КИБЕРБЕЗОПАСНОСТЬ И ПРОФИЛАКТИКА КИБЕРПРЕСТУПНОСТИ В СОЛИГОРСКОМ РАЙОНЕ

ПЛАН-КОНСПЕКТ

«Об актуальных способах совершения киберпреступлений»

Ключевые факторы, влияющие на динамику киберпреступности.

Стремительное развитие цифровых технологий, переход к безналичным расчетам за приобретение товаров и услуг, размещение в сети Интернет персональных данных пользователей, стали следствием ежегодного увеличения количества регистрируемых киберпреступлений.

Проведенный анализ свидетельствует о том, что абсолютное большинство данных преступлении совершено в отношении физических лиц, а основным способом совершения является хищение денежных средств путем модификации компьютерной информации, характеризующиеся преобладанием мошеннических действий в сети Интернет с использованием методов социальной инженерии (вишинг), в том числе с использованием различных торговых площадок, в целях завладения реквизитами банковских платежных карт или доступа к системам дистанционного банковского обслуживания (фишинг).

В сложившейся ситуации наиболее острой проблемой является беспечное отношение граждан к соблюдению базовых правил информационной безопасности. Необходимо понимать, что безопасность в Интернете не имеет возрастных ограничений, поэтому каждый может защитить себя от кибер-преступников, не будучи экспертом в этих вопросах. Все, что необходимо для обеспечения своей безопасности – это руководствоваться следующими правилами:

1. Не доверяйте позвонившим Вам незнакомым лицам.

Кибермошенники могут выдавать себя за кого угодно, например за представителя службы безопасности банка или сотрудника органов внутренних дел. Как правило, предлогом для звонка является обнаружение фактов несанкционированных денежных переводов с банковского счета за рубеж, которых на самом деле не было. Кроме того, часто используется мошенническая схема «оперативная игра». В ходе телефонной беседы в популярных мессенджерах жертве предлагается принять участие в оперативной игре по изобличению неблагонадежного сотрудника банка путем оформления кредита, который зачисляется на банковский счет. При этом могут

использоваться поддельные служебные удостоверения сотрудников органов внутренних дел. Приведенные выше мошеннические схемы направлены не иначе как на хищение денежных средств под благовидным предлогом.

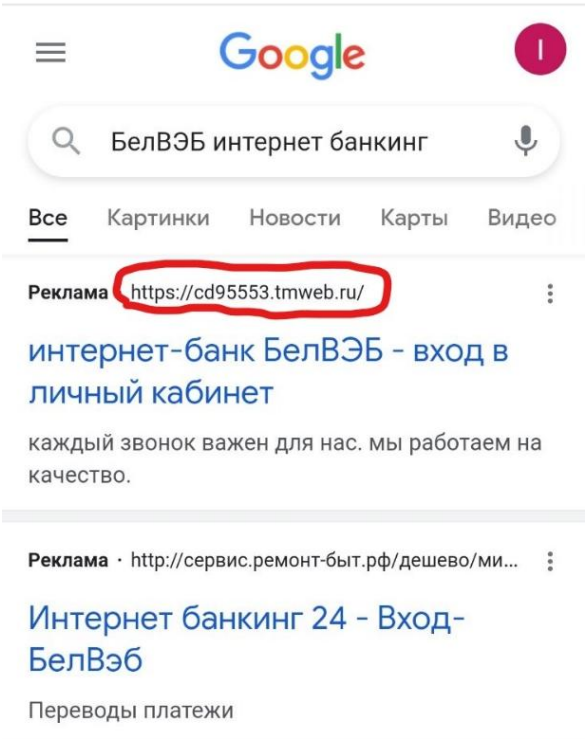
Как Вы можете узнать, что Вас пытаются обмануть? Самый простой способ – это перестать общаться с незнакомцем и перезвонить в свой банк или в территориальный орган внутренних дел. Для этого достаточно набрать номер телефона круглосуточной службы поддержки клиентов банка, указанный на Вашей банковской платежной карте или номер 102, и в ходе телефонного разговора прояснить возникшую ситуацию.

Запомните, что ни при каких обстоятельствах нельзя сообщать (передавать) реквизиты банковских платежных карт (номер карты, срок действия, данные держателя, трехзначный код на обратной стороне карты), их фотографии, «логин» и «пароль» доступа к системе дистанционного банковского обслуживания «Интернет-банкинг» и коды доступа к нему в виде SMS-сообщений, поступающих из банка. Указанная информация является конфиденциальной и не подлежит разглашению даже представителям банка и сотрудникам правоохранительных органов.

2. Безопасно посещайте сайты в сети Интернет.

