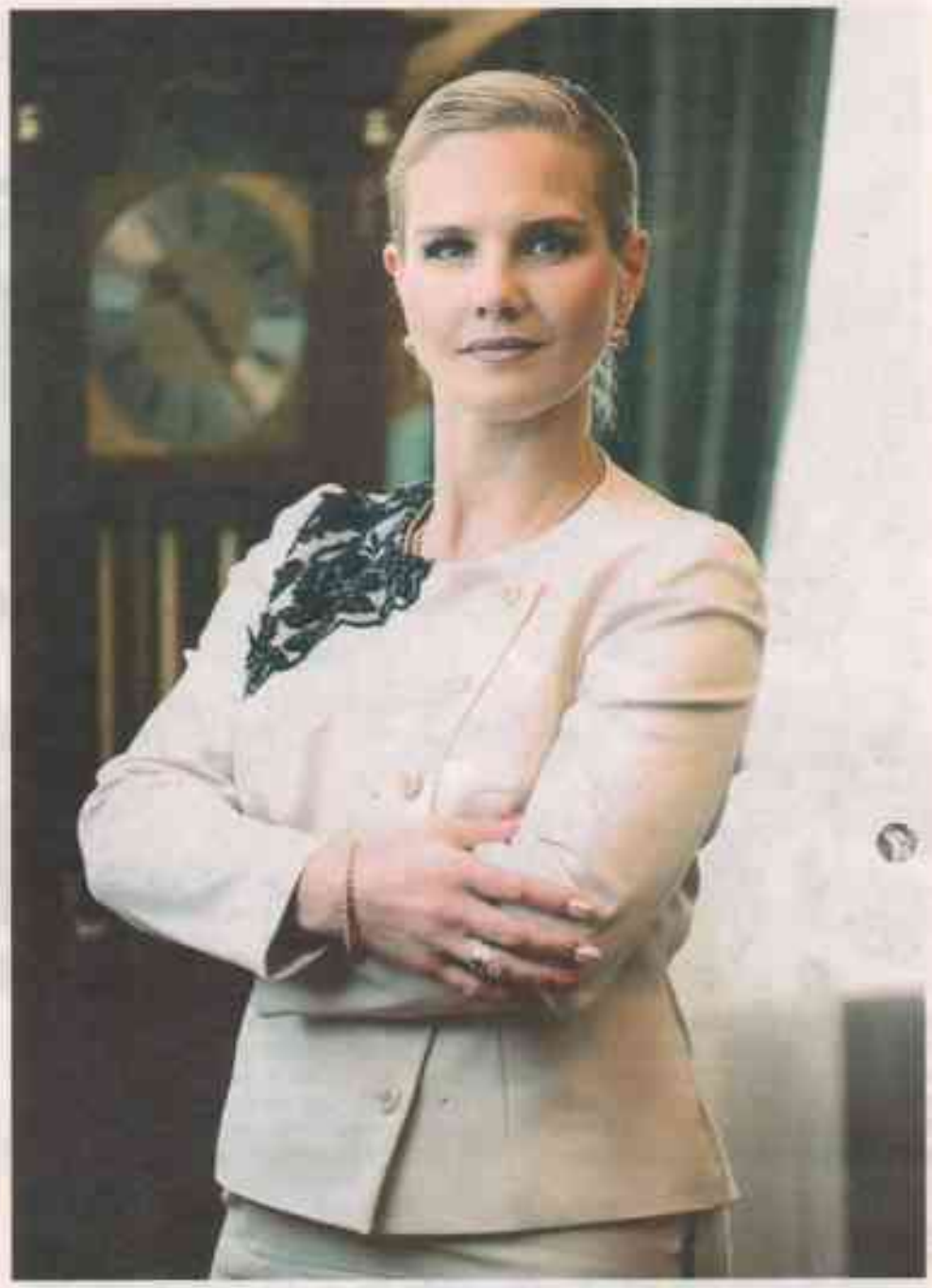
Цифровая самозащита

▶ В конце ноября состоялась традиционная «чёрная пятница» - несколько дней, в течение которых товары можно было прибрести со скидкой. Некоторые онлайн-сервисы и интернет-магазины до сих пор ведут распродажи. Это время не только заманчивых предложений, но и хитрых ловушек. О том, как безопасно совершать покупки в интернете и не стать жертвой мошенников рассказала заместитель управляющего белгородским отделением Банка России Инна Гребенникова.



Опасная рыбалка

- Раз уж мы заговорили о распродажах, то с них и начнём. Чем они опасны?

