УДК 004.056

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ. МОШЕННИЧЕСТВО

Навроцкая А.В.
(научный руководитель – Стрелюхин А.В.)
Белорусский национальный технический университет
Минск, Беларусь

Аннотация. Одной из проблем, которой занимается информационная безопасность, является мошенничество. В работе рассмотрены основные понятия и виды мошенничества, а также методы защиты от него.

Введение. **Что такое мошенничество и его цели**

Согласно Уголовному Кодексу Республики Беларусь, статья 209 определяет мошенничество как «завладение имуществом либо приобретение права на имущество путем обмана или злоупотребления доверием» [1].

Отдельно законом рассматриваются ситуации, когда злоумышленники используют электронные средства платежей и похищают компьютерную информацию. Это определено статьей 212 Уголовного кодекса Республики Беларусь – «хищение путем использования компьютерной техники» [2].

Целью преступника, занимающегося мошенничеством, чаще всего является получение денег. Для этого ему необходимо знать следующие сведения:

– фамилия, имя и отчество гражданина;

– реквизиты банковской карты и/или счетов;

– пароли от учетных записей банковского приложения;

– иная информация, позволяющая получить доступ к деньгам.

Основные виды мошенничества

В интернете наиболее распространёнными видами являются [3]:

1. Фишинг. Основа интернет-мошенничества – приобретение доступа к конфиденциальным данным (для этого используются фишинг-сайты, электронная почта, фишинговые ссылки приложения). Например, стоит зайти в аккаунт фишингового онлайн-банка, как появляется возможность перевода денег, взятия кредитов практически без ограничений по суммам, но при этом у пользователя появляется много проблем.

2. Брашинг. Этот способ мошенничества используется на маркетплейсах, досках объявлений и интернет-аукционах. Маркетплейсы сегодня стали действительно популярны, но и с ними связаны опасности. Обман процветает даже на официальных ресурсах. Подделки становятся все более изощренными, особенно в сфере одежды, аксессуаров и парфюмерии.

3. Оплачиваемые опросы. За опросы действительно могут платить деньги. Это один из основных способов «маркетингового исследования рынка». Только если сотрудничать с поддельным агентством, есть вероятность столкнуться с потерей денег после попытки вывода начислений в личном кабинете. Никаких денег приобрести не получится, т.к. цель мошенников, наоборот, списать их с карты пользователя.

4. Каперство. Такой вид мошенничества в сети также представляет серьезную угрозу. Злоумышленники могут завладеть вашими данными и требовать выкуп за их возвращение. В этом случае используются слабые пароли или уязвимости в безопасности для получения контроля над вашими ресурсами.

5. Мошенничество с криптовалютами. В настоящее время это серьезная проблема, с которой сталкиваются многие инвесторы. Особенно опасны поддельные обменники и схемы, связанные с покупкой цифровых монет. Иногда мошенники получают доступ к личным аккаунтам, тогда все средства оттуда уходят на чужие счета.

6. Программы-вымогатели. Такой вид мошенничества все еще является популярным, хотя и известен очень давно. Пользователю присылают ссылку на вирус, который заблокирует компьютер и будет требовать перевода денег на указанные реквизиты. Такие схемы действуют уже более десяти лет и не теряют своей актуальности.

7. Кликджекинг. Этот термин подразумевает мошенничество, при котором используются невидимые элементы на сайте. Заполучить на компьютер или смартфон вирусный файл можно при просмотре фильма на обычном сайте. Злоумышленники размещают на страницах невидимые элементы, на которые человек нажимает попутно с «полезными действиями». Например, вместе с запуском проигрывания кино будет дано согласие на обработку персональных данных в какой-либо микрофинансовой организации.

В «реальной» жизни с мошенничеством можно столкнуться в следующих ситуациях.

1. Социальная инженерия. Социальная инженерия – это крайне опасная практика, в которой злоумышленники используют психологические уловки чтобы обманом получить доступ к личной информации и ресурсам жертвы. Они могут выдавать себя за доверенных лиц, таких как друзья, коллеги или даже представителей банков или служб поддержки. Важно быть предельно внимательным и не разглашать личные данные по просьбам неизвестных лиц, особенно в онлайн-средах.

2. СМС от «лжебанка». Один из распространённых способов преступников заключается в маскировке под официальные банки. Многие люди, прочитав СМС со знакомых номеров, нажимают ссылки, чтобы посмотреть новые предложения по случаю наступающих праздников или по другому событию. Мошеннику остается только оформить сообщение в «фирменном» стиле и подставить ссылку на поддельный сайт. Это также может сопровождаться звонком сотрудника «лжебанка», чтобы усилить доверие и убедить жертву предоставить информацию.

3. Мошенничества в сетях GSM. Даже в сфере сотовой связи, мошенники могут предложить услуги под видом бесплатных или временно доступных. Например, они предлагают бесплатный доступ на 1 месяц к одному из своих сервисов, а потом начинают незаметно списывать за него абонентскую плату. Клонирование SIM-карт представляет наиболее

серьезную угрозу, поскольку злоумышленники могут получить доступ к личным аккаунтам и данным.

4. Мошенничество через благотворительность. Схема с «благотворительностью» известна достаточно давно. Злоумышленники могут обращаться к людям в мессенджерах, личных сообщениях, социальных сетях с просьбами о финансовой помощи на лечение или благотворительность, при этом подделывая реальные реквизиты и собирая деньги на собственные цели.

Заключение

Основной способ защиты от мошенничества – быть внимательным. Причем необходимо быть внимательным «всегда и везде»: на просматриваемых сайтах, при прочтении любого электронного сообщения, при скачивании информации и т.д.

Оценить мошенничество можно по следующим признакам [4]:

– на вас выходят сами;

– разговор касается денег или вашей банковской карты;

– делают выгодное предложение или пугают;

– морально давят, требуют принять решение немедленно;

– запрашивают информацию о банковской карте и т.д.

Большинство современного программного обеспечения для работы в интернете имеют встроенные средства защиты от мошенничества, поэтому есть смысл обращать внимание на их предупреждения. Каждое действие нужно сначала обдумать – точно ли был запрос на смену пароля, знаком ли номер телефона, откуда пишут о просьбе занять денег и т.д. При создании пароля необходимо стараться делать его сложным и уникальным, а также разным для разных аккаунтов [5].

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Ваш гид в законодательстве Республики Беларусь [Электронный ресурс]. – Режим доступа: https://zakony-by.com/ugolovnyj_kodeks_rb/209.htm. – Дата доступа: 12.04.2024.

2. Ваш гид в законодательстве Республики Беларусь [Электронный ресурс]. – Режим доступа: https://zakony-by.com/ugolovnyj_kodeks_rb/212.htm. – Дата доступа: 12.04.2024.

3. Виды мошенничества в Интернете [Электронный ресурс]. – Режим доступа: https://cisoclub.ru/moshenniki-v-internete. – Дата доступа: 12.04.2024.

4. 5 главных признаков телефонного мошенничества [Электронный ресурс]. – Режим доступа: https://www.sibsoc.ru/telefonnoe-moshennichestvo/. – Дата доступа: 12.04.2024.

5. Как защитить себя и близких от мошенников? Советы экспертов [Электронный ресурс]. – Режим доступа: https://m.sport-express.ru/zozh/hobby/reviews/kak-zaschititsya-ot-moshennikov-2046641/. – Дата доступа: 12.04.2024.