Безпека в Інтернеті: що потрібно знати

Від соціальних мереж – до онлайн-банкінгу: сьогодні Інтернет проник у наше життя і діяльність. Окрім комп'ютерів та ноутбуків, ми підключаємо до Інтернету все – мобільні телефони, планшети, холодильники, телевізори й багато інших портативних пристроїв. Саме тому дуже важливо знати якомога більше про безпеку у Всесвітній мережі.
Необхідно віднайти правильні способи захисту нашого приватного життя, коли ми перебуваємо онлайн.

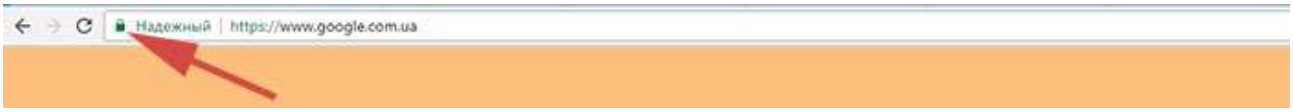
Багато хто думає, що безпека в Інтернеті – це ілюзія, і бути захищеним зараз неможливо, адже веб-сайти збирають конфіденційну інформацію так тонко, що ми навіть не знаємо що саме їм відомо. Це, можливо, й так, але ця невпевненість – ще одна причина, щоб зберегти свою приватність та уникнути витоку персональних даних в Інтернет.

Чи є щось, що ми можемо зробити, аби бути більш захищеним коли займаємося серфінгом в Інеті, крім того, що не показувати свої паролі, або не надавати забагато особистої інформації?

Ось декілька непоганих способів, які можна використовувати для збереження вашої персональної інформації.

Оновлення програмного забезпечення

Найкращим захистом від вірусів є не антивірусний захист, своєчасне оновлення програмного забезпечення. Адже його розробники слідкують за можливими загрозами і намагаються захистити свої продукти нововведеннями. Тому, коли ваш пристрій пропонує вам оновлення – не ігноруйте це!



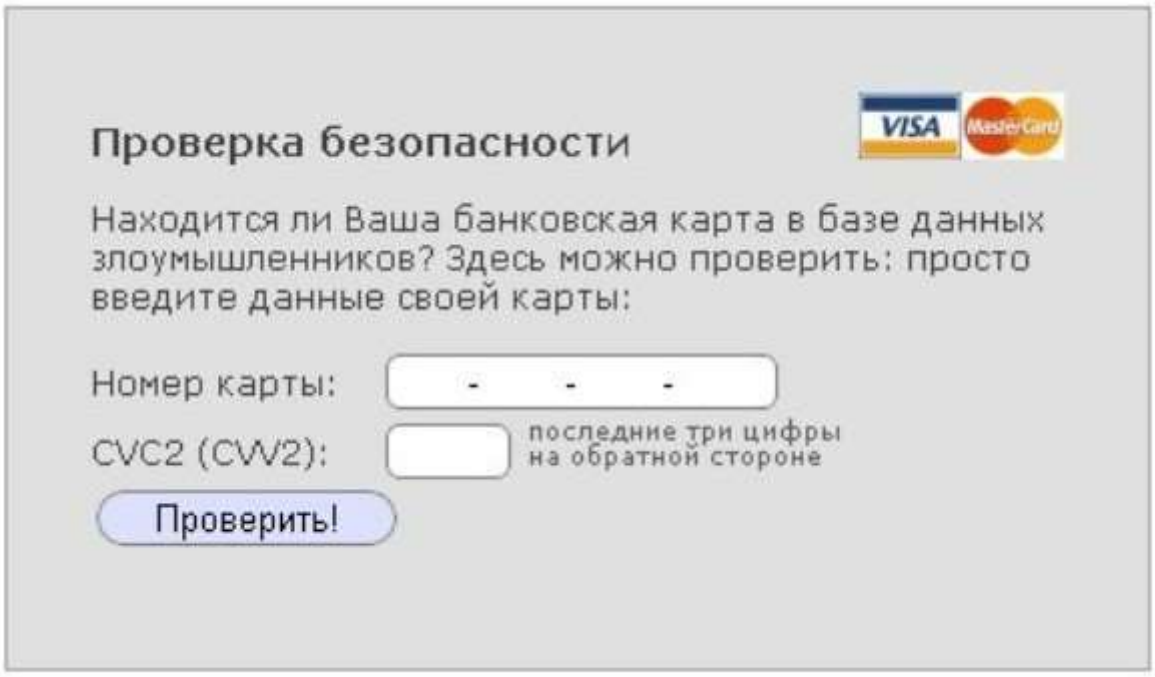
Перевірка сайтів

Наполегливо рекомендуємо не вводити персональну інформацію (логін, пароль, номер телефону чи платіжної карти) на запити неперевірених сайтів.

Такі дані можна надавати лише тим ресурсам, які вже пройшли вашу перевірку, або відомим мережам (наприклад, Google, Facebook, Rozetka, ваші блоги на інформаційних ресурсах тощо).

І ще – обов'язково перевіряйте назву сайту в адресному рядку браузера (www.google.com.ua а не www.goolge.com.ua).

Вводити ж інформацію з платіжних карток чи паролі від них можна лише на сайтах зі значком «замочка» в адресному рядку. Таке з'єднання вважається захищеним, а ваші дані не потраплять до рук сторонніх осіб.



Фішинг – виловлювання інформації

Останнім часом став популярним такий різновид шахрайства як фішинг. Мета фішингу – отримання доступу до конфіденційної інформації користувача (логінів, паролів, даних платіжних карток). Фішингові повідомлення, зазвичай, приходять на електронну пошту і спонукають до негайних дій, не залишаючи часу на роздуми. Шахрайські повідомлення найчастіше надходять від імені відомих брендів, знайомих, друзів чи банків та впливають на емоційне сприйняття інформації. Вони можуть:

– викликати тривогу за стан своїх банківських рахунків;

– обіцяти грошові вигоди з докладанням мінімальних зусиль (лотереї, повідомлення про можливий неочікуваний спадок тощо);

– пропонувати фінансові угоди з неймовірно вигідними умовами;

– закликати до пожертв після новин про стихійні лиха чи ще щось або ж звертатися до вашого милосердя, пропонуючи допомогти хворим дітям.

Фішинг може використовувати не лише розсилку листів на електронні адреси, але й онлайн-оголошення, результати пошукових систем, імітацію «випливаючих» вікон із системними повідомленнями, смс-повідомлення розповсюдження інформації у соціальних мережах.

Не натискайте на подібні оголошення. Перевірте їх. Задля простої і швидкої перевірки – рідним чи друзям можна зателефонувати, благодійні фонди чи банки мають офіційні контакти, через які можна уточнити будь-яку інформацію, а якщо листи від незнайомих вам осіб чи джерел – просто ігнорувати її.

Увага! Пароль!
Безпечний пароль – це перша гарантія того, що ваша особиста інформація перебуває під надійним «замком».
Пароль має бути складним (букви й цифри, великі й малі, не менше ніж 8 символів). Паролі до різних ресурсів мають бути різними.

Запам'ятайте, пароль не має містити особистих даних (наприклад, прізвище чи дату народження).

Паролі до важливих ресурсів (електронна пошта, сторінка в соціальній мережі) потрібно змінювати хоча б раз у 3 місяці. Якщо ж у вас багато паролів до різних ресурсів записуйте їх або використовуйте програми зберігання паролів, наприклад, KeePass**.**

Для надійнішого захисту використовуйте двохфакторну автентифікацію, де це можливо!
Відділ технічного забезпечення та захисту інформації