- Сегодня мы часто встречаемся с акциями, сейлами, распродажами. Конечно, мы видим красивую картинку и хотим в этом поучаствовать, потому что понимаем, что это скидки, выигрыши, экономия. Но к этому нужно подходить взвешенно. Ведь порой, приходя в магазин, чтобы купить чайник за три тысячи рублей, мы приобретаем два, потому что второй нам предложили взять с 50-процентной скидкой. Это же дёшево! А потом, уже дома, приходит осознание: «А зачем мне второй чайник? Полторы тысячи переплатил…».

Это и говорит о том, что к любым акциям, к любым скидкам надо подходить обдуманно. Никогда не нужно торопиться и поддаваться ажиотажу. Хорошо, если мы купили эти два-три товара, и при этом у нас были денежные средства. Но ведь часто мы совершаем покупки в кредит. Эти моменты всегда нужно просчитывать и, конечно, очень тщательно подходить к своим расходам. Они не должны превышать наши доходы.

Но, кроме того, мы нередко приобретаем товары онлайн. В интернете нас тоже поджидают акции и распродажи. Здесь нужно быть вдвойне внимательнее, потому что в Сети существуют так называемые фишинговые сайты.

- Фишинговые - это от слова «рыбалка»? Fish с английского языка - рыба.

- Да, примерно так. Фишинг - это способ выманить у вас конфиденциальную информацию, поймать на крючок в тот момент, когда вы приобретаете товары в интернете, переходя по ссылкам. Обычно на телефон или иной гаджет приходит сообщение о том, что такой-то производитель сейчас проводит такую-то распродажу как раз того, что нам нужно. И вот тут мы, переходя по ссылке, можем попасть на фишинговый сайт.

Почему фишинговый? Потому что от официального сайта любого бренда, производителя или организации он может отличаться одним символом или одной буквой в адресной строке.

- А визуально можно заметить отличие от настоящего сайта?

- Если специально не всматриваться и не вдаваться в детали, то ничего подозрительного и явно наводящего на мысль о том, что это поддельный сайт, вы не увидите. Это сайт-двойник, сайт-обманка.

Но если быть внимательным, то можно заметить, что около адресной строки сайта нет характерного символа-«замочка», говорящего о том, что наши сведения защищены. Отсутствие «замочка» - это уже стоп-фактор, чтобы задуматься и перепроверить адресную строку.

Если вы уже совершали покупки у какого-то производителя, мы рекомендуем вам сохранить его, например, на вкладке «Избранное» в вашем браузере. Если не сохранили, то наберите адрес сайта вручную и перепроверьте, действительно ли этот бренд предоставляет эту акцию, участвует ли нужный вам товар в этой акции. И только после этого совершайте покупку на официальном сайте.

А при получении с незнакомых номеров ссылок и рассылок будьте вдвойне внимательны и не переходите по ним. С такими сообщениями нужно быть очень осторожным. Ведь это наши деньги, наши доходы. А киберпреступники не дремлют. Они мимикрируют под условия, в которых мы живём. Наступила пандемия - все перешли в «цифру», в онлайн-покупки, и мошенники начали работать там.

- Опасен сам переход на фишинговый сайт или те действия, которые мы на нём производим?

- Перейдя на этот сайт, вы попадаете в некое приложение. Вводите пароль, логин - предоставляете какую-то информацию. И вот тут вы не только даёте злоумышленникам сведения о себе, вы отправляете данные о своей карте, с которой в последствии мошенники могут списать деньги. Ведь когда вы введёте все цифры своей карты и нажмёте «Оплатить», будет уже поздно.

«Вас беспокоит служба безопасности банка»

- Как можно защитить свои средства, совершая покупки в интернете?

- Мы рекомендуем завести отдельную карту для онлайн-покупок, если вы часто приобретаете товары в интернете. На эту карту стоит переводить ровно ту сумму, которую вы собираетесь сейчас потратить. В итоге карта будет у вас «нулевой».

Кроме того, часто мы храним банковские карты в кошельке. Этого делать нельзя. При утере кошелька вы расстанетесь и с наличными, и с безналичными деньгами.

- Что ещё поможет не попасться на удочку мошенников? Блокировка входящих сообщений от каких-то номеров? Антивирус?

- Во-первых, антивирусные программы, которые постоянно обновляются, - хороший способ защиты, используйте его. Во-вторых, ни в коем случае не переходите по ссылкам от незнакомых номеров. И не заполняйте никакие анкеты, если у вас есть сомнения в том, что вы находитесь на официальном сайте производителя товаров или услуг. Мы сами о себе в интернете оставляем очень много информации, а потом удивляемся, почему мошенники нам звонят и всё про нас знают. А ведь мы сами оставляем эти сведения в соцсетях и на различных сайтах. Поделились фотографией, указали какую-то информацию, а мошенники этим пользуются.

