РАЙОННЫЙ МАТЕРИАЛ
для членов информационно-пропагандистских групп
(ноябрь 2024г.)

ПРОФИЛАКТИКА И ПРОТИВОДЕЙСТВИЕ КИБЕРПРЕСТУПНОСТИ

Материал подготовлен
отделом внутренних дел Лельчицкого райисполкома

Все чаще мошенники для получения доступа к персональным данным, реквизитам банковских платежных карточек, паролям и другой конфиденциальной информации используют методы «социальной инженерии» *(социальная инженерия – это совокупность способов психологического воздействия на поведение человека с целью получения выгоды*): не взламывают устройства, а **выманивают нужную информацию, используя эмоции абонента**.

С клиентом банка посредством телефонного звонка или в социальных сетях связывается мошенник под видом представителя банка или с аккаунта друга, родственника.

В ходе звонка или переписки собеседник описывает свою сложную жизненную ситуацию и просит ему материально помочь или «запугивает» ложной информацией о сомнительных операциях с банковской карточкой (*наличии заявки на кредит, блокировке счета, мошеннических атаках и др.*), представляясь работником банка, и предлагает для сохранения оставшихся денежных средств перевести их на новый счет. Собеседник говорит очень убедительно и, как правило, торопит развивающиеся события.

Сценарии могут быть разными, а **итог один**: клиент самостоятельно предоставляет все секретные данные, коды из смс-сообщений банка, логин и пароли. Поэтому такие случаи не относятся к принципу «нулевой ответственности» банка, так как конфиденциальные данные злоумышленнику сообщил сам клиент.

Обезопасить себя от данного типа мошенничества можно, **соблюдая простые меры безопасности и проявляя разумную бдительность**.

Если собеседник представился сотрудником банка и пытается получить персональные данные, рекомендуется незамедлительно завершить диалог и самостоятельно обратиться в банк по номеру, указанному на банковской карте, официальном сайте либо прийти в офис лично.

Основные правила, соблюдение которых позволит не стать жертвой злоумышленников:

1. Перед тем как откликнуться на просьбу друга в социальной сети созвонитесь с ним или найдите способ убедиться в том, что его аккаунт не взломан (*задайте другу вопрос, ответ на который знаете только вы оба*);
2. У банков нет совместных контактных центров и служб безопасности, следовательно, переключение между ними невозможно. Если звонящий говорит о таком «переключении», прервите разговор и перезвоните в банк по номерам, указанным на вашей банковской карте либо официальном сайте финансового учреждения;
3. Если смс-сообщение о подозрительной операции по карточке приходит в новую ветку переписки, в которой ранее не было сообщений от банка – это повод уточнить ее достоверность и перезвонить в финансовое учреждение по официальным номерам;
4. Работники банка никогда не просят озвучить смс-код, который необходим для подтверждения совершения банковской операции, а также никогда не спрашивают логин или пароль для входа в систему Интернет-банкинга. В такой ситуации немедленно прервите разговор и свяжитесь с банком по официальным номерам.
5. Никому не сообщайте данные своей карточки и всегда держите её в поле зрения при совершении платежей;
6. Обязательно подключите 3D-secure и смс-оповещение;
7. Используйте только официальный сайт для входа в систему Интернет-банкинга или официальное мобильное приложение соответствующего банковского учреждения;
8. Регулярно обновляйте пароли, используемые для входа в систему Интернет-банкинга, а также для подтверждения платежей;
9. В случае выявления действий по карточке, которые не совершались ее держателем, необходимо оперативно обратиться в банк по официальным номерам или заблокировать карточку самостоятельно в Интернет/М-банкинге (*при наличии такой возможности*).

Стоит помнить, что **мошенники идут в ногу со временем**, поэтому в любой ситуации нужно **оставаться предельно внимательным** и досконально разобраться в случившемся, прежде чем сообщить кому-то свои персональные данные.

Как не стать жертвой преступлений в социальных сетях

На сегодняшний день все больше людей зарегистрированы в социальных сетях «ВКонтакте», «Фейсбуке», «Инстаграмм» и др., каких-либо тематических форумах или иных площадках для виртуального общения. Однако в отдельных случаях неопытность, наивность и доверчивость приводят к негативным последствиям.

Социальные сети, форумы, блоги – это среда с **практически мгновенной скоростью распространения информации** и довольно сильным эффектом памяти (*содержимое многих социальных ресурсов индексируется и доступно из поисковиков*). Кроме того, растет индекс доверия к этим источникам информации.

Основная проблема социальных сетей – это доверие к тем, кто внесен в список «друзей». Бездумное предложение «дружбы» от неизвестных или малоизвестных людей может привести к драматическим последствиям. Очевидно, что уровень доверия к тем, кто находится в списке «друзей», по определению всегда будет выше, чем к случайным людям. С одной стороны, это хорошо, так как формирует лояльную аудиторию вокруг человека, но с другой – **открывает двери для злоумышленников**.

«Дружеский» стиль общения, распространенный в социальных сетях, обманчив. Он может создать **ложное ощущение**, что вокруг только друзья и доброжелатели, с которыми можно делиться любой информацией.

