ДНІПРОПЕТРОВСЬКА ОБЛАСНА ДЕРЖАВНА АДМІНІСТРАЦІЯ

ДЕПАРТАМЕНТ ОСВІТИ І НАУКИ

вул. Володимира Антоновича,70, м. Дніпро, 49006, тел. 770-87-42, факс (056) 770-68-00
e-mail: osvita@adm.dp.gov.ua, http://www.osvita-dnepr.com, Код ЄДРПОУ 25927519

Керівникам закладів вищої, фахової передвищої та професійної (професійно-технічної) освіти

Про інформування

Департамент освіти і науки облдержадміністрації інформує про створення Національною поліцією України інформаційно-профілактичних матеріалів з метою протидії шахрайства, запобігання зростання їх кількості, що пов'язані із здійсненням фінансових операцій через мережу Інтернет, шахрайськими (фішинговими) повідомленнями, інтернет-жебрацтвом та шахрайством з надзвичайною ситуацією.

Враховуючи вищезазначене, просимо поширити інформацію серед здобувачів освіти, педагогічних та науково-педагогічних працівників.

Додатки: на 3 арк. в 1 прим.

Директор департаменту Павло БЕРНАЗ

Владислав ЛІСОВЕНКО 770-68-47

019567

Дніпропетровська обласна державна адміністрація
Департамент освіти і науки
Вих№ 3334/0/211-23 від 28.06.2023

Продаж дешевих товарів «з рук в руки»

Якщо незнайомі люди прийшли до вас і пропонують купити дешеві товари – будьте насторожі. Це можуть бути шахраї! У такий спосіб вони намагаються дізнатися, де ви зберігаєте свої заощадження, а потім непомітно для вас викрасти гроші.

Що робити?

1. Пам'ятайте: «безкоштовний сир – тільки в мишоловці».
2. Не пускайте незнайомців додому.
3. Залучіть до розмови сусідів або зателефонуйте родичам: це може відлякати шахраїв.
4. Якщо до вас приходили шахраї, повідомте про це поліцейським за номером 102.

«Грошова реформа»

Якщо до вас навідаються незнайомці і скажуть, що у зв'язку з проведенням грошової реформи треба замінити старі купюри на нові, знайте: це – 100% шахраї.
У такий спосіб вони намагаються привласнити всі ваші заощадження.

Що робити?

1. Не довіряйте незнайомцям і не пускайте їх у свою домівку.
2. Розкажіть про візит родичам.
3. Завжди радьтеся з тими, кому довіряєте.
4. Якщо до вас приходили шахраї, повідомте про це поліцейським за номером 102.

НАЦІОНАЛЬНА
ПОЛІЦІЯ

Шахрайські схеми
Прості правила безпеки

Війна в Україні стала підґрунтям для поширення шахрайських схем, заснованих на вразливому емоційному стані та зловживанні вашою довірою.
При цьому кмітливість шахраїв виходить за рамки вже добре знайомих українцям афер, тож з'являються нові способи ошукування.

Національна поліція України розповідає про найпоширеніші схеми шахрайств та основні правила безпеки, які допоможуть викрити аферистів.

«Дзвінки від імені представників банків»

«Вашу карту заблоковано», «з вашого рахунку хочуть списати гроші», «нові правила під час воєнного стану» - зловмисники, які представляються співробітниками банку, використовують різні способи, аби отримати доступ до ваших банківських карток.
Як тільки невідомі просять надати номер картки, пін-код, кодове слово, тризначний номер на звороті картки і термін її дії або ж ввести пароль, який надійшов у СМС, знайте: це – шахраї.

Пам'ятайте: навіть в умовах війни справжні співробітники банку ніколи не запитують таку інформацію.

Що робити?

1. Покладіть слухавку.
2. Повідомте про подію поліцейським за номером 102.

«Ваш родич у біді»

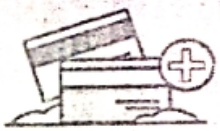
Якщо вам телефонують (часто вночі або вранці) та повідомляють, що родич потрапив у біду, і просять передати гроші – це шахрайство.
Зловмисники можуть видавати себе за сина/дочку, онука/онучку, які начебто потрапили у біду (скоїли ДТП, опинилися у поліції тощо). А можуть представлятися лікарями або поліцейськими і пропонувати свою допомогу у вирішенні «проблеми» за винагороду, яка може становити від тисячі до десятків тисяч гривень, а інколи – навіть кілька тисяч доларів США.

Пам'ятайте: так діють шахраї!

Що робити?

1. Покладіть слухавку.
2. Перевірте, де ваш родич.
3. Повідомте про подію поліцейським за номером 102.

