Przypominamy i apelujemy, ?e oszu?ci wykorzystuj? OLX, WhatsApp czy Vinted!

Data publikacji

19.01.2023

Mieszka?cy

Przypominamy i apelujemy, ?e oszu?ci wykorzystuj? OLX, WhatsApp czy Vinted!

Od pewnego czasu oszu?ci w celu wy?udzenia danych z naszej karty pos?uguj? si? platform? OLX, VINTED oraz komunikatorem WhatsApp. W zwi?zku z tym ca?y czas przypominamy u?ytkownikom o metodach jakimi pos?uguj? si? przest?pcy, by wy?udzi? nasze dane, a w konsekwencji wyczy?ci konto bankowe. Wskazujemy jak unikn?? oszustwa oraz co zrobi?, gdy zostaniemy oszukani. Apelujemy do u?ytkowników o rozwag? i ostro?no??!

OSZU?CI NA PLATFORMIE OLX lub VINTED

Najbardziej popularne platformy do dokonywania oszustwa wobec u?ytkowników serwisu og?oszeniowego to OLX lub VINTED. Chocia? scenariusz ataku z biegiem czasu jest modyfikowany, schemat, wed?ug którego dzia?aj? atakuj?cy, pozostaje niemal niezmienny.

1. Przest?pcy kontaktuj? si? w sprawie zakupu przedmiotów wystawionych na sprzeda?,

wykorzystuj?c komunikator WhatsApp.
2. Proponuj? sfinalizowanie transakcji z wykorzystaniem us?ugi p?atno?ci, ?wiadczon? przez portal. Je?li sprzedawca si? zgodzi, wysy?aj? spreparowany link, który swoj? szat? graficzn?, co prawda, przypomina OLX, ale zawiera fa?szywy formularz p?atno?ci.
3. Na fa?szywej stronie ofiara jest nak?aniana do podania szczegó?owych danych karty p?atniczej w celu rzekomego odebrania op?aty za wystawiony przedmiot (Uwaga! Serwis OLX ?wiadczy us?ug? p?atno?ci, ale nigdy nie prosi o dane karty p?atniczej ani dane logowania do konta bankowego).
4. Atak ko?czy si? kradzie?? danych karty kredytowej i wy?udzeniem ?rodków finansowych nie?wiadomego u?ytkownika.

FA?SZYWE WIADOMO?CI SMS

Kto z nas nie dosta? nigdy SMS-a z informacj?, ?e min?? termin zap?aty jakiej? nale?no?ci lub z innego rodzaju przypomnieniem? Takie wiadomo?ci to wygodna i szybka forma komunikacji z zapominalskim klientem. Niestety przest?pcy o tym wiedz? i tworz? fa?szywe ponaglenia, celuj?c w roztargnione osoby, które uwierz?, ?e rzeczywi?cie maj? nieuregulowane rachunki. Oszust wysy?a swój SMS do jak najwi?kszej liczby losowych numerów. W wiadomo?ci umieszcza link do fa?szywej strony p?atno?ci. Podobnie jak w przypadku omówionego wcze?niej oszustwa, celem tego ataku jest wy?udzenie pieni?dzy. Fa?szywe SMS-y informuj? np. o konieczno?ci dop?aty do szczepionki lub zach?caj? do zarejestrowania si? (odp?atnie) na szczepienie. Pojawiaj? si? równie? wiadomo?ci, których tre?? nie jest zwi?zana z pandemi?, np. dotycz? uregulowania nale?no?ci za energi? elektryczn?, wyrównania niedop?aty podatku lub mandatu karnego.

Kwota okre?lona w wiadomo?ci jest zwykle niewielka. Przest?pcy licz? na to, ?e odbiorca nie b?dzie drobiazgowo weryfikowa?, czy nale?no?? jest zasadna. Czekaj? na osoby, które b?d? sk?onne zap?aci? „dla ?wi?tego spokoju”. Niestety podanie danych logowania na fa?szywej stronie p?atno?ci mo?e doprowadzi? do utraty du?o wi?kszej sumy ni? wymieniona w wiadomo?ci.

JAK UNIKN?? OSZUSTWA?

Czytaj SMS-y od Banków. Zwró? uwag? na to, co autoryzujesz.

Poznaj zasady bezpiecze?stwa swojego banku i stosuj si? do nich gdy korzystasz z portali aukcyjnych

Miej ograniczone zaufanie do potencjalnych kontrahentów.

Rozliczaj si? bezpo?rednio przez dany portal. Unikaj bezpo?rednich transakcji. Uwa?aj na próby nawi?zania kontaktu poza portalem, np. przez WhatsApp czy Messenger. Zobacz instrukcje p?atno?ci z OLX

Oszu?ci mog? podrobi? stron? portalu aukcyjnego – tak samo jak i ka?d? inn? stron?, równie? nasz?. Dlatego zwracaj uwag? na adres widoczny w przegl?darce. Zobacz poradnik OLX

Zwró? uwag? na poprawno?? j?zykow? strony, na której przekazujesz dane karty. Fa?szywe strony cz?sto zawieraj? b??dy, s? napisane niegramatycznie.

CO ROBI?, GDY ZOSTANIESZ OSZUKANY?

Koniecznie skontaktuj si? ze swoim Bankiem przez infolini?.

Mo?esz od r?ki zastrzec swoj? kart? w bankowo?ci lub aplikacji swojego banku. Karta w ten sposób przestanie dzia?a? równie? w Google Pay i Apple Pay.

Poinformuj Policj?.

Na oficjalnym blogu OLX mo?emy przeczyta? „Pami?taj, ?e OLX nie generuje linków do op?acenia zakupu, czy do podania danych do otrzymania p?atno?ci za oferowany przez Ciebie przedmiot. Jedyn? stron?, do której przekierujemy Ci? podczas finalizacji P?atno?ci OLX, jest Dotpay – za jej po?rednictwem realizowana jest wp?ata.”

Pami?taj! Weryfikuj kto i co do Ciebie pisze. Nie wpisuj nigdzie numeru swojej karty. Nie klikaj w nieznajome linki do stron.

Policja apeluje o zachowanie szczególnej ostro?no?ci. Nie korzystajcie nigdy z linków, które przychodz? w wiadomo?ciach. Najbezpieczniej jest wpisa? samodzielnie adres internetowy strony

danego serwisu og?oszeniowego lub banku. Sprawdzajmy zawsze, czy witryna jest bezpieczna. Je?li korzystamy z kodów autoryzacyjnych przes?anych SMS-em przez bank lub inne instytucje sprawdzajmy zawsze, czy zawiera polskie znaki.
Trzeba te? pami?ta?, by przy podawaniu danych karty bankowej zachowa? szczególn? ostro?no??. Nale?y upewni? si?, czy oszu?ci nie zastawili na nas pu?apki.
Przed potwierdzeniem operacji zawsze sprawd?my te?, czy zgadza si? numer konta odbiorcy oraz kwota, jak? chcemy przela?. To mo?e nas uratowa? przed utrat? pieni?dzy.
Pami?tajmy zatem ostro?no??, czujno?? i metoda ograniczonego zaufania pozwol? nam unikn?? problemów i nie sta? si? kolejn? ofiar? oszusta!