

Фішингові посилання

Популярність маркетплейсів серед українців зростає, що створює поле діяльності для шахраїв. Одна з найпоширеніших схем аферистів – фішингові посилання, які імітують вигляд маркетплейсів та мають на меті виманити дані банківських карток.



Як захистити себе від фішинг-афери на маркетплейсах: поради для українців

Популярність онлайн-торгівлі в Україні зростає з кожним роком, і маркетплейси стають основними майданчиками для покупок. Але з цим приходять і нові загрози, зокрема, шахрайські схеми, спрямовані на виманювання особистих даних та грошей у користувачів. Однією з найбільш поширених схем є фішингові посилання, що імітують вигляд популярних маркетплейсів.

Що таке фішинг і як він працює?

Фішинг — це шахрайська практика, коли зловмисники намагаються отримати конфіденційну інформацію користувача, наприклад, логіни, паролі чи дані банківських карток. Для цього вони створюють фальшиві веб-сайти, які виглядають схожими на справжні платформи, такі як маркетплейси. Відвідавши таке посилання, користувачі можуть випадково ввести свої персональні дані або оплатити покупку через небезпечний ресурс.

Як розпізнати фішинг?

✓ **Перевірте URL-адресу.** Офіційні сайти маркетплейсів мають правильні та безпечні доменні імена (наприклад, "rozetka.ua" або "olx.ua"). Якщо ж у посиланні присутні сумнівні символи, додаткові цифри чи літери, або якщо адреса виглядає трохи зміненою, наприклад, "roz3tka.ua" або "olx.com.ua", це може бути ознакою фішингу.

✓ **Перевірте дизайн сайту.** Фальшиві сайти часто виглядають схоже на оригінальні, але зазвичай мають низьку якість графіки, помилки у тексті або незвичну структуру. Якщо ви помітили подібні недоліки, краще покинути сайт.

✓ **Звертайте увагу на розсилки.** Легітимні маркетплейси зазвичай не просять вводити особисту інформацію через електронну пошту або месенджери. Якщо ви отримали таку вимогу, будьте обережні.

✓ **Перевірка через офіційний сайт або додаток.** Якщо вам здається, що з вами зв'язуються з офіційного маркетплейсу, краще зайти на сайт або відкрити додаток через перевірений канал, а не за посиланням у листі чи повідомленні.

✗ **Остерігайтеся підозрілих повідомлень.** Якщо ви отримали листи або повідомлення через соцмережі з посиланнями на "подарунки" чи "знижки", це може бути спробою заманити вас на фальшивий сайт. Часто такі повідомлення містять заклики терміново ввести дані або здійснити оплату.

Як захистити себе від фішингу?

✓ **Використовуйте двофакторну автентифікацію.** Більшість сучасних маркетплейсів пропонують додаткові засоби безпеки, такі як SMS-коди або підтвердження через додаток. Це знижує ризик несанкціонованого доступу до вашого акаунту.

✓ **Перевіряйте покупку через додаток чи офіційний сайт.** Не вводьте платіжні дані на сторонніх сайтах. Завжди використовуйте лише перевірені ресурси.

✓ **Слідкуйте за оновленнями безпеки.** Переконайтеся, що ваш браузер та операційна система оновлені до останніх версій. Це допоможе захистити вас від багатьох онлайн-загроз.

✓ **Будьте обережні з публічними Wi-Fi мережами.** Уникайте здійснювати покупки чи вводити особисті дані, коли підключені до незахищених мереж.

✗ **Не довіряйте занадто гарним пропозиціям.** Якщо якась пропозиція здається надто вигідною, щоб бути правдою, швидше за все, це пастка.