Новина розміщена в рамках співпраці ЗЗСО м.Рівне з Відділом протидії кіберзлочинам в Рівненській області

Що робити, щоб не попастися на хитрощі кібермародерів

1. Грошова допомога

В популярних месенджерах та соцмережах кібермародери під виглядом міжнародних організацій, соціальної платформи єДопомога, порталу державних послуг Дія, відомих українських брендів тощо пропонують громадянам, що постраждали від війни, отримати грошову допомогу.

Якщо хтось вам пропонує отримати грошову допомогу через чат-бот, — це шахрайська схема! Якщо для отримання допомоги потрібно сплатити державне мито — це також шахрайська схема, оскільки під час отримання допомоги державне мито не сплачується.

Будьте уважними до деталей під час введення своїх персональних даних, паролів, карткових реквізитів. Завжди звертайте увагу на доменне ім'я та зону сайту.

2. Інтернет-торгівля

Купувати в Інтернеті вигідно, але стережіться шахраїв!

Кібершахраї виманюють у громадян грошові кошти, карткові реквізити та облікові записи онлайн-банкінгу.

Поради користувачам OLX: Що робити?

1. Звертайте увагу на адресу (OLX має вигляд olx.ua, а мобільна версія сайту – m.olx.ua). Решта: olxposhta.com, olx.cx, 0lx.in.ua тощо – шахрайські сайти-клони.

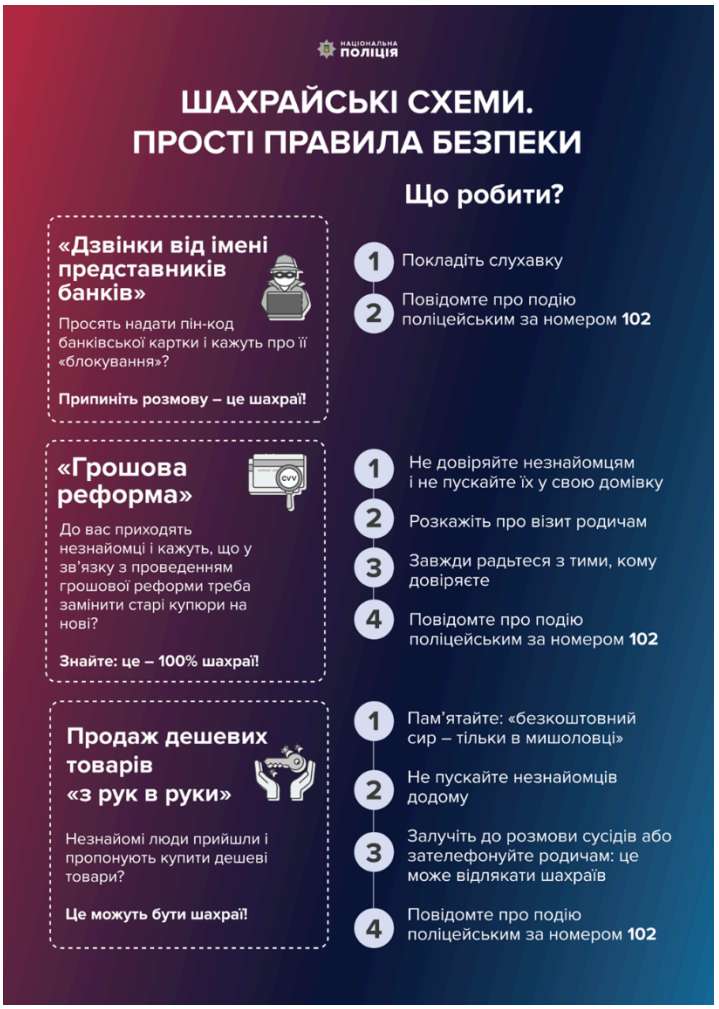
2. Оговорюйте деталі угод лише в особистому кабінеті OLX!

Не переходьте у месенджери (Viber, Skype, Telegram, WhatsApp тощо) – там вас OLX вже не захистить.

3. Оформлюйте угоди з «OLX Доставка» лише на OLX.UA – в особистому кабінеті.

Користуючись послугами торгових онлайн-майданчиків або дошок оголошень, не йдіть у месенджери, листуйтесь лише в чаті сервісу.

Лише номер картки! — Пам’ятайте, для отримання будь-якого переказу на вашу картку достатньо надати покупцеві (відправнику грошей) лише її номер.



3. Телефонне шахрайство

Три речі, які вам ніколи не запропонує зробити дійсний співробітник банку або мобільного оператора:

1. Надати трьохзначний код безпеки зі звороту вашої картки, ПІН-код та облікові записи до онлайн-банкінгу.
2. Надати банківські SMS-коди та коди, отримані від мобільного оператора.
3. Встановити на телефон або ноутбук програму для віддаленого доступу (TeamViewer, AnyDesk, RMS, RDP, Radmin, Ammyy Admin, AeroAdmin).

Пам’ятайте, у разі шахрайської операцій банк блокує рух коштів на картці, і сам клієнт телефонує для розблокування, називаючи кодове слово та надаючи персональну інформацію для віддаленої ідентифікації; зворотна ситуація — це шахрайство.

4. Викрадення акаунтів у соціальних мережах та месенджерах

На ваш акаунт була подана скарга. Будь ласка, підтвердить Ваш обліковий запис в Телеграм.

Кібермародери зламують акаунти користувачів у Facebook, Instagram, Telegram, Viber тощо для подальшої розсилки повідомлень з проханням позичити грошей, поширення шкідливого програмного забезпечення та дезінформації.

Двофакторна автентифікація (2ФА) не захистить ваш акаунт на 100%, – втім, від більшості поширених скамів вона допоможе.

Створюйте складні та унікальні паролі. Складні – це з літерами, цифрами та спеціальними символами. Пароль повинен бути унікальним та не містити персональної інформації про Вас.

Перевіряйте електронну пошту та SMS. Коли ви реєструєтеся у соціальній мережі або месенджері, то прив’язуєте до облікового запису свій e-mail та телефон, на які сервіси надсилають автоматичне повідомлення про вхід до облікового запису з нового пристрою.