

ЯК НЕ СТАТИ ЖЕРТВОЮ КІБЕРЗЛОЧИНЦІВ

2021 © Українська міжбанківська Асоціація членів платіжних систем «ЕМА»

Захисти акаунти двічі

Встанови сильний пароль та двоетапну аутентифікацію всюди, де можливо (ігришки, Insta, Facebook, пошта, Viber, WhatsApp, Телеграм, пошта, Viber...).

Не юзай один пароль усюди.
Два – теж замало. Кожному сервісу – свій, окремий і унікальний, пароль!

Захисти свої пристрої

Регулярно оновлюй програми на компі та мобільні застосунки. Не забувай і про версію операційної системи. Розробники самі повідомляють про оновлення, – дотримуйся їхніх рекомендацій. Не підключайся до невідомих вайфаїв.

Захисти свої дані

Під час вводу даних на сайті звертай увагу на його адресу. Шахраї часто створюють сайти-клони і крадуть там логіни, паролі, карткові дані... і гроші. Повна копія, але адреса інша. Схожа, але трохи інша.

Дивись, куди тицяєш

Отримав посилання? – не поспішай клікати! Перевір відправника, текст і сам гіперлінк. Шахраї розсилають шкідливі посилання для зараження пристроїв вірусом або викрадення персональних даних та секретних карткових реквізитів.

Легкі гроші

Ігноруй нав'язливу рекламу легкого заробітку. Не переходь за посиланнями від незнайомих в мейлах, месенджерах та соцмережах.

Зроби собі окрему картку

Для оплати в Інтернет оформи окрему платіжну картку з мінімальним балансом або віртуальну.

Контролюй інфу

Усе, що потрапляє у мережу, залишається там назавжди. Не варто публікувати про себе все! Заборони відмічати себе на фото.

Адреса, телефон, дані платіжної картки, паспорт, інформація щодо покупок та подорожей... Усе може бути використано злочинцями, щоб підібрати спосіб атаки на тебе.

Безкоштовний сир буває лише в мишоловці

Не вір обіцянкам призів і знижок від блогерів і зірок. Перш ніж ввести дані своєї платіжної картки у форму оплати, вивчи адресу сайту, заугли його назву та перевір, коли сайт був створений. Якщо сайту кілька місяців – з великою ймовірністю, він шахрайський. Якщо повідомляють, що ти виграв багато грошей або коштовний приз, та для їх отримання потрібно «лише сплатити комісію», – це пастка!

Спитай у тих, хто вже спробував

Спитай у людей, яким ти довіряєш, що вони думають про нову гру, перш ніж грати в неї або завантажити.

Особисте тримай при собі

Не ділись особистими фото та відео з людьми, з якими спілкуєшся лише онлайн. Твої фото можуть бути використані проти тебе.

Не розголошуй персональні дані!

Не розголошуй в соціальних мережах персональну інформацію про себе і свою сім'ю (вік та дату народження, паспортні дані, номер телефону, адресу проживання, номер школи, дані банківських карток).

Будь-які прохання завантажити файли та встановити програми мають розцінюватися як підозрілі.

Блокуй хейтерів

Блокуй відправників неприємних для тебе повідомлень. Не соромся скажитися адміністрації соцмереж на образливі пости та коментарі, це – анонімно.

Хто ти, «френд»?

У соцмережах додавай у друзі лише тих, кого знаєш особисто, або тих, кого особисто знають твої друзі. Не довіряй незнайомцям у мережі! Фото, обличчя на аватарці, ім'я, вік та стать твого віртуального друга можуть бути несправжніми і вигаданими.

