**Основные виды IT-преступлений и их профилактика**

**К наиболее распространенным видам дистанционных мошенничеств относятся:**

– **«ФИШИНГ»** – вид дистанционного мошенничества, при совершении которого злоумышленники (в ходе телефонного разговора, посредством направления электронного письма или смс-сообщения) получают личные конфиденциальные данные о банковской карте, номере счета, логины и пароли для входа в интернет-банк, а также пароли безопасности, позволяющие произвести списание находящихся на банковской карте денежных средств. Жертвами указанного вида мошенничества зачастую становятся незащищенные, малообразованные, доверчивые слои населения. Представляясь зачастую сотрудниками кредитных организаций, преступники вводят в заблуждение граждан относительно совершаемых несанкционированных списаний денежных средств, осуществляемых покупках и т.п., после чего просят назвать конфиденциальные сведения с целью пресечения возможного совершения преступления. Граждане, доверяя полученной информации, желая обезопасить свои денежные средства от преступных посягательств, сообщают запрашиваемую информацию, в результате чего злоумышленники похищают принадлежащие им денежные средства.

– **«ФАРМИНГ»** – процедура скрытого направления на ложный IP-адрес, то есть направление пользователя на фиктивный веб-сайт, чаще всего используемый для приобретения товаров и услуг (ozon.ru, avito.ru, aliexpress.ru, joom, biglion, купинатор, кассир.ру, билетер, сайты по продаже билетов на ж/д и авиатранспорт и др.);  
– **«ДВОЙНАЯ ТРАНЗАКЦИЯ»** (при оплате товаров и услуг продавец сообщает об ошибке, предлагает повторить операцию, а в дальнейшем денежные средства списываются дважды по каждой из проведенных операций)  
– **«ТРАППИНГ»** (манипуляции с картридером банкоматов, позволяющие либо не возвращать карту владельцу, либо списывать все данные карты для дальнейшего их использования).

**Основные схемы телефонного мошенничества:**

1. **Обман по телефону.**  
   Звонок сотрудника банка – когда неизвестный представляется сотрудником службы безопасности какого-либо банка и сообщает, что с Вашего банковского счета происходят операции по несанкционированному списанию денежных средств, и в целях безопасности счета предлагает перевести сбережения на «резервный» или «безопасный» счет. Распространены случае сообщения информации об оформлении на Вас кредита и необходимости пройти в приложении онлайн-Банка по определённой ссылке для его аннулирования (выполнить иные инструкции).  
   Звонок сотрудника правоохранительных органов – когда неизвестный представляется сотрудником полиции, следователем и т.д. и сообщает, что проводится спецоперация по поимке мошенников и для этого необходимо перевести деньги на «специальный» счет. При этом требует не звонить в банк, так как сотрудники банка заодно с мошенниками.  
   Ваш родственник, либо близкий человек попал в беду (например, машиной сбил человека или обвиняется в совершении преступления), и задержан сотрудниками полиции, и неизвестный сообщает, что для освобождения необходимо перевести на счет денежные средства либо для примирения с пострадавшим либо в качестве взятки сотрудникам полиции. Возможны варианты, при которых в разговоре может принять участие якобы сотрудник полиции, который будет подтверждать сказанное.  
   ВАЖНО: Это звонят мошенники (несмотря на то, что определившийся на телефоне номер может соответствовать номеру телефона банка или правоохранительных органов, зачастую – Московского региона (499, 495… и т.д.), так как при помощи специальных устройств мошенники меняют номера на абсолютно любой номер – так называемые подменные номера), сотрудники банков никогда не звонят своим клиентам, и тем более, никогда не требуют переводить с личного счета деньги. Представители правоохранительных органов могут звонить только для вызова в помещения правоохранительных органов с целью получения объяснений, истребования документов по находящимся в производстве уголовным делам и материалам проверок.  
   При поступлении такого звонка необходимо прервать разговор и перезвонить тому, о ком идет речь, либо в указанный государственный орган или кредитную организацию для перепроверки информации.

**2. Обман при покупке (продаже) товара на интернет сайтах.**  
Предоплата за несуществующий товар – подается объявление на востребованный товар с привлекательной ценой (ниже рыночной) с приложением ненастоящих фотографий. В ходе общения «продавец» уклоняется от встречи ввиду житейских причин (нет времени, занятость на работе, удаленность расположения) и предлагает оплатить товар безналичным платежом с гарантированной последующей доставкой через курьера, но после получения денег, продавец- мошенник перестает выходить на связь.  
Оплата муляжа по почте наложенным платежом – злоумышленник пытаются вначале заполучить предоплату на доверии, если не получается, то предлагают получить заказ на  
Покупатель спрашивает номер карты и код из СМС – по Вашему объявлению о продаже товара в интернете Вам позвонил покупатель и попросил сообщить реквизиты банковской карты (предварительно выяснив номер телефона к которому привязана карта) и смс-код, чтобы перевести деньги, якобы это нужно для банковского перевода. На самом деле это мошенник, который пытается войти в личный кабинет онлайн-банка и списать все деньги с Вашего счета.  
ВАЖНО: Оплачивайте товар только после его получения и проверки и не отправляйте деньги в качестве залога (задатка). Для перевода денежных средств достаточно номера телефона и другой дополнительной информации не требуется.

