**Предновогодние онлайн покупки: не оставь мошенникам шанса!**

Психологи утверждают, что конец декабря – время, когда большинство из нас, совершая покупки, в том числе в интернете, ведёт себя скорее эмоционально, нежели рационально. В предновогодней лихорадке легко попасться не только на удочки рекламистов и маркетологов, в этот период заметно активизируют свою деятельность и кибермошенники.

Несомненно, приобретать товары в интернете быстрее, удобнее, чаще всего выгоднее. Но и рисков, возникающих при онлайн-заказах, значительно больше. Заместитель управляющего отделением по Курской области Банка России Александр Устенко делится советами, как сделать покупки в Сети максимально безопасными.

- Около 80% мошеннических операций с банковскими картами происходит именно в интернете. С каждым годом количество таких преступлений растет. Риск возникает во время покупок на сайтах и в приложениях, при использовании электронных кошельков, мобильного и интернет-банкинга. Главное оружие киберпреступников – фишинг. Другими словами – выуживание конфиденциальных данных: паролей, реквизитов карты или счета для кражи денег с карты или из интернет-кошелька.

Как правило, злоумышленники в своих уловках используют психологические методы: рассылают СМС, электронные письма и сообщения в чатах с просьбой, например, «подтвердить аккаунт» или «восстановить доступ к банковскому счету».

Сообщения содержат ссылку на специальный фишинговый сайт – сайт-двойник банка, госоргана или другой организации. Если вы не заметили подмены, то после ввода своего логина, пароля интернет-банка или реквизитов карты ваши деньги поступят на счета мошенников.

Возникает резонный вопрос: как защититься от фишинга и других видов кибермошенничества?

- Во-первых, оплачивайте покупки, заходите в свой интернет-банк или мобильный банк только с личного компьютера, планшета и смартфона. Обязательно ставьте на них пароль.

- Если вы вдруг потеряли телефон или планшет, к которым подключено СМС-информирование или мобильный банк, срочно позвоните в банк и отключите от утерянного номера все услуги.

- Обязательно поставьте антивирус на все свои устройства, включая мобильные, и регулярно обновляйте их. Хороший антивирусный пакет всегда включает защиту от фишинга и вирусных программ.

- Никогда не переходите по ссылкам из писем и СМС от неизвестных отправителей. Даже если сообщение пришло от знакомого вам человека или организации, не спешите открывать их. Возможно, у мошенников появился доступ к их аккаунтам и они хотят заполучить ваши данные.

- Выбирайте известные и проверенные интернет-магазины и сервисы. Изучите отзывы о них от других пользователей, их лучше всего посмотреть на нескольких независимых сайтах. Добросовестный продавец всегда дает полную информацию о себе: телефон, адрес и прочие контактные данные.

- Когда переходите на страницу оплаты, ищите логотипы программ MasterCard SecureCode, Verified by Visa и Mir Accept. Эти программы с помощью технологии 3D-Secure дополнительно защищают вас во время покупок в интернете. Для подтверждения покупки банк отправит СМС с одноразовым паролем на номер мобильного телефона, привязанный к карте или счету.

- Если вы часто делаете покупки или оплачиваете услуги в интернете, например телефонную связь или штрафы, безопаснее использовать для этого отдельную карту. Вносите на нее лишь ту сумму, которую собираетесь потратить, и установите лимит по количеству операций в сутки. Некоторые банки позволяют создать виртуальные карты, которые действительны только для одной онлайн-покупки.

- Никому не сообщайте персональную информацию. Мошенники знают множество уловок, чтобы втереться к вам в доверие. Никогда не сообщайте посторонним данные своей карты, персональные данные и коды из СМС.

- Никому не сообщайте ваш ПИН-код и код проверки подлинности карты (CVV2/CVC2/ППК2) – последние три цифры на ее оборотной стороне. Даже сотрудники банка не вправе требовать от вас эти данные. Если кто-либо пытается их узнать, будьте уверены – это мошенник.

- Подключите СМС-оповещения об операциях по карте. В этом случае вы сразу же узнаете о платеже, которого вы не совершали, и сможете быстро отреагировать: заблокировать карту и опротестовать операцию.

В преддверии нового года количество банковских переводов и платежей традиционно увеличивается, соответственно активизируются и аферисты. Поэтому, будьте начеку и не оставляйте мошенникам ни единого шанса.