ІНТЕРНЬЮЗ
УКРАЇНА

Генрі Дем'яновіч

БАЗОВІ ПОРАДИ З КІБЕР БЕЗПЕКИ

Зміст

КРОК 1:

Подумайте, які активи ви маєте?

Ваш цифровий актив – це гаджети, акаунти та документи, які ви використовуєте у своєму робочому та особистому житті.

Випишіть усі ваші активи на аркуш паперу або в електронний документ.

КРОК 2:

Які небезпеки можуть спіткати ваші активи?

Подумайте, що може статися з кожним із ваших активів?

Наприклад, поштовий обліковий запис можуть зламати, прочитати ваші листування або написати щось від вашого імені. Ноутбук можуть вкрасти, його можна залити водою або він може зламатися. Проаналізуйте кожен пункт вашого списку цифрових активів та додайте потенційні ризики.

КРОК 3:

Як запобігти ризикам?

Для кожного ризику спробуйте знайти відповіді на запитання:

- Що зробити, щоб ризик не стався або як зменшити ймовірність його настання?
- Що варто зробити заздалегідь, щоб у разі настання ризику наслідки були мінімальні?
- Якщо ризик все ж таки станеться, що варто зробити відразу після його настання для мінімізації шкоди?

РОЗГЛЯНЕМО ПРИКЛАД

Мій актив – обліковий запис у Фейсбуці.

Що з ним може статися?

- Я можу втратити доступ до облікового запису, забувши пароль.
- Його можуть зламати.
- Його можуть заблокувати через масову атаку ботів зі скаргами на мої пости.

Для ризику «Злам акаунту у ФБ» відповім на свої запитання:

Що зробити, щоб ризик не стався чи зменшити ймовірність його настання?

Відповідь: Встановити двофакторну аутентифікацію на вхід в обліковий запис, використовувати складний та унікальний пароль.

Що варто зробити заздалегідь, щоб у разі настання ризику наслідки були мінімальні?

Відповідь: Не вести важливих листувань через Фейсбук-месенджер.

Якщо ризик все ж таки станеться, що варто зробити відразу після його настання для мінімізації шкоди?

Відповідь: Сповістити друзів у ФБ про те, що акаунт був зламаний та спробувати відновити доступ до облікового запису через техпідтримку.

Якщо у ФБ велося конфіденційне листування – оперативно сповістити через альтернативні канали зв'язку співрозмовника про те, що акаунт був зламаний і листування могли побачити. Можливо, співрозмовник зможе видалити повідомлення, перш ніж зламувач зможе їх прочитати.

ЗАХИСТ ОБЛІКОВИХ ЗАПИСІВ

КРОК 1:
Які облікові записи потрібно захищати?

Усі – і робочі, і особисті. Важливо використовувати різні паролі для різних акаунтів.

КРОК 2:
Пароль

Декілька ознак надійного пароля

- Довгий (від 8 символів).
- Різноманітний (містить великі, малі літери, цифри).
- Унікальний (різні паролі для різних сайтів).
- Не пов'язаний з вами (не використовуйте в паролях дату народження, нікнейм, прізвисько собаки тощо).

У сучасних реаліях регулярно міняти паролі не потрібно. Вам варто змінити свій пароль тільки в тому випадку, якщо маєте підозру, що хтось його дізнався.

КРОК 3:
Зберігання паролів

Для безпеки варто використовувати унікальні паролі для кожного сайту, але запам'ятати велику кількість унікальних паролів практично неможливо. Тому слід використовувати менеджер паролів. **Якщо у вас iPhone**, швидше за все, ви вже зустрічалися із вбудованим парольним менеджером, який пропонує зберігати паролі з додатків і сайтів, а також вміє генерувати складні паролі при реєстрації.

Якщо ж ви віддаєте перевагу Android, то могли бачити в роботі Google Smart Lock.

Окрім того, всі популярні браузери пропонують вам зберігати паролі в них.

Також є спеціальні менеджери паролів, вони дозволяють зберігати всі паролі в одному додатку, але отримувати доступ до них на будь-якому пристрої. Наприклад, BitWarden.

Якщо ви все ж таки вирішили запам'ятовувати паролі – використовуйте щонайменше три різні паролі:

1. основний, для особистого життя, пошти, банків;
2. для роботи, робочих акаунтів та сайтів;
3. для «сміттєвих» сайтів, де потрібно зареєструватися для чогось разового чи не дуже важливого, наприклад, для завантаження електронної книги.

