ ] Czy zabezpieczyłeś pozostałe konta i skrzynkę e-mail?
- [ ] Czy „posprzątałeś” system i zainstalowałeś zaległe aktualizacje?
- [ ] Czy ostrzegłeś bliskich przed oszustwem?

PROCEDURA RATUNKOWA
– CO ZROBIĆ PO CYBERATAKU?

SZYBKA ŚCIEŻKA DLA PODEJRZANYCH SMS-ÓW:

Otrzymałeś podejrzaną wiadomość? Nie klikaj w odnośnik. Prześlij całą treść tego SMS-a na darmowy, ogólnokrajowy numer **8080**. Wiadomość trafi bezpośrednio do analityków, którzy w ciągu kilku minut mogą zablokować fałszywą stronę w całej polskiej sieci.

PLAN AWARYJNY PO UTRACIE KONTA:

Jeśli straciłeś dostęp do profilu w mediach społecznościowych lub poczty e-mail, czas gra kluczową rolę. Wykorzystaj oficjalne procedury odzyskiwania konta (tzw. "recovery mode") przy użyciu podanych wcześniej kodów zapasowych lub alternatywnego adresu e-mail.

PROCEDURA RATUNKOWA
– CO ZROBIĆ PO CYBERATAKU?

CIEKAWOSTKA:

Zgłoszenie oszukańczego SMS-a na **numer 8080** powoduje, że niebezpieczna domena trafia na oficjalną Listę Ostrzeżeń. Od tego momentu krajowi operatorzy automatycznie blokują do niej dostęp, co oznacza, że jedno Twoje zgłoszenie chroni przed stratą pieniędzy tysiące innych osób.

CZY WIESZ, ŻE...

ZŁOTA ZASADA:

W świecie cyberbezpieczeństwa czas reakcji liczy się tak samo, jak podczas pożaru – im szybciej odetniesz sieć i zgłosisz incydent, tym mniejsze będą straty.

O PROJEKCIE:

E-book powstał w ramach realizacji projektu pt. **„CyberShield – wzmocnienie kompetencji Policji w zakresie zwalczania cyberprzestępczości”** na mocy podpisanego Porozumienia Finansowego nr FBWP.03.01-IZ.00-0002/24 pomiędzy Departamentem Funduszy Europejskich MSWiA, Centrum Obsługi Projektów Europejskich MSWiA oraz Komendantem Wojewódzkim Policji z siedzibą w Radomiu.

Projekt jest współfinansowany ze środków Unii Europejskiej z **Programu Fundusz Bezpieczeństwa Wewnętrznego na lata 2021-2027.**

AUTORZY:

Funkcjonariusze i Pracownicy Komendy Wojewódzkiej Policji z siedzibą w Radomiu oraz Zarządu w Radomiu Centralnego Biura Zwalczania Cyberprzestępczości

WYKAZ OFICJALNYCH ŹRÓDEŁ I FUNDAMENTÓW MERYTORYCZNYCH:

I. Akty prawne i strategiczne:

- Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (t.j. Dz.U. 2024 poz. 1077 z późn. zm.)
- Rozporządzenie Parlamentu Europejskiego i Rady UE 2016/679 (RODO) – w zakresie ochrony danych osobowych i prywatności użytkowników.
- Strategia Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2025–2029
- Dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2555 (NIS2) – w zakresie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii.

II. Standardy techniczne i rekomendacje:

- Standardy NIST (National Institute of Standards and Technology) – w szczególności publikacje NIST CSF 2.0 oraz SP 800-63B dotyczące cyfrowej tożsamości.
- Normy ISO/IEC 27001 oraz ISO/IEC 27032 – dotyczące zarządzania bezpieczeństwem informacji i wytycznych dla cyberbezpieczeństwa.
- Wytyczne ENISA (Agencja Unii Europejskiej ds. Cyberbezpieczeństwa) – w obszarze higieny cyfrowej i ochrony urządzeń końcowych.

III. Materiały instytucjonalne:

- Raporty Roczne CERT Polska (NASK-PIB) – „Krajobraz bezpieczeństwa polskiego internetu”.
- Rekomendacje i Wytyczne Komisji Nadzoru Finansowego (KNF) – w zakresie bezpieczeństwa elektronicznych kanałów dostępu oraz usług płatniczych.
- Biuletyny i Ostrzeżenia Centralnego Biura Zwalczania Cyberprzestępczości (CBZC).

Fundusze Europejskie na Migracje, Granice i Bezpieczeństwo
Rzeczpospolita Polska
Dofinansowane przez Unię Europejską