1. **Телефонные вирусы.**  
   Очень часто используется форма мошенничества с использованием телефонных вирусов. На телефон абонента приходит сообщение следующего вида: «Вам пришло MMS-сообщение. Для получения пройдите по ссылке…». При переходе по указанному адресу на телефон скачивается вирус и происходит списание денежных средств с вашего счета.  
   Другой вид мошенничества выглядит так. При заказе какой-либо услуги через якобы мобильного оператора или при скачивании мобильного контента абоненту приходит предупреждение вида: «Вы собираетесь отправить сообщение на короткий номер …, для подтверждения операции, отправьте сообщение с цифрой 1, для отмены с цифрой 0». При отправке подтверждения, со счета абонента списываются денежные средства. Мошенники используют специальные программы, которые позволяют автоматически генерировать  
   ВАЖНО: Не следует звонить по номеру, с которого отправлен SMS – вполне возможно, что в этом случае с Вашего телефона будет автоматически снята крупная сумма и переходить по сомнительным ссылкам.
2. **Ошибочный перевод средств.**  
   Абоненту поступает SMS-сообщение о поступлении средств на его счет, переведенных с помощью услуги «Мобильный перевод». Сразу после этого поступает звонок и мужчина (или женщина) сообщает, что ошибочно перевел деньги на его счет, при этом просит вернуть их обратно тем же «Мобильным переводом». В действительности деньги не поступают на телефон, а человек переводит свои собственные средства. Если позвонить по указанному номеру, он может быть вне зоны доступа. Кроме того, существуют такие номера, при осуществлении вызова на которые с телефона снимаются все средства.  
   ВАЖНО: Если Вас просят перевести якобы ошибочно переведенную сумму, напомните, что для этого используется чек. Отговорка, что «чек потерян», скорее всего, свидетельствует о том, что с Вами общается мошенник.

##### Мошенничества с банковскими картами

Банковская карта – это инструмент для совершения платежей и доступа к наличным средствам на счёте, не требующий для этого присутствия в банке. Но простота использования банковских карт оставляет множество лазеек для мошенников.  
При проведении операций с картой пользуйтесь только теми банкоматами, которые расположены в безопасных местах и оборудованы системой видеонаблюдения и охраной: в государственных учреждениях, банках, крупных торговых центрах и т.д.  
Совершая операции с пластиковой картой, следите, чтобы рядом не было посторонних людей. Набирая ПИН-код, прикрывайте клавиатуру рукой.   
Обращайте внимание на картоприемник и клавиатуру банкомата. Если они оборудованы какими-либо дополнительными устройствами, то от использования данного банкомата  
В случае некорректной работы банкомата – если он долгое время находится в режиме ожидания или самопроизвольно перезагружается – откажитесь от его использования. Велика вероятность того, что он перепрограммирован злоумышленниками.  
**Как обезопасить себя от мошенников:**  
1. Проверяйте информацию, полученную в ходе телефонного разговора и интернет переписки с неизвестными (они могут представляться сотрудниками правоохранительных органов, представителями кредитных организаций).  
2. Установить на телефон (компьютер) современное лицензированное антивирусное программное обеспечение.  
3. Не устанавливайте и не сохраняйте без предварительной проверки антивирусной программой файлы, полученные из ненадежных источников: скачанные с неизвестных сайтов, присланные по электронной почте (подозрительные файлы лучше сразу удалять).  
4. Используйте пароли не связанные с Вашими персональными данными.  
5. Ни при каких обстоятельствах не сообщайте реквизиты своих банковских счетов (карт), пароли и другую персональную информацию.  
6. Поставьте лимит на сумму списаний или перевода в личном кабинете банка.  
7. По всем возникающим вопросам обращаться в банк, выдавший карту.  
8. Не выполнять никаких срочных запросов к действию, в том числе по установке каких бы то ни было приложений.  
9. Не переходить ни по каким ссылкам, которые приходят на e-mail или по SMS.  
10. Обращать на все сообщения от банка (например, если они содержат грамматические ошибки).  
11. Не перезванивать по номерам которые приходят на e-mail или по SMS.  
12. Перепроверяйте подлинность интернет-сайтов, на которых осуществляете заказ товара.