КРОК 3:
Двофакторна автентифікація

Більшість сайтів дозволяють налаштувати двофакторну автентифікацію. Іноді це називають двоетапною перевіркою. Першим фактором є ваш пароль. Другим чинником може бути щось із переліку:

- Pop-up повідомлення з текстом «Ви входите у свій обліковий запис, підтвердіть вхід»
- Одноразовий SMS-код
- OTP-код із програми Google Authenticator (або аналогічної програми, що генерує коди)
- USB-ключ (виглядає як флешка)
- Резервні коди відновлення (генеруються після налаштування як другий фактор будь-якого іншого фактора)

Ви можете вибрати будь-який зручний для вас другий фактор, проте слід знати деякі особливості кожного з них.

- **Pop-up повідомлення** буде доступне лише на смартфонах, на яких здійснено вхід до облікового запису. Цей спосіб працює з обліковими записами Google, Facebook та деякими іншими. Більшість сайтів та програм не підтримують такий метод.

- **СМС-код** – стандартний другий фактор, його підтримує більшість сервісів. Проте варто розуміти, що СМС можна перехопити, і якщо у зловмисника буде мета зламати персонально вас, незважаючи на ціну атаки, або якщо опонентом буде держава – СМС-код не зможе вас захистити.
- **OTP-ключ** – найпоширеніший та найнадійніший спосіб двофакторної автентифікації. Ви можете вибрати одну з багатьох програм для генерації ключів, але важливо пам'ятати, що стандартний Google Authenticator не дозволяє вам робити резервну копію ваших кодів доступу. Це означає, що ви втратите доступ до своїх облікових записів, якщо випадково видалите Google Authenticator зі смартфона або якщо втратите доступ до самого смартфона. Щоб цього уникнути, можна використовувати Aegis. Ця програма дозволяє робити резервні копії ваших кодів, захистити копії паролем та доступ до кодів також буде надійно захищений.
- **USB-ключ** – чудовий спосіб входу. Microsoft пропонує відмовитися від пароля на користь USB-ключа. Ключ може працювати і з комп'ютером, і зі смартфоном. Існують також бездротові ключі NFC. Особливість ключа в тому, що він фізично один, і щоб отримати доступ до облікового запису, необхідно тримати його в руках. Якщо ваш ключ лежить у надійному місці – ніхто ніяк не зможе отримати доступ до облікового запису, навіть маючи ваш пароль. Але і ви не зможете отримати доступ до свого облікового запису, поки не візьмете ключ до рук.
- **Резервні коди** – останній рубіж, який може врятувати вас у критичній ситуації. Резервні коди слід роздрукувати на папері та відкласти у надійне місце. За умови втрати доступу до свого другого фактора, вони можуть вас врятувати.

  Надійний пароль та налаштована двофакторна автентифікація – запорука безпеки ваших облікових записів.

КРОК 5:
Безпарольні облікові записи

На деякі сайти та деякі програми можна входити без пароля. Ви можете зайти, використовуючи свій обліковий запис у Google або Facebook. Вхід у такому разі станеться буквально однією кнопкою. Небезпека такого входу полягає в тому, що ви можете ненароком передати сайту набагато більше інформації про вас, ніж він просить. Уважно читайте, які доступи отримає сайт під час авторизації через Google або Facebook. Зазвичай сайт отримає ваше ім'я, пошту, можливо, аватарку і дату народження. Якщо сайт вимагає більше інформації – це привід задуматися про його безпечність.

В цілому, використання Google або Facebook облікових записів для авторизації на інших сайтах значно надійніше, ніж реєстрація на них із паролем. Адже вам достатньо захистити лише свій Google або Facebook, а не всі облікові записи на всіх сайтах.

ЗАХИСТ НОУТБУКА ТА КОМП'ЮТЕРА

КРОК 1:
Встановлення пароля входу

Пароль на вхід у ноутбук чи комп'ютер захистить вас від короткострокового доступу до техніки третіх осіб. Якщо ви залишите ноутбук без пароля на 5 хвилин, хтось може зайти в нього та швидко подивитися щось (наприклад, історію браузера).

Пароль не захистить вас у разі крадіжки або втрати доступу до ноутбука.

