4.

USUŃ ŚLADY

Przeglądarka w telefonie przechowuje wiele informacji na twój temat – gdzie się znajdujesz, co wyszukujesz, z jakich stron internetowych korzystasz – i może je przekazać dalej. Ale kilka zmian pomoże ci przejąć kontrolę.

Telefony, tablety i komputery mają zwykle fabrycznie zainstalowane przeglądarki, dla których twoja prywatność nie jest priorytetem. Zamiast nich możesz **pobrać i stosować przeglądarkę**, która **domyślnie chroni** twoją aktywność w sieci, zabezpieczając cię przed trackerami.

Jeszcze większą prywatność dadzą ci dodatki i rozszerzenia (łatwe do zainstalowania miniprogramy dla przeglądarki, które **zwiększają prywatność online**).

5.

ODTAGUJ SIEBIE I INNYCH

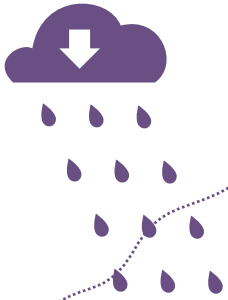
Zdarzyło ci się otagować zdjęcie i posty znajomych i dołożyć swoją cegiełkę do sterty zgromadzonych o nich danych?

Ulżyj im (i przy okazji swojemu sumieniu) i **odtaguj ich** z jak największej ilości zdjęć i postów.

Dziel się wiedzą! Zachęcaj znajomych, rodzinę i współpracowników do opanowania wymykających się spod kontroli danych. Jeśli wszyscy przyłożymy się do kontroli naszych cyfrowych śladów, pomożemy sobie nawzajem w detoksie.

Żeby zablokować szpiegujące cię reklamy i niewidzialne trackery, zainstaluj uBlock Origin (dla przeglądarek Chrome, Safari i Firefox) lub Privacy Badger (dla przeglądarek Chrome, Firefox i Opera).

Żeby zapewnić bezpieczne połączenie ze stronami internetowymi, o ile to możliwe, zainstaluj HTTPS Everywhere: rozszerzenie dla przeglądarki, które szyfruje i zabezpiecza twoje połączenie z wieloma popularnymi stronami internetowymi podczas przesyłu danych. Jeśli korzystasz z Safari, możesz ustawić domyślną wyszukiwarkę na produkt, który nie należy do firmy Google, na przykład DuckDuckGo, i będzie automatycznie przekierowywał cię na szyfrowane połączenia.



DATA DETOX KIT

KONTROLUJ DANE NA SMARTFONIE

i prywatność online

Mogłoby się wydawać, że twoje dane nie mówią o tobie nic wielkiego. W końcu kogo obchodzi, czy lubisz muzykę country, kupujesz za wiele par butów, czy planujesz wakacje z rocznym wyprzedzeniem?

Problem leży w tym, co się z twoimi danymi dzieje. Z czasem ze zgromadzonych na twój temat danych wyłaniają się prywatne informacje – o twoich nawykach, aktywności, relacjach, preferencjach, przekonaniach i tajemnicach. Stają się one widoczne dla tych, którzy je analizują i czerpią z nich korzyści, na przykład firm i brokerów danych.

Z Data Detox Kit dowiesz się, jak i dlaczego tak się dzieje. I poznasz praktyczne sposoby na kontrolowanie śladów swojej obecności w sieci.

Zaczynamy!