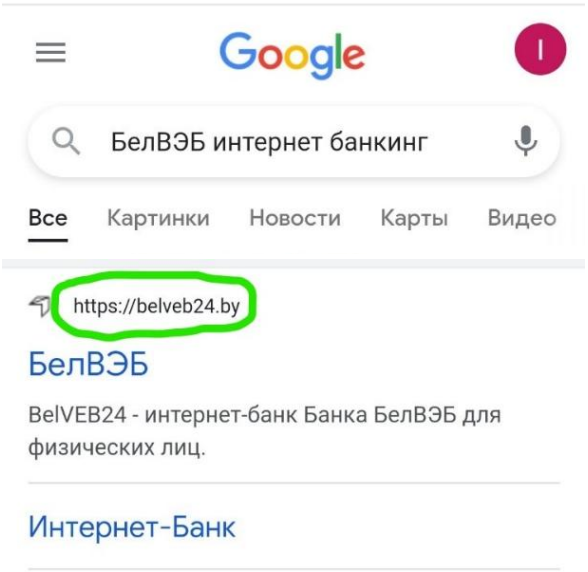
Если Вы используете систему дистанционного банковского обслуживания «Интернет-банкинг» для расчетов за коммунальные услуги, денежных переводов, проверки факта зачисления на счет заработной платы (пенсий, пособий и т.п.), Вам необходимо удостовериться в подлинности веб-ссылки, предназначенной для авторизации на интернет-сайте банка.

Дело в том, что кибермошенники временно размещают в сети Интернет веб-ссылки, которые ведут на поддельные (фишинговые) веб-сайты, внешне не отличающиеся от оригинальных.



Пример «фишинговой» ссылки на интернет-банкинг, обнаруженной в

результате поискового запроса в браузере «Google».



Подлинная ссылка на веб-сайт интернет-банкинга «Банк БелВЭБ», обнаруженная в результате того же поискового запроса в браузере «Google».

В случае перехода на поддельный веб-сайт, Вам будет предложено ввести «логин» и «пароль» для авторизации. Если Вы это сделаете, то киберпреступники получат доступ к Вашему интернет-банкингу, а находящиеся на банковском счету денежные средства будут похищены. Также Вам не следует переходить по ссылкам, которые Вы получили от неизвестных людей в социальных сетях или мессенджерах. С большой долей вероятности, данные ссылки являются «фишинговыми».

Для безопасного совершения онлайн платежей рекомендуется использовать специальные приложения для мобильных устройств «Мобильный банкинг», которые доступны для скачивания в Google Play Market (для Android) или App Store (для iOS).

3. Исключите возможность компрометации реквизитов банковских платежных карт.

На поверхность банковской платежной карты нанесена информация о номере банковского счета, его владельце, сроке действия карты, трехзначный код (CVV-код). Этих данных достаточно, чтобы производить платежи за товары и услуги в сети Интернет. Утеря банковской платежной карты или ее временное нахождение, даже с Вашего согласия, в распоряжении посторонних лиц создают условия для компрометации ее реквизитов.

Иногда бывает так, что банковскую платежную карту хранят в кошельке вместе с пин-кодом, записанным на ее поверхности или на листке бумаги. В случае утраты кошелька в результате утери или кражи, лицо им завладевшее получает возможность полного доступа к Вашему банковскому счету.

Запомните, что нанесенная на поверхность банковской платежной карты информация является конфиденциальной и не подлежит разглашению посторонним лицам. Не храните Вашу банковскую платежную карту совместно с пин-кодом.

4. Социальные сети как платформа для киберпреступлений.

На сегодняшний день почти 100% населения пользуется различными социальными сетями, такими как «Вконтакте», «Instagram», «Facebook» и т.д. В социальной сети «Вконтакте» популярен метод мошенничества, когда от лица знакомого «пользователя» приходит сообщение с просьбой одолжить денежных средств на несколько дней, для чего отправляется фотография либо сообщение с реквизитами БПК. В таком случае самый верный способ не стать жертвой мошенником, позвонить на мобильный телефон своему знакомому и уточнить, действительно ли он пишет вам, либо кто-то получил к его странице несанкционированный доступ. Несанкционированный доступ к учетной записи в социальных сетях получается не без участия самого пользователя. На многих интернет-ресурсах имеется возможность авторизации с помощью социальных сетей. Авторизовываясь с помощью социальных сетей на каком-либо интернет-ресурсе, вы передаете указанному интернет-ресурсу свои «логин» и «пароль», и в том случаи, если вы осуществили авторизацию на «фишинговом» сайте, то вы передали свои «логин» и «пароль» и в дальнейшем мошенник может пользоваться вашей учетной записи без вашего ведома.

Что касается социальной сети «Instagram», то в указанной социальной сети мошенники действуют под предлогом Instagram-магазинов. Указанные магазины работают якобы по частичной предоплате, либо по полной предоплате, переводы денежных средств осуществляются на карточки физических лиц. Чтобы не стать жертвой мошенников в указанной социальной сети, следует обращать внимание на дату размещения записей указанного магазина, на количество «подписчиков», на оставленные отзывы пользователей и возможность написать указанным пользователям, и самое главное, что стоит понимать, что на сегодняшний день по предоплате работают только мошенники.

Солигорский РОВД