Dzień Bezpiecznego Internetu (DBI) to cykliczne wydarzenie w kalendarzu szeroko zakrojonych świąt i eventów dedykowanych głównie dzieciom i młodzieży – ale nie tylko. Przypadające zawsze na pierwszą połowę lutego obchody po raz pierwszy zapisały się na kartach historii w roku 2004, zainicjowane i ustanowione **przez Komisję Europejską**.

1. Ogranicz dane osobowe, które udostępniasz w sieci

Im mniej Twoich **danych osobowych** w sieci, tym lepiej – taka jest podstawowa zasada bezpiecznego korzystania z Internetu. Każda, nawet banalna informacja, może posłużyć przestępcom do ataku.

Imię i nazwisko, data urodzenia, numer karty kredytowej, numer PESEL, adres zamieszkania, bank, z którego usług korzystasz – to wszystko **informacje bezcenne dla cyberprzestępców**. Mogą wykorzystać je np. do phishingu (więcej na ten temat dowiesz się niżej) czyli **najbardziej popularnego rodzaju ataku** wymierzonego w każdego użytkownika sieci.

Im mniej prywatnych informacji podasz w Internecie, tym mniejsze ryzyko, że padniesz ofiarą np. **cyberstalkingu** czyli nękanie, gróźb i ataków przy użyciu sieci.

2. Używaj silnych i unikalnych haseł

“Admin_1234” – kto nie zna najsłynniejszego i ponoć najbardziej popularnego hasła używanego do dowolnego konta? To jeden z najstarszych żartów o internecie, ale niestety zawiera ziarno prawdy. Używanie **słabego hasła** lub jednego hasła do zabezpieczenia wielu kont, to recepta na kłopoty. Przestępca może okraść Twoje konto, zaciągnąć kredyt, użyć skrzynki e-mail do ataku na innych użytkowników czy też wykraść dane.

Rozwiązanie? **Używaj silnych, nie powtarzających się haseł**. To podstawowa zasada higieny korzystania z m.in. bankowości elektronicznej, poczty e-mail i niezliczonej ilości usług w sieci, w których musisz używać hasła.

Hasła możesz tworzyć polegając na własnej przemyślności i sprawdzonych porad dot. tworzenia silnych i trudnych do złamania haseł lub skorzystać z menedżera haseł. Menedżer haseł to program, który generuje i przechowuje dane logowania powiązane z kontami internetowymi. Dzięki niemu musisz pamiętać wszystkich haseł, wystarczy **hasło główne do menedżera**. Użycie takiego programu to praktyczny i zaawansowany sposób na poprawę bezpieczeństwa w sieci. Warto wybrać program typu open source z **szyfrowaniem typu end-to-end** i **weryfikacją dwuskładnikową**.

Jeżeli przestępca pozna jedno z Twoich haseł, to używając różnych haseł do różnych kont, nie musisz bać się o swoje dane na innych serwisach.

3. Używaj weryfikacji dwuetapowej

Weryfikacja dwuetapowa (2FA) to opcja dostępna w wielu serwisach (Facebook, Google), która zdecydowanie poprawi Twoje cyberbezpieczeństwo. Tego typu uwierzytelnienie wymaga przynajmniej dwóch kroków: podania hasła oraz wprowadzenia tymczasowego kodu wysłanego przez serwis w sms-ie lub przy użyciu specjalnej aplikacji (np. Google Authenticator).

Możesz również zdecydować się na **stosowanie klucza U2F** czyli fizycznego przedmiotu przypominającego pendrive’a lub brelok do kluczy – ta metoda jest najbardziej odporna na phishing.

Pamiętaj, że uwierzytelnienie przy użyciu SMS jest mniej bezpieczne od dobrej aplikacji do weryfikacji dwuetapowej.

Oto **zestawienie weryfikacji 2FA** od najbardziej do najmniej bezpiecznych:

- klucz U2F,
- kody czasowe w aplikacji,
- kody jednorazowe SMS,
- kody wysyłane przez e-mail.

Dzięki uwierzytelnieniu wieloskładnikowemu skomplikujesz życie cyberprzestępcom i lepiej zabezpieczysz się jeżeli dane Twoje konta wyciekną lub zostaną wykradzione.

4. Nie korzystaj z jednej skrzynki pocztowej

Wiele osób używa jednego adresu e-mail do obsługi spraw związanych z pracą/firmą, rejestracji do najróżniejszych newsletterów, zakupów czy też aplikacji w chmurze. To nie jest dobry pomysł.

