4.

ЗАХИСТІТЬ СВОЇ ВІРТУАЛЬНІ ЦІННОСТІ

Так само, як ви піклуєтеся про цінні речі в себе вдома, те саме слід робити з інформацією, яку ви зберігаєте віртуально. Не має значення, йдеться про фінансовий стан, скани паспорта чи навіть адресу й номер телефону, — варто подумати, де ви зберігаєте найбільш цінні особисті дані та як їх захистити.

Швидке очищення — хороший варіант маленького покращення за кавою. Знайдіть конкретну інформацію, яка зберігається у вас в електронній пошті, і видаліть її: наприклад, скани паспорта, банківські дані чи інформацію про страховку. Якщо вам це ще раз знадобиться, можна завантажити чи роздрукувати цю інформацію, а потім видалити з поштової скриньки.

Глибоке очищення більш ретельне, і ним корисно займатися раз на рік. Заархівуйте все на електронній пошті чи в соцмережі, завантажте все на комп'ютер та видаліть вміст з облікового запису, щоб почати з чистого аркуша.

Підказка: не просто видаляйте — також очистіть кошик і видаліть тимчасові файли!

Що робити з резервною копією, вирішуєте ви: її можна завантажити у хмару чи зберегти на зовнішній жорсткий диск або флешку. Не має значення, який варіант обирати — головне, щоб ви не втратили цю інформацію, вона була захищена надійним паролем, а вам було зручно користуватися цим способом.

5.

ПЕРЕДАЙТЕ ДАЛІ

Про це часто забувають, але мережа інтернет не просто так називається "мережею". Ми всі поєднані онлайн, не лише як "друзі" в соцмережах, але й через контакти в електронних листах та фото, якими ми ділимося. Коли ви налаштовуєте безпеку облікових засобів, підбираєте надійні паролі та чистите інформацію про себе онлайн, це приносить користь не лише вам — завдяки вашим зусиллям також покращується безпека інших.

Коли ви чистите електронну скриньку й акаунти в соцмережах, подумайте, що ще такого можна завантажити і видалити, що може допомогти вашим друзям чи колегам: банківську інформацію сестри, код доступу до офісу або скан синового паспорта — їх легко видалити, але вони можуть завдати чимало турбот, якщо потраплять до людини з поганими намірами.

Передайте далі! Кількох простих кроків достатньо, щоб покращити рівень онлайн-безпеки. Поділіться цією інструкцією для цифрового детоксу з друзями, рідними чи колегами, щоб і вони могли змінити свої цифрові звички так, як їм це зручно.

DATA DETOX KIT

SHIFT СВОЇ НАЛАШТУВАННЯ,*

щоб ваші дані були в безпеці

Якби інтернет потрібен був лише для того, щоб ділитися фоточками собак у костюмі динозавра, паролі були б не надто й потрібні.

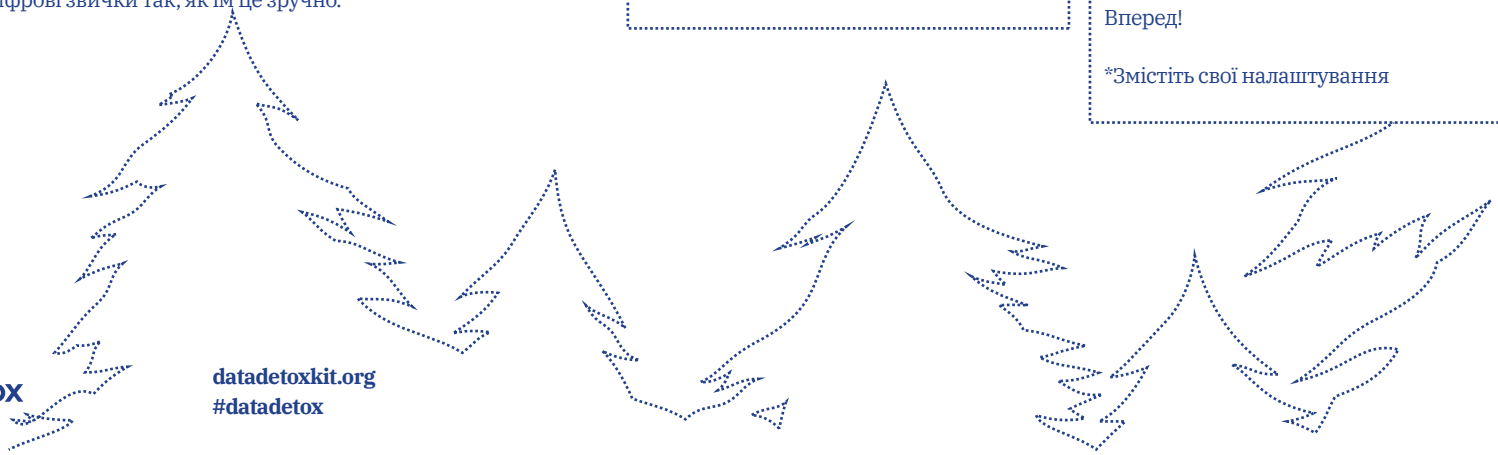
Але в інтернеті ви також сплачуєте рахунки, записуєтесь до лікаря, змінюєте виборчу адресу.

