Виды и способы совершения ИТТ-преступлений.

Слайд 1-2

В настоящее время можно выделить **3 группы** мошенничеств, совершаемых с применением информационно-телекоммуникационных технологий:

1. ***Телефонные мошенничества*** - мошенничества с использованием средств сотовой связи;
2. ***Кибермошенничества*** - вирусное заражение смартфона для получения доступа к данным, системам онлайн банкинга для последующего похищения денежных средств со счета;
3. ***Мошенничества, совершаемые в сети интернет*** - мошенничества при покупках или продажах через сеть Интернет (онлайн магазины, соц.сети), оказание услуг, а также финансовые пирамиды, фиктивные инвестиции.

Слайд 3-6

1-й вид телефонные мошенничества

мошенничества с использованием средств сотовой связи

«СРОЧНЫЙ ЗВОНОК» - в ходе телефонного разговора злоумышленники представляются: сотрудниками банка, правоохранительных органов, социальных служб, специалистами портала «Госуслуги», близкими родственниками, сообщают о проблемной ситуации, требующей незамедлительного реагирования, например: третьи лица пытаются оформить кредит, по банковской карте/счету производятся/совершены подозрительные операции, банковский счет заблокирован, близкий родственник попал в беду, необходимы деньги и др., после чего предлагают потерпевшему в целях решения проблемы совершить следующие действия:

- Произвести операции по указанию злоумышленника через банкомат или в режиме онлайн через приложение;
- Скачать под видом антивирусного или иного приложения для безопасности, программу удаленного доступа;
- Снять денежные средства с банковского счета/карты, оформить кредит, а после перевести денежные средства на «специальный безопасный счет»;
- Сообщить номер банковской карты, CVC — код, коды из СМС сообщений;
- Передать денежные средства третьему лицу.

Примеры:

1. Гр. В. позвонили неустановленные лица, представились сотрудниками полиции, сообщили, что мошенники оформили на его имя кредит в сумме 300 000 рублей. Для отмены всех операций необходимо подать встречную заявку для понижения кредитного потенциала и

перевести деньги на «застрахованные, безопасные» банковские счета. Заявитель оформил онлайн-кредит, перевел деньги злоумышленникам.

2. Гр. Д. позвонили неустановленные лица, которые представились сотрудниками полиции, в ходе разговора сообщили, что родственник попал в аварию ему требуется дорогостоящая операция, для ее проведения срочно необходимо перевести денежные средства (передать курьеру).

Слайд 7

Способы защиты:

- Не отвечайте на звонки с незнакомых номеров;
- Прервите разговор если разговор касается финансовых вопросов;
- Не торопитесь принимать решения;
- Позвоните своим близким родственникам и проверьте информацию в «Интернете»;
- Не перезванивайте по незнакомым номерам;
- Самостоятельно позвоните в полицию, банк или организацию;
- Не сообщайте сведения о картах особенно CVV/CVC-коды, не производите манипуляции при помощи банкомата;

2-й Вид – Кибермошенничества

Слайд 8

В настоящее время выделяют **3 вида** кибермошенничеств:

- «Фишинг» (сайты двойники);
- Взлом Госуслуг;
- Вирусы и программы удаленного доступа;

Фишинг – сайт двойник или зеркальный сайт

Слайд 9-10

Преступником создается сайт «двойник», визуально схожий на какой-либо известный официальный сайт (в названии имеются отличия).

При проверке необходимо обратить внимание на домен (имя) сайта: мошенники заменяют буквы символами – например, ЦИФРА 1 вместо БУКВЫ «I» (onL1ne вместо onLIne); Имя сайта максимально приближено к оригиналу (onLLine.sberbank.ru вместо onLine.sberbank.ru). Фейковый сайт может располагаться в нестандартной зоне, например rzd.INFO или rzd.NET, когда оригинал: rzd.RU;

Пример: *Гр. А. в сети интернет нашел ссылку на сайт по приобретению билетов со скидками в кинотеатры г. Улан-Удэ. Перейдя по ссылке забронировал билеты на 2 персоны и произвел оплату, в результате чего произошло списание денежных средств в сумме 8 978 рублей.*

Взлом личного кабинета портала «Госуслуги», социальных сетей: «В контакте», «Одноклассники», мессенджеры «Телеграмм», «Вайбер», «Ватсап»

Слайд 11-13

Злоумышленниками осуществляется неправомерный доступ (взлом) к личным кабинетам портала «Госуслуги», с последующим оформлением микрозаймов.

Взлом аккаунтов в социальных сетях/мессенджерах осуществляется с целью хищения денежных средств под предлогом их займа у находящихся в друзьях пользователей. Получившие доступ к аккаунту, злоумышленники вымогают средства под угрозой распространения личной переписки/фотографий компрометирующего характера.

Пример: *Гр. С. на сотовый телефон поступил звонок от оператора сотовой связи «МТС», который сообщил что заканчивается срок действия договора, предложил продлить дистанционно, сообщив поступивший код в смс — сообщении. После поступил звонок от работника портала «Госуслуги» и сообщил, что мошенники пытаются взломать личный кабинет, и для предотвращения мошеннических попросил продиктовать пришедшие в СМС коды. В результате взлома личного кабинета на портале «Госуслуги» на гр. С. оформлены микрозаймы.*

Вирусы и программы удаленного доступа

Слайд 14

Потерпевшим по указанию злоумышленника, устанавливается программа удаленного доступа, под видом антивируса, после чего, преступник получает доступ к содержимому телефона или компьютера потерпевшего.

В результате взлома мессенджера («ватсап», «вайбер», «телеграм») производится рассылка всем контактам с интернет-ссылкой следующего содержания: «Проголосуй за моего племенника», после перехода по указанной ссылке на телефон устанавливается вирус (программа шпион) которая в последующем может быть использована для совершения вышеперечисленных мошенничеств.