Autorzy
TACTICAL TECH

Wsparcie
Firefox

datadetoxkit.org
#datadetox

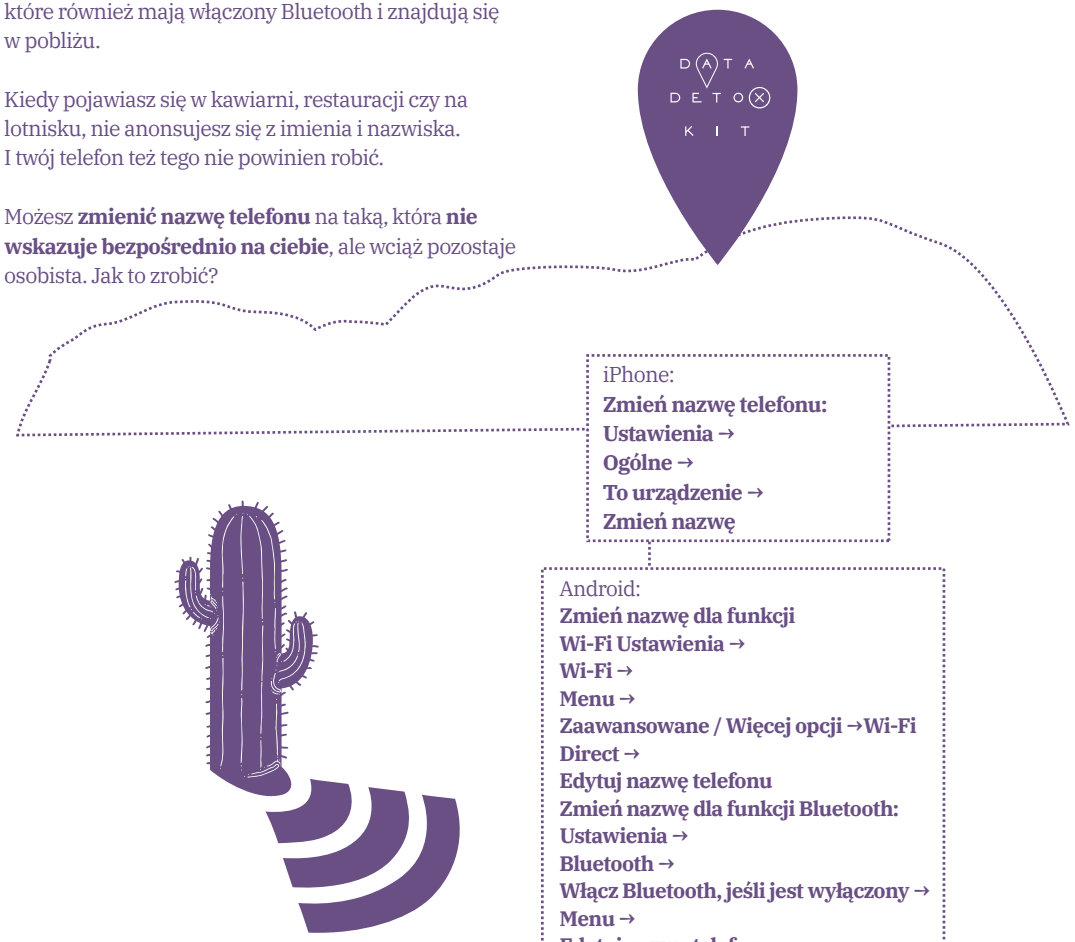
1.

ZMIEŃ NAZWĘ URZĄDZENIA

W którymś momencie telefon otrzymał od ciebie „imię", które pojawia się, kiedy korzystasz z funkcji *Wi-Fi* i *Bluetooth*. Nazwa telefonu mogła również zostać automatycznie wygenerowana w trakcie konfiguracji. Oznacza to, że nazwa „Telefon Janka Nowaka" wyświetla się właścicielom sieci Wi-Fi oraz, jeśli masz włączony Bluetooth, wszystkim osobom, które również mają włączony Bluetooth i znajdują się w pobliżu.

Kiedy pojawiasz się w kawiarni, restauracji czy na lotnisku, nie anonsujesz się z imienia i nazwiska. I twój telefon też tego nie powinien robić.

Możesz **zmienić nazwę telefonu** na taką, która **nie wskazuje bezpośrednio na ciebie**, ale wciąż pozostaje osobista. Jak to zrobić?



iPhone:
Zmień nazwę telefonu:
Ustawienia →
Ogólne →
To urządzenie →
Zmień nazwę

Android:
Zmień nazwę dla funkcji Wi-Fi Ustawienia →
Wi-Fi →
Menu →
Zaawansowane / Więcej opcji →Wi-Fi Direct →
Edytuj nazwę telefonu
Zmień nazwę dla funkcji Bluetooth:
Ustawienia →
Bluetooth →
Włącz Bluetooth, jeśli jest wyłączony →
Menu →
Edytuj nazwę telefonu
Wyłącz Bluetooth

2.

