**Памятка**

**Об основных схемах кражи денежных средств мошенниками**

**в интернете и способы обезопасить себя**

В связи с участившимися случаями мошенничества с использованием высокотехнологичных устройств – мобильных телефонов, планшетов, компьютеров, а также пластиковых и виртуальных банковских карт, предлагается изучить основные схемы кражи денежных средств мошенниками в интернете и способы обезопасить себя:

Риск возникает во время покупок на сайтах и в приложениях, использования 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.

**Способы предотвращения:**

**Пользуйтесь только личными устройствами**

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

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

**Защититесь от вирусов**

Обязательно поставьте антивирус на всех своих устройствах, включая мобильные, и регулярно обновляйте их. Хороший антивирусный пакет всегда включает защиту от фишинга и вирусных программ.

**Выбирайте безопасные сайты**

* 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 получить доступ и к вашим данным.
* Набирайте интернет-адрес банка вручную, а еще лучше — сохраняйте в закладках адреса ваших банков, госорганов и других организаций.
* Всегда проверяйте адресную строку браузера. Иногда можно попасть на фишинговый сайт при переходе с одной страницы известного вам портала на другую.
* Делайте покупки только на сайтах, которые обеспечивают безопасное соединение. Адрес такого ресурса начинается с https://. В адресной строке есть значок в виде закрытого замка.
* Еще лучше — проверять сертификат безопасности сайта. Для этого нажмите на значок замка и в открывшемся окне выберите «Просмотр сертификатов». Убедитесь, что сертификат выдан именно тому сайту, на котором вы находитесь, и срок его действия еще не закончился.
* Выбирайте известные интернет-магазины и сервисы. Изучите отзывы о них от других пользователей. Лучше всего посмотреть отзывы на нескольких независимых сайтах. Добросовестный продавец всегда дает полную информацию о себе: телефон, адрес и прочие контактные данные.

**Используйте систему безопасных платежей**

Когда переходите на страницу оплаты, ищите логотипы программ MasterCard SecureCode, Visa Secure и Mir Accept. Эти программы с помощью технологии 3D-Secure дополнительно защищают вас во время покупок в интернете.

Если онлайн-магазин поддерживает эту технологию, после ввода реквизитов карты он перенаправит вас на безопасную интернет-страницу банка. Для подтверждения покупки банк отправит СМС с одноразовым паролем на номер мобильного телефона, привязанный к карте или счету. Никому не сообщайте этот код — просто введите его в специальное поле на странице оплаты.

**Заведите отдельную карту для покупок в интернете**

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**

Чаще всего в краже средств со счета виноваты вовсе не банки, платежные системы или онлайн-магазины, а сами доверчивые пользователи.

Мошенники знают множество уловок, чтобы втереться к вам в доверие. И ваша задача на эти уловки не попасться. Никогда не сообщайте посторонним данные своей карты, персональные данные и коды из СМС.

Никому не говорите 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.

Тех же правил следует придерживаться и при пользовании интернет-кошельком: никогда и никому не сообщайте логин и пароль от своего аккаунта.

**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.

1. **Сервис объявлений**

Если вы решили купить товар с рук или продать ненужную вам вещь, будьте внимательны — мошенники нередко играют роль покупателей или продавцов. На ваш товар находится крайне заинтересованный покупатель, который готов перевести аванс на ваш счет и просит у вас не только номер карты или номер телефона, но и код проверки подлинности карты (три цифры на обратной стороне, например, CVV или CVC). Такой подход должен вас насторожить — ведь для перевода денег достаточно знать только номер карты.

Если вы покупаете товар с рук, у вас могут попросить предоплату и сообщить все данные карты. Если перед вами мошенник, то в лучшем случае вы останетесь без денег, которые отправили авансом. В худшем — если у вас попросили все данные карты — рискуете остаться и без средств на счете.