Способы защиты:

Слайд 15

- При проверке необходимо обратить внимание на домен (имя) сайта: мошенники заменяют буквы символами – например, ЦИФРА 1 вместо БУКВЫ «I» (onL1ne вместо onLIne). Имя сайта максимально приближено к оригиналу (onLLine.sberbank.ru вместо onLine.sberbank.ru). Фейковый сайт может располагаться в нестандартной зоне, например rzd.INFO или rzd.NET, когда оригинал: rzd.RU;

- Никому не сообщайте код из СМС-сообщения, поступивший с портала «Госуслуги». Настройте вход на портал «Госуслуги» по паролю и коду из СМС-сообщения. Регулярно, раз в полгода, меняйте пароли доступа;
- В целях безопасности рекомендуется использовать программы по блокировке спам-звонков, и «Антивирусы».

3-й вид мошенничества, совершаемые в сети интернет

Слайд 16

Мошенничества при покупках или продажах через сеть Интернет (онлайн магазины, соц. сети), оказание услуг, а также финансовые пирамиды, фиктивные инвестиции.

В настоящее время выделяют **3 способа** мошенничества, совершаемые в сети интернет:

- Мошенничества в сфере купли и продажи;
- Мошенничества, совершаемые под предлогом оказания услуг;
- Финансовые пирамиды, фиктивные инвестиции.

Мошенничества в сфере купли и продажи:

Слайд 17-18

Преступления, совершенные с использованием или применением социальных сетей. Преступником в сети «Интернет» создается сообщество (группа) по продаже какой – либо продукции (Авито, Дром и т.д.).

Слайд 19-21

Примеры:

1. Гр. И. на сайте «Авито» выложила объявление о продаже детской коляски, после с ней связался покупатель который пояснил, что хочет его приобрести для себя безопасным способом через «Авито-доставка». После чего он скинул в мессенджере «Ватсап» ссылку для безопасной сделки. Пройдя по ссылке потерпевшая указала реквизиты своей банковской карты на которую на которую должна была поступить оплата. Далее ей на сотовый телефон пришел пароль, который она также указала в ссылке, в результате со счета были списаны денежные средства в сумме 9 700 рублей.

2. Гр. В. на сайте «Авито» увидел объявление о продажи двигателя по цене ниже рыночной стоимости. В ходе телефонного разговора с продавцом последний попросил перевести задаток, так как у него имеются еще клиенты на данный двигатель. Гр. В. перевел продавцу денежные средства в сумме 25 000 рублей по указанному в объявлении абонентскому номеру, после чего объявление было снято с публикации, продавец перестал выходить на связь.

Мошенничества совершенные под предлогом оказания услуг, *заработка*

Слайд 22

Преступником используются различные программы (приложения) («вайбер», «ватсап», «телеграмм») для того, чтобы вступить в переписку с потерпевшим.

Слайд 23-24

Пример:

1. гр. А. размещает объявление о поиске работы на различных сайтах (Авито.вакансии, hh.ru и др.) после чего с ним связываются и предлагают удаленную работу, далее ему рекомендуют пройти верификацию или подтвердить личность через приложение дистанционного банковского обслуживания, действуя по указанию злоумышленников, гр. А. предоставляет доступ к своим счетам.

Финансовые пирамиды, фиктивные инвестиции

Слайд 25-26

Злоумышленники под видом участия в торгах на «бирже», создают сайты, на которых в личных кабинетах размещают информацию о приросте денежных средств, вложенных потерпевшим под видом инвестиций.

Пример:

1. Гр. А. оформил дебетовую и кредитную банковскую карты АО «Тинькофф банк» и подключил услугу «Инвестиции». Далее на сотовый телефон гр. А. позвонил мужчина, который представился сотрудником банка АО «Тинькофф банк» и предложил заработать на инвестициях, установив приложение «Bybit» для обмена денежных средств на криптовалюту, и приложение «Терминал» для пополнения счета. После установки приложения заявитель перевел с денежные средства в сумме 10 000 руб. на счет приложения «Терминал», где через некоторое время увидел, что сумма повысилась на 1 800 руб. Далее гр. А. предложили получить еще больше прибыли, заявитель вновь внес денежные средства в сумме 180 000 руб., 600 000 руб., и 500.000 руб. После пришло уведомление о том, что приложение «Терминал» заблокировано, для разблокировки необходимо внести 1 000 000 руб.

Гр. А. оформил несколько кредитов в ПАО «Сбербанк», АО «Тинькофф банк» на супругу в сумме 1 986 000 руб.и совершал переводы злоумышленникам, полагая, что инвестирует свои денежные средства.

Способы защиты:

Слайд 27-28

- Покупайте и продавайте из рук в руки, не осуществляйте предоплату, называйте только абонентский номер для перевода денежных средств, этого достаточно для осуществления перевода. Настаивайте на наложенном платеже без предоплаты, проверяйте данные покупателя и продавца в интернете, не переходите по неизвестным ссылкам;
- Не совершайте платежи/переводы в адрес потенциального работодателя, даже если вам объясняют их необходимость для будущей работы, например, плата за обучение, рабочую форму или рабочие инструменты. Не выполняйте действия в «Банковских приложениях» по указанию посторонних лиц, например для открытия «Рабочего счета» и др.;
- Проверяйте брокерскую компанию на сайте Банка России на наличие лицензии, не доверяйте рекламе о биржах в социальных сетях, внимательно читайте пункты договора (если он составляется). Не верьте заманчивым и убедительным словам о высоких доходах при низком риске.

ОБК МВД по Республике Бурятия