**Існують основні правила захисту грошей на банківських картках, а також правила кібергігієни, яких потрібно дотримуватися, щоб не стати жертвою шахраїв які шукають способи, щоб нажитися на ваших грошах.**

Про ці правила розповідає начальник управління протидії кіберзлочинам в Запорізькій області Департаменту кіберполіції Національної поліції України **Валентин СОЛДАТЕНКО**.

«Найрозповсюдженіші схеми зловмисників полягають у продажу неіснуючих товарів, телефонних шахрайствах та фішингу. Ніколи не залишайте свої персональні дані на незнайомих або підозрілих сайтах. Останній вид шахрайства полягає у створенні сайтів-двійників (фішингові сайти). Сторінка, яку ви відвідуєте, візуально виглядає як справжня: має ту ж кольорову гаму, містить приблизно ту ж саму інформацію, що й офіційний сайт, однак у гіперпосиланні назви сайту, вказані зайві букви або цифри. Оплативши товари чи вказавши власні персональні дані на сайті-двійнику, ви потрапляєте у пастку шахраїв. Необхідні вам товари чи послуги ви не зможете отримати, а ваші персональні дані можуть бути використані проти вас. Тому перед введенням своїх даних переконайтеся, що ви точно перебуваєте на офіційному сайті.

Іншим поширеним видом інтернет-шахрайства є функціонування несправжніх інтернет-магазинів. Такі магазини можуть пропонувати товари, яких у них немає в наявності або вони у неналежному стані. Остерігайтесь продавців, які пропонують товари за дуже низькою ціною, але з частковою або повною передоплатою. Для купівель в інтернеті краще використовувати перевірені інтернет-майданчики, адміністратори яких можуть гарантувати вам повернення коштів у разі, якщо товар не буде відправлено або він буде неналежної якості. Якщо ж у вас є необхідність скористатися послугами невідомого вам інтернет-магазину, тоді обов’язково на інших ресурсах вивчіть відгуки про продавця та купуйте товари з накладеним платежем – сплачуйте вартість товару після отримання та огляду.

Для захисту грошей на банківських рахунках треба не повідомляти стороннім дані банківських карт, не переходити за сумнівними гіперпосиланнями, а для купівлі-продажу обирати лише перевірені сервіси.

Від початку повномасштабної війни додалися ще схеми псевдоевакуаційних перевезень та інші шахрайськи схеми, пов’язані з шахрайськими діями на тимчасово окупованих територіях чи стосовно них, а також надання в оренду неіснуючого житла, продажу неіснуючих товарів військового призначення тощо. Також дуже актуальні схеми псевдоволонтерських зборів», - розказав керівник кіберполіції. Він рекомендує громадянам переказувати гроші на благодійність лише перевіреним особам або офіційним фондам. «Завжди звертайте увагу на наповнення сторінки волонтера, дату завантаження матеріалів, кількість підписників, у більшості публічних діячів профілі в соцмережах верифіковані, на це також варто звертати увагу», - наголосив він.

Ще одним поширеним видом інтернет-шахрайства є надсилання на електронні пошти або у соціальні мережі повідомлень різного характеру, які зводяться до того, що вам необхідно сплатити певну суму коштів. Так, наприклад, часто надсилаються повідомлення щодо виграшу великої суми коштів або цінного призу. Автори повідомлень вказують на необхідність сплати певного відсотку від виграшу задля покриття комісій та інших витрат, пов’язаних конвертацією з коштів чи відправкою призу. Варто пам’ятати золоте правило – «безкоштовний сир тільки у мишоловці». Для початку згадайте чи брали ви участь у якихось акціях. Дізнайтесь у представників офіційні умови акції, поцікавтесь назвою та сайтом компанії, що проводила акцію. У разі, якщо ви сплатите кошти на вказані рахунки, то швидше за все ніяких грошей та цінних призів ви не отримаєте, а автор повідомлення перестане відповідати на ваші листи.

Старший інспектор з оперативного пошуку та партнерства у сфері інформаційних технологій управління протидії кіберзлочинам в Запорізькій області Департаменту кіберполіції Національної поліції України **Олег КИРБЯТ’ЄВ** зазначає, що перераховані вище варіанти інтернет-шахрайства є найпоширенішими, але не виключними. З кожним днем з’являються нові види шахрайства в інтернеті. Для того, щоб не втрапити у пастки шахраїв, варто під час здійснення операцій в інтернеті дотримуватися таких правил:

* нікому не повідомляти та не вводити на підозрілих сайтах термін дії банківської карти, її номер та 3-значний CVV-код;
* перевіряти гіперпосилання та наповнення сайту на відповідність офіційним даним компаній;
* у разі отримання спірних листів чи повідомлень не здійснювати ніякої оплати до встановлення обставин ситуації, що виникла;
* не робити передплат у неперевірених інтернет-магазинах;
* не користуватися неперевіреними оголошеннями щодо роботи, яка обіцяє швидкий заробіток за внесення завдатку.

Нижче надаємо визуалізовані актуальні шахрайські схеми та поради щодо дій, які допоможуть уникнути їх та зберегти свої гроші, не стати жертвою зазначених видів шахрайств.

Просимо, уважно з ними ознайомитися та завжди пам’ятати про них, особливо під час знаходження у віртуальному просторі, у якому практично всі з нас перебувають щоденно, спілкуючись, отримуючи інформацію, шукаючи потрібне чи купуючи щось через мережу інтернет. Якщо у якійсь ситуації маєте сумніви – краще не поспішайте щось робити, а перепитайте у близьких, знайомих, дітей, родичів тощо. Можна звернутися на гарячу лінію свого банку.

Поінформований значить озброєний. Користуючись вказаними порадами ваші шанси на те, щоб не втратити свої гроші, зростають у десятки разів. Лише тільки варто про них пам’ятати.

**Управління протидії кіберзлочинам в Запорізькій області ДКП НПУ**