Adres e-mail używany w celach służbowych/biznesowych często zawiera Twoje imię i nazwisko. Warto mieć **nieformalny adres mailowy**, który zapewni Ci większą anonimowość w sieci. Im mniej Twoich danych osobowych w sieci, tym lepiej, pamiętasz?

Ciekawym rozwiązaniem jest **Proton** – to cały ekosystem, którego celem jest zapewnienie użytkownikowi bezpieczeństwa podczas korzystania z sieci (dostępny również w opcji darmowej). Najbardziej ceniony jest Proton Mail. To usługa, w której **każdy mail i załącznik jest zaszyfrowany** – odczyta go tylko zamierzony odbiorca. Proton korzysta z szyfrowania typu end-to-end (E2EE). E2EE uchodzi za **złoty standard zabezpieczenia komunikacji** w poczcie elektronicznej.

Co ważne, szyfrowaną wiadomość można wysłać do osoby, która nie korzysta z Proton. Wystarczy, że będzie ona dysponowała ustalonym wcześniej hasłem. Więcej dowiesz się w recenzji Proton Mail i poradnika dot. bezpieczeństwa i prywatności e-mail.

5. Skasuj niepotrzebne/nieużywane konta

Im więcej masz kont założonych na różnych serwisach, tym **większe ryzyko wycieku** Twoich danych. Większość z nas ma konta na stronach, z których już nie korzysta. Dobrym pomysłem jest ich skasowanie.

Jak znaleźć stare konta, skoro najpewniej od dawna się na nich nie logowałeś/aś? Przejrzyj swój menadżer haseł, skrzynkę e-mail oraz Facebooka i Google – wiele usług umożliwia logowanie za pomocą tych stron.

Niestety, z doświadczenia wiem, że wiele serwisów nie ułatwia zadania i **skasowanie konta** może być drogą przez mękę.

6. Uważaj na phishing i ransomware – podejrzane maile i SMS-y

Największym zagrożeniem w sieci jest malware czyli **złośliwe oprogramowanie**. Wśród takich programów prym wiodą ransomware i programy do phishingu.

Ransomware to oprogramowanie szantażujące. Po instalacji takiego programu dane na zaatakowanym komputerze są szyfrowane. Klucz do szyfru ma tylko twórca ransomware. Ofiara otrzymuje informację, że **musi zapłacić okup** – najczęściej w kryptowalutach – i wtedy odzyska dostęp do plików i dysków. Przestępcy często nie dotrzymują słowa (czasem ransomware nieodwracalnie niszczy pliki) lub ponownie atakują i żądają większego okupu.

Teraz phishing – co to jest? **Phishing to forma oszustwa**: przestępca podszywa się pod inną osobę czy też instytucję (finansową, państwową) żeby wyłudzić informacje, zainfekować komputer/smartfon złośliwym oprogramowaniem lub nakłonić ofiarę do określonych działań.

Przestępca może np. **podszyć się pod pracownika banku**, użyć bramki internetowej, która umożliwia dzwonienie z autentycznego numeru i zdobywszy zaufanie ofiary, zachęcić do **udostępnienia danych** (numeru karty kredytowej, hasła) lub zainstalowania oprogramowania (np. AnyDesk) do zdalnego zarządzania pulpitem ofiary.

Agresor ma potem z górki: **wyczyszcza konto ofiary**, a nawet zaciąga kredyt w jej imieniu.

Z raportu CERT Polska za 2021 rok wynika, że 76,57 proc. wszystkich ataków to **phishing** (prawie dwa razy więcej niż rok wcześniej).

Malware rozprzestrzenia się za pomocą e-maili, zainfekowanych stron www oraz coraz częściej SMS-ów. Wystarczy kliknąć w link podany w załączniku lub pobrać zainfekowany plik. Bardzo często ofiara nie wie, że zainstalowała złośliwe oprogramowanie na komputerze.

Jak uchronić się przed phishingiem i ransomware (oraz innymi rodzajami złośliwego oprogramowanie, np. spyware)? To najlepsze metody samoobrony:

- wpisuj adres banku lub innej instytucji ręcznie – nie korzystaj z linków otrzymanych mailem lub SMS-em,
- przed zalogowaniem się sprawdź czy jesteś na autentycznej i zabezpieczonej stronie – czy jest chroniona certyfikatem SSL (świadczy o tym zamknięta kłódka); kliknij na kłódkę przy adresie URL

i zobacz czy certyfikat został wystawiony dla Twojego banku, biura maklerskiego lub instytucji publicznej,
- ostrożnie szukaj strony do logowania przy pomocy wyszukiwarki www – przestępcy umieszczają w reklamach linki prowadzące do podstawionych stron, które do złudzenia przypominają prawdziwe, a służą do wyłudzania danych do logowania,
- pobieraj aplikacje – przede wszystkim służące do korzystania z bankowości mobilnej – tylko z oficjalnych sklepów (Google Play, AppStore) lub ze strony usługodawcy.