ZNIKNIJ Z MAPY

Dane o lokalizacji to na pozór *przypadkowe strzępki* informacji, ale gdy spojrzy się na nie całościowo, mogą wyjawić coś **ważnego o tobie** i twoich zwyczajach, na przykład to, gdzie mieszkasz, gdzie pracujesz i gdzie lubisz spotykać się ze znajomymi. Dlatego tak wiele firm i brokerów danych chce je pozyskać.

To całkiem zrozumiałe, że apka do nawigacji ma dostęp do twojego położenia. Ale zaskoczyć cię może, jak wiele innych aplikacji dostało od ciebie zgodę na dostęp do danych o lokalizacji.

Przejrzyj zgody na dostęp dla każdej aplikacji i wyłącz usługi lokalizacji w tych, które ich nie potrzebują (czy gra naprawdę musi wiedzieć, gdzie jesteś?), i tych, którym nie chcesz zdradzać swojego położenia.

3.

POSPRZĄTAJ W APKACH

Apki do mediów społecznościowych, gier czy pogody są zainteresowane twoimi danymi. I mogą zebrać ich sporo.

Pozbywając się apek, z których nie korzystasz, zafundujesz sobie porządny cyfrowy detoks.

Poza tym takie porządki *zwalniają miejsce* w telefonie, zmniejszają zużycie danych i *zwiększają wydajność baterii*. A w zależności od usuniętej aplikacji poprawić się może również wydajność całego urządzenia.

Android:
Ustawienia →Aplikacje→
Ustaw dostęp do lokalizacji dla poszczególnych aplikacji

iPhone:
Ustawienia →Prywatność →
Usługi lokalizacji
Ustaw dostęp do lokalizacji dla poszczególnych aplikacji

Android:
Ustawienia → Aplikacje →
Wybierz apkę, którą chcesz usunąć
Odinstaluj

iPhone:
Naciśnij i przytrzymaj ikonę apki do momentu, w którym pojawi się menu.

Wybierz opcję usunięcia aplikacji z listy.

Potwierdź usunięcie apki.

4.

CHROŃ WIRTUALNE SKARBY

Informacje, które przechowujesz online, traktuj tak, jak cenne przedmioty w domu. Zastanów się, gdzie trzymasz najcenniejsze osobiste dane, jak informacje o finansach, skany paszportu czy nawet adres i numer telefonu. Pomyśl też, jak możesz je chronić.

Doraźne porządki to świetny sposób na wprowadzenie kilku szybkich ulepszeń. Wyszukaj konkretne informacje w skrzynce mailowej lub na innych kontach i je usuń. *Skany dowodu tożsamości, dane bankowe lub informacje o ubezpieczeniu zdrowotnym* to tylko kilka przykładów. Jeśli są to dane, które będą ci później potrzebne, pobierz je lub wydrukuj przed usunięciem.

Gruntowne porządki wymagają więcej pracy, ale i dają lepsze efekty. Dobrze je zrobić raz do roku. Zarchiwizuj wszystko, co trzymasz w skrzynce mailowej lub na kontach w mediach społecznościowych, pobierz dane na komputer, usuń z sieci i ciesz się odzyskanym *czystym kontem.*

Wskazówka: Usunięcie danych to nie koniec – wyczyść również kosz i pliki tymczasowe!

Zdecyduj, czy kopię zapasową swojego archiwum i dokumentów zachowasz w chmurze czy na zewnętrznym dysku lub nośniku USB. Niezależnie od metody – nie zgub danych, chroń je silnym hasłem i przechowuj w sposób, który jest dla ciebie najsensowniejszy.

5.