КРОК 2:
Використання шифрування BitLocker

Для захисту інформації на вашому гаджеті можна встановити шифрування диска BitLocker. Воно доступне в Pro версії Windows 7, 8, 8.1, 10.

На старіших ноутбуках і комп'ютерах вам потрібно буде придумати пароль, який слід вводити додатково до пароля на вхід до системи. На новіших ноутбуках і комп'ютерах пароль вигадувати не доведеться.

При увімкненні BitLocker система запропонує зберегти або роздрукувати ключ відновлення. Обов'язково збережіть його будь-де – цей ключ допоможе вам відновити доступ до всіх ваших файлів.

КРОК 3:

Увімкнення Windows Defender

Захисник Windows – надійний антивірус, вбудований у систему. Його достатньо для базового захисту системи від стандартних загроз. У більшості випадків використання безкоштовних антивірусів не має сенсу, до того ж, жоден із них не буде так глибоко інтегрований у систему, як вбудований у неї захисник.

Якщо ви використовуєте гаджет з системою iOS, ви можете встановити додаток за посиланням: http://malwarebytes.com/.

КРОК 4:

Перевірка налаштувань приватності

Windows 10 якісно захищає нашу приватність. Ви можете дізнатися, які програми отримували доступ до вашої камери та мікрофона і чи якась програма чи непомічений вірус слідкує за вами.

Для цього зайдіть у **Установки > Конфіденційність і в лівому меню виберіть «Мікрофон» або «Камера»**. Ви побачите програми з магазину Windows, яким дозволено та заборонено доступ до камери та мікрофона. Трохи нижче ви побачите список усіх програм (зокрема, і не з магазину), які отримували доступ до камери або мікрофона. Якщо ви помітите там щось зайве, це привід звернутися за консультацією до фахівця з кібербезпеки. Можливо, хтось підслуховував чи підглядав за вами.

Важливо розуміти принцип роботи веб-камери. Якщо ваш ноутбук має індикатор роботи камери і він справний (світиться, коли камера працює) – ви можете бути впевнені, що за вами ніхто не підглядає. Наразі неможливо отримати доступ до камери ноутбука та програмно відключити індикатор роботи. Він гарантовано горітиме, коли камера працюватиме, якщо тільки повністю не вийде з ладу.

ЗАХИСТ СМАРТФОНА

КРОК 1:
Встановлення пароля або PIN-коду на вхід

Графічний ключ для входу в систему є найменш надійним. Його можна підглянути, вгадати, відновити за слідами на екрані. Більшість людей використовують один із 20–30 стандартних патернів малюнків, які легко підібрати.

Використовуйте пароль або PIN-код.

Ви також можете використати відбитки пальців для входу, однак варто бути обережними із Face ID, адже в деяких смартфонах цей захист можна обійти за допомогою фото.

КРОК 2:
Перевірка налаштувань приватності

У налаштуваннях вашого смартфона є пункт **«Захист приватності»** або аналогічний залежно від системи. У ньому ви можете побачити, які програми мають доступ до вашої камери, мікрофона, геолокації. У деяких версіях Android ви також можете побачити, коли востаннє програма отримувала доступ.

Якщо ви бачите у списку програми, яких там бути не повинно, видаліть їх, а також зверніться за консультацією до фахівця.

КРОК 3:

Програмне забезпечення – лише з офіційних джерел

Завжди встановлюйте програми тільки з офіційних магазинів програм, як-от Play Market, App Gallery, Galaxy Store, F- Droid, App Store. Ніколи не намагайтеся знайти потрібний вам додаток у гуглі за запитом «завантажити *додаток* безкоштовно apk», адже в такому випадку ви майже гарантовано заразите свій смартфон шкідливою програмою.

Саме шкідливою програмою, але не вірусом. Справа в тому, що вірусів у тому ж значенні, що і на ПК, на смартфонах майже немає. Замість цього ви можете встановити шкідливу програму, яка при установці вимагатиме доступу до всього, до чого зможе дотягнутися – до файлів, камери, мікрофона, дзвінків, контактів. Так шкідливі програми можуть шпигувати за вами або показувати свою рекламу.

КРОК 4:

Екстрене скидання смартфона з повним очищенням

Іноді буває потреба терміново скинути смартфон до заводських налаштувань, вилучивши всі дані на ньому. Ви можете скористатися для цього програмою **Locker**, яку необхідно встановити з магазину програм F-Droid.