7. Zainstaluj mocny program antywirusowy

Są osoby, które nie używają antywirusów. Jednak dla większości osób, to nie jest optymalne rozwiązanie. Antywirus da Ci spokojną głowę oraz **zabezpieczenie przed najbardziej popularnymi zagrożeniami**.

Na rynku dostępne są dziesiątki antywirusów. Który wybrać?

Dobrym pomysłem jest **przejrzenie testów programów antywirusowych** wykonanych przez niezależne laboratoria, m.in. AV-Comparatives i AV Test. Eksperci oceniają m.in. skuteczność ochrony, jak bardzo antywirus obciąża procesor komputera, jak często myli się ogłaszając fałszywe alarmy czy też jego zdolność obrony urządzenia przed zaawansowanymi atakami.

Inne kryteria wyboru to cena, dostępność na różne urządzenia i systemy operacyjne oraz **dodatkowe funkcje** oferowane przez producenta. Te dodatkowe funkcje to m.in. VPN, ochrona rodzicielska, menedżer haseł, szyfrowanie plików.

Z pewnością wiele osób skuszą **darmowe AV**. Czy ich wybór to dobre rozwiązanie? Użytkownicy Windows 10 i Windows 11 domyślnie korzystają z bezpłatnego antywirusa czyli Windows Defendera. Jednak płatne programy antywirusowe mają więcej funkcji niż ich gratisowe odpowiedniki oraz oferuje klientom **zaawansowaną pomoc techniczną**.

Możesz skorzystać z **darmowych okresów próbnych** płatnych produktów. Przez 30 dni masz dostęp do pełnych wersji AV, a po upływie tego okresu zdecydujesz czy wykupić stały dostęp.

Nasze rekomendacje i porównania poznasz w rankingu najlepszych programów antywirusowych.

8. Używaj sieci Tor i/lub VPN

Sieć Tor to bardzo skuteczny sposób na bezpieczne i prywatne korzystanie z sieci. Zapytanie z komputera przechodzi przez kolejne węzły (serwery) i **jest szyfrowane**. Efekt? Twój **adres IP jest maskowany**, a potencjalny obserwator nie wie jakie strony odwiedziłeś i co na nich robiłeś.

Wadą sieci Tor jest jej wolne działanie, a niektóre usługi (np. bankowość elektroniczna) blokują użytkowników Tor. Sieć nie nadaje się również do przesyłania i ściągania dużych plików, a także strumieniowania filmów.

Bardzo dobrym narzędziem na uzyskanie anonimowości w Internecie jest **VPN**. Ta usługa szyfruje cały ruch między Twoim urządzeniem a serwerem z odwiedzaną stroną. VPN działa szybko, ukrywa IP (zob. Jak zmienić adres IP komputera i telefonu?), umożliwia bezpieczną wymianę plików np. przez BitTorrent.

Musisz jednak pamiętać, żeby wybrać **zaufanego dostawcę VPN**, który nie zbiera logów (informacji o aktywności) i udostępnia ich podmiotom trzecim.

9. Unikaj przeglądania stron bez certyfikatu SSL

SSL to protokół sieciowy, który **służy do bezpiecznych połączeń** internetowych. Takie połączenia nawiązywane są przy użyciu certyfikatów – dlatego mówimy o certyfikacie SSL. Strony z takim certyfikatem poznasz na pierwszy rzut oka – mają w adresie URL oznaczenie **https://** oraz symbol kłódki (w przeciwieństwie do stron http://).

SSL szyfruje połączenie między serwerem, a przeglądarką www. **Chroni dane**, które podajesz na odwiedzanych stronach – od imienia i nazwiska, przed adres e-mail, po numer karty kredytowej – przed dostępem niepowołanych osób. Takich informacji nie należy podawać na stronach z http czyli bez certyfikatu.

To nie wszystko. SSL zabezpiecza też m.in. przed przekierowaniem na inną stronę, przechwyceniem danych użytych przy realizacji e-płatności oraz przez kradzieżą haseł, numerów kart i kont.

