Увага! Фішинг.

Популяризація та зростання платіжних інструменті для безготівкових розрахунків провокують розвиток шахрайства у цій сфері, у тому числі створення та розвиток фіктивних сайтів, що імітують роботу інтернет-ресурсів банків, фінансових установ, організацій – фішингових сайтів.

Фішинг- популярний вид шахрайства метою якого є отримання персональних даних клієнтів (логін, пароль, реквізити банківської картки) з використанням сервісів онлайн аукціонів, сервісів з переказу, обміну валюти, інтернет-магазинів.

Шахраї отримуючи персональні дані власників платіжних засобів (карток) отримують доступ до їх рахунків та крадуть грошові кошти.

Щоб заманити користувачів шахраї імітують діяльність банків, фінансових установ, компаній активно використовуючи SMS повідомлення, електронну пошту, соціальну мережу.
Наприклад:

- ✓ на Ваш номер телефону може надійти SMS повідомлення с пропозицією придбати, чи обміняти товар, з інформацію про начебто отриманий виграш з посиланням на фішинговий сайт, на сторінку з вірусом, або пропозицією зателефонувати на зазначений номер телефону;
- ✓ Вам можуть написати від імені вашого знайомого, з невідомого облікового запису (аккаунту) з проханням перейти за запропонованим посиланням.
- ✓ Вам можуть надходити листи по електронній пошті з повідомленнями про вигаданий злам електронної пошти, сторінки в соціальній мережі, про блокування банківського рахунку, повідомлення начебто від органів влади, благодійних організацій, судових інстанцій, тощо які будуть містити посилання для переходу на фіктивні сайти. Посилання може бути оформлене у вигляді QR-коду.

Щоб не стати жертвами шахраїв ніколи не вказуйте на підозрілих сайтах дані своєї платіжної карти (номер карти, термін її дії та тризначний код безпеки CVV2/CVC2, який вказують на зворотному боці картки).

Основні ознаки на які необхідно звернути увагу та які можуть вказувати на фіктивність сайту та його небезпечність.

- Якщо домен сторінки починається з http\, а не з https\ і не має значка «замок», який повідомляє про встановлення безпечного http-з'єднання, то сайт якщо і не є фіктивним, але є небезпечним. Адреса сторінки, на якій здійснюється оплата, має починатися з https\\, – це означає, що сайт використовую безпечне з'єднання з сервером. Якщо адреса починається з http\\ – це вказує, що сайт не підтримує безпечне з'єднання, відповідно власник платіжного засобу, залишаючи на такому сайті реквізити своєї платіжної картки дуже ризикує.
- Реєстрація сайту, який надає послуги з поповнення мобільного рахунку, переказу коштів з картки на картку, онлайн-кредитування знаходиться не на домені національного рівня. ua. Більшість вітчизняних топ-платіжних сервісів зареєстровано на домені. ua, на якому можуть зареєструватися власники торгових марок. А фіктивні сайти навпаки, реєструються на доменах, де відсутні обмеження для реєстрації (наприклад: .ru, .com.ua, .top, .in.ua, .kiev.ua, тощо.).
- Відсутність комісій, дуже низькі комісії за послугу та інші «вигідні» пропозиції. Фіктивні сайти часто заманюють клієнтів пропозицією дуже низьких чи нульових комісій за свої послуги. Деякі маскуються під сайти неіснуючих акцій чи розіграшів, обіцяючи дорогі призи.
- Видимі недоліки в контенті, наприклад, відмінності у назві домену в адресному рядку і в тексті, або на банері;
- В адресному рядку відображається однакова адреса для всіх сторінок сайту;
- Карткові реквізити не маскують зірочками. Офіційні (легітимні) сайти завжди маскують карткових реквізитів, що вводяться, або використовують віртуальну клавіатуру, а фіктивні сайти – ні.