Памятка
по видам и способам совершения ИТТ-преступлений при проведении профилактических мероприятий с населением

ВНИМАНИЕ!

1. Перед проведением профилактического мероприятия по видам и способа совершения ИТТ-преступлений и защите от них, необходимо самостоятельно изучить понять цифровую модель ИТТ-преступлений.

2. При доведении информации необходимо взаимодействовать с аудиторией закреплять информацию путем повторения (с приведением примеров) по каждому способ совершения ИТТ-преступления.

1. «ТЕЛЕФОННЫЙ ЗВОНОК»

В ходе телефонного разговора злоумышленники представляются: сотрудниками банка правоохранительных органов, социальных служб, специалистами портала «Госуслуги», близкими родственниками, которые сообщают о проблемной ситуации, требующей незамедлительного реагирования. Например: третьи лица пытаются оформить кредит; по банковской карте/счет 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;
- 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).

Способы защиты:

- Не отвечайте и не перезванивайте на незнакомые номера;
- Прервите разговор если он касается финансовых вопросов;
- Позвоните своим близким,родственникам, проверьте информацию;
- Обратитесь в полицию, банк или организацию;
- Не сообщайте сведения о картах (CVV/CVC-коды);
- Не переводите денежные средства по просьбе (требованию) неизвестных лиц.

2. Взлом личного кабинета портала «Госуслуги»

Основные схемы взлома:

1. Злоумышленниками, путем обзвона граждан, осуществляется неправомерный доступ (взлом) личным кабинетам портала «Госуслуги», с последующим оформлением микрозаймов кредитов.
   В ходе телефонного разговора мошенники представляются сотрудниками сотовых компани (работниками портала «Госуслуги»). Под видом продления срока действия SIM-карты, либ подтверждения личности на портале «Госуслуги», просят продиктовать код, поступивший SMS-сообщении. В это время, злоумышленник в приложении «Госуслуги» вводит абонентски номер потерпевшего, и ожидает когда ему продиктуют код, получая тем самым доступ личному кабинету портала.

   Пример: *Гр. С. на сотовый телефон поступил звонок от злоумышленника, представившимс сотрудником сотовой компании «МТС», который сообщил что заканчивается срок действи SIM-карты, предложил продлить дистанционно, сообщив поступивший код в SMS - сообщении. Гр. С. продиктовал, поступивший в SMS-сообщении код, тем самым предостави доступ в личный кабинет портала «Госуслуги».*

   В результате взлома личного кабинета на портале «Госуслуги» на гр. С. оформлен микрозаймы.

2. Одним из способов возможности получения доступа к личному кабинету портала «Госуслуги является несвоевременное открепление абонентского номера в случае прекращения ег использования (смена номера). Злоумышленники покупая новые SIM-карты восстанавливаю пароль на портале «Госуслуги».

   Пример: *Мошенник производит покупку SIM-карты, которая не использовалась от 2-6 месяце далее он производит проверку привязки личного кабинета на портале «Госуслуги», после то как мошенник обнаруживает, что номер не отвязан от личного кабинета, то о восстанавливает к нему доступ и совершает оформления микрозаймов/кредито*

Способы защиты:

- Не отвечайте и не перезванивайте на незнакомые номера;
- Никому не сообщайте коды из SMS-сообщений (в т. ч. поступившие с портала «Госуслуги»
- Установите дополнительную защиту для входа на портал Госуслуги: SMS-пароль контрольный вопрос.
- Регулярно меняйте пароли доступа.

3. Фишинг – сайт двойник или зеркальный сайт

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

Пример: *Гр. А. в сети интернет нашел ссылку на сайт (k1no.trc-forum.ru) по приобретени билетов со скидками в кинотеатры г. Улан-Удэ. Перейдя по ссылке забронировал билеты на 2 персо и произвел оплату, в результате чего произошло списание денежных средств в сумме 8 978 рублей.*

Способ защиты:

- ❖ При проверке обратите внимание на:

- Мошенники заменяют буквы символами – например, ЦИФРА 1 вместо БУКВЫ «I (onL1ne вместо onLIne);
- Имя сайта максимально приближено к оригиналу (onLLine.sberbank.ru вмест onLine.sberbank.ru); Фейковый сайт может располагаться в нестандартной зон например **rzd.INFO** или **rzd.NET**, когда оригинал: **rzd.RU**.

4. Мошенничества, совершаемые в сети интернет

Преступления, совершаемые в социальных сетях, мессенджерах, торговых площадках в сет Интернет (Авито, Дром и т.д.).

Примеры:

1. Потерпевший - продавец: гр. «М.» на сайте «Авито» выложила объявление о продаже детско коляски, после с ней связался покупатель который пояснил, что хочет приобрести товар для себ безопасным способом через «Авито-доставка». После чего он скинул в мессенджере «WhatsApp» е ссылку для безопасной сделки по которой она перешла и указала реквизиты банковской карты н которую она хотела получить оплату, после чего ей на сотовый телефон пришел пароль, который он также указала в ссылке, в результате со счета были сняты денежные средства в сумме 9 700 рублей.

2. Потерпевший - покупатель: гр. «В» на сайте Авито увидел объявление о продаже двигателя п цене ниже рыночной стоимости. Позвонив продавцу по телефону указанному в объявлении, продав попросил перевезти задаток, так как у него имеются еще желающие приобрести данный двигатель он должен точно понимать, что гр. «В» его приобретет. Покупатель перевел продавцу денежны средства в сумме 25 000 рублей на указанный в объявлении абонентский номер. После чего объявлени было заблокировано.

Способы защиты:

- Не осуществляйте предоплату;
- Называйте только абонентский номер для перевода денежных средств (достаточно дл осуществления перевода);
- Оплачивайте покупки только после доставки.
- Проверяйте рейтинг продавца и отзывы.

5. Фиктивные «инвестиции»

Злоумышленники под видом участия в торгах на «бирже», создают сайты, на которых люд вкладывают денежные средства под видом инвестиций, при этом предоставляют потерпевш ложную информацию об увеличении дохода.

Пример:

1. Гр. А. оформил дебетовую и кредитную банковскую карты АО «Тинькофф банк» и подключ услугу «Инвестиции». Далее на сотовый телефон гр. А. позвонил мужчина, который представил сотрудником банка АО «Тинькофф банк» и предложил заработать на инвестициях, установ приложение «Bybit» для обмена денежных средств на криптовалюту, и приложение «Терминал» д пополнения счета. После установки приложения заявитель перевел с денежные средства в сумме 10 0 руб. на счет приложения «Терминал», где через некоторое время увидел, что сумма повысилась на 1 8 руб. Далее гр. А. предложили получить еще больше прибыли, заявитель вновь внес денежные средств сумме 180 000 руб., 600 000 руб., и 500.000 руб. После пришло уведомление о том, что приложен «Терминал» заблокировано, для разблокировки необходимо внести 1 000 000 руб.

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

Способ защиты:

- Проверяйте брокерскую **компанию на сайте Банка России – crb.ru** (пример сай связанного с фиктивными «инвестициями» - *compire-group.com*).
- Не доверяйте рекламе о биржах в сети Интернет.
- **Не верьте заманчивым и убедительным словам о высоких доходах при низком рис**