DZIEL SIĘ WIEDZĄ

Łatwo zapomnieć, że internet nazywamy siecią nie bez powodu. **Jesteśmy połączeni online** nie tylko jako „znajomi" w mediach społecznościowych, ale również przez kontakty na kontach mailowych oraz za pomocą zdjęć, które udostępniamy online.

Jeśli zabezpieczysz swoje konta, wzmocnisz hasła i wyczyścisz dane, nie tylko ty na tym zyskasz – **każda osoba z twojej sieci kontaktów będzie dzięki tobie trochę bezpieczniejsza.**

Dziel się wiedzą! Zwiększenie bezpieczeństwa online to kwestia kilku prostych kroków. Przekaż Data Detox Kit znajomym, rodzinie i współpracownikom, żeby pomóc im zmienić cyfrowe nawyki zgodnie z ich potrzebami.

DATA DETOX KIT

ZMIEŃ USTAWIENIA

i zabezpiecz dane

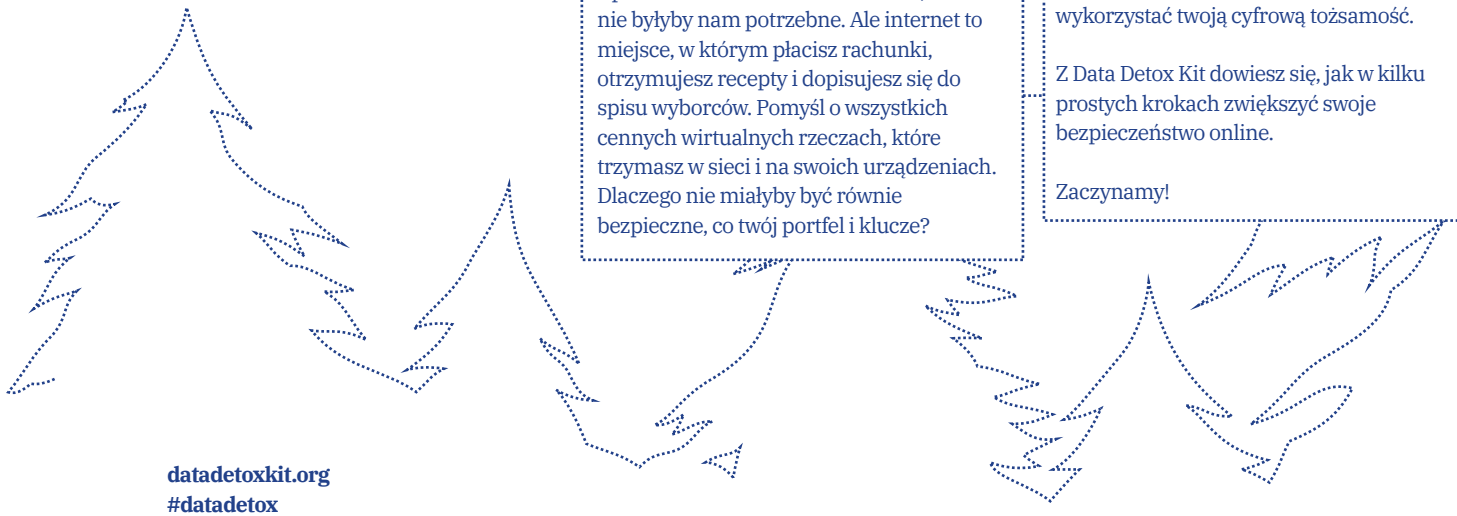
Gdyby po internecie krążyły tylko obrazki z psami w kostiumach dinozaurów, hasła nie byłyby nam potrzebne. Ale internet to miejsce, w którym płacisz rachunki, otrzymujesz recepty i dopisujesz się do spisu wyborców. Pomyśl o wszystkich cennych wirtualnych rzeczach, które trzymasz w sieci i na swoich urządzeniach. Dlaczego nie miałyby być równie bezpieczne, co twój portfel i klucze?

Jest jeden prosty sposób na utrudnienie innym dostępu do twoich wirtualnych skarbów: nie ułatwiaj im odgadnięcia twojego hasła. Większość włamywaczy nie potrzebuje wyspecjalizowanych technicznych umiejętności, żeby dostać się na twoje konto – wystarczy kilka propozycji hasła i zautomatyzowany program.

