Загальні поняття

Інформація – найстрашніша зброя з усіх існуючих. Головне – правильно її використовувати.

1. Краще бути революційно-пильним живим параноїком, ніж мертвим (чи винним у загибелі інших) пофігістом. Плекай і вирощуй в собі параною, бо то насправді – інстинкт самозбереження.
2. Тебе ЗАВЖДИ слухають і ЗАВЖДИ бачать. Що б, як і з ким ти не говорив. Пам'ятай, що твій телефон слухають, смс та повідомлення в соцмережах читають не тільки адресати, розмови в реальному житті підслуховуються (навіть якщо ти впевнений, що це не так). Враховуй це, і завжди ретельно фільтруй те, що ти говориш/пишеш/сигналізуєш морзянкою/показуєш жестами/голосно думаєш.
3. Розлогінюйся! Завжди знайдуться ті, кому цікаво почитати повідомлення на необережно залишеній відкритою сторінці.
4. Запаролюй! Телефони, ноутбуки, аккаунти в соцмережах – все має бути під паролем, все має блокуватися, навіть якщо ти «відійшов на секундочку».
5. Не полегшуй задачі ворогу! Якщо на всі ресурси в тебе один і той самий пароль – твої ресурси взагалі не запаролені.
6. Захисту багато не буває! На всі свої онлайн-сторінки активізуй подвійну аутентифікацію із підтвердженням входу за допомогою мобільного телефону.
7. Будь уважним! Інтернет-ресурси зазвичай за замовчуванням ставлять галочку «запам'ятати мене». Один раз запам'ятав – назавжди відкрив доступ браузеру до своїх даних.
8. Немає неважливої інформації – є не ті вуха. Будь-яка дрібниця, сказана тобою, може виявитись цінними даними для ворога.
9. Шифруй! Вивчай програми, які дозволяють зберігати дані у зашифрованому вигляді і під паролем, завжди користуйся ними для збереження своєї інформації.
10. Не завжди є час замітати сліди! Всі файли з важливою інформацією тримай на зовнішніх носіях, які легко знищити. Краще завжди робити декілька дублюючих носіїв з однаковими даними і зберігати їх у різних місцях.
11. Не підставляйся! Не тримай нічого вдома чи у очевидних місцях – там шукатимуть в першу чергу, а обшуки у квартирах активістів вже стали повсякденністю.
12. Не передавай носії на зберігання третім особам.
13. Диск С існує виключно для операційної системи. Все інше зберігається на запаролених логічних дисках D://, E://, etc! Так, робочий стіл – то теж диск С.
14. Онлайн-банкінг. Банківські картки небезпечно прив'язувати до загальновідомих номерів. Отримання доступу до них не складає серйозної задачі, а ризики високі. Важливо – для убезпечення власних фінансів під час використання онлайн-банкінгу бажано використовувати ВПН або анонімні вікна браузеру.

Інформаційна гігієна за захист в соцмережах

Важливі правила.

1. ретельно перевіряти джерела інформації. Сайти типу elise.ua та bbccnn.ua - розповсюджувачі фейків, а не достовірних даних.
2. Онлайн-тести «який ти герой фільму» чи подібні – замасковані під невинну розвагу сервіси для збору інформації не лише про Вас, а про Ваших знайомих.
3. Важливо не відкривати сторонніх відео/файли (особливо архіви), які надсилають малознайомі користувачі.
4. Файли з розширенням .exe можуть ховати в собі віруси або рекламний софт, який має на меті збір інформації або вимагання грошей шляхом блокування комп'ютера.
5. Розсилки «передай повідомлення 100500 друзям» або «хворіє 10-місячна дитина» - вірусні, також мають на меті збір інформації про зв'язки між користувачами та зацікавлення.
6. Алгоритми фб працюють на збір даних про історію дзвінків, повідомлень, відвідування сторінок в браузері. Уважно відслідковуйте рекламні пропозиції фб та по максимуму блокуйте доступ сторонніх ресурсів до вашого аккаунту.

Попередній пункт так само стосується дочірніх проектів ФБ – інстаграм та ватсапп. Дані додатки встановлюються на телефон, та відслідковують також дзвінки та платежі через онлайн-банкінг.