Uwaga! Certyfikat SSL nie znaczy, że jesteś **w 100 proc. bezpieczny** i znalazłeś się na właściwej stronie www. Większość certyfikatów (DV) weryfikuje tylko domenę, a ta może celowo wprowadzać w błąd. Przestępca może np. zarejestrować domenę pkopp.pl – celowa zbieżność z pkobp.pl – i wyłudzać dane do logowania do bankowości elektronicznej.

Cyberdranie standardowo używają protokołu SSL, żeby wzbudzić zaufanie ofiar. Przed podaniem na stronie wrażliwych danych, sprawdź, **co kryje się za kłódką przy adresie URL**. Po kliknięciu w kłódkę dowiesz się m.in.: czy połączenie jest bezpieczne, jakiego certyfikatu użyto, dla kogo został

wystawiony oraz jaki ma termin ważności. Najbezpieczniejsze są strony używające certyfikaty OV i EV czyli ze **sprawdzoną tożsamością firmy**, która o nie wystąpiła.

10. Zwiększ ustawienia prywatności na swoich kontach w mediach społecznościowych

Z zasady osoby, które korzystają z mediów społecznościowych mają **ograniczoną prywatność**. Właściciele serwisów zbierają informacje na temat ich zachowania w sieci, a potem wykorzystują do targetowania reklam lub **sprzedają zewnętrznym marketerom**.

Jeżeli chcesz być bardziej bezpieczny – mniej narażony na szpiegowanie i precyzyjnie dobierane reklamy – możesz **ograniczyć zakres informacji** zbieranych o tobie przez Facebooka, Twittera, Tik Toka czy Instagram. Zrobisz to w ustawieniach prywatności.

Dobrym pomysłem jest również ograniczenie innym osobom możliwości **oznaczania Cię na zdjęciach lub w wydarzeniach**. Po wprowadzeniu zmian zatwierdzisz lub odrzucisz tagowanie. Sprawdź również, kto może widzieć Twoje posty i mieć dostęp do informacji o wspólnych znajomych.

Serwisy społecznościowe często zmieniają regulaminy i wprowadzają nowe zasady dotyczące prywatności użytkowników. Regularnie monitoruj, co zbierają o tobie serwisy społecznościowe i reaguj w razie konieczności.

11. Aktualizuj system operacyjny i programy

Jednym z poważniejszych zagrożeń w sieci są **złośliwe programy typu exploit.** To malware, które wyszukują luki w programach, a potem wykorzystują je do zainfekowania urządzenia innymi złośliwymi programami.

Za sprawą exploit Twój komputer może być zainfekowany np. **keyloggerem** (służy m.in. do rejestracji klawiszy używanych przez ofiarę ataku), **ransomware** (oprogramowanie szantażujące) czy też **spyware** (oprogramowanie szpiegujące).

Groźba ściągnięcia na komputer/smartfona exploita to jedne z argumentów za regularną **aktualizacją systemu operacyjnego i programów** zainstalowanych na urządzeniu. Programiści starają się szybko załatać dziury wykryte w oprogramowaniu. Exploit musi wykorzystać swoje okienko możliwości – czas do wypuszczenia **łatki bezpieczeństwa**. Im szybciej zrobisz aktualizację, tym mniejsze ryzyko skutecznego ataku.

Idealne rozwiązanie to ustawienie **automatycznej aktualizacji** systemu operacyjnego i programów.

12. Zaszyfruj dysk komputera i laptopa, zabezpiecz router i sieć WiFi

Odpowiednie **zabezpieczenie urządzeń**, których używasz podczas korzystania z sieci, może przesądzić o bezpieczeństwie Twoich pieniędzy i danych.

Router to brama, która oddziela Twoją domową sieć od Internetu i czyhających w nim zagrożeń. Może być otwarta dla przestępców lub zamknięta i zabezpieczona solidnym zamkiem.

Ustawienie dobrego hasła do sieci WiFi, zmiana domyślnej nazwy sieci, wybór bezpiecznego protokołu, zmniejszenie zasięgu WiFi – to niektóre sposoby, żeby agresor nie wykorzystał Twoich urządzeń do **zdalnego przejęcia kontroli** nad siecią domową (sprawdź więcej sposobów i szczegółów zabezpieczenia routera i sieci WiFi).