A kiedy już uda im się na nie dostać, mogą spróbować użyć odgadniętego hasła na innych kontach, zgromadzić dane o tobie i twoich nawykach, przejąć konta, a nawet wykorzystać twoją cyfrową tożsamość.

Z Data Detox Kit dowiesz się, jak w kilku prostych krokach zwiększyć swoje bezpieczeństwo online.

Zaczynamy!



Autorzy
TACTICAL TECH

Wsparcie
Firefox

datadetoxkit.org
#datadetox

1.

ZAMKNIJ CYFROWE DRZWI

Blokady ekranu, z których korzystasz – hasło, wzór, odcisk palca czy technologia identyfikacji twarzy – to jeden z **najlepszych sposobów ochrony** przed intruzami. Istnieje wiele rodzajów blokad, a wybór tej najodpowiedniejszej może nastręczać trudności.

Jakaś blokada w telefonie, tablecie czy komputerze jest lepsza niż żadna. Ale tak jak z różnymi zamkami do drzwi, **niektóre blokady ekranu są skuteczniejsze od innych.**

Odblokowujesz telefon machnięciem palca na ekranie? Możesz ulepszyć zabezpieczenia i ustawić długie hasło. A może korzystasz z blokady w formie wzoru? Rozważ dłuższą kombinację. Twój kod PIN to 1234? Propozycja: rzuć kostką siedem razy i zapamiętaj PIN, który wskażą ci wyrzucone oczka.

Mała zmiana może w dużym stopniu przyczynić się do zwiększenia kontroli nad urządzeniem.

2.

WPUSZCZAJ MILE WIDZIANYCH

Stworzenie świetnego hasła to łatwizna. Wystarczy zastosować się do kilku podstawowych zasad. Hasło powinno być:

długie: **dobrze by miało przynajmniej osiem znaków, a jeszcze lepiej, żeby zawierało ich 16–20,**

unikalne: **każde hasło do każdej strony internetowej powinno być inne,**

losowe: **hasło nie powinno wynikać z logicznego schematu ani być łatwe do odgadnięcia; niezwykle pomocne są tu menedżery haseł.**

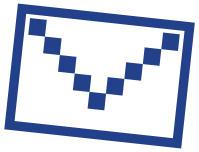
Najsilniejsze hasło to kombinacja liter, cyfr i znaków specjalnych. Ta stara zasada to nadal najlepszy sposób na stworzenie silnego, trudnego do odgadnięcia hasła. Niestety niektóre systemy nie przyjmują haseł ze znakami specjalnymi (takimi jak @#$%-=+), ale długi ciąg liter i cyfr jest zawsze lepszy niż krótki.

Do generowania i przechowywania haseł najlepiej jest używać **wyspecjalizowanego menedżera haseł**. Menedżer haseł – na przykład 1Password lub KeePassXC, często polecane przez ekspertów od bezpieczeństwa – to aplikacja, która służy wyłącznie do ochrony twoich danych logowania i innych ważnych informacji.

3.

DODAJ DRUGI KLUCZ

Ustaw uwierzytelnianie dwuetapowe (2FA, two-factor authentication) lub wieloetapowe (MFA, multi-factor authentication). Dzięki temu nawet jeśli ktoś pozna twoje hasło, **prawdopodobnie nie będzie mieć dodatkowego elementu niezbędnego do uzyskania dostępu.**



Przejrzyj ustawienia bezpieczeństwa na stronach internetowych i w aplikacjach, z których korzystasz najczęściej. Sprawdź, czy możesz ustawić w nich dodatkową warstwę zabezpieczeń. Zacznij od najważniejszych – aplikacji do finansów lub usług takich jak poczta mailowa, które są ci niezbędne do odzyskania dostępu do innych kont.