**Способы предотвращения:**

Будьте осторожны, покупая товары с рук через социальные сети или специальные сайты. Всегда старайтесь проверить потенциального покупателя или продавца по отзывам. В сообществах и на сервисах обычно есть «черный список» (и покупателей, и продавцов) и модераторы. Проверьте профиль продавца — часто мошенники создают фальшивые страницы с минимумом информации.

## Социальные сети и мессенджеры

## Знакомый прислал вам личное сообщение с просьбой одолжить денег или со странной ссылкой. Это значит лишь одно — аккаунт вашего друга взломали.

Часто мошенники представляются сотрудниками известных брендов и компаний из любых областей. Вам обещают кредиты под низкий процент, большие скидки, бесплатные товары или говорят, что вы выиграли в конкурсе. Чтобы получить приз или скидку, от вас требуется всего ничего — сообщить данные вашей карты, паспорта или все сразу.

**Способы предотвращения:**

Если странные сообщения через социальные сети шлет ваш друг, как можно скорее позвоните ему и выясните, действительно ли ему нужна помощь. Или мошенники взломали его аккаунт — и могут обмануть кого-то еще. Например, его бабушку!

Если незнакомцы пишут вам от лица компании или бренда, лучше уточнить информацию на официальном сайте компании или ее странице в социальной сети — крупные компании редко проводят конкурсы, в которых вы можете победить, даже не участвуя, и никогда просто так не запрашивают ваши личные данные, а тем более данные карты.

## Электронная почта

Вам на почту присылают письма с обещанием подарков, денег и кредитов. Мошенники пытаются заманить вас чем угодно. Пишут, что вы выиграли машину. Присылают ответ на якобы ваше письмо. Просто хотят «познакомиться поближе».

В строке отправителя может быть как неизвестный вам человек (часто иностранец), так и известный сайт, платежная система, онлайн-сервис или банк. Ничего страшного не произойдет, если вы просто откроете письмо, но не переходите по ссылкам и не скачивайте вложения из письма — так вы рискуете заразить компьютер вирусом, который позволит мошенникам его контролировать. И тем более не вводите данные вашей карты.

**Способы предотвращения:**

В почте есть встроенный спам-фильтр — часть подозрительных писем всегда попадает в специальную папку. Но несмотря на это всегда обращайте внимание на заголовок письма, его отправителя и содержание. Компании всегда рассылают почтовые рассылки с одних и тех же адресов и редко допускают ошибки в письмах — а вот мошенники часто пишут с большим количеством ошибок, нечитаемых системой символов и перевирают название компании в адресе. Не переходите по ссылкам из таких писем и не скачивайте вложения из них.

## Сайт-двойник

Мошенники копируют известные сайты, используя похожее название компании и оформление. Например, вы хотите узнать, есть ли у вас штрафы в ГИБДД или как оформить кредит онлайн, а попадаете на фишинговый сайт, то есть сайт-клон. Если вы введете на таких сайтах свои данные, они попадут в руки злоумышленников.

**Способы предотвращения:**

Всегда обращайте внимание на адресную строку браузера: на сайте-клоне будет допущена ошибка. Оплачивайте покупки только через сайты с защищенным соединением и значком платежной системы. Внимательно изучите и содержание сайта — злоумышленники часто невнимательно относятся к наполнению сайта. Добавьте в закладки сайты, которыми часто пользуетесь, чтобы не набирать адрес вручную — так вы не ошибетесь в названии и попадете на нужный вам сайт.

## Ваш смартфон

Зловредные программы умеют маскироваться под мобильные банки и таиться в разных приложениях, которые вы скачиваете на телефон.

**Способы предотвращения:**

Скачивайте приложения на телефон только в официальном магазине. Обращайте внимание в первую очередь на разработчика программы — в официальных банковских приложениях указан сам банк. Внимательно читайте описание и не скачивайте приложения сторонних разработчиков.

Информацию подготовил:

Заместитель Борзинского

транспортного прокурора

К.Л. Галинецкий