Dobrym rozwiązaniem jest zaszyfrowanie dysku na komputerze lub telefonie. Dzięki temu niepowołana osoba nie będzie miała dostępu do wyniku Twojej pracy, prywatnych zdjęć czy też wrażliwych danych. Pamiętaj, że najlepszym sposobem na ochronę wszystkich danych jest **pełne szyfrowanie dysku**. Służą do tego aplikacje, m.in. BitLocker, FileVault 2 i VeraCrypt.

13. Pamiętaj o zasadach bezpiecznego korzystania z zasobów Dark Web

Dark Web to część sieci niedostępnej za pośrednictwem zwykłych przeglądarek. Można korzystać z niej przy użyciu specjalnego oprogramowania, np. **przeglądarki Tor Browser**.

Dark Web jest popularny ze względu na **wysoki poziom anonimowości użytkowników**. W darknecie można nabyć przedmioty, które są nieosiągalne w "zwykłym" internecie. To m.in. narkotyki, broń, dane wykradzione ze sklepów online, fałszywe dokumenty, materiały pedofilskie. Dostępne są również nielegalne usługi, np. wynajem morderców na zlecenie.

Jednak darknet oferuje również **legalne usługi** dobrze znane z ogólnodostępnego internetu (webmail, kantory wymiany walut, usługi finansowe) oraz możliwość **swobodnej wymiany informacji i wiedzy**, z której korzystają dziennikarze, działacze społeczni i zwykli obywatele (to oczywiście wywołuje wściekłość władz państw rządzonych autorytarnie, np. Rosji, Arabii Saudyjskiej, Chin, Turcji).

Jeżeli chcesz bezpiecznie korzystać z Dark Web to z oczywistych względów narażasz się na **konsekwencje prawne** kupując nielegalne towary/usługi. To nie wszystko. Pliki pobierane z anonimowych źródeł mogą zawierać **złośliwe oprogramowanie**. Dobrą zasadą, jest zachowanie maksymalnej ostrożności przy pobieraniu jakichkolwiek materiałów z Darknetu.

14. Bezpiecznie używaj sieci P2P

P2P (peer-to-peer) to rozproszona sieć powiązanych urządzeń służąca do **przechowywania i wymiany plików oraz innych zasobów.** Do obsługi P2P służą dedykowane aplikacje, np. słynny **BitTorrent.** Dzięki tej sieci możesz m.in.. udostępniać i pobierać dowolne pliki, handlować kryptowalutami, kupować lub sprzedawać towary/usługi na internetowych giełdach czy też strumieniować dane.

Zastosowań P2P jest bardzo dużo, właściwie ograniczeniem jest tylko wyobraźnia użytkowników. Za dużymi możliwościami idą też duże wyzwania, a jednym z nich jest bezpieczne korzystanie z tego narzędzia.

To, co jest zaletą rozproszonej sieci może być jej wadą. W P2P nie ma podmiotu trzeciego, który pełni **rolę strażnika i egzekwuje zasady**. To znaczy, że użytkownik bywa łatwiejszym celem dla oszustów lub nieuczciwych sprzedawców. W sieci wypracowane są mechanizmy ochrony przed takimi zagrożeniami, jednak handlując kryptowalutami, pożyczając pieniądze lub wymieniając waluty, musisz zachować ostrożność.

Decydując się na korzystanie z peer-to-peer wybierz **godny zaufania program** – popularny i sprawdzony przez użytkowników. Jak zawsze, najbezpieczniej pobierzesz go z oficjalnej strony producenta.

Pliki pobrane w sieci P2P mogą zawierać malware, np. programy szpiegujące (spyware) lub szantażujące (ransomware). Poza zdrowym rozsądkiem trzeba uzbroić się w **mocny program antywirusowy**. Np. przeskanować każdy plik przed otwarciem używając programu korzystającego z 57 antywirusów na raz.

Pamiętaj, że pobierając i udostępniając pliki przy pomocy np. BitTorrenta ryzykujesz **naruszenie praw autorskich**.

15. Zdobywaj wiedzę na temat bezpieczeństwa w sieci

Wiedza to potężna broń – to zasada dotyczy również bezpiecznego korzystania z Internetu. Dodam: aktualizowana wiedza.

Cyfrowy świat zmienia się każdego dnia. Informacje sprzed roku o cyberzagrożeniach i sposobach ich zwalczania mogą być dzisiaj nieskuteczne. Warto sprawdzać dobre serwisy, które na bieżąco informują o najważniejszych wydarzeniach ze świata cyberbezpieczeństwa.