Google:
Zaloguj się na: myaccount.google.com →
Bezpieczeństwo →
Weryfikacja dwuetapowa →
Rozpocznij

Facebook:
Menu →
Ustawienia →
Bezpieczeństwo i logowanie →
Używaj uwierzytelniania dwuskładnikowego

Wskazówka: Ustawiając kolejny etap uwierzytelniania, musisz wybrać drugi sposób potwierdzenia, że ty to ty. Unikaj SMS-ów jako drugiego składnika na wypadek zgubienia telefonu. Wiadomość mailowa jest zwykle bardziej niezawodna.

4.

KOMENTUJ

Jeśli nie podoba Ci się, że strony internetowe i apki, z których korzystasz, stosują techniki uzależniającego i perswazyjnego projektowania lub dezinformację, możesz w mailu czy poście na Twitterze dać znać firmom, że nie zgadzasz się z takimi praktykami. Kiedy firmy poczują, że presję wywierają ich najcenniejsze „zasoby" – użytkownicy – istnieje szansa, że wprowadzą zmiany.

Jeśli uważasz, że twoja opinia nie została wysłuchana, jest na to niezwykle silna odpowiedź: skorzystaj z innej strony lub apki. Jeśli dasz znać firmie, że nie podoba ci się coś w jej stronie lub apce, a potem przestaniesz z niej korzystać – i zrobi to wystarczająco dużo osób – **zostanie to zauważone.**

5.

PODAJ DALEJ

Dziel się wiedzą! To wskazówka, o której łatwo zapomnieć, a która może przynieść duże efekty. Opowiadaj znajomym, rodzinie i współpracownikom o tym, co zauważasz, a nawet zaproponuj, żeby dołączyli do detoksu!

Wszyscy mamy problemy z kontrolowaniem nawyków korzystania z telefonu. Ważne, żeby znaleźć sposób, który najbardziej odpowiada tobie i twojemu stylowi życia. Eksperymentuj do momentu, w którym znajdziesz najlepszą metodę, a potem dostosowuj nawyki na bieżąco. Nie ma jednego, uniwersalnego rozwiązania.

I na koniec: opowiadaj o swoich technologicznych wyborach otoczeniu. Jeśli nie można się z tobą skontaktować przez komunikator po 20.00, ponieważ wtedy zaczynasz swój czas bez ekranu, daj znać rodzinie i znajomym, że o tej porze lepiej do ciebie zadzwonić.

DATA DETOX KIT

WYRABIAJ NAWYKI

i świadomość cyfrową

Kiedy ostatni raz zdarzyło ci się „odłączyć" i nie używać żadnych technologii przez dzień albo choćby przez godzinę?

Zacznijmy od tego, że nieodparty pociąg, jaki czujesz do technologii, nie jest twoją winą! Może cię to zaskoczy, ale twoje ulubione apki i strony internetowe zostały zaprojektowane tak, żeby każda funkcja, kolor czy dźwięk zatrzymywały cię na jak najdłużej i zachęcały do częstych powrotów.

Chcesz osiągnąć równowagę między życiem online a światem offline? Właśnie o tym jest ta część Data Detox Kit. Nauczysz się z niej, jak odrzucić to, co zbędne, i sprawić, że technologia będzie dodawać skrzydeł zamiast utrudniać życie.

Zaczynamy!

Autorzy
TACTICAL TECH

Wsparcie
Firefox

datadetoxkit.org
#datadetox

1.

ĆWICZ UWAŻNOŚĆ

To trudniejsze, niż mogłoby się wydawać. Uważność wymaga codziennego treningu. Jak mięśnie, które regularnie trzeba ćwiczyć, żeby je wzmocnić. Zacznij od przeanalizowania swojej relacji z technologią.

Ile czasu spędzasz, korzystając z telefonu?

Jeśli nie podoba ci się odpowiedź na to pytanie, możesz wykorzystać konkretne strategie, które pozwolą ci odzyskać kontrolę.

Jeśli chcesz spędzać mniej czasu na Facebooku, Instagramie czy Snapchacie, zmień ustawienia i uprawnienia dla tych apek, żeby lepiej odpowiadały twoim potrzebom.

Niektóre apki, na przykład Instagram, mają nawet opcję przypominania o osiągnięciu dziennego limitu.