Програма вимагатиме права адміністратора пристрою – дайте їх їй, адже тільки так вона зможе зробити повне скидання. Скидання відбудеться при неправильному введенні PIN-коду кілька разів (кількість попередньо задається в налаштуваннях). Ви також можете увімкнути або вимкнути повідомлення про те, що телефон буде скинутий під час неправильного введення коду.

ЗАХИСТ ДАНИХ

КРОК 1:

Захист від втрати

Для того, щоб не втратити доступ до своїх даних, потрібно регулярно (наприклад, раз на тиждень) робити резервну копію всієї важливої інформації на один із зовнішніх пристроїв:

флешку

зовнішній жорсткий диск

хмару

На ноутбуці або комп'ютері можна використовувати спеціальні програми, які дозволяють створити хмарну папку прямо на диску. У такому випадку все, що вам потрібно – це зберігати важливі файли всередині цієї хмарної папки. Така папка зберігається на вашому комп'ютері, всі файли будуть доступні без інтернету, але вона завжди синхронізується з хмарою, роблячи резервну копію всіх файлів автоматично.

Одним із таких рішень є **OneDrive**, вбудований у Windows. Ви можете використовувати 5 безкоштовних гігабайт або купити 1000 гігабайт у хмарі за 6 доларів на місяць. OneDrive дозволяє не тільки створити хмарну папку на диску, але й автоматично синхронізувати папки «Документи», «Робочий стіл» та «Зображення».

Ви також можете використовувати будь-який інший хмарний сервіс (наприклад, Google Drive або власна копія OwnCloud, запущена на персональному сервері чи сервері організації.

КРОК 2:

Захист від крадіжки та компрометації

Для захисту інформації від крадіжки варто подбати про безпеку пристроїв, на яких інформація зберігається:

- **для ноутбука:** встановіть пароль на вхід та увімкніть шифрування диска BitLocker,
- **для хмари:** використовуйте надійний пароль, налаштуйте двофакторну автентифікацію,
- **для флешки:** зашифруйте флешку чи саму інформацію. Для цього можна використовувати BitLocker (тоді флешку можна використовувати лише з комп'ютерами на ОС Windows). Ви також можете використовувати спеціальну програму для шифрування флешки або деяких файлів – VeraCrypt. У такому випадку ви зможете отримати доступ до файлів на будь-якому пристрої, на якому встановлена ця програма.

Якщо ви шифруєте файли, то їхні резервні копії також мають бути зашифровані. Водночас вам не обов'язково шифрувати файли перед збереженням їхньої копії в хмару – достатньо захистити свій хмарний обліковий запис.

КРОК 3:
Відновлення даних

Не всі дані можна відновити, деякі з них втрачаються назавжди. Ви можете відновити будь-які дані, збережені у хмарних сховищах Microsoft OneDrive та Google Drive. Ви можете відновити навіть файли, видалені з кошика (на це в залежності від сервісу у вас буде від 14 до 120 днів).

Якщо ви використовуєте для зберігання даних HDD диски – ви, ймовірно, можете відновити нещодавно видалені дані з них. Однак ви скоріш за все не зможете відновити дані з диска SSD, який може бути встановлений у вашому ноутбуці або комп'ютері.

Саме тому варто регулярно робити резервну копію всіх важливих для вас даних.

Завжди зберігайте всі важливі файли щонайменше у 2 різних місцях, але не забувайте захистити кожне з них.

ЗАХИСТ ТАЄМНИЦІ ЛИСТУВАННЯ

КРОК 1:
Електронна пошта

Усі стандартні послуги електронної пошти шифрують з'єднання з вашим браузером або поштовим клієнтом. Це означає, що всі листи, які ви надсилаєте та отримуєте, можете бачити тільки ви, ваш співрозмовник та сам поштовий сервіс. Сторонні можуть отримати доступ до вашого листування двома способами:

- зламати ваш обліковий запис,
- отримати юридичний ордер на перегляд вашого листування, який буде зобов'язаний виконати ваш поштовий оператор.

Існує два шляхи для захисту вашого листування: шифрування пошти на стороні клієнта або використання зашифрованої пошти.