- Но ведь не только мошенники просят указать некоторые сведения о себе. Допустим, для перевода денег нужны реквизиты. Что мы можем говорить, а какие данные предоставлять ни в коем случае нельзя?

- Можно указать номер телефона. Система быстрых платежей (СБП) позволяет провести быструю операцию по номеру телефона. Для совершения операции в СБП номера телефона и банка, к карте которого он привязан, вполне достаточно. А если речь идёт о юридическом лице, можно попросить предоставить номер расчётного счёта, состоящий из 20 цифр. Это открытая информация, и для совершения платежа её достаточно.

Если перевод осуществляется физическим лицом без использования системы быстрых платежей, то может понадобиться ещё и номер вашей карты. Эта информация допустима для использования. Но если вам звонят и представляются специалистами банка, то они точно не будут уточнять номер карты - настоящие сотрудники и так всё знают. Из банка вам могут позвонить только в том случае, если поступили сведения о сомнительных действиях. Но при этом спрашивать данные карты никогда не будут.

А вот если вы сами звоните в банк, чтобы задать беспокоящий вас вопрос, например, о транзакции, которую вы не совершали, но СМС о которой получили, то в таком случае сотрудник банка может запросить личную информацию: Ф. И. О., дату рождения, последние четыре цифры банковской карты. Это нужно, чтобы быстро идентифицировать клиента и посмотреть последние совершённые операции.

- А вам самой звонили мошенники? Были какие-нибудь интересные истории?

- У меня было несколько историй. И от окружающих слышу то же самое. Ведь мошенники нередко работают годами по отлаженным схемам. Если мы говорим о телефонных звонках, то это уже не кибермошенничество, а социальная инженерия - морально-психологические методы, которые мошенники используют, чтобы выведать у вас конфиденциальную информацию. Создание стрессовой ситуации, запугивание, давление - так людей выводят на эмоции и подталкивают к необдуманным решениям.

Мне как-то позвонили и сказали: «Час назад вы перевели столько-то тысяч рублей». Мошенник озвучил именно ту сумму, которую я действительно недавно переводила. Но я сразу по тону голоса и манере общения поняла, что это мошенник, ведь уже давно с таким сталкиваюсь по работе. Однако простым гражданам бывает сложно обнаружить обман на ранних стадиях. Мошенник представляется, входит в доверие, точно называет переведённую вами сумму. Потом злоумышленник говорит, что эти деньги находятся в опасности и что некие мошенники хотят их украсть. Далее он настаивает на необходимости временно перебросить эту сумму на какой-то определённый счёт. Всё это происходит в спешке и под давлением, поэтому жертва даже не успевает подумать и оценить ситуацию. Для убедительности преступник даже может прислать фото «удостоверения» сотрудника банка, которое, конечно же, является подделкой.

Важно помнить: если вам позвонили из Центрального банка - нельзя верить. Центральный банк никогда никому не звонит и в принципе не работает с физическими лицами.

Что делать, если вам позвонили мошенники? Постарайтесь завершить разговор или повесить трубку. Если мошенник ведёт

Основные правила кибербезопасности >>

- Не переходите по неизвестным ссылкам.
- Заведите отдельную карту для онлайн-покупок.
- Храните карты отдельно от наличных.
- Установите антивирусную защиту и своевременно обновляйте ПО.
- Не заполняйте анкеты на непроверенных сайтах.
- Ограничьте функционал карты (например, задайте лимит на переводы) в мобильном приложении банка.
- В любой сомнительной ситуации обратитесь к сотруднику банка или в службу поддержки.

себя настойчиво - а это главный признак того, что здесь что-то не так, - скажите, что обратитесь в правоохранительные органы. Всегда работает.

В случае, когда у вас остались сомнения, позвоните в банк самостоятельно по номерам, указанным на сайте банка или в мобильном приложении. Но ни в коем случае не перезванивайте по тому номеру, с которого вам звонили «сотрудники службы безопасности банка».

Что делать?

- Как поступить, если вы всё-таки уже выдали какую-то информацию?