Подумайте про всі ваші "віртуальні цінності", які ви завантажуєте в інтернет — і зберігаєте на своїх пристроях — чому б не стежити за їхньою безпекою так само, як за гаманцем чи ключами?

В рамках Цифрового детоксу ви дізнаєтеся, що можна зробити, щоб покращити рівень своєї безпеки онлайн.

Вперед!

*Змістіть свої налаштування



створено
TACTICAL TECH

за підтримки
Firefox

datadetoxkit.org
#datadetox

1.

ЗАМКНІТЬ СВОЇ ЦИФРОВІ ДВЕРІ

Блокування екрану: пароль, графічний ключ, відбиток пальця чи ідентифікація за обличчям, які ви використовуєте, щоб розблокувати свій пристрій — один з найкращих способів захисту від людей, які хочуть без дозволу добратися до вашого телефона. Але блокування є різні, а вибрати між ними часом важко. Будь-який спосіб блокування телефона, планшета чи комп'ютера — краще, ніж взагалі жодного. Але так само, як бувають різні замки на двері, деякі способи блокування екрану надійніші за інші.

Найбільш надійний метод блокування — довгі унікальні паролі. Це означає, що ви розблоковуєте пристрій за допомогою пароля, який включає літери, цифри та спеціальні знаки.

Скажімо, ви зараз розблоковуєте телефон за допомогою свайпу. Ви можете відразу ж покращити рівень безпеки за допомогою довгого пароля. Чи може, ви використовуєте графічний ключ? Можливо, варто зробити його довшим? Чи у вас пін-код 1234? Спробуйте кинути гральні кубики сім разів і використати результат у якості піну.

2.

ВПУСТИ (ЛИШЕ) МЕНЕ

Створити якісний пароль просто. Потрібно лише дотримуватися кількох базових принципів. Ваші паролі мають бути:

Довгими: **паролі мають складатися принаймні з 8 знаків. А краще з 16-20.**

Унікальними: **кожен пароль, який ви використовуєте — на кожному сайті — має бути інакшим.**

Довільними: **паролі не мають бути логічними і їх не має бути легко вгадати. Для цього корисні менеджери паролів.**

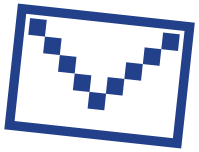
У найкращих паролях використовується поєднання літер, цифр та спеціальних знаків. Ця перевірена часом порада досі допомагає створювати більш надійні паролі, які важче зламати. На жаль, деякі системи не дозволяють використовувати спеціальні знаки (такі як @#$%-=+) у паролях, але довга комбінація літер і цифр все одно краща за коротку.

В ідеалі слід використовувати спеціальний менеджер паролів, щоб створювати і зберігати паролі. Менеджер паролів — наприклад, 1Password і KeePassXC, які рекомендують експерти з безпеки — це по суті додаток, який створений спеціально для того, щоб зберігати інформацію про ваші облікові записи та інші конфіденційні дані.

3.

ДОДАЙТЕ ДРУГИЙ КЛЮЧ

Налаштування двофакторної авторизації (2FA) чи багатофакторної авторизації (MFA) означає, що навіть якщо хтось і дізнається ваш пароль, ця людина, швидше за все, не матиме додаткового елемента, або фактора, який потрібен, щоб зайти в обліковий запис.



Подивіться на налаштування сайтів і додатків, якими ви користуєтеся найчастіше, щоб перевірити, чи можете ви налаштувати цей додатковий "ключ". Починайте з найважливіших додатків — тих, які пов'язані з фінансами, а також з електронної пошти, якою ви користуєтеся, щоб відновити доступ до інших облікових записів.

Google:
Залогіньтеся в myaccount.google.com → Безпека → 2-етапна перевірка → Почати

Facebook:
меню → Налаштування → Безпека та вхід → Двоетапна перевірка

Підказка: Коли ви налаштовуєте другий рівень перевірки, вам знадобиться додатковий спосіб підтвердити, що це ви. Намагайтеся уникати смс-ок в якості другого фактора, бо ви можете загубити телефон. Електронна пошта зазвичай надійніша.