Перший спосіб доволі трудомісткий:

1. Ви та ваш співрозмовник генеруєте собі зв'язки ключів: публічний та приватний. Ви можете скористатися браузерним розширенням Mailvelope або ви створити ключі в поштовому клієнті Mozilla Thunderbird.
2. Ви зі співрозмовником обмінюєтеся своїми ПУБЛІЧНИМИ ключами та імпортуєте їх у свої поштові клієнти (або в браузерне розширення Mailvelope).
3. Під час створення листа ви вмикаєте режим шифрування.
4. Ви обмінюєтеся зашифрованими листами.

У такому разі, якщо ви зайдете у свій поштовий обліковий запис на будь-якому іншому пристрої, зашифроване листування буде виглядати як безглуздий набір тексту або як обмін текстовими файлами із незрозумілим набором знаків у них. Ні ви (без вашого ключа), ні поштовий сервіс, ні будь-хто інший не зможе прочитати ваше листування. Однак у відкритому вікні будуть деякі дані, як-от адреси відправника та одержувача, деяка сервісна інформація.

Як альтернативу можна використовувати будь-який сервіс безпечної пошти, наприклад Protonmail. Важливо розуміти, що зламавши ваш обліковий запис на подібному сервісі, зловмисник зможе побачити все листування, на відміну від першого варіанту, при якому зловмисник побачить безглуздий набір символів.

КРОК 3:
Месенджери

Розглянемо три популярні месенджери: **Telegram**, **WhatsApp**, **Signal**.

Signal – один із найзахищеніших месенджерів у світі. У ньому ви знайдете базовий функціонал, листування, дзвінки, стікери та смайли. Ви можете налаштувати автоматичне видалення повідомлень.

WhatsApp – аналог Signal із технічної точки зору, адже у них однаковий алгоритм шифрування. В обох месенджерах ваше листування – це ваша відповідальність, воно зберігається на ваших пристроях, але WhatsApp дозволяє робити резервні копії.

Telegram – дуже популярний месенджер, але вважається найменш безпечним серед згаданих. Варто використовувати секретні чати в Telegram, які працюють за тим самим принципом, що й Signal і WhatsApp. Вони зберігаються лише на ваших пристроях (на одному конкретному пристрої, з якого чат було розпочато) і до них не можна отримати доступ навіть зламавши обліковий запис.

Можливостей цих трьох месенджерів вистачить вам для того, щоб бути в безпеці, а ваші листування залишалися конфіденційними. Але важливо розуміти, що месенджери не пропонують вам анонімність – всі вони пов'язують ваш профіль із номером телефона.

Кожен із цих месенджерів можна додатково захистити: увімкнути пін-код для входу в месенджер на конкретному пристрої або двофакторну автентифікацію..

КРОК 1:
Програми смартфона

Для пошуку програм для смартфона використовуйте вбудований у систему магазин програм (App Store, Play Market, App Gallery, Galaxy Store тощо).

Ви також можете використовувати магазин вільного ПЗ F- Droid для Android.

КРОК 2:
Програми для ноутбука та комп'ютера

Для початку скористайтеся вбудованим у систему магазином програм (Windows Store, Mac App Store) – можливо, потрібна вам програма є там.

Якщо потрібної програми немає у стандартному магазині програм – відвідайте офіційний сайт видавця програми. Не завантажуйте програми з неперевірених джерел, оскільки вони можуть мати прихований шкідливий функціонал та заразити вашу систему вірусами.

КРОК 3:
Встановлення програм

Будьте уважні під час встановлення програм. Завжди вибирайте докладний режим установки там, де це можливо. Під час встановлення уважно читайте всю інформацію на кожному кроці. Дуже часто на деяких кроках ви зустрінете автоматично поставлені галочки згоди із встановленням додаткового, сміттєвого програмного забезпечення. Завжди

відключайте такі галочки, адже таким чином у вашу систему може потрапити небажане програмне забезпечення, будь-які рекламні банери, зайві браузери або доповнення до них. Найчастіше серед цих програм не буде вірусів, але самі по собі ці додаткові програми – сміття, яке захаращує систему і заважає вам ефективно використовувати ваш комп'ютер.

