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

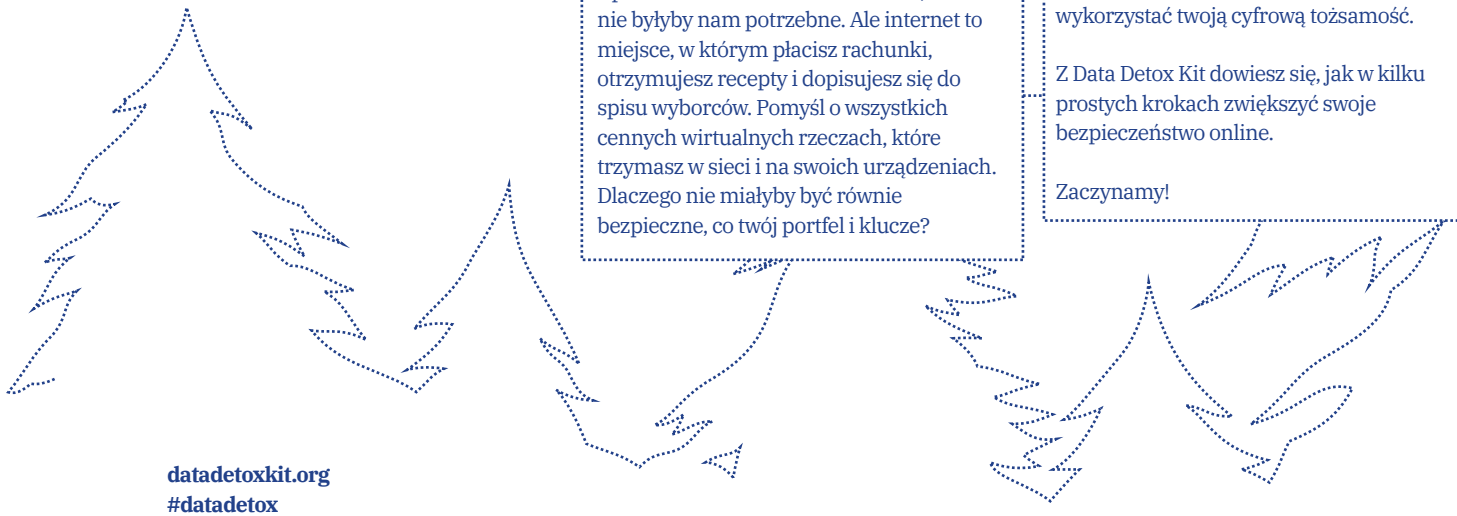
Gdyby po internecie krążyły tylko obrazki z psami w kostiumach dinozaurów, hasła nie byłyby nam potrzebne. Ale internet to miejsce, w którym płacisz rachunki, otrzymujesz recepty i dopisujesz się do spisu wyborców. Pomyśl o wszystkich cennych wirtualnych rzeczach, które trzymasz w sieci i na swoich urządzeniach.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

DATA DETOX KIT

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.