- Первое: если вы стали жертвой мошенника и денежные средства без вашего ведома украли с банковской карты, в первую очередь нужно позвонить в банк на горячую линию и заблокировать свою карту. Второе: если отделение банка от вас в шаговой доступности, придите туда и немедленно напишите заявление, чтобы дальше работала уже настоящая служба внутренней безопасности. Если возможности оперативно попасть в отделение банка нет, можно воспользоваться мобильным приложением - там есть подобные функции. И, наконец, необходимо обратиться в правоохранительные органы и написать заявлении о факте совершившегося мошенничества. Но помните, что если вы перевели злоумышленникам деньги сами, пусть и под давлением, их уже, к сожалению, не вернуть.

- Как быть дальше? Банк выдаст новую карту?

- Всё верно. Банк её вам перевыпустит, но, естественно, с новыми реквизитами, новым паролем. Данные вашей старой карты будут уже недействительны.

Не забывайте и о том, что наш телефон привязан к приложениям, картам и банкам. В случае утери гаджета постарайтесь как можно скорее разорвать эту связь и ограничить доступ.

- А можно как-то ограничить функционал, связанный с мобильным приложением? Например, установить лимит для переводов средств?

Что делать, если уже попались на уловки мошенников и выдали информацию?

1. Позвоните в банк и заблокируйте карту.
2. Сходите в отделение банка и напишите заявление.
3. Обратитесь в правоохранительные органы.

- Очень актуальный вопрос. С 1 октября как раз появилась такая функция. Это сделано как раз для защиты от мошенников. Можно отключить возможность оформления офлайн-кредита. Можно ограничить размер перевода или вообще сделать перевод недоступным. Тогда злоумышленники точно не совершат ничего без вашего ведома.

- Получается, каждый банк в своём приложении ввёл эту систему защиты от мошенничества?

- Да, каждый банк разрабатывает спектр услуг, который позволяет самому клиенту блокировать или ограничивать те или иные операции. Это бесплатно. Год от года совершенствуя эти системы, мы защищаем вас и себя от мошенничества. Мы говорим, показываем, рассказываем, предупреждаем. Но, к великому сожалению, иногда всё же становимся жертвами мошенников.

Ещё раз подчеркну: если есть хоть малейшие сомнения, мы тут же прекращаем разговор с подозрительным «сотрудником банка» и не берём трубку, если звонки с этого номера продолжаются. Главное - не общаемся, потому что под давлением можно что-то случайно рассказать.

Если вы уже стали жертвой злоумышленников, необходимо сразу обратиться в правоохранительные органы. Нельзя бояться, стесняться или просто махнуть на всё рукой, мол, это уж случилось, и деньги не вернуть. Нет. Правоохранительные органы в любом случае должны знать об этих инцидентах и разбираться в каждом конкретном случае.

К сожалению, даже самые опытные люди с высоким уровнем финансовой грамотности попадаются на уловки мошенников: как в интернет-пространстве, так и в ситуациях с социальной инженерией. Как показывает практика, сейчас зачастую жертвами становятся даже не представители старшего поколения, а люди в возрасте от 25 до 40 лет.

- Вы упомянули о мобильных приложениях банков. Откуда их можно скачивать? Ведь этот процесс тоже может таить в себе опасность: случайно скачаешь приложение с фишингового сайта или получишь СМС с оповещением о необходимости провести обновление и ссылку - и привет.

- Возвращаемся к началу нашего разговора: ни в коем случае по ссылкам из СМС не переходим. Если есть сомнения, обращайтесь к сотруднику банка. Есть техническая поддержка, её сотрудники вам всё расскажут: где скачать, как обновить, как защитить. Банки заинтересованы в своих клиентах. Они не заинтересованы в том, чтобы людей обманывали мошенники. Это и репутационные, и имиджевые риски. Все банки нацелены на то, чтобы защитить денежные средства своих клиентов. Первая цель у всех - минимизировать эти риски. Поэтому мы и говорим о том, что всё нужно делать спокойно, обдуманно, внимательно и без спешки. Это касается и онлайн-покупок, и телефонных разговоров, и общения в интернете, и действий в приложениях.

- Вернёмся к акциям и распродажам. Скидки могут распространяться на какие-то банковские услуги?

- Могут быть какие-то акции, но надо вдумчиво читать все условия и чётко понимать её рамки. Есть сомнения - задавайте вопросы. Всегда можно взять договор домой и в течение пяти дней его изучить, чтобы принять решение о заключении сделки.

И, конечно же, постоянно нужно развивать уровень финансовой грамотности.

Сергей ЕЛИСЕЕВ,
Мария ЛЕБЕДЕВА

ФОТО ПРЕСС-СЛУЖБЫ БАНКА РОССИИ