Instagram:
Profil → Menu → Ustawienia → Twoja aktywność→ Ustaw codzienne przypomnienie

Jeśli telefon przerywa ci rozmowy w realnym życiu dzwonkami, wibracjami czy błyskami, możesz go **wyciszyć tymczasowo**, odłożyć ekranem do dołu, a nawet włożyć z powrotem do kieszeni lub torby, żeby nie mieć go w zasięgu wzroku.

2.

POZNAJ SZTUCZKI DIZAJNU

Projektowanie perswazyjne, tak zwane zwodnicze praktyki (dark patterns), to metoda tworzenia projektów oparta na ludzkiej psychologii, która ma cię sprowokować do zapisania się do czegoś, kupienia czegoś bądź udostępnienia większej ilości informacji, mimo że nie leżało to w twoich zamiarach.

Powszechnie stosowane bodźce (nudges), zwane również zapalnikami bądź impulsami, to na przykład konkretne kolory i rozmieszczenie przycisków. Lub niejasne teksty bądź niekompletne informacje. Czasami takie sztuczki są oczywiste, ale kiedy indziej trudniej je dostrzec. Możliwe, że zdarzyło ci się już zetknąć z nimi podczas subskrybowania czegoś albo zakupów online. Dlaczego są tak powszechnie stosowane? Ponieważ są skuteczne – sprawiają, że klikamy, subskrybujemy, kupujemy i wracamy po więcej. Im większą masz świadomość istnienia tych subtelnych zachęt i manipulacji na stronach internetowych, tym lepiej możesz się przed nimi chronić.

Jest kilka rzeczy, które możesz zrobić, żeby przechytrzyć swoje aplikacje.

Rozpoznaj moment pojawienia się bodźca: Po pierwsze wystarczy już sama świadomość, że takie techniki są stosowane.

Zrób zdjęcie i je udostępnij: Zrób zrzut ekranu, kiedy natkniesz się na przykład projektowania perswazyjnego w sieci, i udostępnij go znajomym (bez informacji, które pozwolą zidentyfikować jakiekolwiek osoby – prywatność przede wszystkim!). Możesz również poprosić firmę o zmianę praktyk.

Zachowaj spokój: Jeśli na stronie sklepu znajduje się zegar odliczający czas do końca zakupów, zapytaj „Czy to naprawdę takie pilne?". Jeśli złapiesz się na tym, że klikasz przycisk, którego nie chcesz kliknąć, zwróć uwagę na treść na przycisku i zastosowane kolory. Jeśli czujesz zdezorientowanie, nie zakładaj od razu, że to twoja wina – przyjrzyj się tekstom na stronie lub w apce, bo mogą być niejasne.

3.

ORIENTUJ SIĘ W MEDIACH

Możesz się nauczyć, jak przechytrzyć funkcje i dizajn, które namawiają cię do przewijania i klikania. I możesz też się dowiedzieć, jak zauważać informacje i posty, które celowo mają cię wprowadzić w błąd.

„Dezinformacja" i „fałszywe wiadomości" (fake news) to terminy, które na pewno obiły ci się o uszy. Nauczysz się rozpoznawać dezinformujące treści, jeśli będziesz zadawać krytyczne pytania wobec wszelkich informacji, które do ciebie docierają, w szczególności tych, które wydają się zaskakujące, bulwersujące lub zbyt dobre, by mogły być prawdziwe.

Z jakiej strony internetowej jest ta informacja?

Kto (i kiedy) ją stworzył?

Na jakie źródła powołują się autorzy?

Koniec końców chodzi o to, żeby sprawdzić, czy informacja jest prawdziwa czy fałszywa. Szczególnie jeśli chcesz się nią podzielić z rodziną lub znajomymi.

Jeśli uważasz, że tekst jest przykładem dezinformacji, i nie chcesz, żeby był szerzony, możesz zgłosić to na platformie, na której się pojawił – większość platform to umożliwia. Zastanów się też, czy dalej chcesz obserwować konto, na którym został opublikowany.