Как защитить себя от интернет-мошенников

Как рассказал первый заместитель начальника Берестовицкого РОВД Олег Станиславович Лозовицкий: «способы, которыми пользуются интернет-мошенники, достаточно разнообразные. Так, наиболее распространенными являются следующие. Первый способ. Граждане выставляют на продажу свои вещи на интернет-площадке. Через определенное время с просьбой приобрести данный товар в мессенджерах с ними связываются «заинтересованные покупатели», которые представляются вымышленными именами и говорят: «Мы находимся не в Берестовице, сейчас оплатим и кинем ссылку для получения денег, а вы перешлете по такому-то адресу данную посылку». Граждане получают эту ссылку, переходят по ней (в ссылке указана поддельная (фейковая) страница), вводят туда свои реквизиты банковской платежной карточки, причем с CVC-кодом, после чего у них списываются с карт-счета денежные средства.

Второй способ связан с одним из банков. Появился новый вид хищения денежных средств с карт-счетов граждан при осуществлении платежей в интернет-банкинге. Так, работая в браузере, у пользователя начинает зависать страница, после чего появляется окно «Ведутся технические работы. Обновите страницу». При повторном обновлении страницы пользователь осуществляет повторный ввод логина и пароля, тем самым происходит денежных средств с карт-счета. Во избежание подобных ситуаций рекомендуем в настоящее время воздержаться от осуществления платежей за услуги с компьютера через интернет-банкинг.

Помимо перечисленных примеров самым популярным способом интернет-мошенничества является «телефонное мошенничество». На мобильный телефон гражданина поступает звонок от неизвестного лица, которое, представляясь сотрудником банка, говорит: «У вас произошло хищение денежных средств с карт-счета. С целью блокировки счета назовите либо ваши паспортные данные, либо номер банковской карты с CVC-кодом». Ничего не подозревая, потерпевшие называют все сведения, после чего происходит хищение денежных средств.

Уважаемые пользователи сети Интернет, вы также можете поспособствовать снижению роста кибератак, соблюдая некоторые рекомендации:

- Ни в коем случае не передавайте никому данные ваших пластиковых карт. Даже если вам звонят люди, представившись сотрудниками банка, помните об угрозе!

- Используйте лицензионное программное обеспечение. В таком случае отсутствует риск заразить компьютер или мобильное устройство при установке неизвестной программы.
- Установите антивирусную программу не только на персональный компьютер, но и на смартфон и планшет.
- Не переходите по ссылкам, содержащимся в спаме и других подозрительных письмах. При работе с электронными почтовыми ящиками необходимо настроить автоматическое блокирование приходящего спама, а также механически сортировать корреспонденцию, своевременно удаляя подозрительные письма без их просмотра.
- Аккаунты в социальных сетях, как и электронные почтовые ящики, периодически подвергаются хакерским атакам, поэтому необходимо минимизировать передачу персональных данных в электронном виде, особенно не указывать логины и пароли мобильного банка, электронных кошельков, номера, пароли и коды банковских карт.
- Воздержитесь от покупок на малоизвестных и подозрительных интернет-сайтах и у лиц, осуществляющих продажу товаров или услуг в социальных сетях, особенно при необходимости внесения полной предоплаты за товар или услуги.
- Используйте сложные пароли, состоящие из комбинаций цифр и букв или иных символов. Воздержитесь от паролей-дат рождения, имен, фамилий, то есть тех, которые легко вычислить либо подобрать.

Внимательное и бережное отношение к своим учетным и персональным данным поможет защитить вас от злоумышленников.

Первый заместитель начальника Берестовицкого РОВД Лозовицкий О.С.