В настоящее время актуальны **следующие виды киберугроз**, с которыми можно столкнуться на просторах Интернета:

Вишинг – один из методов мошенничества с использованием социальной инженерии, который заключается в том, что злоумышленники, используя телефонную коммуникацию и играя определенную роль, под разными предлогами выманивают у держателя платежной карты конфиденциальную информацию, или побуждают, убеждают вероятную жертву к совершению определенных действий со своей банковской платежной картой;

Фишинг – вид мошенничества, целью которого является получение доступа к конфиденциальным данным пользователей – логинам, паролям, данным лицевых счетов и банковских карт с использованием поддельных интернет-ресурсов, контролируемых злоумышленниками, внешне схожих с настоящими (*например, поддельные страницы услуги «Интернет-банкинг» различных банков*);

Заражение вирусным и вредоносным программным обеспечением – внедрение злоумышленниками специализированного программного обеспечения (далее – ПО) в компьютерную систему пользователя для хищения его конфиденциальных данных, завладения ценной информацией, шифрования данных с требованием выкупа, использования компьютера или иного устройства в специализируемых сетях с целью совершения иных преступлений.

В рамках проводимой работы органами внутренних дел было установлено, что рассматриваемый вид преступной деятельности осуществляется **не одиночками**, а, как правило, в составе групп, имеющих отдельные признаки организованных, члены которых обычно лично не знакомы друг с другом (*такие группы имеют некоторое сходство с интернет-магазинами по торговле наркотиками и психотропами*).

Разделение функций в таких группах может осуществляться по следующим категориям участников:

1) **Веб-разработчики.** Обладая навыками программирования, создают основу фишинговых сайтов с заложенным механизмом динамического добавления в них веб-страниц, а также программы для автоматизации и интерактивности процесса создания таких веб-страниц. Веб-разработчики могут не являться непосредственными участниками преступных групп, а только инициативно или под заказ разрабатывать скрипты и продавать их иным заинтересованным лицам.

2) **Администраторы.** Осуществляют регистрацию доменных имен и подбор хостинга для новых сайтов; обеспечивают их оплату, загружают на хостинг файлы фишинговых сайтов, настройку сайтов и их взаимодействие с Telegram-ботами; контролируют функционирование указанных ресурсов; обеспечивают систему вывода денежных средств с карт-счетов граждан посредством создания (*подыскивания зарегистрированных на подставных лиц*) карт-счетов, электронных кошельков, криптокошельков и управления данными средствами платежей; обеспечивают функционирование системы подсчета заработка и выплаты вознаграждения исполнителям.

3) **Операторы.** Осуществляют администрирование форумов, Telegram-чатов, Telegram-каналов, чат-ботов, ориентированных на данный способ хищения денежных средств; обеспечивают набор новых исполнителей; их обучение навыкам создания фишинговых вебстраниц, обмана потерпевших, обеспечения анонимности, вывода похищенных денежных средств; разрешают споры с исполнителями по поводу выплат.

4) **Исполнители.** Как правило, обладают низким уровнем образования и ориентированы на получение быстрых и легких заработков. Именно они подбирают объявления, например на «kufar.by», используя предоставленный им инструментарий, создают фишинговую вебстраницу; по абонентскому номеру автора объявления находят его в одном из мессенджеров; вступают в общение с потерпевшим под предлогом желания купить выставленный на продажу товар и убеждают в необходимости перехода на фишинговую веб-страницу и ввода необходимых данных. Посредством чат-бота они получают сведения о действиях потерпевшего на фишинговом сайте, сумме похищенных средств.

Содействовать совершению преступлений могут **и иные лица, осуществляющие незаконную деятельность**: осуществляющие регистрацию на подставных лиц абонентских номеров, электронных кошельков, банковских счетов (карт); оказывающие содействие в транзите похищаемых безналичных денежных средств через управляемые ими банковские счета и электронные кошельки; с использованием вредоносного ПО или социальной инженерии завладевающие аккаунтами пользователей мессенджеров с целью их использовании в переписке с потерпевшими.

Сватинг – заведомо ложный вызов милиции, аварийно-спасательных служб, путем фальшивых сообщений о минировании, убийствах, захвате заложников и т.п.

Этот термин происходит от названия штурмовой группы «SWAT» (special weapons and tactics) – специализированной полицейской единицы в США и многих других странах. Если есть угроза, при которой необходимо вмешательство этой единицы, последствиями иногда становится эвакуация школ, деловых учреждений. В западных странах «сватинг» расценивается как разновидность терроризма, поскольку его используют для запугивания.

Сваттинг в первую очередь свойственен среде, где люди (*чаще всего молодые*) объединяются с какой-либо целью. Например, в онлайн-играх. У них есть термин «вызвать милицию на дом» – когда для того, чтобы, к примеру, досадить обидчику, ему на дом вызывают правоохранителей, либо сообщают о заминировании какого-либо объекта.

В последние годы «сватинг» из забавы любителей онлайн-игр и хакеров превратился в массовое явление и большую проблему для правоохранительных органов различных стран.

В Республике Беларусь в последние годы возросло количество случаев поступления сообщений на электронную почту о ложном минировании объектов. Подобные «шалости» дорого обходятся государству, а для виновных чреваты весьма нешуточными последствиями.

Возраст привлечения к административной ответственности по статье 19.6 «Заведомо ложное сообщение» Кодекса Республики Беларусь об административных правонарушениях **наступает с 16 лет**. Санкция статьи предусматривает наложение **штрафа в размере до 30 базовых величин**.

Кроме того, предусмотрена уголовная ответственность (с 16 лет) предусмотренной статьей 340 «Заведомо ложное сообщение об опасности» Уголовного Кодекса Республики Беларусь. Санкция статьи предусматривает наказание в виде **лишения свободы на срок до 7 лет**.