«Соціальні виплати під час війни»



«Під час війни ви можете отримати соціальну допомогу» – найчастіше шахраї надсилають смс-повідомлення про отримання різноманітних виплат від органів влади або благодійних фондів та просять надати таку інформацію: ваші анкетні дані, номер картки, пін-код, кодове слово, тризначний номер на звороті картки і термін її дії.

Пам'ятайте: назвавши ці дані, ви надаєте шахраям доступ до вашого рахунку, тож вони можуть вкрасти всі ваші заощадження.

Що робити?

1. Покладіть слухавку.
2. Зверніться до своїх родичів або представників влади і перевірте, чи дійсно ви можете отримати такі виплати.
3. Якщо вам телефонували шахраї, повідомте про це поліцейським за номером 102.

Виграші призів (авто, побутова техніка)

«Ви виграли автомобіль або побутову техніку» – не поспішайте виконувати всі настанови незнайомців. Зазвичай у надісланому смс вказаний номер, за яким можна отримати детальну інформацію. Коли телефонуєте, вам розповідають умови, які потрібно виконати, щоб отримати «приз».
Як правило, вам пропонують сплатити 1% від вартості виграного товару. Але як тільки ви це зробите, незнайомці перестають виходити на зв'язок і зникають.

Пам'ятайте: так діють шахраї!

Що робити?

1. Подумайте, чи брали ви участь у акціях чи конкурсах.
2. Не перераховуйте гроші незнайомцям.
3. Якщо вам телефонували шахраї, повідомте про це поліцейським за номером 102.

«Обирайте післяплату» - це основна порада поліції для тих, хто купує товари в мережі Інтернет.

Нині продаж неіснуючих товарів є одним із поширеніших сценаріїв шахрайства. При цьому зловмисники роблять усе, щоби максимально замаскуватися під справжніх продавців товарів.

Варто пам'ятати: шахраї створюють ілюзію роботи справжнього онлайн-магазину: у них гарні фото товарів, вони оперативно відповідають на повідомлення потенційних покупців, консультують і допомагають підібрати потрібну річ і головне обіцяють швидку доставку.

Та найцікавіше починається тоді, коли ви визначилися з покупкою: вам пропонують здійснити повну передплату, а якщо ви не погоджуєтеся – часто ідуть «на поступки» і пропонують часткову оплату товару.

Особливо «підковані» шахраї можуть не зупинитися на отриманні передплати за товар, які навіть не планували вам надсилати, а натомість намагаються привласнити всі кошти, які є на вашому банківському рахунку.

Уважно прочитайте, як це відбувається.

Після того, як ви визначилися з покупкою, домовилися про доставку і здійснили повну чи часткову оплату, шахраї повідомляють, що потрібного товару немає. При цьому запевняють, що вони готові повернути кошти: і для цього потрібно авторизуватися на сайті інтернет-магазину та ввести всі реквізити своєї картки. Як тільки вони отримали ці дані, одразу привласнюють усі гроші з вашої банківської картки.

Тож повернімося до того, з чого розпочинали:

1. Обирайте післяплату.
2. Остерігайтеся онлайн-магазинів, які пропонують товари за цінами, значно нижчими, ніж у інших магазинах
3. Не вводьте реквізитів платіжних карток на незнайомих платформах.
4. Безкоштовно перевірте сайт онлайн-магазину на сервісі Кіберполіції "STOP FRAUD" https://cyberpolice.gov.ua/stopfraud/ або на сервісі Асоціації "ЄМА" CheckMyLink https://check.ema.com.ua/.

ВАЖЛИВО! Схема шахрайства може бути абсолютно новою або добре прихованою. Тому, крім перевірки на сайті Кіберполіції в розділі "STOP FRAUD" та сервісі CheckMyLink, здійснюйте також власну перевірку: почитайте відгуки про продавця та дізнайтеся історію роботи Інтернет-магазину.

Не дайте шансу шахраям ошукати вас!

https://dp.npu.gov.ua/news/obyraite-pisliaplatu-tse-osnovna-porada-politsii-dlia-tykh-khto-kupuie-tovary-v-merezhi-internet

Короткі відео для вашого ознайомлення:

https://drive.google.com/file/d/1EPMNnvgDJsFQ1YuhCHTSPd5XGdBLAJTm/view?usp=drive_link

https://drive.google.com/file/d/1-6ww9EAUE-yVD7kSA3lqZDWkpQcdMu_-/view?usp=drive_link

https://drive.google.com/file/d/1pHjhRarmnctVxfPHN9AJBF4PmKcOJ5xl/view?usp=drive_link