КРОК 4:

Оновлення програмного забезпечення

Для підтримки високого рівня безпеки системи завжди варто оновлювати систему, програми, драйвери до останньої актуальної версії. Регулярно у програмах чи операційних системах знаходять недоліки у безпеці. Видавець програмного забезпечення (ПЗ) вносить необхідні виправлення, як тільки йому стає відомо про ваду. Усі виправлення надходять до вас у вигляді оновлень. Іноді оновлення додають функціонал, виправляють помилки, але іноді закривають прогалини у безпеці.

Завжди використовуйте останню актуальну версію системи, ПЗ та драйверів, щоб максимально знизити ризики використання вразливостей у програмній та апаратній частині вашого пристрою.

БЕЗПЕЧНИЙ ІНТЕРНЕТ

КРОК 1:
Використовуйте довірені мережі

Довіреними ви можете вважати мережі, які самі налаштовували або які налаштовувалися для вас. Ваші домашня та робочі мережі можна вважати довіреними.

КРОК 2:
HTTPS Everywhere

Під час серфінгу в Інтернеті переконайтеся, що всі сайти, з якими ви взаємодієте, підтримують протокол зв'язку HTTPS. Для цього зверніть увагу на адресний рядок. Біля адреси сайту має стояти замочок. Він означає, що між вами та сайтом встановлено зашифроване з'єднання, ніхто крім вас та сервера не зможе дізнатися, що конкретно ви робите на сайті, які дані передаєте чи завантажуєте.

Ви можете встановити у свій браузер розширення HTTPS Everywhere, воно попередить вас про те, що якийсь сайт не використовує протокол HTTPS і тому його не можна вважати безпечним.

Важливо розуміти, що «замочок» на сайті не означає автоматично, що сайт безпечний. Йдеться лише про те, що між вами та сайтом встановлено безпечне захищене з'єднання.

КРОК 3:
VPN

VPN – це віртуальна приватна мережа. Використовуючи VPN, ви створюєте захищений зашифрований тунель між вами та VPN сервісом. Ніхто на шляху від вас до сервера VPN не зможе не тільки перехопити ваш трафік, але й дізнатися, куди ви прямуєте. VPN приховує від сторонніх очей пункт вашого призначення – сайт або сервер програми, на яку ви заходите. Він також приховує все, що ви передаєте всередині тунелю: повідомлення, дані, файли.

Ви можете використовувати VPN, перебуваючи в невідомих мережах, наприклад, у готелі, ресторані або на міській площі.

Проте VPN не врятує вас від загроз на стороні вашого пристрою (віруси, шкідливі програми) та на стороні сайту, на який ви заходите. Деякі сайти можуть бути вразливими до зламу і через них можна буде зламати вас.

КРОК 4:
Фільтруйте сайти, які ви відвідуєте

Більшість усіх відомих сайтів з мільйонами відвідувань на день безпечні для вас. Загрози можуть приховувати маловідомі сайти, на які ви потрапили випадково.

На такому вебсайті можуть бути віруси. З ними впорається ваш антивірус, але будьте обережні з кнопками. Яскраві кнопки «Скачати» можуть завантажити на ваш комп'ютер програму, яка показуватиме вам рекламу. Такі програми можуть оминати антивірус, оскільки вони і є вірусами. Уважно дивіться розширення файлу, який завантажуєте: розширення*. exe свідчитиме про те, що, можливо, це шкідлива програма.

ВИСНОВКИ

Цифрова безпека – це не лише встановлення антивірусу. Це постійний та тривалий процес, який має стати звичкою. Безумовно, ви можете просто зараз перевірити всі ваші пристрої та облікові записи, переконатися, що вони в безпеці, зашифрувати всю важливу інформацію та зробити резервні копії. Але якщо зробити це лише один раз – результат вас не потішить. Хибне почуття безпеки, створене під час захисту, може спричинити безтурботність і відкрити пролом у системі вашої безпеки. Ви можете думати «У мене все налаштовано» і перестати стежити за своїми діями, адже ви вже в безпеці. Саме тоді вас можна атакувати, і саме тоді ви найбільш уразливі.

Безпека – це процес, який не можна переривати. Вам слід виховувати в собі звички безпечної поведінки, наприклад, завжди закривати кришку ноутбука, коли відходите від нього, або завжди дивитися на адресний рядок, коли заходите на будь-який, навіть звичний, сайт.

Абсолютної безпеки не існує. Проте існують правила, звички та щоденні дії, які вас до неї наблизять. Нові загрози, як і нові рішення, виникають постійно.